

Elementi Di Teoria Degli Insiemi

APPUNTI DEL CORSO DI ELEMENTI DI TEORIA DEGLI INSIEMI
TENUTO DAL PROF. MARCELLO MAMINO

DIEGO MONACO
d.monaco2@studenti.unipi.it
UNIVERSITÀ DI PISA

Anno Accademico 2022-23



Indice

1 Prologo nel XIX secolo	6
1.1 Digressione: insiemi numerabili	8
1.2 Tornando agli insiemi di unicità	11
1.3 Giochi di parole	13
1.4 Scopi del corso	14
2 Il linguaggio della teoria degli insiemi	15
2.1 Le regole di inferenza	17
3 I primi assiomi	19
3.1 Assiomi dell'insieme vuoto e di estensionalità	19
3.2 Assioma di separazione	20
3.3 Classi e classi proprie	21
3.4 Assioma del paio e coppia di Kuratowski	22
3.5 Assioma dell'unione e operazioni booleane	25
3.6 Assioma delle parti e prodotto cartesiano	28
3.7 Relazioni di equivalenza e di ordine, funzioni	29
4 Assioma dell'infinito e numeri naturali	35
4.1 Gli assiomi di Peano	37
4.2 L'ordine di omega	39
4.3 Induzione forte e principio del minimo	43
4.4 Ricorsione numerabile	44
5 Cardinalità	52
5.1 Teorema di Cantor-Bernstein	53
5.2 Teorema di Cantor	56
5.3 Operazioni fra cardinalità	56
6 Cardinalità finite	59
6.1 Principio dei cassetti	59
6.2 Operazioni fra le cardinalità finite	63
7 La cardinalità del numerabile	66
7.1 Insiemi numerabili in pratica	70
7.2 Prodotto di numerabili è numerabile	71
7.3 Numeri interi e razionali	73
7.4 Ordini densi numerabili	79
7.5 Il grafo random	85
8 \mathbb{R} e la cardinalità del continuo	88
8.1 Caratterizzazione dei reali come ordine	91
8.2 La cardinalità del continuo è 2^{\aleph_0}	93
8.3 Operazioni che coinvolgono la cardinalità del continuo	93
8.4 Sottrarre un numerabile dal continuo	94
8.5 (\star) Alternativa per la cardinalità di \mathbb{R}	97
8.6 (\star) $(F, 0, 1, +, \cdot, \leq)$	99
Stato del corso	100

9 I buoni ordinamenti	101
9.1 Operazioni aritmetiche fra buoni ordinamenti	107
9.2 Gli ordinali di Von Neumann	113
9.3 L'assioma del rimpiazzamento	119
9.4 Induzione e ricorsione transfinite	124
9.5 Operazioni fra gli ordinali	130
10 Aritmetica ordinale e forma normale di Cantor	134
10.1 Sottrazione e divisione euclidea	138
10.2 La forma normale di Cantor	140
10.3 Punti fissi e ε -numbers	141
10.4 Operazioni in forma normale di Cantor	146
11 Gli aleph	151
11.1 Teorema di Hartogs	152
11.2 Somme e prodotti di aleph	155
12 L'assioma della scelta	159
12.1 Buon ordinamento \rightarrow AC	161
12.2 AC \rightarrow buon ordinamento (idea)	161
12.3 Zorn \rightarrow buon ordinamento	162
12.4 AC \rightarrow Zorn	163
12.5 Conseguenze immediate di AC	165
12.6 Esempi di applicazione di AC	170
12.7 Basi di spazi vettoriali	170
12.8 Invariante di Dehn	174
12.9 Insieme di Vitali	176
12.10 Il teorema di Cantor-Bendixson	178
12.11 Riepilogo forme equivalenti di AC	182
12.12 $ X = X \times X \rightarrow$ AC (Tarski)	183
13 Aritmetica cardinale	184
13.1 Somme e prodotti infiniti	185
13.2 Teorema di König	188
13.3 Cofinalità	191
13.4 Formula di Hausdorff	198
14 La gerarchia di Von Neumann e l'assioma di buona fondazione	204
14.1 Formule relativizzate ad una classe	206
14.2 Assioma di buona fondazione	210
14.3 Principio di ϵ -induzione	211
A Appendice	221
A.1 Cardinalità note	221
A.2 Forma normale di ω_α	235
A.3 Sottoinsiemi infiniti di cardinalità fissata	236
A.4 Sottrazione cardinale	236
A.5 Rango ordinale	237
A.6 Teorema di Cantor-Lebesgue	238
A.7 ϵ -ricorsione	240

Bibliografia

242

Premessa

Queste dispense sono la quasi esatta trascrizione in L^AT_EX delle dispense del corso di Elementi di Teoria degli Insiemi [1], tenuto dal prof. Marcello Mamino nell'anno accademico 2022-23 presso l'Università di Pisa.

Ringraziamenti

Francesco Sorce, Rubens Martino, Lorenzo Picinelli, Andrea Snaidero, Alessandro Avellino, Lorenzo Bonetti.

Quest'opera è stata rilasciata con la licenza Creative Commons Attribuzione - Condividi allo stesso modo 4.0 Internazionale. Per leggere una copia della licenza visita il sito web <https://creativecommons.org/licenses/by-nc/4.0/deed.it>.



§1 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 un'introduzione possibile.

Problema 1.1. 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.

Definizione 1.2. 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:

$S(x)$ converge a 0 per tutti gli $x \notin X \implies$ tutti i coefficienti c_0, a_i, b_i sono nulli

Esempio 1.3

Per il risultato di Cantor, \emptyset è di unicità.

Problema 1.4. Quali sottoinsiemi di \mathbb{R} sono di unicità?

Fatto 1.5 (Criterio per gli insiemi di unicità)

Dato $X \subseteq \mathbb{R}$ se (ma non solo se) **ogni funzione continua $f : \mathbb{R} \rightarrow \mathbb{R}$ che soddisfi:**

- per ogni intervallo aperto $]a, b[$ con $]a, b[\cap X = \emptyset$, $f|_{]a, b[}$ è lineare.
- per ogni $x \in \mathbb{R}$, se f ha derivate destre e sinistre in x , allora queste coincidono^a.

è **lineare^b**, allora X è di unicità.

^aOvvero f non ha punti angolosi.

^b $f(x) = \alpha x + \beta$.

D'ora in avanti diremo che un insieme rispetta le ipotesi criterio, o ha la proprietà (\star) , se soddisfa il fatto in **viola**, e quindi è di unicità per il fatto sopra.

Esempio 1.6

$X = \{\dots, a_{-2}, a_{-1}, a_0, a_1, a_2, \dots\} = \{a_i | i \in \mathbb{Z}\}$ con $\dots < a_{-2} < a_{-1} < a_0 < a_1 < a_2 < \dots$, $\lim_{i \rightarrow +\infty} a_i = +\infty$, $\lim_{i \rightarrow -\infty} a_i = -\infty$ ha la proprietà data dal **Fatto 1.5**, quindi è di unicità.

NON Esempio 1.7

L'intervallo $[0, 1]$ o \mathbb{R} non hanno la proprietà espressa dall'**Fatto 1.5**.

NON Esempio buffo 1.8

Per l'**insieme di Cantor** non vale il **Fatto 1.5**.

Possiamo costruire l'insieme di Cantor a partire dall'intervallo $C_0 = [0, 1]$ nel seguente modo:

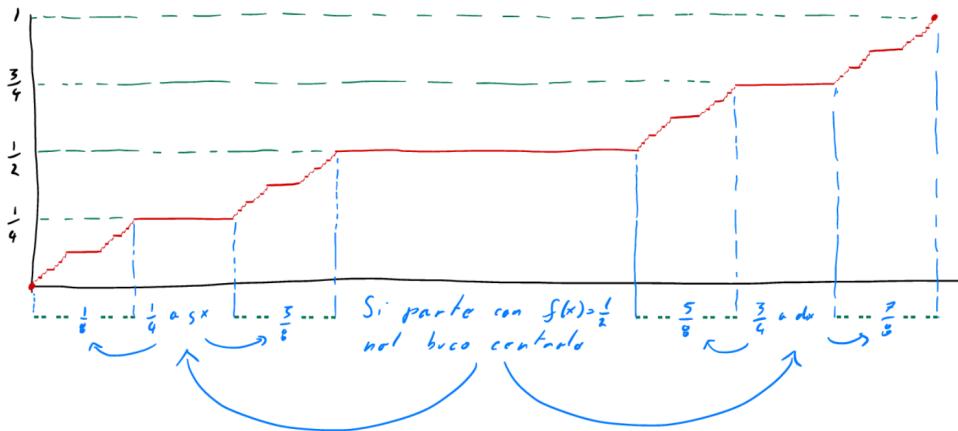
$$\begin{aligned}
 C_0 &= [0, 1] \\
 C_1 &= [\frac{0}{3}, \frac{1}{3}] \cup [\frac{2}{3}, 1] \\
 C_2 &= [\frac{0}{3}, \frac{1}{3}] \cup [\frac{2}{3}, \frac{1}{3}] \cup [\frac{2}{3}, \frac{3}{3}] \cup [\frac{3}{3}, 1] \\
 C_3 &= [\frac{0}{3^2}, \frac{1}{3^2}] \cup [\frac{2}{3^2}, \frac{1}{3^2}] \cup [\frac{2}{3^2}, \frac{3}{3^2}] \cup [\frac{3}{3^2}, \frac{1}{3^2}] \cup [\frac{2}{3^2}, \frac{5}{3^2}] \cup [\frac{5}{3^2}, \frac{3}{3^2}] \cup [\frac{5}{3^2}, \frac{7}{3^2}] \cup [\frac{7}{3^2}, \frac{1}{3^2}]
 \end{aligned}$$

etc.

ovvero, preso l'intervallo $[0, 1]$ possiamo dividerlo in tre parti e rimuovere la parte centrale $[\frac{1}{3}, \frac{2}{3}]$, chiamiamo gli intervalli rimanenti C_1 , possiamo iterare il procedimento sui due segmenti di C_1 ed ottenere $C_2, C_3, \dots, C_{n+1} = \frac{C_n}{3} \cup (\frac{C_n}{3} + \frac{2}{3})$, ..., a questo punto definiamo l'insieme di Cantor C come:

$$C := \bigcap_{i \in \mathbb{N}} C_i$$

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



tale funzione si costruisce aggiungendo tratti costanti (prima $\frac{1}{2}$, poi $\frac{1}{4}$, $\frac{3}{4}$ e così via, dividendo l'intervallo $[0, 1]$ sull'asse delle ordinate in parti uguali) alle parti eliminate sull'intervallo $[0, 1]$ sull'asse delle ascisse per costruire l'insieme di Cantor.

Nota 1.9 — Per \mathbb{Q} e C non vale il [Fatto 1.5](#) ma, in realtà, sono di unicità.

Esempio buffo 1.10 ($a_n \uparrow l$)

L'insieme degli elementi di una successione crescente col suo limite è un esempio di insieme di unicità.

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

Dimostriamo quindi che X è un insieme di unicità.

Dimostrazione. Per ipotesi 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 ovviamente derivata destra e sinistra. Siccome, sempre per ipotesi, f è continua e non ammette punti angolosi, questi punti non possono essere angolosi, per cui $f'_-(a_i) = f'_+(a_i)$, ovvero le rette $f|_{]-\infty, a_0[}$, $f|_{]a_0, a_1[}$, etc. hanno lo stesso coefficiente angolare. Pertanto, per continuità, $f|_{]-\infty, l[}$ è lineare e per ipotesi lo è anche $f|_{]l, +\infty[}$, quindi f è lineare. \square

Esempio più buffo 1.11 (Successione di successioni crescenti)

L'insieme degli elementi di una successione crescente di successioni crescenti è un insieme di unicità.

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

da cui: $a_{i,0} \uparrow l$ per $i \rightarrow +\infty$
 $a_{i,j} \uparrow a_{(i+1)0}$ per $j \rightarrow +\infty$ con i fissato.

Dimostriamo che X è di unicità.

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

§1.1 Digressione: insiemi numerabili

Definizione 1.12. 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 $i \neq j$.¹

¹O in altre parole se esiste $f : \mathbb{N} \rightarrow X$ biunivoca.

Esempio 1.13

Alcuni esempi di insiemi numerabili sono:

- \mathbb{N} , l'insieme dei numeri naturali, infatti, la successione $a_i = i$ realizza la biogezione.
- I numeri dispari, con la biogezione data da $a_i = 2i + 1$.
- I numeri primi, $a_i = p_i$, con p_i i -esimo numero primo.
- \mathbb{Z} l'insieme dei numeri interi, con la biogezione data da $a_i = (-1)^i \lceil \frac{i}{2} \rceil$.

Esempio meno immediato 1.14

L'insieme $\mathbb{N} \times \mathbb{N} = \{(x, y) | x, y \in \mathbb{N}\}$ è numerabile.

Dimostrazione. La funzione $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} : (x, y) \mapsto 2^x(1 + 2y) - 1$ è biunivoca (perché?), quindi $a_i = f^{-1}(i)$ enumera $\mathbb{N} \times \mathbb{N}$. \square

Proposizione 1.15

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

Dimostrazione. Sia $Y \subseteq X$ con Y infinito e $X = \{a_i | i \in \mathbb{N}\}$. 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:

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

dove i minimi esistono perché Y non è finito. \square

Proposizione 1.16

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

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

Esempio 1.17

\mathbb{Q} è numerabile.

Dimostrazione. \mathbb{Q} è in corrispondenza biunivoca con:

$$F = \{(\text{num.}, \text{den.})^2 | \text{num.} \in \mathbb{Z} \wedge \text{den.} \in \mathbb{N}_{>0} \wedge \text{M.C.D.}(\text{num.}, \text{den.}) = 1\} \subseteq \mathbb{Z} \times \mathbb{N}$$

\square

²num. = numeratore, den. = denominatore.

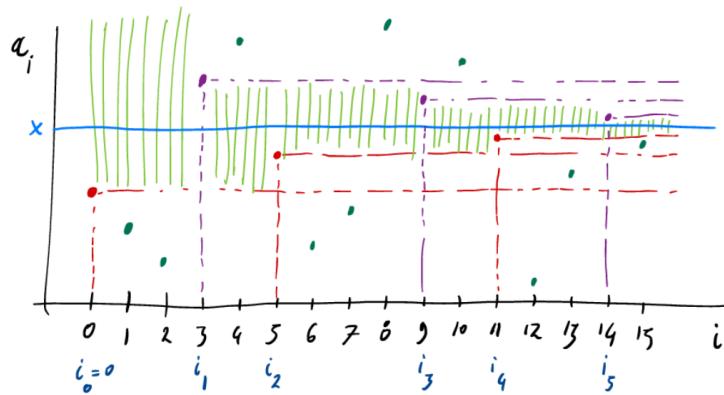
NON Esempio 1.18

\mathbb{R} non è numerabile.

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

$$i_0 = 0 \quad i_1 = \min\{i | a_i > a_0\} \quad i_{j+1} = \min\{i | a_i \text{ è compreso tra } a_{i_{j-1}} \text{ e } a_{i_j}\}$$

graficamente:



Si vede facilmente (esercizio!) che la successione $\{a_{i_{2k}}\}_k$ è crescente, $\{a_{i_{2k+1}}\}_k$ è decrescente e $\lim_{k \rightarrow +\infty} a_{i_{2k}} \leq \lim_{k \rightarrow +\infty} a_{i_{2k+1}}$. Fissiamo x tale che $\lim_{k \rightarrow +\infty} a_{i_{2k}} \leq x \leq \lim_{k \rightarrow +\infty} a_{i_{2k+1}}$. 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 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 1.19. Completare la dimostrazione nel caso $n < i$.

Esercizio 1.20. Dimostrare che l'insieme di Cantor C non è numerabile.

□

§1.2 Tornando agli insiemi di unicità

Teorema 1.21 (Cantor-Lebesgue)

Se $X \subseteq \mathbb{R}$ è chiuso e numerabile, allora X soddisfa (\star) , e quindi è di unicità.

La strategia di dimostrazione passa attraverso una definizione.

Definizione 1.22. 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 di accumulazione** se $\exists \varepsilon > 0 :]a - \varepsilon, a + \varepsilon[\cap X = \{a\}$).

Osservazione 1.23 (Derivato di un chiuso soddisfa $(\star) \implies$ chiuso soddisfa (\star)) —

Se X è chiuso e X' soddisfa (\star) - per cui X' è di unicità per il criterio -, allora anche X è di unicità.

Dimostriamo questo fatto.

Dimostrazione. Occorre dimostrare che se $f : \mathbb{R} \rightarrow \mathbb{R}$ è continua, lineare quando ristretta agli intervalli aperti che non intersecano X , e non ha punti angolosi, allora f è lineare, in tal modo sono soddisfatte le ipotesi del [Fatto 1.5](#) ed X è di unicità.

Per fare ciò osserviamo che, data f come sopra, se dimostriamo che quando è ristretta agli intervalli aperti che non intersecano X' è lineare (e non avendo punti angolosi in generale quest'ipotesi è in automatico verificata) - essendo che quest'ultimo rispetta (\star) , cioè verifica le ipotesi del [Fatto 1.5](#) - allora si ottiene che f è in generale lineare e quindi anche X soddisfa le ipotesi del criterio.

Consideriamo un intervallo aperto che non interseca X' , $]a, b[\cap X' = \emptyset$, dobbiamo verificare che $f|_{]a, b[}$ è lineare. Ci basta dire che per ogni $\varepsilon > 0$, $f|_{[a+\varepsilon, b-\varepsilon]}$ è lineare - cioè che è lineare su ogni sottointervallo, dopodiché è banale che se vale per ogni $\varepsilon > 0$, vale in generale, e quindi $f|_{]a, b[}$ è lineare -.

Siccome per ipotesi $]a, b[\cap X' = \emptyset$, allora $]a, b[\cap X \subseteq \{\text{punti isolati di } X\}$. Quindi l'intersezione con un sottointervallo chiuso $[a + \varepsilon, b - \varepsilon] \cap X$ è finita, se così non fosse, avrebbe che esiste nell'intersezione un punto di accumulazione α che naturalmente non può essere un punto isolato di X \nless . Per cui $f|_{[a+\varepsilon, b-\varepsilon]}$ è lineare a tratti, e, siccome per ipotesi non ha punti angolosi (ed è continua), è lineare su tutto il sottointervallo. \square

Corollario 1.24 (Derivato n -esimo soddisfa $(\star) \implies$ insieme soddisfa (\star))

Detto $X^{(n)}$ il derivato n -esimo di X , se per $X^{(n)}$ vale (\star) , per qualche $n \in \mathbb{N}$, allora anche per X vale (\star) , quindi per il [Fatto 1.5](#) è di unicità.^a

^aIl caso con $X^{(n)} = \emptyset$ scritto da Mamino nelle note è un caso particolare di questo.

Dimostrazione. È una facile induzione su n , il caso 0 è banale, mentre per il caso $n = 1$ vale l'osservazione vista sopra. Supponiamo ora che se $X^{(n-1)}$ soddisfa (\star) , allora anche X soddisfa (\star) , e verifichiamo che se $X^{(n)}$ soddisfa (\star) allora anche X lo soddisfa.

Detto $X^{(n-1)} = Y$, allora $Y' = X^{(n)}$, dunque vale l'osservazione sopra, quindi $Y = X^{(n-1)}$ soddisfa (\star) e per ipotesi induttiva anche X soddisfa (\star) . \square

Il guaio è che ci sono chiusi numerabili per cui $X^{(n)} \neq \emptyset$, qualunque sia n - per cui non possiamo usare il corollario sopra per dedurre che sono di unicità -.

Esempio 1.25

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 $a_i \nearrow \infty$ per $i \rightarrow \infty$.



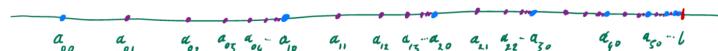
Tutti i punti sono isolati, $X' = \emptyset$.

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



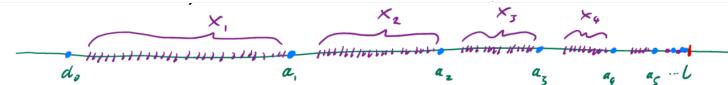
“Successione con punto limite”. Tutti i punti sono isolati salvo l , quindi $X' = \{l\}$ e $X'' = \emptyset$.

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



“Successione di successioni”, $X' = \{a_{10}, a_{20}, \dots, l\}$, $X'' = \{l\}$ e $X''' = \emptyset$.

Si vede che possiamo proseguire, in qualche 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 , $X_\omega^{(n)} \neq \emptyset$. D’altro canto, X_ω soddisfa il [Fatto 1.5](#), perché f deve essere lineare in ciascuno degli intervalli $[a_n, a_{n+1}]$, perché X_{n+1} soddisfa il [Fatto 1.5](#), quindi ci si riduce al caso della successione.

Esercizio 1.26. Perché X_ω è numerabile?

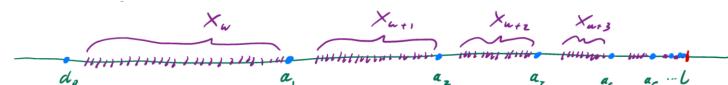
Ora potremmo pensare che, pazienza se X_ω non si smonta a furia di derivati, sarà un caso particolare. Però adesso, possiamo fare una successione di insiemi come X_ω , chiamiamola $X_{\omega+1}$, e una successione di questi $X_{\omega+2}$, etc.

Al diavolo, serve un nuovo corollario!

Corollario 1.27

Se $X^{(n)}$ è di “tipo X_ω ”, allora per X vale il [Fatto 1.5](#).

Ok, questo corollario copre X_ω , $X_{\omega+1}$, $X_{\omega+2}$, ma copre anche $X_{\omega+2}$?



No: occorre un nuovo corollario.

Corollario 1.28

Se $X^{(n)}$ è di “tipo $X_{\omega \cdot 2}$ ”, allora per X vale il [Fatto 1.5](#).

E poi un altro per $X_{\omega \cdot 3}$, e un altro per $X_{\omega \cdot 4}$, etc.

E ora abbiamo finito? No, perché possiamo costruire una nuova successione con $X_\omega, X_{\omega \cdot 2}, X_{\omega \cdot 3}$, etc.

Se chiamiamo questa follia $X_{\omega \cdot \omega}$, ecco che si riparte a fare successioni di $X_{\omega \cdot \omega}$. Ora si sarà capito che definiremo una serie aritmetica di queste cose, per cui potremo fare anche $\omega^\omega, \omega^{\omega^\omega}$, etc. È questa la soluzione allora?

No, ogni sforzo di trovare l’induzione a capo delle induzioni è vano. Se ho $X_\omega, X_{\omega^\omega}, X_{\omega^{\omega^\omega}}$, etc., allora, ecco che faccio una successione con queste cose, la battezzo in qualche modo - ad esempio, 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 1.29 (per la fine del corso). Dimostrare il teorema di [Cantor-Lebesgue](#).

§1.3 Giochi di parole

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

Paradosso di Russell

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

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

la collezione delle collezioni che non sono membri di se stessi - la N sta per collezioni normali. Quindi ci chiediamo se $N \in N$ oppure no? $N \in N$ se e solo se per definizione $N \notin N$, che è assurdo.

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:

$$h = \text{“il più piccolo numero naturale che l’italiano non può descrivere con meno di cento parole”}$$

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 esprimano le proposizioni della teoria degli insiemi, e occorre fissare un sistema di assiomi, espressi in questo linguaggio, che dicono 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.

§1.4 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.

§2 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:

$$\text{variabile} = \text{variabile} \quad \text{variabile} \in \text{variabile}^3$$

sono formule atomiche $x = y, x = x, \alpha = C$, e anche $x \in y, x \in x, \alpha \in C$.

- Le formule atomiche si combinano tra loro mediante:

- **connettivi logici** ovvero il “non” la “e” e la “o” (inclusiva):

$$\neg \text{formula} \quad \text{formula} \wedge \text{formula} \quad \text{formula} \vee \text{formula}$$

quindi ad esempio:

$\neg\Phi \equiv$ “ 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** ovvero quello universale “per ogni” e quello esistenziale “esiste”:

$$\forall x \text{ formula} \quad \exists x \text{ formula}$$

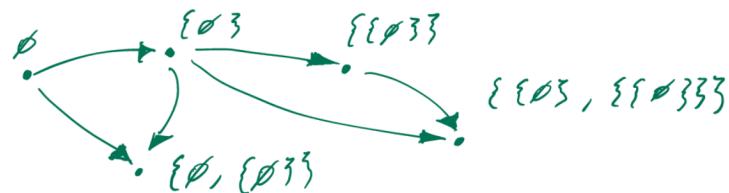
ad esempio:

$\forall x \Phi \equiv$ “ Φ è vera qualunque sia l’insieme x ”

$\exists x \Phi \equiv$ “c’è un insieme x che fa sì che Φ sia vera”

Esercizio 2.1. 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.



³ “appartiene a”.

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

“ a è un elemento di un certo b ” \equiv “c’è un percorso di due frecce fra a e b ”

che corrisponde mediante formule insiemistiche a $\exists x(a \in x \wedge x \in b)$. E ancora:

“ a è un sottoinsieme di b ” \equiv “ogni elemento di a è elemento di b ” \equiv

\equiv “non c’è un insieme che è elemento di a e non di b ” \equiv

\equiv “non c’è un vertice con una freccia verso a e non una verso b ”

che corrisponde mediante formule insiemistiche a $\neg\exists x(x \in a \wedge \neg x \in b)$ (tutto ciò che raggiunge a deve raggiungere anche 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:

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

Non useremo, in generale, questa notazione, ma useremo le parentesi selettivamente per evitare ambiguità.⁴

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:

$$x \neq y \stackrel{\text{def}}{=} \neg x = y^5 \quad x \notin y \stackrel{\text{def}}{=} \neg x \in y \quad \exists x \Phi \stackrel{\text{def}}{=} \neg \exists x \Phi$$

$$\Phi \rightarrow \psi \stackrel{\text{def}}{=} \psi \vee \neg \Phi \quad \Phi \leftrightarrow \psi \stackrel{\text{def}}{=} (\Phi \rightarrow \psi) \wedge (\psi \rightarrow \Phi)$$

$$\exists x \in y \Phi \stackrel{\text{def}}{=} \exists x(x \in y \wedge \Phi) \quad \forall x \in A \Phi \stackrel{\text{def}}{=} \forall x(x \in A \rightarrow \Phi)$$

$$\exists! x \Phi(x) \stackrel{\text{def}}{=} \exists x(\Phi(x) \wedge \forall y(\Phi(y) \rightarrow y = x))$$

$$\exists! x \in A \Phi(x) \stackrel{\text{def}}{=} \exists! x(x \in A \wedge \Phi(x))$$

$$A \subseteq B \stackrel{\text{def}}{=} \forall x(x \in A \rightarrow x \in B) \quad A \subsetneq B \stackrel{\text{def}}{=} (A \subseteq B) \wedge (A \neq B)$$

$$C = A \cup B \stackrel{\text{def}}{=} \forall x x \in C \leftrightarrow (x \in A \vee x \in B)$$

$$C = A \cap B \stackrel{\text{def}}{=} \forall x x \in C \leftrightarrow (x \in A \wedge x \in B)$$

Nota 2.2 — 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.

⁴In questo caso si useranno più parentesi, qualora alcune formule risultassero più leggibili in tal modo.

⁵Cioè “non è vero che x è uguale a y ”.

Esercizio 2.3. Esprimi queste proposizioni mediante formule insiemistiche pure:

- gli elementi degli elementi 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^a

^aQui assumi che l'unione e intersezione esistano e siano uniche.

§2.1 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 che specificano precisamente quali passaggi sono leciti nelle dimostrazioni. Possiamo immaginare questa 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 algebrica. Noi non vedremo le regole di inferenza, e voglio spiegare qui il perché.

- 1 Sono argomento del corso di logica.
- 2 In realtà, scrivere le dimostrazioni in maniera formale, le renderebbe lunghissime e particolarmente 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 pericolose.
- 4 Conoscere le regole - fidatevi - 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 ($\neg, \wedge, \vee, \rightarrow, \leftrightarrow$) delle stesse formule - “**combinazioni booleane**” - alle volte, dicono la stessa cosa. Per esempio, $\neg\Phi \vee \neg\psi \equiv^6 \neg(\Phi \wedge \psi)$. Per verificare questo fatto basta considerare tutte le possibili combinazioni di valori di verità che possono assumere le formule combinate - nell'esempio Φ e ψ - compilando una “**tavella 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

Come si osserva le due colonne corrispondenti ai valori di verità delle nostre formule iniziali hanno gli stessi valori di verità in ogni caso.

Conviene tenere a mente alcune delle equivalenze elementari:

$$\begin{aligned} \neg\neg\Phi &\equiv \Phi & \Phi \wedge (\psi \vee \Theta) &\equiv (\Phi \wedge \psi) \vee (\Phi \wedge \Theta) & \Phi \vee (\psi \wedge \Theta) &\equiv (\Phi \vee \psi) \wedge (\Phi \vee \Theta) \\ \neg(\Phi \wedge \psi) &\equiv \neg\Phi \vee \neg\psi & \neg(\Phi \vee \psi) &\equiv \neg\Phi \wedge \neg\psi^7 & \\ \Phi \rightarrow \neg\psi &\equiv \psi \rightarrow \neg\Phi & \Phi \rightarrow \psi &\equiv \neg\psi \rightarrow \neg\Phi \end{aligned}$$

⁶ “equivale a”.

⁷ Leggi di De Morgan.

Esercizio 2.4. Dimostrare le equivalenze delle formule elencate sopra.

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

$$\neg \forall x \Phi \equiv \exists x \neg \Phi \quad \neg \forall x \neg \Phi \equiv \exists x \Phi$$

$$\neg \exists x \Phi \equiv \forall x \neg \Phi \quad \neg \exists x \neg \Phi \equiv \forall x \Phi$$

Esercizio 2.5. Convinciti della validità delle equivalenze precedenti.

Esercizio 2.6. Dimostra che:

$$\neg \forall x \in A \Phi \equiv \exists x \in A \neg \Phi \quad \neg \exists x \in A \Phi \equiv \forall x \in A \Phi$$

Esercizio 2.7. Dimostra che:

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

Esercizio 2.8. Secondo te, la seguente formula è vera?

$$\forall A((\exists x x \in A) \rightarrow \exists x \in A(x \in B \rightarrow \forall y \in A y \in B))$$

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**.

§3 I primi assiomi

§3.1 Assiomi dell'insieme vuoto e di estensionalità

Assioma 3.1 (Assioma dell'insieme vuoto)

Esiste un insieme vuoto.

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

Nota 3.2 — Questo assioma non sarebbe strettamente necessario, in quanto potremmo ottenere un insieme vuoto anche come sottoprodotto, per esempio, dell'assioma dell'infinito che vedremo in seguito. Tuttavia è bello poter partire avendo per le mani almeno un insieme.

Assioma 3.3 (Assioma di estensionalità)

Un insieme è determinato dalla collezione dei suoi elementi. Due insiemi coincidono se e solo se hanno i medesimi elementi.

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

Esercizio 3.4. Dimostra che la freccia $a = b \rightarrow \forall x(x \in a \leftrightarrow x \in b)$, in realtà, segue dal fatto che se $a = b$ allora a e b sono indistinguibili^a.

^aNel senso che abbiamo descritto in precedenza, cioè sono nomi della stessa cosa.

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

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

Proposizione 3.5 (Unicità dell'insieme vuoto)

C'è un unico insieme vuoto.

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

Dimostrazione. 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:

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

[sono coimplicate logicamente] perché $y \in x_1$ e $y \in x_2$ sono entrambe necessariamente false (quindi la proposizione così com'è scritta è sempre vera). Per **estensionalità**, la proposizione sopra (sempre vera) è equivalente a $x_1 = x_2$ (che quindi a sua volta sarà sempre vera), e quindi abbiamo la tesi. \square

Dimostrazione formale. 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 $\exists!$, ciò equivale a:

$$\exists x_1((\forall y y \notin x_1) \wedge \forall x_2((\forall y y \notin x_2) \rightarrow x_2 = x_1))$$

Per l'[assioma del vuoto](#), $\exists x_1 \forall y y \notin x_1$: fissiamo questo x_1 . Resta da dimostrare che:

$$(\forall y y \notin x_1) \wedge \forall x_2 (\forall y y \notin x_2) \rightarrow x_2 = x_1$$

Per costruzione, $\forall y y \notin x_1$, è vera (avendo fissato x_1), quindi resta:

$$\forall x_2 (\forall y y \notin x_2) \rightarrow x_2 = x_1$$

Ora prendiamo un x_2 qualunque, dobbiamo dimostrare:

$$\forall y (y \notin x_2) \rightarrow x_2 = x_1$$

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 $\forall y y \notin x_1$, [vera] per costruzione, sia $\forall y y \notin x_2$, [vera] 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 la verità dell'implicazione iniziale. \square

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

Notazione 3.6 — L'unicità dell'insieme vuoto ci giustifica ad introdurre delle nuove abbreviazioni:

$$x = \emptyset \stackrel{\text{def}}{=} \forall y y \notin x \quad \emptyset \in x \stackrel{\text{def}}{=} \exists z (z = \emptyset \wedge z \in x)$$

§3.2 Assioma di separazione

Assioma 3.7 (Assioma di separazione)

Se A è un insieme, e $\psi(x)$ una formula insiemistica qualunque, allora $\{x \in A | \psi(x)\}$ ^a è un insieme.

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

^aStiamo usando già questa notazione, ma la definiremo a breve.

Nota 3.8 — 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.

Proposizione 3.9

Fissati A e $\psi(x)$, l'insieme $\{x \in A | \psi(x)\}$ è univocamente definito. Ossia:

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

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

$$\forall x x \in B_1 \leftrightarrow (x \in A \wedge \psi(x)) \quad \forall x x \in B_2 \leftrightarrow (x \in A \wedge \psi(x))$$

Allora, $\forall x x \in B_1 \leftrightarrow (x \in A \wedge \psi(x)) \leftrightarrow x \in B_2$, quindi ciò coimplica, per [estensionalità](#), che $B_1 = B_2$. \square

Esercizio 3.10 (Transitività della coimplicazione). Verificare che se $\psi \leftrightarrow \Phi$ e $\Phi \leftrightarrow \Theta$, allora $\psi \leftrightarrow \Theta$.

Notazione 3.11 — Vista l'unicità, possiamo introdurre una nuova abbreviazione:

$$B = \{x \in A | \psi(x)\} \stackrel{\text{def}}{=} \forall x x \in B \leftrightarrow (x \in A \wedge \psi(x))$$

Osserviamo che l'assioma di separazione è una forma indebolita del principio di collezione⁸. Rimpiazzando il principio con questo assioma, il Paradosso di Russell diventa una proposizione.

Proposizione 3.12 (Insieme di tutti gli insiemi)

Non esiste l'insieme di tutti gli insiemi.

$$\exists V \forall x x \in V$$

Dimostrazione. Supponiamo, per assurdo, che esista questo V . Allora, per [separazione](#) con la formula $\psi(x) \equiv x \notin x$, esiste l'insieme:

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

che, per definizione (via separazione), ha la proprietà:

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

Per ipotesi assurda, $x \in V$ è sempre vera (stiamo considerando l'insieme di tutti gli insiemi), quindi quanto scritto si riduce a:

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

prendendo ora come insieme N : $x = N$, abbiamo $N \in N \leftrightarrow N \notin N$, assurdo. \square

§3.3 Classi e classi proprie

Sebbene, abbiam detto che 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 $\psi(x)$.⁹

Non avrebbe senso scrivere $C \in \text{qualcosa}$, perché il simbolo \in in $x \in C$ non ha senso (ha senso solo tra oggetti di tipo insieme), se non nel tutt'uno $\in C$. In altri termini, se scriviamo $x \in C$ in luogo di $\psi(x)$ è solo come ausilio dell'intuizione (per comodità insomma, senza intendere qualcosa di formale all'interno della teoria degli insiemi): avremmo potuto decidere di scrivere $x \clubsuit$, o nient'altro che $\psi(x)$.

⁸Quel principio che definisce gli insiemi come tutte le cose che soddisfano una certa formula.

⁹Ovvero per tutti gli oggetti (solo gli insiemi in questo caso) che soddisfano una tale formula $\psi(x)$.

Definizione 3.13 (Classe universale). La classe V si dice **classe universale** ed è la classe di tutti gli insiemi.

$$x \in V \stackrel{\text{def}}{=} x = x^{10}$$

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

Notazione 3.14 (Uguaglianza tra classi) — Date due classi C e D , che, ricordiamo, non significa altro che “date due formule...”, definiamo l’abbreviazione:

$$C = D \stackrel{\text{def}}{=} \forall x((x \in C) \leftrightarrow (x \in D))^{10}$$

¹⁰Non è altro che un’abbreviazione per dire che le formule che definiscono le classi C e D sono soddisfatte dagli stessi insiemi x .

Ora, dato un qualunque insieme A , possiamo definire la classe \hat{A} degli x tali che $x \in A$ (cioè la classe degli x che soddisfano $\psi(x) : x \in A$). Se $\hat{A} = \hat{B}$, per l’abbreviazione data non stiamo dicendo altro che:

$$\forall x((x \in A) \leftrightarrow (x \in B))$$

che equivale $A = B$ per **estensionalità**. Ha quindi senso, con un leggero abuso di notazione, omettere il cappelletto $\hat{\cdot}$ 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.¹¹

Esempio 3.15

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.

§3.4 Assioma del paio e coppia di Kuratowski

I primi tre assiomi ci dicono, a grandi linee, che, entro i limiti di quanto si può fare rinunciando al principio di collezione - che esiste $\{x \mid \text{una qualunque proprietà}\}$ - , 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 sono elencati esplicitamente, fare prodotti di insiemi esistenti, considerare le funzioni fra insiemi esistenti, etc.

¹⁰Cioè la classe degli insiemi che soddisfano il predicato $\psi(x) : x = x$ (ovvero tutti gli insiemi per quanto assunto all’inizio della teoria), $V = \{x \mid \psi(x)\} = \{x \mid x = x\}$ (dove naturalmente non sto usando separazione ma il principio di collezione perché stiamo definendo una classe).

¹¹Essere un insieme per una classe significa quindi moralmente identificarvisi nel senso riportato sopra, se ciò non fosse possibile parliamo di classi proprie.

Assioma 3.16 (Assioma del paio)

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

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

Proposizione 3.17 (Unicità del paio)

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 3.18. Dimostra la proposizione precedente.

Soluzione. Supponiamo che esistano P_1 e P_2 tali che:

$$\forall x(x \in P_1 \leftrightarrow (x = a \vee x = b)) \quad \text{e} \quad \forall x(x \in P_2 \leftrightarrow (x = a \vee x = b))$$

da ciò segue che:

$$\forall x(x \in P_1 \leftrightarrow x \in P_2)$$

dunque per **estensionalità** l'espressione sopra equivale a $P_1 = P_2$. \square

Proposizione 3.19 (Esistenza dei singoletti)

Dato a , esiste ed è unico $\{a\}$.

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

Dimostrazione. Ponendo $b = a$ nella proposizione precedente, si ha che:

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

ora $x = a \vee x = a$ equivale a $x = a$ ¹². \square

Notazione 3.20 (Paio (o coppia) e singoletto) — Possiamo ora introdurre delle abbreviazioni per il paio (o coppia) ed i singoletti:

$$P = \{a, b\} \stackrel{\text{def}}{=} \forall x x \in P \leftrightarrow (x = a \vee x = b)$$

$$S = \{a\} \stackrel{\text{def}}{=} \forall x x \in S \leftrightarrow x = a$$

Osservazione 3.21 — Osserviamo che $\{a, b\} = \{b, a\}$.

Dimostrazione. Segue dal fatto che \vee è commutativo:

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

quindi per **estensionalità** $\{a, b\} = \{b, a\}$. \square

¹²Stiamo dicendo che in generale $\{a, a\} = \{a\}$ poiché $a \vee a = a$ (in base alle regole dei connettivi logici).

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

Definizione 3.22 (Coppia di Kuratowski). Definiamo la **coppia di Kuratowski**:

$$(a, b) \stackrel{\text{def}}{=} \{a, \{a, b\}\}$$

Proposizione 3.23 (Proprietà di coppia ordinata)

La coppia di Kuratowski (a, b) rappresenta la coppia ordinata di a e b , ossia vale che:

$$(a, b) = (a', b') \leftrightarrow (a = a' \wedge b = b')$$

Dimostrazione. Detto $c = (a, b)$, vogliamo determinare univocamente a e b . Osserviamo che a è determinata da:

$$x = a \leftrightarrow \forall y \in c(x \in y)^{13}$$

la freccia \rightarrow segue da come è definita la coppia (a, b) , mentre \leftarrow segue dal fatto che, sempre per definizione di coppia di Kuratowski, $\{a\} \in c = (a, b)$, per cui:

$$\forall y \in c(x \in y) \stackrel{\text{ipotesi}}{\implies} x \in \{a\} \stackrel{\text{singoloetto}}{\implies} x = a$$

Determiniamo ora univocamente b . Studiamo prima il caso in cui $\exists!x(x \in c)$ - cioè il caso in cui abbiamo $(x, x) = \{\{x\}\}$ -:

$$\exists!x(x \in c) \iff \{a\} = \{a, b\} \iff b = a$$

In questo caso b è determinato. Se non fosse così allora $\{a, b\}$ avrebbe due elementi distinti e b sarebbe univocamente determinato da:

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

□

Definizione 3.24 (n -upla ordinata). Possiamo estendere la definizione di coppia ordinata con il seguente trucco:

$$\begin{aligned} (a, b, c) &\stackrel{\text{def}}{=} ((a, b), c) \\ (a, b, c, d) &\stackrel{\text{def}}{=} (((a, b), c), d) \\ (a_1, a_2, \dots, a_n) &\stackrel{\text{def}}{=} ((a_1, a_2, \dots, a_{n-1}), a_n) \end{aligned}$$

Nota 3.25 — 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 -upla (a_1, \dots, a_n) tale che...”. Però, per ogni n dato, chissà 92, possiamo scrivere esplicitamente una formula che dice $x = (a_1, a_2, a_3, \dots, a_{92})$.

¹³Sostanzialmente stiamo dicendo che a è identificato univocamente come l'elemento che appartiene ad entrambi gli elementi di (a, b) .

Proposizione 3.26 (Proprietà di n -upla ordinata)

Si ha che:

$$(a, b, c) = (a', b', c') \leftrightarrow a = a' \wedge b = b' \wedge c = c'$$

$$(a_1, \dots, a_n) = (a'_1, \dots, a'_n) \leftrightarrow a_1 = a'_1 \wedge \dots \wedge a_n = a'_n$$

Esercizio 3.27. Dimostra la prima e convinciti che, dato un qualunque n esplicito, potresti dimostrare la seconda.

§3.5 Assioma dell'unione e operazioni booleane**Axioma 3.28** (Axioma dell'unione)

Dato un insieme A esiste un insieme B i cui elementi sono gli elementi degli elementi di A . Ovvero, dato un insieme A esiste l'unione degli elementi di A .

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

^aCioè x è un elemento di B se e solo se è un elemento di un elemento di A .

Proposizione 3.29 (Unicità dell'unione)

Vale l'unicità dell'unione:

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

Dimostrazione. Supponiamo di avere B_1 e B_2 tali che:

$$\forall x x \in B_1 \leftrightarrow \exists y \in A x \in y$$

$$\forall x x \in B_2 \leftrightarrow \exists y \in A x \in y$$

quindi $\forall x(x \in B_1 \leftrightarrow x \in B_2)$, e per **estensionalità** $B_1 = B_2$. \square

Notazione 3.30 (Unione di un insieme) — Possiamo introdurre l'abbreviazione:

$$B = \bigcup A^a \stackrel{\text{def}}{=} \forall x (x \in B \leftrightarrow \exists y (x \in y))$$

^a “Unione di A ”.

Esercizio 3.31. Dimostra che l'assioma dell'unione segue che:

$$\forall A \exists B (\forall y \in A \forall x \in y x \in B)^a$$

^aCioè per ogni insieme esiste l'insieme di tutti gli elementi degli elementi di A .

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

Definizione 3.32 (Unione di insiemi). Poniamo:

$$a \cup b \stackrel{\text{def}}{=} \bigcup \{a, b\}$$

Proposizione 3.33 (Caratterizzazione unione di insiemi)

Dati a, b e $a \cup b$ vale che:

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

Dimostrazione. Dire che x è un elemento di $a \cup b$ equivale a dire che x è un elemento di un elemento di $\{a, b\}$, ossia che x è un elemento di uno tra a e b ($x \in a \vee x \in b$). \square

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

Definizione 3.34 (Intersezione di un insieme). Sia C una classe¹⁴ non vuota. L'insieme B è l'**intersezione** di C se:

$$B = \bigcap C \stackrel{\text{def}}{=} \forall x(x \in B \leftrightarrow \forall y \in C(x \in y))$$

cioè x sta in b se è elemento di ogni elemento di C .

Proposizione 3.35 (Esistenza e unicità dell'intersezione)

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

$$\forall A(A \neq \emptyset \rightarrow \exists! B \forall x(x \in B \leftrightarrow \forall y \in A(x \in y)))$$

Nota 3.36 — L'ipotesi $C \neq \emptyset$ è necessaria perché altrimenti si avrebbe che $\bigcap \emptyset$ è la classe universale V ($x \in \bigcap \emptyset \leftrightarrow \forall y \in \emptyset(x \in y)$ (dove il RHS è sempre falso per costruzione, quindi gli x che soddisfano l'enunciato sono tutti)), che non è un insieme.

Dimostrazione. L'unicità segue per **estensionalità** al solito modo. Veniamo all'esistenza. Dal momento che C non è vuota esiste $z \in C$, dunque per separazione possiamo costruire l'insieme:

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

e verificare che tale insieme è proprio l'intersezione che stiamo cercando di costruire. Infatti, $x \in B \implies \forall y \in C(x \in y)$, d'altro canto, $\forall y \in C(x \in y)$ implica, in particolare, $y \in z$, per cui $y \in B$. Abbiamo così verificato che $x \in B \leftrightarrow \forall y \in C(x \in y)$, ossia $B = \bigcap C$. \square

Notazione 3.37 (Intersezione e differenza di insiemi) — Poniamo:

$$a \cap b \stackrel{\text{def}}{=} \bigcap \{a, b\} \quad \text{e} \quad a \setminus b \stackrel{\text{def}}{=} \{x \in a \mid x \notin b\}$$

¹⁴Quindi, in particolare, C può essere un insieme (in questo caso la definizione è comunque lecita in generale con le classi, i cui elementi sono appunto insiemi).

Proposizione 3.38 (Caratterizzazione intersezione e differenza di insiemi)

Vale che:

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

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

Esercizio 3.39. Dimostrare la proposizione precedente (la seconda è semplicemente la definizione).

Proposizione 3.40 (Proprietà di unione, intersezione e differenza di insiemi)

Alcune proprietà delle operazioni \cup , \cap , \setminus :

commutatività:

$$a \cup b = b \cup a \quad \text{e} \quad a \cap b = b \cap a$$

associatività:

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

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

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:

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

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

Dimostrazione. Tutte queste proprietà su deducono immediatamente dalle corrispondenti proprietà dei connettivi logici, le quali, a loro volta, si vedono con le tabelle di verità. Per esempio, dimostriamo la prima delle leggi di De Morgan (facendo uso della corrispondente legge per i connettivi logici):

$$\begin{aligned} x \in a \setminus (b \cup c) &\iff x \in a \wedge x \notin (b \cup c) \\ &\iff x \in a \wedge \neg(x \in b \vee x \in c) \\ &\stackrel{\text{De Morgan}}{\iff} x \in a \wedge x \notin b \wedge x \notin c \\ &\iff x \in a \wedge x \notin b \wedge \underbrace{x \in a}_{\text{non cambia nulla}} \wedge x \notin c \\ &\iff x \in (a \setminus b) \wedge x \in (a \setminus c) \\ &\iff x \in (a \setminus b) \cap (a \setminus c) \end{aligned}$$

□

Ora possiamo costruire insiemi finiti elencandone gli elementi, come si fa di solito, con la notazione $\{\dots\}$ ¹⁵.

¹⁵Paradossalmente prima di aggiungere l'assioma dell'unione alla teoria potevamo costruire n -uple ordinate di lunghezza arbitraria, ma non un insieme con più di due elementi.

Notazione 3.41 (Insiemi di n elementi) — Possiamo ora introdurre un'abbreviazione per indicare insiemi con più di due elementi (costruiti usando l'[assioma dell'unione](#)):

$$\begin{aligned}\{a, b, c\} &\stackrel{\text{def}}{=} \{a\} \cup \{b\} \cup \{c\} \\ \{a, b, c, d\} &\stackrel{\text{def}}{=} \{a\} \cup \{b\} \cup \{c\} \cup \{d\} \\ \{a_1, \dots, a_n\} &\stackrel{\text{def}}{=} \{a_1\} \cup \dots \cup \{a_n\}\end{aligned}$$

Proposizione 3.42 (Caratterizzazione di insieme con n elementi)

Vale che:

$$\begin{aligned}x \in \{a, b, c\} &\leftrightarrow (x = a \vee x = b \vee x = c) \\ x \in \{a_1, \dots, a_n\} &\leftrightarrow (x = a_1 \vee \dots \vee x = a_n)\end{aligned}$$

Esercizio 3.43. Dimostrare la proposizione precedente.

§3.6 Axioma delle parti e prodotto cartesiano

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

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

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

Axioma 3.44 (Axioma delle parti)

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

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

Proposizione 3.45 (Unicità delle parti)

Vale che:

$$\forall A \exists! B \forall x x \in B \leftrightarrow x \subseteq A$$

Dimostrazione. Segue come sempre per [estensionalità](#), in quanto, se avessimo B_1, B_2 , allora:

$$\forall x(x \in B_1 \leftrightarrow x \subseteq A) \quad \text{e} \quad \forall x(x \in B_2 \leftrightarrow x \subseteq A)$$

quindi $\forall x((x \in B_1) \leftrightarrow (x \subseteq A) \leftrightarrow (x \in B_2)) \leftrightarrow \forall x(x \in B_1 \leftrightarrow x \in B_2) \leftrightarrow B_1 = B_2$. \square

Notazione 3.46 (Insieme delle parti - o insieme potenza) — Data l'unicità possiamo porre:

$$B = \mathcal{P}(A) \stackrel{\text{def}}{=} \forall x x \in B \leftrightarrow x \subseteq A$$

Proposizione 3.47 (Esistenza ed unicità del prodotto cartesiano)

Dati A e B esiste ed è unico insieme $A \times B$ tale che:

$$\forall z(z \in A \times B) \leftrightarrow \exists x \in A \exists y \in B z = (x, y)^{\text{a}}$$

^aOssia, informalmente, $z \in A \times B$ se e solo se si può scrivere come coppia ordinata di un elemento di A ed uno di B .

Dimostrazione. L'unicità è conseguenza immediata della definizione e dell'[assioma di estensionalità](#) (stessa dimostrazione di sempre). Per l'esistenza, definiamo per [separazione](#):

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

così come scritto, siamo sicuri che è un insieme che contiene coppie ordinate di elementi di A e B , tuttavia, affinché tale insieme che abbiamo costruito nella teoria, rispetti la definizione data di prodotto cartesiano, dobbiamo anche dimostrare anche che ogni coppia (x, y) con $x \in A$ e $y \in B$ appartiene a questo insieme. Per fare ciò bisogna dimostrare che tutte queste coppie appartengono a $\mathcal{P}(\mathcal{P}(A \cup B))$.^{16 17}

$$\begin{aligned} a \in A \wedge b \in B &\implies \{a\}, \{a, b\} \subseteq A \cup B \\ &\implies \{a\}, \{a, b\} \in \mathcal{P}(A \cup B) \\ &\stackrel{\text{paio}}{\implies} (a, b) = \{\{a\}, \{a, b\}\} \subseteq \mathcal{P}(A \cup B) \\ &\implies (a, b) \in \mathcal{P}(\mathcal{P}(A \cup B)) \end{aligned}$$

pertanto tutte le coppie ordinate di elementi di A e B appartengono a $A \times B$, che quindi rispetta proprio la definizione di prodotto cartesiano voluta. \square

Nota 3.48 — Avremmo potuto costruire $A \times B$ usando, anziché l'[assioma delle parti](#), l'[assioma del rimpiazzamento](#), che vedremo più avanti.

§3.7 Relazioni di equivalenza e di ordine, funzioni

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

Definizione 3.49 (Relazione binaria). Si dice [relazione binaria](#) fra A e B un sottoinsieme di $A \times B$.

Notazione 3.50 (Relazione binaria) — Data una relazione $\mathcal{R} \subseteq A \times B$, definiamo l'abbreviazione:

$$a \mathcal{R} b \stackrel{\text{def}}{=} (a, b) \in \mathcal{R}$$

¹⁶Poniamo $a, b, \dots \in z \stackrel{\text{def}}{=} a \in z \wedge b \in z \wedge \dots$ e $a, b, \dots \subseteq z \stackrel{\text{def}}{=} a \subseteq z \wedge b \subseteq z \wedge \dots$

¹⁷Tutte le implicazioni si basano sul fatto che se un oggetto è sottoinsieme di un qualche insieme allora è un elemento del corrispondente insieme delle parti per definizione.

Esempio 3.51

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

Considerando il caso di $A \times A$ possiamo definire le seguenti relazioni.

Definizione 3.52. Una relazione $\sim \subseteq A \times A$ è una **relazione di equivalenza** se è:

- (i) **riflessiva**: $\forall x \in A \ x \sim x$.
- (ii) **simmetrica**: $\forall x, y \in A$ ¹⁸ $x \sim y \leftrightarrow y \sim x$.
- (iii) **transitiva**: $\forall x, y, z \in A \ (x \sim y \wedge y \sim z) \rightarrow x \sim z$.

Definizione 3.53. $\leq \in A \times A$ è una **relazione di ordine (largo)** se è:

- (i) **riflessiva**: $\forall x \in A \ x \leq x$.
- (ii) **antisimmetrica**: $\forall x, y \in A \ (x \leq y \wedge y \leq x) \rightarrow x = y$.
- (iii) **transitiva**: $\forall x, y, z \in A \ (x \leq y \wedge y \leq z) \rightarrow x \leq z$.

Definizione 3.54. $< \in A \times A$ è una **relazione di ordine stretto** se è:

- (i) **irriflessiva**: $\forall x \in A \ \neg(x < x)$.
- (ii) **transitiva**: $\forall x, y, z \in A \ (x < y \wedge y < z) \rightarrow x < z$.

Esercizio 3.55. Dimostra che una relazione di ordine stretto $<$ su A è automaticamente asimmetrica:

$$\forall x, y \in A \ x < y \rightarrow \neg(y < x)$$

Soluzione. Se valesse che $\forall x, y \in A \ x < y \rightarrow y < x$, allora sarebbero contemporaneamente vere $x < y$ e $y < x$, da cui, per transitività si avrebbe $x < x$ che è falso. \square

Proposizione 3.56 (Corrispondenza tra ordini stretti e larghi)

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

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

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

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

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

^aFormalmente: $\{z \in A \times A \mid \exists x, y \in A \ z = (x, y) \wedge \dots\}$.

^bCome la nota sopra.

¹⁸ $\forall x_1, \dots, x_n \stackrel{\text{def}}{=} \forall x_1 \dots \forall x_n$, e lo stesso con \exists e con i quantificatori limitati.

Dimostrazione. Definiamo la **diagonale di una relazione** di $A \times A$ come:

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

Allora è facile verificare che, se $<$ è una relazione di ordine stretto, allora $< \cap \Delta_A = \emptyset$ e $< \cup \Delta_A$ è una relazione di ordine largo corrispondente. Viceversa, 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. \square

Notazione 3.57 (Relazioni d'ordine strette e larghe) — Fissata una relazione di ordine largo \leq su A , ci sentiremo liberi di usare la corrispondente relazione di ordine stretto $<$ fintanto che la scelta del simbolo sia indizio sufficiente dell'operazione. Inoltre scrivremo $x > y$ per $y < x$ e $x \geq y$ per $y \leq x$.

Definizione 3.58 (Relazione di ordine totale). Una **relazione di ordine totale** su A è una relazione di ordine \leq tale che:

$$\forall x, y \in A (x \leq y) \vee (x = y) \vee (y \leq x)$$

Esercizio 3.59. Formula la definizione precedente per ordini stretti.

Soluzione. Diciamo che $<$ è un ordinamento totale (stretto) su A se:

$$\forall x \in A \forall y \in A (x \neq y \wedge ((x < y) \vee (x > y))) \vee (x = y)$$

o anche semplicemente:

$$\forall x \in A \forall y \in A (x = y) \vee (x < y) \vee (x > y)$$

E per quanto detto possiamo anche pensare che:

$$\leq \text{ordine totale} \iff < \cup \Delta_A \text{ ordine totale}$$

(infatti nella prima definizione non è strettamente necessario che compaia l'uguaglianza, la si può ottenere quanto entrambe le diseguaglianze sono vere per antisimmetria, mentre per ordini stretti è necessario aggiungere la diagonale nella definizione di totalità). \square

Definizione 3.60 (Restrizione di una relazione). Data una relazione $\mathcal{R} \subseteq A \times B$, e dati $A' \subseteq A$, $B' \subseteq B$, possiamo definire la **restrizione** di \mathcal{R} a $A' \times B'$:

$$\mathcal{R}|_{A' \times B'} \stackrel{\text{def}}{=} \mathcal{R} \cap (A' \times B')$$

“restrizione di \mathcal{R} a $A' \times B'$ ”.

Esercizio 3.61. Data \mathcal{R} relazione di equivalenza/ordine su A e $A' \subseteq A$, dimostra che $\mathcal{R}|_{A' \times A'}$ è una relazione di equivalenza/ordine su A' .

Soluzione. Vediamolo per le relazioni di equivalenza. È facile osservare che $\forall a' \in A'$, vale che $(a', a') \in \mathcal{R}|_{A' \times A'}$ (sta in $A' \times A'$ per definizione di prodotto cartesiano e sta in \mathcal{R} essendo una relazione di equivalenza per ipotesi (vale il per ogni)), analogamente valgono simmetria e riflessività. \square

Definizione 3.62 (Dominio e immagine di una relazione). Data una relazione $\mathcal{R} \subseteq A \times B$, definiamo:

$$\begin{aligned}\text{Dom}(\mathcal{R}) &\stackrel{\text{def}}{=} \{x \in A \mid \exists y \in B \ x \mathcal{R} y\} && \text{dominio di } \mathcal{R} \\ \text{Im}(\mathcal{R}) &\stackrel{\text{def}}{=} \{y \in B \mid \exists x \in A \ x \mathcal{R} y\} && \text{immagine di } \mathcal{R}\end{aligned}$$

(notare che $\text{Dom}(\mathcal{R})$ e $\text{Im}(\mathcal{R})$ non coincidono necessariamente con A e B).

Definizione 3.63 (Funzione). Chiamiamo **funzione** $f : A \rightarrow B$ 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 3.64 (Immagine e immagine di un sottoinsieme) — Data una funzione f possiamo indicare la coppia $(x, y) \in f$ con la seguente abbreviazione:

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

Dato $S \subseteq \text{Dom}(f)$, indichiamo l'immagine di un sottoinsieme (ovvero l'insieme delle immagini del sottoinsieme) come:

$$f[S] \stackrel{\text{def}}{=} \{y \in \text{Im}(f) \mid \exists x \in S \underbrace{y = f(x)}_{=(x,y) \in f}\} = \underbrace{\{f(x) \mid x \in S\}}_{\text{informalmente}}$$

Definizione 3.65 (Iniettività, suriettività e bigettività). Una funzione $f : A \rightarrow B$ è:

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

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

bigettiva se: è sia iniettiva sia surgettiva.

Definizione 3.66 (Funzione inversa). Data f iniettiva:

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

Osservazione 3.67 (Funzione inversa e controimmagine) — Se f iniettiva, $f^{-1} : \text{Im}(f) \rightarrow \text{Dom}(f)$ è una funzione^a a sua volta iniettiva (basta pensare alla definizione di f^{-1} iniettiva e usare che per l'iniettività di f c'è un'unica $x \in \text{Dom}(f)$ tale che $y = f(x)$). In particolare se $f : A \rightarrow B$ è bigettiva, allora f^{-1} è bigettiva.

^aAltrimenti è la semplice controimmagine di un sottoinsieme dell'immagine (che non è una funzione).

Definizione 3.68 (Restrizione di una funzione). Data $f : A \rightarrow B$ e $A' \subseteq A$ definiamo:

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

“ f **ristretta** ad A' ” è una funzione: $A' \rightarrow B$.

Definizione 3.69 (Composizione di funzioni). Date $g : A \rightarrow B$ e $f : B \rightarrow C$:

$$f \circ g \stackrel{\text{def}}{=} \{(x, z) \in A \times C \mid z = f(g(x))\}^{19}$$

“ f **composta** con g ” è una funzione: $A \rightarrow C$.

¹⁹O più formalmente $\exists y (y = g(x) \wedge z = f(y))$.

Notazione 3.70 (Funzione identità) — Indichiamo con id_A la **funzione identità** su A :

$$\text{id}_A \stackrel{\text{def}}{=} \{(x, y) \in A \times A \mid x = y\} = \Delta_A$$

Osservazione 3.71 (Caratterizzazione funzione inversa) — Data $f : A \rightarrow B$ bigettiva e $g : B \rightarrow A$ è equivalente scrivere:

$$g = f^{-1} \quad g \circ f = \text{id}_A \quad f \circ g = \text{id}_B$$

Esercizio 3.72 (Composizione di funzioni iniettive/surgettive/biggettive). Data $f : A \rightarrow B$ e $g : B \rightarrow C$, sotto quali condizioni $g \circ f$ è iniettiva, suriettiva, bigettiva?

Soluzione. Indaghiamo il problema partendo prima dalle singole funzioni con delle proprietà e componendole. Se f e g sono iniettive, allora $g \circ f$ è iniettiva, infatti:

$$g(f(x)) = g(f(y)) \stackrel{g \text{ iniett.}}{\iff} f(x) = f(y) \stackrel{f \text{ iniett.}}{\iff} x = y \quad \forall x, y \in A$$

che è equivalente alla definizione di $g \circ f : A \rightarrow C$ iniettiva. Se f e g sono surgettive, allora $g \circ f$ è surgettiva:

$$\begin{aligned} g \text{ surgettiva} &\iff \forall z \in C \exists y \in B g(y) = z \\ f \text{ surgettiva} &\iff \forall y \in B \exists x \in A f(x) = y \end{aligned}$$

che messe assieme ci danno che $g(f(x)) = z$, cioè per ogni $z \in C$ esiste $x \in A$ tale che $(g \circ f)(x) = z$, che è equivalente alla definizione di $g \circ f$ surgettiva. Naturalmente, mettendo assieme i risultati precedenti, otteniamo che f e g biggettive implica $g \circ f$ bigettiva. Viceversa, osserviamo che se $g \circ f$ è iniettiva, allora f è iniettiva, infatti, se per assurdo $f(x) = f(y)$, con $x \neq y$, allora, applicando g , si ha $g(f(x)) = g(f(y))$ (perché immagini di cose uguali), ma per iniettività di $g \circ f$, ciò equivale a $x = y$, che è assurdo, pertanto $x = y$ ²⁰. Se $g \circ f$ è surgettiva, allora g è surgettiva, infatti, per ipotesi, $\forall z \in C \exists x \in A g(f(x)) = z$, e, dato che $f(x) \in B$, abbiamo trovato che per ogni $z \in C$ esiste $y = f(x) \in B$ tale che $g(y) = z$, ovvero g surgettiva.

Infine, verrebbe da chiedersi, se date f iniettiva e g surgettiva, $g \circ f$ sia necessariamente bigettiva (così da avere magari un'equivalenza tra la bigettività della composizione e le proprietà delle funzioni in partenza), sfortunatamente ciò è falso: presa $f : \{0, 1\} \hookrightarrow \{0, 1, 2, 3\}$ e $g : \{0, 1, 2, 3\} \twoheadrightarrow \{0, 1, 2\}$, con:

$$\begin{aligned} g(0) &= 0 & f(0) &= 0 \\ g(1) &= 0 & f(1) &= 1 \\ g(2) &= 2 \\ g(3) &= 3 \end{aligned}$$

abbiamo f iniettiva, g surgettiva, ma $g \circ f$ non è né iniettiva ($g(f(0)) = g(f(1))$) né surgettiva ($\text{Im}(g \circ f) = \{0\}$). \square

²⁰Abbiamo dimostrato per assurdo che $f(x) = f(y) \implies x = y$ (sotto l'ipotesi che $g \circ f$ iniettiva), il viceversa è banale e con questo si ha l'equivalenza con la definizione di f iniettiva

Esercizio 3.73 (Insieme quoziente e proiezione). Data una relazione di equivalenza \sim su A , dimostra che esiste un insieme A/\sim ed una funzione surgettiva i_\sim da A a A/\sim tale che:

$$\forall x, y \in A \ x \sim y \leftrightarrow i_\sim(x) = i_\sim(y)$$

Soluzione. Possiamo definire l'insieme A/\sim per separazione nelle parti di A come segue:

$$A/\sim \stackrel{\text{def}}{=} \{B \in \mathcal{P}(A) \mid \forall x \in A \ \forall y \in B \ x \sim y \leftrightarrow x \in B\}$$

Osserviamo che per ogni $B, C \in A/\sim$, vale che $B \cap C \neq \emptyset \iff B = C$, infatti, se esiste $x \in B \cap C$, allora $x \sim y, \forall y \in B$, e $x \sim z, \forall z \in C$. Da cui $w \in B \iff w \sim x \iff w \in C$ e quindi per l'arbitrarietà di x , vale $B = C$.²¹

Da quanto appena osservato segue quindi che ogni $x \in A$ appartiene ad una e una sola **classe di equivalenza** (gli elementi di A/\sim), in quanto è sempre almeno in relazione con se stesso per riflessività, possiamo quindi definire i_\sim come la funzione da A a A/\sim che manda x nella sua classe di equivalenza. Naturalmente $i_\sim(x) = i_\sim(y)$ equivale al dire che le due classi di equivalenza sono la stessa, dunque per definizione si ottiene proprio che $x \sim y$. Inoltre i_\sim è surgettiva in quanto in ogni classe di equivalenza di A/\sim c'è almeno un elemento (per la riflessività delle relazioni di equivalenza), la cui immagine via i_\sim dà appunto la classe. \square

Esercizio 3.74 (Primo teorema di “omomorfismo”, per insiemi). Data una relazione di equivalenza \sim su A e $f : A \rightarrow B$, affinché esista la funzione $\tilde{f} : A/\sim \rightarrow B$ tale che $f = \tilde{f} \circ i_\sim$, è necessario e sufficiente che $\forall x, y \in A \ x \sim y \rightarrow f(x) = f(y)$.

Soluzione. Osserviamo che²² $f(x) = (\tilde{f} \circ i_\sim)(x), \forall x \in A$ se e solo se $f(x) = \tilde{f}(i_\sim(x))$, ora ciò equivale al fatto che l'immagine dell'elemento $x \in A$ al LHS è uguale a quella della classe di equivalenza (che è un sottoinsieme di A) $i_\sim(x)$ tramite \tilde{f} al RHS. Per rispettare la relazione richiesta (che sarebbe poi la commutatività di un diagramma) possiamo definire $\tilde{f}(C), C \in A/\sim$, come $f(z)$ per un qualunque $z \in C$.

Ora ci basta osservare che questa è una buona definizione, e lo è in quanto tutti gli elementi in C sono in relazione \sim tra loro e per ipotesi tale relazione è che la loro immagine via f sia la stessa, pertanto $f(x) = f(y), \forall x, y \in C$. Infine, poiché $\forall x \in A \ x \in i_\sim(x)$, si ha proprio che $\tilde{f}(i_\sim(x)) = f(x)$. Abbiamo quindi dimostrato che l'uguaglianza iniziale è vera se \sim è definita come nelle ipotesi, osserviamo che se tale uguaglianza funziona, allora due elementi sono in relazione via \sim se e solo se hanno la stessa immagine. Infatti, si avrebbe che:

$$\begin{aligned} f(x) = f(y) &\iff \tilde{f}(i_\sim(x)) = \tilde{f}(i_\sim(y)) \\ &\iff i_\sim(x) = i_\sim(y) \\ &\iff x \sim y \end{aligned}$$

dove la prima equivalenza è l'assunto, la seconda è la definizione di \tilde{f} (che è una bigezione tra A/\sim e $\text{Im}(f)$, per questo abbiamo usato l'iniettività), mentre l'ultima equivalenza è la definizione di classi di equivalenza. \square

²¹Essendo che ogni elemento, per quanto detto è in una classe di equivalenza di A/\sim , si ha anche che $\bigcup A/\sim = A$, dunque le classi di equivalenza sono disgiunte e la loro unione dà proprio l'insieme, pertanto si dirà che formano una **partizione** dell'insieme A .

²²Per essere formalissimi, staremmo usando che $f = \tilde{f} \circ i_\sim \iff f(x) = (\tilde{f} \circ i_\sim)(x), \forall x \in A$, ovvero l'estensionalità per funzioni vista in un'osservazione precedente.

§4 Assioma dell'infinito e 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 insieme. 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:

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

Sceglieremo, invece, quest'altra codifica:

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

$$0 = \emptyset \quad 1 = \{0\} \quad 2 = \{0, 1\} \quad 3 = \{0, 1, 2\} \quad \text{etc.}$$

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 “ereditariamente finiti”, ad essere precisi: definiremo questi concetto a tempo debito).

Servirà un nuovo assioma. E 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} .

Definizione 4.1 (Successore). Definiamo il **successore** di x :

$$s(x) \stackrel{\text{def}}{=} x \cup \{x\}$$

Definizione 4.2 (Insiemi induttivi). Diciamo che A è un **insieme induttivo** se contiene \emptyset ed è chiuso per successori²³, ossia:

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

Assioma 4.3 (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 ω - come l'intersezione della classe, non vuota per l'assioma dell'infinito, di tutti gli insiemi induttivi.²⁴

²³Ciò non esclude che ci possano essere altri elementi oltre a \emptyset che non siano successori (questa cosa è sempre falsa in ω).

²⁴Aver introdotto l'assioma dell'infinito ci assicura che tale intersezione è non vuota, e ciò basta affinché ω sia un insieme (in caso contrario avremmo avuto l'intersezione del vuoto, che, come visto, non è un insieme).

Definizione 4.4 (Numeri naturali). L'insieme ω è l'intersezione di tutti gli insiemi induttivi, ossia ω è l'unico insieme tale che:

$$\forall x(x \in \omega \leftrightarrow (\forall A \text{ "A è induttivo" } \rightarrow x \in A))^{25}$$

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

Definizione 4.5 (Codifica dei numeri naturali). Definiamo:

$$0 \stackrel{\text{def}}{=} \emptyset \quad 1 \stackrel{\text{def}}{=} s(0) \quad 2 \stackrel{\text{def}}{=} s(1) \quad 3 \stackrel{\text{def}}{=} s(2) \quad \text{etc.}$$

Esercizio 4.6. Dimostra che $0, 1, 2, 3 \in \omega$.

Soluzione. Avendo definito ω come:

$$\omega = \bigcap_{A \text{ induttivo}} A$$

sappiamo che $\emptyset \in A$, per ogni insieme induttivo (per definizione), dunque $0 \in \omega$. Inoltre vale che l'intersezione di insiemi induttivi è chiusa per successore (e quindi per quanto appena mostrato è a sua volta un insieme induttivo), infatti:

$$\forall x \in \bigcap_{A \text{ induttivo}} A \leftrightarrow \forall A A \text{ induttivo } (x \in A)$$

ed essendo tutti gli A chiusi per successore (in quanto induttivi) segue che:

$$s(x) \in \bigcap_{A \text{ induttivo}} A \implies s(x) \in \omega$$

Pertanto, avendo osservato che $0 \in \omega$, si avrà anche che $1 = s(0) \in \omega$, $2 = s(1) \in \omega$, $3 = s(2) \in \omega$ e così via. \square

Un esercizio un po' più difficile è esibire insiemi che non appartengono a ω .

Esercizio 4.7. Dimostra che $\{\{\emptyset\}\} \notin \omega$.^a

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

Soluzione. Osserviamo che $\{\{\emptyset\}\}$ non è un successore, se fosse che $s(x) = x \cup \{x\} = \{\{\emptyset\}\}$, dato che x è elemento di $s(x)$ e che $\{\{\emptyset\}\}$ ha un solo elemento, per **estensionalità** deve essere che che $x = \{x\} = \{\emptyset\}$ (ossia tutti gli elementi di $s(x)$ devono essere uguali all'unico elemento di $\{\{\emptyset\}\}$). Pertanto avremmo che $x = \{\emptyset\}$, ma $s(x) = s(\{\emptyset\}) = \{\emptyset\} \cup \{\{\emptyset\}\} =^{26} \{\emptyset, \{\emptyset\}\}$, ma $\{\emptyset\} \neq \emptyset$, perché $\{\emptyset\}$ è non vuoto e \emptyset è proprio il vuoto.

Avendo dimostrato che $\{\{\emptyset\}\}$ non è né un successore né (ovviamente) il vuoto, ci basta mostrare mostrare che non appartiene ad un insieme induttivo A che non ha altri elementi (oltre a \emptyset) che non sono successori. Dando per buono che ω non contenga elementi che non sono successori, si ottiene che $\{\{\emptyset\}\} \notin \omega$.²⁷ \square

²⁵Cioè x è in ω se e solo se è elemento di qualsiasi insieme induttivo (nella classe degli insiemi induttivi), e, inoltre, essendo l'intersezione di una classe, è in particolare un insieme (perché per definizione stiamo intersecando gli elementi di una classe, che sono insiemi).

²⁶Volendo essere pignoli possiamo usare la definizione dell'unione come il prendere gli elementi degli elementi: $\{\emptyset\} \cup \{\{\emptyset\}\} = \bigcup \{\{\emptyset\}, \{\{\emptyset\}\}\}$, e l'unione di tale insieme è formata appunto da tutti gli elementi degli elementi (quindi naturalmente il vuoto \emptyset e anche $\{\emptyset\}$).

²⁷Non abbiamo usato l'hint di Mamino e abbiamo usato un fatto non dimostrato.

§4.1 Gli assiomi di Peano

Per convincerci, però, che ω 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 di successore, **per noi diventano dei teoremi** che dimostreremo a proposito dell'insieme ω ²⁸. In questo senso²⁹, quindi, ω codifica legittimamente i numeri naturali.

Definizione 4.8 (Assiomi di Peano al secondo ordine³⁰). Dato un insieme \mathbb{N} , un elemento $0 \in \mathbb{N}$, e una funzione:

$$\text{succ} : \mathbb{N} \rightarrow \mathbb{N}$$

diciamo che $(\mathbb{N}, 0, \text{succ})$ ³¹ soddisfa gli assiomi di Peano se:

- (a) Il successore è iniettivo:

$$\forall n, m \in \mathbb{N} \text{ succ}(m) = \text{succ}(n) \rightarrow m = n$$
³²

- (b) Lo zero non è un successore:

$$\nexists n \in \mathbb{N} \text{ succ}(n) = 0$$

- (c) **Principio di induzione**: data una qualunque formula insiemistica (proprietà) $\Phi(n)$ vale:

$$(\Phi(0) \wedge \forall n \in \mathbb{N} \Phi(n) \rightarrow \Phi(\text{succ}(n))) \rightarrow \forall n \in \mathbb{N} \Phi(n)$$

<i>Axiomata.</i>
1. $1 \in \mathbb{N}$.
2. $a \in \mathbb{N} \therefore a = a$.
3. $a, b, c \in \mathbb{N} \therefore a = b \Rightarrow b = a$.
4. $\forall a, b \in \mathbb{N} \therefore a = b \wedge b = c \therefore a = c$.
5. $a = b \wedge b \in \mathbb{N} \therefore a \in \mathbb{N}$.
6. $a \in \mathbb{N} \therefore a + 1 \in \mathbb{N}$.
7. $a, b \in \mathbb{N} \therefore a = b \Rightarrow a + 1 = b + 1$.
8. $a \in \mathbb{N} \therefore a + 1 = 1$.
9. $k \in \mathbb{K} \therefore 1 \in k \therefore a \in \mathbb{N} \wedge x \in k \therefore a + 1 \in k \therefore a \in \mathbb{N} \wedge x \in k$.

Apparivano così in “*Arithmetices principia*”, nel 1889, gli assiomi di Peano.

Teorema 4.9 (ω soddisfa gli assiomi di Peano)

La funzione $\text{succ} : \omega \rightarrow \omega : n \mapsto s(n)$, è ben definita e $(\omega, \emptyset, \text{succ})$ soddisfa gli assiomi di Peano.

²⁸Cioè gli assiomi di Peano diventano enunciati dimostrabili all'interno della ZFC.

²⁹Classicamente gli assiomi definivano \mathbb{N} a meno di isomorfismo, mostrando che ω li soddisfa siamo sicuri di avere l'oggetto (insieme) \mathbb{N} definito da tali assiomi nella ZFC, e tale oggetto è appunto ω .

³⁰qualunque cosa questo significhi...

³¹La 3-upla ordinata formata dai tre insiemi $\mathbb{N}, 0, \text{succ}$: $((\mathbb{N}, 0), \text{succ}) = \{(\mathbb{N}, 0), \{(\mathbb{N}, 0), \text{succ}\}\} = \{\{\mathbb{N}, \{\mathbb{N}, 0\}\}, \{\{\mathbb{N}, \{\mathbb{N}, 0\}\}, \text{succ}\}\}$.

³²L'altra freccia è banale e sarà data sempre per scontata.

Dimostrazione. Prima di procedere con le verifiche controlliamo che la funzione $\text{succ} = s$ sia ben definita. Occorre assicurarsi che se $n \in \omega$, allora $\text{succ}(n) = s(n) \in \omega$. Fissiamo $n \in \omega$ e consideriamo un qualunque insieme induttivo A . Siccome A è induttivo $\omega \subseteq A$, 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 all'intersezione, ovvero ω).

Dimostriamo ora che ω rispetta gli assiomi di Peano. Iniziamo con dimostrare (b) e (c), poi passeremo ad (a):

(b) Supponiamo, per assurdo, $s(n) = \emptyset$. Abbiamo allora che:

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

contro la definizione di \emptyset .

(c) Per verificare il principio di induzione, date le ipotesi, occorre verificare che il sottoinsieme di ω degli elementi per cui è vera $\Phi(n)$ è proprio tutto ω , dunque se dimostriamo che l'insieme $A = \{n \in \omega \mid \Phi(n)\} \subseteq \omega$ è induttivo, avendo gratis il primo contenimento, si ha $\omega = A$.

(1) Per ipotesi abbiamo che $\Phi(\emptyset)$, quindi $\emptyset \in A$.

(2) $n \in A \xrightarrow{\text{def. } A} \Phi(n) \xrightarrow{\text{passo indutt.}} \Phi(\text{succ}(n)) = \Phi(s(n)) \xrightarrow{\text{def. } A} s(n) \in A$

(a) La dimostrazione passa attraverso due lemmi.

Lemma 4.10 (Lemma 1)

L'unione di un elemento di ω è contenuta nell'elemento: $\forall n \in \omega \ \bigcup n \subseteq n$.^a

^aE.g. $\bigcup 3 = \bigcup \{0, 1, 2\} = \{0, 1\} = 2$.

Dimostrazione. Avendo dimostrato in (c) che in ω vale l'induzione possiamo usarla con $\Phi(n) \stackrel{\text{def.}}{=} \bigcup n \subseteq n$.

$$\boxed{\Phi(\emptyset)} \quad \bigcup \emptyset = \emptyset \subseteq \emptyset$$

$$\boxed{\Phi(n) \rightarrow \Phi(s(n))} \quad \bigcup s(n) = \bigcup (n \cup \{n\}) \stackrel{*}{=} \underbrace{\left(\bigcup_{\subseteq n} n \right)}_{\text{Hyp. indutt.}} \subseteq n \cup n = n \subseteq s(n)$$

(si noti che il passo base è coerente con le definizioni delle abbreviazioni date), e $*$ vale in quanto:

$$\begin{aligned} x \in \bigcup (n \cup \{n\}) &\stackrel{\text{def.}}{\iff} \exists y (x \in y) \wedge (y \in (n \cup \{n\})) \\ &\stackrel{\text{caratt. } \cup}{\iff} \exists y (x \in y) \wedge (y \in n \vee y = n) \\ &\stackrel{\text{distrib. } \wedge}{\iff} \exists y (x \in y \wedge y \in n) \vee (x \in y \wedge y = n) \\ &\iff \exists y (x \in y \wedge y \in n) \vee \exists y (x \in y \wedge y = n) \\ &\stackrel{\text{def.}}{\iff} x \in \bigcup n \vee x \in n \\ &\stackrel{\text{caratt. } \cup}{\iff} x \in \left(\bigcup n \right) \cup n \end{aligned}$$

(dove alla secondo membro della seconda equivalenza abbiamo che $y \in \{n\}$ e per **estensionalità** equivale a $y = n$). \square

Lemma 4.11 (Lemma 2)

L'unione dei successori di un elemento in ω è proprio l'elemento: $\forall n \in \omega \cup s(n) = n$.

Dimostrazione. Ricopiamo quanto fatto nel passo induttivo della dimostrazione precedente abbiamo:

$$\bigcup s(n) = \bigcup (n \cup \{n\}) = (\bigcup n) \cup n \stackrel{*}{\subseteq} n$$

dove in $*$ abbiamo usato che $\bigcup n \subseteq n$, non per ipotesi induttiva (visto che non stiamo facendo alcuna induzione), ma stiamo usando direttamente il risultato del Lemma 1. Naturalmente vale anche che $n \subseteq \bigcup s(n)$ (ogni elemento di n è elemento dell'elemento n in $s(n)$), dunque vale la tesi. \square

Finalmente abbiamo che, per il Lemma 2:

$$s(m) = s(n) \implies \bigcup s(m) = \bigcup s(n) \xrightarrow{\text{Lemma 2}} m = n$$

dove la prima freccia è data dal fatto che stiamo considerando l'unione di insiemi uguali, dunque succ: $\omega \rightarrow \omega$ è iniettiva.

\square

§4.2 L'ordine di omega

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

Notazione 4.12 (Relazione di ordine su ω) — Dati $m, n \in \omega$, scriviamo:

$$m < n \stackrel{\text{def}}{=} m \in n^a$$

^aPer essere precisi non stiamo usando \in come una relazione (visto che abbiamo assunto all'inizio che fosse un simbolo del linguaggio della teoria degli insiemi), ma stiamo definendo $< \stackrel{\text{def}}{=} \{(m, n) \in \omega \times \omega \mid m \in n\}$. Inoltre se aggiungiamo la diagonale Δ_ω a $<$, otteniamo \leq (cioè $m \leq n \stackrel{\text{def}}{=} (m \in n) \vee (m = n)$), che, come visto, è legata alla corrispondente relazione d'ordine stretto, e godrà di tutte le stesse proprietà (come vedremo man mano).

Proposizione 4.13 (Ordinamento totale di ω)

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

Per dimostrare questa proposizione, sono comodi alcuni lemmi.

Osservazione 4.14 (Successore del secondo termine in un'appartenenza) — Si osserva che valgono le seguenti cose:

(1) $m \in n \rightarrow m \in s(n)$, infatti $n \subseteq n \cup \{n\} = s(n)$ (banalmente se m è contenuto in n allora è contenuto anche nel suo successore).

(2) $m \in s(n) \rightarrow (m \in n \vee m = n)$, cioè se m è nel successore di n , allora è n stesso o un suo elemento, infatti:

$$\begin{aligned} m \in s(n) = n \cup \{n\} &\iff m \in (n \cup \{n\}) \\ &\iff (m \in n) \vee (m \in \{n\}) \\ &\iff (m \in n) \vee (m = n) \end{aligned}$$

(nella seconda equivalenza si è usata la caratterizzazione data dell'appartenenza ad un'unione di insiemi, e nella terza il fatto che se m appartiene ad un singoletto, allora per **estensionalità** è proprio l'unico elemento del singoletto).

Lemma 4.15 (Successore del primo termine in un'appartenenza)

$\forall a, b \in \omega \ a \in b \rightarrow (s(a) \in b \vee s(a) = b)$.^a

^aMoralmente: se un numero è strettamente più piccolo di un altro, o il suo successore è a sua volta più piccolo del secondo numero, o coincide con quest'ultimo.

Dimostrazione. Procediamo per induzione su b .

caso $b = 0$ $a \in \emptyset \rightarrow \dots$ vera a vuoto, perché $a \in \emptyset$ è falsa (dunque l'implicazione è sempre vera, indipendentemente dal valore di verità dell'antecedente).

caso $b = s(n)$ L'ipotesi induttiva è $a \in n \rightarrow (s(a) \in n \vee s(a) = n)$. Dobbiamo dimostrare:

$$a \in s(n) \rightarrow (s(a) \in s(n) \vee s(a) = s(n))$$

abbiamo che $a \in s(n) \iff a \in n \cup \{n\} \iff a \in n \vee a = n$. Quindi abbiamo due casi:

$$\begin{aligned} a \in n &\stackrel{\text{Hp. indutt.}}{\implies} (s(a) \in n) \vee (s(a) = n) \stackrel{\text{def. } s(n)}{\iff} s(a) \in s(n) \\ a = n &\iff s(a) = s(n) \end{aligned}$$

(la seconda equivalenza è giustificata dal fatto che abbiamo dimostrato che la funzione successore in ω è iniettiva).

□

Possiamo ora dimostrare la proposizione iniziale.

Dimostrazione. Per verificare che $<$ è una relazione di ordine stretto totale, dobbiamo verificare che è irriflessiva, transitiva e totale (cioè presi qualsiasi due elementi di ω la loro coppia ordinata appartiene a $<$).

transitività Vogliamo verificare che $(a \in b \wedge b \in c) \rightarrow a \in c$. Procediamo per induzione su c :

caso $c = 0$ la premessa $b \in c$ è falsa, quindi l'implicazione è vera a vuoto (l'antecedente è sempre falso, quindi l'implicazione sempre vera).

caso $c = s(n)$ assumiamo per ipotesi induttiva $(a \in b \wedge b \in n) \rightarrow a \in n$, e vogliamo dimostrare:

$$(a \in b \wedge b \in s(n)) \rightarrow a \in s(n)$$

Osserviamo che $a \in b \implies a \in s(b)$, e che $b \in s(n) \stackrel{\text{Lemma}}{\implies} s(b) \in s(n) \vee s(b) = s(n)$, abbiamo quindi due casi in base a $s(b)$:

$$\begin{aligned} s(b) = s(n) &\implies a \in s(b) = s(n) \implies a \in s(n) \\ s(b) \in s(n) &\implies a \in s(b) \in s(n) \implies a \in s(n) \end{aligned}$$

questo usando il lemma precedente, potevamo anche scegliere di usare l'osservazione per dire che $b \in s(n) \implies b = n \vee b \in n$ e ottenere ancora i casi:

$$\begin{aligned} b = n &\implies a \in b = n \stackrel{\text{Oss.}}{\implies} a \in s(n) \\ b \in n &\implies a \in b \in n \implies a \in n \stackrel{\text{Oss.}}{\implies} a \in s(n) \end{aligned}$$

irriflessività Vogliamo verificare $\neg a \in a$, e lo facciamo per induzione su a :

caso $a = 0$ $\neg \emptyset \in \emptyset$, vero per definizione di \emptyset .

caso $a = s(n)$ L'ipotesi induttiva è $\neg n \in n$, e vogliamo verificare che $\neg s(n) \in s(n)$. Procediamo per assurdo, supponiamo che $s(n) \in s(n)$, e per l'osservazione abbiamo due casi:

$$\begin{aligned} s(n) = n &\implies n \in n \not\in \\ s(n) \in n &\implies n \in s(n) \in n \implies n \in n \not\in \end{aligned}$$

($n \in n$ è falso perché per ipotesi induttiva $\neg(n \in n)$ è vero).

totalità Vogliamo dimostrare che $\forall a, b \in \omega (a \in b) \vee (a = b) \vee (b \in a)$. Iniziamo per induzione su a :

caso $a = 0$ La tesi diventa $\forall b \in \omega (\emptyset \in b) \vee (\emptyset = b) \vee (b \in \emptyset)$ ³³. Procediamo quindi per induzione su b :

- * **caso $b = 0$** La tesi diventa $(\emptyset \in \emptyset) \vee (\emptyset = \emptyset)$, dove naturalmente la prima affermazione è sempre falsa, mentre la seconda è sempre vera, dunque la tesi è vera.
- * **caso $b = s(m)$** La tesi è $(\emptyset \in s(m)) \vee (\emptyset = s(m))$, con ipotesi induttiva $\overline{(\emptyset \in m) \vee (\emptyset = m)}$. Abbiamo quindi due casi in base all'ipotesi induttiva:

$$\begin{aligned} \emptyset \in m &\implies \emptyset \in s(m) \\ \emptyset = m &\implies \emptyset \in \{\emptyset\} = s(m) \end{aligned}$$

in entrambi casi è vera la tesi perché è sempre vero il primo termine.

caso $a = s(n)$ La tesi è $\forall b \in \omega (s(n) \in b) \vee (s(n) = b) \vee (b \in s(n))$, mentre l'ipotesi induttiva è $(n \in b) \vee (n = b) \vee (b \in n)$. Dall'ipotesi induttiva abbiamo quindi tre casi:

$$\begin{aligned} n \in b &\stackrel{\text{Lemma}}{\implies} s(n) \in b \vee s(n) = b \\ n = b &\stackrel{\text{Iniett. del succ.}}{\implies} s(n) = s(b) \implies b \in s(b) = s(n) \implies b \in s(n) \\ b \in n &\stackrel{\text{Oss.}}{\implies} b \in s(n) \implies b \in a \end{aligned}$$

³³Ovviamente quest'ultimo caso è sempre falso e quindi può essere escluso.

in tutti e tre i casi almeno una delle tre proposizioni della tesi è vera, dunque la tesi è sempre vera.

□

Osservazione 4.16 (\leq ordina totalmente ω) — Avendo dimostrato che $<$ è un ordine totale su ω , abbiamo dimostrato in automatico che anche $\leq = < \cup \Delta$ lo è, infatti, per la corrispondenza tra i due (come si è visto precedentemente in una proposizione), anche le definizioni di ordine totale sono corrispondenti (in particolare per \leq ci basta che valga una tra \leq e \geq , se valgono entrambe c'è l' $=$, mentre per $<$ chiedevamo nella definizione che valesse $<$, $>$ o $=$, quindi se nella dimostrazione precedente avessimo usato \leq al posto di $<$ avremmo ottenuto lo stesso risultato perché le richieste nella definizione di ordine totale sono le stesse).

Corollario 4.17 (Rappresentazione dei numeri naturali)

Un numero naturale è l'insieme dei numeri naturali minori di lui.

$$\forall m \in \omega \ m = \{n \in \omega \mid n < m\}$$

Dimostrazione. Vogliamo dire che $m = \{n \in \omega \mid n \in m\}$, ossia per definizione di sottoinsieme che $m \subseteq \omega$. Per induzione: $\emptyset \subseteq \omega$ è vera (perché ω è induttivo). Assumiamo che $m \subseteq \omega$, allora $s(m) = \underbrace{m}_{\subseteq \omega} \cup \{m\}$ e $\{m\} \subseteq \omega$ perché $m \in \omega$ per ipotesi iniziale, quindi si conclude che $s(m) \subseteq \omega$. □

Corollario 4.18 (Più piccolo = contenuto)

$$\forall m, n \in \omega (m \leq n \leftrightarrow m \subseteq n).$$

^aNaturalmente il lemma vale anche con $<$ e \subsetneq .

Dimostrazione. Siccome ω è totalmente ordinato, si danno due casi (nel primo dimostro \rightarrow , nel secondo dimostro che la negazione della premessa implica la negazione della conseguenza, che è equivalente [via contronominale] a \leftarrow):

$$\begin{aligned} m \leq n &\implies \forall x \in \omega (x < m \rightarrow x < n) \stackrel{\text{def. } <}{\implies} \forall x \in \omega (x \in m \rightarrow x \in n) \stackrel{\text{def. } \subseteq}{\implies} m \subseteq n \\ n < m &\implies n \in m \text{ tuttavia } n \notin n \text{ quindi non può essere che } m \subseteq n \text{ ovvero } m \not\subseteq n \end{aligned}$$

($n \notin n$ perché abbiamo dimostrato che $<$ è di ordine stretto su ω , quindi irriflessiva, inoltre, nella dimostrazione del primo caso, si osserva che nel secondo passaggio è indifferente usare $<$ o \leq nell'enunciato e dimostrazione del corollario³⁴). □

³⁴Mamino li mischia, ma valgono entrambi gli enunciati e le dimostrazioni.

§4.3 Induzione forte e principio del minimo

Teorema 4.19 (Principio di induzione - forma forte)

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

$$(\forall n \in \omega (\forall x < n \Phi(x)) \rightarrow \Phi(n)) \rightarrow \forall n \in \omega \Phi(n)$$

ovvero, se assumendo $\Phi(x)$ per tutti gli $x < n$, abbiamo $\Phi(n)$, allora $\Phi(n)$ è vera per tutti i numeri n .

Osservazione 4.20 — Chiaramente questa forma è “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 .

Dimostrazione. Definiamo $\psi(m) \stackrel{\text{def}}{=} \forall x < m \Phi(x)$ e dimostriamo per induzione debole che $\forall m \in \omega \psi(m)$, cioè che per ogni fissato naturale Φ è vera per i naturali più piccoli, in tal modo, per ogni $n \in \omega$ sappiamo che è vera $\psi(n+1) \implies \Phi(n)$, che è proprio la tesi.

$m = 0$ Abbiamo che $\psi(0) = \forall x < 0 \Phi(x) \equiv \forall x (x < 0 \rightarrow \Phi(x))$, che è vera a vuoto in quanto $x < 0 \equiv x \in \emptyset$ che è sempre falso, dunque l’implicazione tra parentesi è sempre vera.

$m \implies m + 1$ Assumiamo che $\psi(m) = \forall x < m \Phi(x)$ sia vera e mostriamo che $\psi(m+1) = \forall x < m+1 \Phi(x)$ è vera. Per un lemma visto $x < s(m) \implies x < m \vee x = m$, nel primo caso $\Phi(x)$ è vera per ipotesi induttiva. Nel caso di $\Phi(m)$, abbiamo per ipotesi che $\forall n \in \omega (\forall x < n \Phi(x)) \rightarrow \Phi(n)$, dunque, per $n = m$, abbiamo visto nel primo caso che $\forall x < m \Phi(m)$, per cui l’ipotesi (vera) ha antecedente vero, che ci dà necessariamente conseguente $\Phi(m)$ vero.

□

Teorema 4.21 (Principio del minimo)

Sia $A \subseteq \omega$. Se $A \neq \emptyset$ allora esiste $n \in A$ tale che $\forall x \in A n \leq x$. Ovvero, ogni sottoinsieme non vuoto di ω ha un minimo elemento.

Possibile idea di dimostrazione: dimostriamo per induzione forte che se $n \in A$ - che è equivalente a $A \subseteq \omega \wedge A \neq \emptyset$ -, allora A ha un minimo. Per ipotesi induttiva assumiamo che $\forall x < n x \in A \rightarrow A$ ha minimo, e dimostriamo che se $n \in A$, allora A ha minimo. Dato $n \in A$, se esiste $x \in n$ tale che $x \in A$, allora A ha minimo per ipotesi induttiva, altrimenti, se $\forall x < n x \notin A$, allora n è il minimo di A .

Dimostrazione. Dimostriamo la contronominale della tesi, ovvero se $A \subseteq \omega$ non ha un elemento minimo, allora A è vuoto, cioè $\forall n \in \omega n \notin A$. Procediamo per induzione forte, assumendo per ipotesi induttiva che $\forall x < n x \notin A$, mostriamo che $n \notin A$. Più precisamente vogliamo dimostrare che $(\forall x < n x \notin A) \rightarrow n \notin A$, ma ciò è equivalente al fatto che A non abbia un minimo:

$$\begin{aligned} (\forall x < n x \notin A) \rightarrow n \notin A &\iff \neg(\exists x < n x \in A) \rightarrow n \notin A \\ &\iff n \in A \rightarrow \exists x < n x \in A && \text{(contronominale)} \\ &\iff A \text{ non ha minimo} \end{aligned}$$

abbiamo quindi dimostrato che l'implicazione che vogliamo dimostrare è equivalente all'ipotesi per cui è vera, inoltre per l'ipotesi induttiva l'antecedente dell'implicazione è vero, per cui, dalla tavola di verità, l'unica possibilità è che anche il conseguente $n \notin A$ sia vero. Ciò verifica il passo induttivo e quindi l'induzione forte ci garantisce la contronominale della tesi - che naturalmente è equivalente a quest'ultima -. \square

Osservazione 4.22 — Per completare l'equivalenza tra induzione, induzione forte e principio del minimo, andrebbe dimostrato anche che principio del minimo \Rightarrow induzione.

Definizione 4.23 (Insieme ben ordinato). Un insieme totalmente ordinato $(S, <)$ si dice **bene ordinato** se ogni sottoinsieme non vuoto ha un minimo.³⁵

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

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 4.24

$(\omega, <)$ è un insieme bene ordinato^a per quanto visto nel teorema precedente.

^aSi usa la notazione di coppia ordinata per indicare sia l'insieme sia la relazione che c'è sopra.

Esercizio 4.25. Dimostra che $X = s(s(s(\omega)))$ è bene ordinato dalla relazione $a < b \stackrel{\text{def}}{=} a \in b$.

Soluzione. Dato $(\omega, <)$, basta considerare la seguente relazione:

$$\prec := < \cup (\omega \times \{\omega\}) \cup (s(\omega) \times \{s(\omega)\}) \cup (s(s(\omega)) \times \{s(s(\omega))\})^{\text{36}}$$

dove $(x, y) \in \prec \leftrightarrow x \in y$. Si vede quindi che $(s(s(s(\omega))), \prec)$ è un ordine totale (fondamentalmente perché $<$ lo è, e le coppie che abbiamo aggiunto sono costruite apposta per rispettare la definizione di ordine [stretto] totale). Abbiamo costruito \prec in modo che $\forall n \in \omega \ n \prec \omega$, inoltre vale anche [per costruzione] che $\omega \prec s(\omega) \prec s(s(\omega))$, dunque, dato $S \subseteq s(s(s(\omega)))$, se $S \cap \omega \neq \emptyset$, allora il minimo esiste ed è dato da $\min_{\prec}(S \cap \omega)$. Se $S \cap \omega = \emptyset$ (ovvero se S è un sottoinsieme di $\{\omega, s(\omega), s(s(\omega))\}$), allora per definizione di \prec (come scritto sopra), per tutti i sottoinsiemi possibili abbiamo sempre un minimo [per la totalità di \prec]. Pertanto $\forall S \subseteq s(s(s(\omega)))$ c'è un minimo e quindi in $s(s(s(\omega)))$ vale il principio del minimo, cioè è ben ordinato. \square

§4.4 Ricorsione numerabile

La ricorsione è il procedimento per cui si costruisce una funzione $f : \omega \rightarrow$ qualcosa, 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 pensare gli infidi puntini (...). Vediamo qualche esempio.

³⁵Cioè se vale il principio del minimo c(ome vale in ω).

³⁶Che formalmente è un sottoinsieme di $s(s(s(\omega))) \times s(s(s(\omega)))$.

Esempio 4.26 (Operazioni aritmetiche)

Possiamo definire somma e prodotto come:

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

anziché $a + b = \underbrace{s(s(\dots a \dots))}_{b \text{ successori}}$ (abbiamo il caso base con 0, e poi si procede ricorsivamente dal caso base fino a b) e $a \cdot b = \underbrace{a + a + \dots + a}_{b \text{ volte}}$ (ricorsivamente ad un certo punto si partirà da a e si inizierà a sommare).

Esempio 4.27 (Potenza e fattoriale)

Possiamo definire ricorsivamente potenze e fattoriali come segue:

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

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

Esempio 4.28 (Sommatoria)

Possiamo definire la sommatoria come:

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

anziché $\sum_{i=0}^a f(i) = f(0) + f(1) + \dots + f(a)$ (cioè con la sommatoria definita ricorsivamente stiamo eliminando il fastidioso discorso (poco formale) dei puntini \dots).

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

Esempio 4.29 (Esempio di applicazione della ricorsione)

In quanti modi posso coprire una sequenza di n caselle $\underbrace{\square \square \square \dots \square \square}_n$ con tessere di una o due caselle, \square e $\square \square$, che non si sovrappongano e non lascino caselle scoperte?

Soluzione. Detto F_n il numero di ricoprimenti di una sequenza lunga n , vediamo che la tessera più a sinistra può essere \square o $\square \square$. Nel primo caso, ci sono F_{n-1} modi di completare

il ricoprimento, nel secondo caso F_{n-2} . Abbiamo quindi trovato una relazione ricorsiva del numero di ricoprimeti in funzione di n :

$$F_n = F_{n-1} + F_{n-2}^{37}$$

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

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 sapere $f(n)$. 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 della ricorsione.

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

Osservazione 4.30 (Estensionalità per funzioni) — Date $f, g : A \rightarrow B$, allora:

$$f = g \leftrightarrow \forall x \in A \ f(x) = g(x)$$

(dove l'uguaglianza di funzioni non è altro che uguaglianza di sottoinsiemi in $A \times B$).

Dimostrazione. Si osserva che:

$$(x, y) \in f \stackrel{\text{def. } f}{\iff} y = f(x) \stackrel{\text{Hyp.}}{\iff} y = g(x) \stackrel{\text{def. } g}{\iff} (x, y) \in g$$

e si conclude per **estensionalità** che quanto scritto sopra equivale a dire che gli insiemi f e g sono uguali. \square

Notazione 4.31 (Insieme delle funzioni da A a B) — Indichiamo con ${}^A B$ l'insieme delle funzioni da A a B , che esiste per **separazione** in $\mathcal{P}(A \times B)$.

Teorema 4.32 (Ricorsione numerabile - prima forma)

Dato un insieme A , un elemento $k \in A$ e una funzione:

$$h : \omega \times A \rightarrow A$$

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

$$f(0) = k \quad \wedge \quad \forall n \in \omega \ f(s(n)) = h(n, f(n))$$

Esempio 4.33 (Potenza e fattoriale con la ricorsione numerabile)

Per definire a^b considero $k = 1$, $h(n, x) = a \cdot x$, e $h(0, x) = k = 1$. Per definire il fattoriale $k = 1$, $h(n, x) = s(n) \cdot x$ e $h(0, x) = k = 1$.

³⁷Cioè il numero totale di modi di ricoprire la sequenza di n caselle deriva dalla somma dei due casi, che rappresentano i modi di ricoprire le altre caselle fissata quella/e iniziale/i, ciò fissati i casi base ci definisce bene (via ricorsione numerabile) una successione che conta il numero di ricoprimeti in funzione di n .

Esercizio 4.34. Come potrei costruire F_n usando questo teorema?

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 $\omega \times A$ (in tal modo f è una funzione da ω ad A) usando la formula Φ . Dire “ $y = f(x)$ ” vuol dire “i primi x passaggi della ricorsione, partendo da k , conducono a y ”.

Dimostrazione. Dato $x \in \omega$ diciamo che g è una **x -approssimazione** - per la h fissata nell’ipotesi - se la vale:

$$g \text{ } x\text{-approssimazione} \stackrel{\text{def}}{=} \begin{cases} g \in {}^{s(x)}A \\ g(0) = k \\ \forall n \in x \ g(s(n)) = h(n, g(n)) \end{cases}$$

di fatto g è la ricorsione che stiamo cercando di definire, date le ipotesi, fatta un numero finito di passi - $x \in \omega$ -. Iniziamo a dimostrare quindi che questa ricorsione finita esiste per ogni numero finito di iterazioni $x \in \omega$ fissato.

Il vantaggio di tagliuzzare f in x -approssimazioni è che così otteniamo un parametro, x , su cui impostare un’induzione.

Lemma 4.35 (Esistenza e unicità delle x -approssimazioni in ω)

$\forall x \in \omega$, fissata h come nelle ipotesi del teorema di ricorsione, $\exists! g$ “ g è una x -approssimazione per h ”.

Dimostrazione. Fissato $x \in \omega$, possiamo procedere per induzione - di fatto sul numero di iterazioni della ricorsione - .

$x = 0$ Basta osservare che l’unica 0-approssimazione è la funzione $\{(0, k)\}$. Infatti il dominio è $\{0\}$ per definizione, $g(0) = k$, e vale a vuoto la terza condizione, l’unicità è banale, pertanto l’unica 0-approssimazione possibile per h è proprio la funzione $g = \{(0, k)\}$.

$x = s(a)$ Per ipotesi induttiva abbiamo che esiste ed è unica una a -approssimazione per h , diciamo g , vogliamo dimostrare che esiste ed è unica una $s(a)$ -approssimazione per h . Per ipotesi $g \in {}^{s(a)}A$, $g(0) = k$ e $\forall b \in a \ g(s(b)) = h(b, g(b))$, possiamo quindi estendere g a $s(a)$ come segue:

$$g' = g \cup \{(s(a), h(a, g(a)))\}$$

A questo punto è immediato verificare che g' è una $s(a)$ -approssimazione, infatti, $\text{Dom}(g') = \text{Dom}(g) \cup \{s(a)\} = s(a) \cup \{s(a)\} = s(s(a))$, $g'(0) = g(0) = k$ e $\forall t \in a \ g'(s(t)) = g(s(t)) = h(t, g(t))$, e per costruzione, $g'(s(a)) = h(a, g(a))$. Per l’unicità, sappiamo per ipotesi induttiva che esiste un’unica a -approssimazione per h , quindi, date g' e g'' due $s(a)$ -approssimazioni per h , si ha necessariamente che $g'_{|s(a)} = g''_{|s(a)}$, e in particolare ciò significa che $g'(a) = g''(a)$, da cui:

$$g'(s(a)) \stackrel{\text{def.}}{=} h(a, g'(a)) \stackrel{\text{H.p. indutt.}}{=} h(a, g''(a)) \stackrel{\text{def.}}{=} g''(s(a))$$

□

Il lemma appena dimostrato ci garantisce esistenza e unicità di funzioni ricorsive finite - di lunghezza arbitraria fissata - che rispettano le stesse proprietà di f nella tesi (ad eccezione del dominio naturalmente), vogliamo ora far vedere che esiste una funzione con tali proprietà con dominio tutto ω . Introduciamo la formula Φ :

$$\Phi(x, y) \stackrel{\text{def}}{=} \exists g \in {}^{s(x)}A \text{ ``tale che } g \text{ è una } x\text{-approssimazione''} \wedge g(x) = y$$

Per l'unicità delle x -approssimazioni possiamo scrivere $\forall x \in \omega \exists! y \Phi(x, y)$. Possiamo quindi finalmente definire f per separazione in $\omega \times A$:

$$f := \{(x, y) \in \omega \times A \mid \Phi(x, y)\}^{38}$$

L'unicità di y osservata prima ci garantisce che f è una funzione, occorre dunque verificare che soddisfi le proprietà richieste nella tesi.

$f(0) = k$ Abbiamo visto che esiste un'unica 0-approssimazione, $g = \{(0, k)\}$, e per definizione di f , abbiamo proprio che $f(0) = g(0) = k$.

$f(s(n)) = h(n, f(n))$ Segue per costruzione di f che $f(s(n)) = g(s(n))$, con $g \in {}^{s(s(n))}A$ che è una $s(n)$ -approssimazione, pertanto, $g(s(n)) = h(n, g(n))$, ora $g(n) = g|_{s(n)}(n)$ è una (l'unica) n -approssimazione per h (lo si verifica facilmente), per cui, per definizione di f , $f(n) = g(n)$ e rimettendo tutto assieme si ottiene:

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

Ciò dimostra che una f ottenuta per separazione soddisfa la tesi del teorema di ricorsione numerabile. L'unicità di f segue facilmente per induzione, Date f' e f'' che soddisfano la ricorsione abbiamo:

$$f'(0) = k = f''(0) \quad f'(s(n)) = h(n, f'(n)) \stackrel{\text{Hyp. indutt.}}{=} h(n, f''(n)) = f''(s(n))$$

e per estensionalità di funzioni si conclude che $f' = f''$. \square

Procedendo come negli esempi all'inizio di questa sezione, il [teorema di ricorsione numerabile](#) ci consente di costruire le operazioni aritmetiche, le potenze, etc. A titolo di esempio, vediamo nel dettaglio, il caso della somma.

Esempio 4.36 (Costruzione di $+ : \omega \times \omega \rightarrow \omega$)

Vogliamo formalizzare la definizione:

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

Per il [teorema di ricorsione numerabile](#) sappiamo che, per ogni $a \in \omega$ fissato, esiste un'unica $f : \omega \rightarrow \omega$ tale che:

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

Scriviamo quindi:

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

³⁸Di fatto stiamo costruendo f con le ricorsioni finite - cioè f manda x nell'unico y raggiungibile iterando la ricorsione x volte, in altre parole è la successione delle ricorsioni troncate -, che però ora sappiamo ci sono e sono uniche qualsiasi sia la lunghezza - quindi per infiniti valori di $x \in \omega$ -.

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.

Teorema 4.37 (Unicità dei numeri naturali)

Supponiamo che $(\mathbb{N}, 0, \text{succ})$ soddisfi gli assiomi di Peano, allora $(\mathbb{N}, 0, \text{succ})$ e (ω, \emptyset, s) sono strutture isomorfe - **ossia, formalmente, esiste:** $f : \omega \rightarrow \mathbb{N}$ **bigettiva** tale che:^a

- (i) $f(\emptyset) = 0$.
- (ii) $\forall n \in \omega f(s(n)) = \text{succ}(f(n))$.

^aCioè gli assiomi di Peano hanno un unico modello a meno di isomorfismo di strutture.

Fa comodo isolare la seguente osservazione.

Osservazione 4.38 (Ogni numero in $\omega \setminus \emptyset$ è successore) — $\forall x \in \omega x \neq 0 \rightarrow \exists y \in \omega x = s(y)$, ovvero ogni numero diverso da 0 è il successore di qualcos'altro.

Dimostrazione. Induzione su x . Il caso $x = 0$ è vero a vuoto (essendo la premessa sempre automaticamente falsa). Nel caso $x = s(m)$ basta prendere $y = m$ e si ha $x = s(y)$. \square

Dimostrazione. Per il **teorema di ricorsione** (stiamo prendendo $A = \mathbb{N}$, e $k = 0$ e $h = \text{succ}$) c'è un'unica f che soddisfa le condizioni $f(\emptyset) = 0$ e $\forall n \in \omega f(s(n)) = \text{succ}(f(n))$. Resta da constatare che f è bigettiva.

Surgettività Per ipotesi $(\mathbb{N}, 0, \text{succ})$ soddisfa gli assiomi di Peano, per cui vale il principio di induzione. Dimostriamo quindi per induzione in $(\mathbb{N}, 0, \text{succ})$ la surgettività di f .

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

$y = \text{succ}(n)$ Per ipotesi induttiva esiste $x \in \omega$ tale che $f(x) = n$, da cui si ottiene, per definizione di f che $f(s(x)) = \text{succ}(n)$.

Iniettività Per assurdo supponiamo ci sia un elemento in ω con la stessa immagine di un altro. Sia $x := \min\{n \in \omega \mid \exists y \in \omega f(n) = f(y)\}$, dunque, per minimalità di x , esiste $y \in \omega$ con $y > x$, tale per cui $f(x) = f(y)$. Poiché $y > x$ si ha che $y > 0$, per cui $y = s(y')$ per qualche $y' \in \omega$, distinguiamo quindi due casi.

$x = 0$ In tal caso si deve avere che:

$$\text{succ}(f(y')) \stackrel{\text{def. } f}{=} f(s(y')) \stackrel{y=s(y')}{=} f(y) \stackrel{\text{Hp. assurda}}{=} f(x) \stackrel{\text{def. } f}{=} 0$$

per cui 0 è successore di qualcosa in \mathbb{N} , che è contro gli assiomi di Peano.

$x \neq 0$ Per l'osservazione possiamo scrivere $x = s(x')$, da cui:

$$\text{succ}(f(x')) \stackrel{\text{def. } f}{=} f(s(x')) = f(x) \stackrel{\text{Hp. assurda}}{=} f(y) = f(s(y')) \stackrel{\text{def. } f}{=} \text{succ}(f(y'))$$

e dagli assiomi di Peano in \mathbb{N} , per l'iniettività del successore, si ha $f(x') = f(y')$, con $x' < x$, per cui contro la minimalità di x . \square

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, perché F_n non dispense 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 $n \mapsto (F_n, F_{n+1})$ da ω a $\omega \times \omega$. È comodo, però, disporre di una versione più versatile del teorema di ricorsione numerabile.

Teorema 4.39 (Ricorsione numerabile - seconda forma)

Dato un insieme A , denotiamo con A^* il sottoinsieme delle funzioni con dominio un naturale, $A^* = \bigcup_{n \in \omega} {}^n A$. Sia $h : A^* \rightarrow A$, allora esiste un'unica funzione $f : \omega \rightarrow A$ tale che:

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

^aIn altre parole $f(n)$ può dipendere in maniera arbitraria dai valori assunti da f su n , dove tale arbitrarietà è stabilità da h , la quale valuta una funzione, definita su un dominio finito, su alcuni suoi fissati - in funzione di n - valori.

L'idea è di definire, mediante la prima forma del teorema di ricorsione, la successione della troncata di f , ossia la funzione $f' : n \mapsto f|_n$, e da questa definire poi la f voluta - un modo alternativo, sarebbe ripetere la dimostrazione della prima forma -.

Dimostrazione. Definiamo per **ricorsione numerabile v.1** la successione delle ricorsioni date da h troncate al valore n - cioè $f'(s(n))$ è la funzione che fa la ricorsione determinata da h fino ad n -:

$$f' : \omega \rightarrow A^* : \begin{cases} f'(0) = 0 \\ f'(s(n)) = f'(n) \cup \{(n, h(f'(n)))\} \end{cases}$$

che appunto esiste ed è unica per il teorema di ricorsione numerabile ed è la successione delle (funzioni) troncate della funzione che vogliamo costruire.

Definiamo ora $f(n) := (f'(s(n)))(n) = h(f'(n))$ - cioè f calcolata al valore n -esimo è data dal valore della $n+1$ -esima troncata della ricorsione determinata da h , calcolata in n -, in tal modo abbiamo che $f : \omega \rightarrow A$ esiste ed è unica (come conseguenza dell'esistenza e dell'unicità di f'), pertanto non ci resta altro che verificare per induzione che effettivamente f' sia la successione della troncata di f , cioè $\forall n \in \omega \ f|_n = f'(n) \in A^*$ - in tal modo $h(f'(n)) = h(f|_n)$ -.

$n = 0$ In tal caso si vede subito che $f|_0 = \emptyset$, infatti qualsiasi funzione ristretta al vuoto dà il vuoto, d'altra parte, per costruzione, si ha anche che $f'(0) = 0$.

$n = s(m)$ Per ipotesi induttiva $f|_m = f'(m)$, vogliamo verificare che $f|_{s(m)} = f'(s(m))$:

$$\begin{aligned} f|_{s(m)} &= f|_m \cup \{(m, f(m))\} && (\text{def. funzione}) \\ &= f'(m) \cup \{(m, f'(s(m))(m))\} && (\text{Hyp. indutt. + def. } f) \\ &= f'(m) \cup \{(m, h(f'(m)))\} = f'(s(m)) && (\text{def. } f') \end{aligned}$$

Infine, quindi, $f(n) \stackrel{\text{def. } f}{=} f'(s(n))(n) \stackrel{\text{def. } f'}{=} h(f'(n)) \stackrel{\text{appena visto}}{=} h(f|_n)$. \square

Esempio 4.40 (Esempio di applicazione)

Per costruire la successione di Fibonacci, definiamo $h(g)$ in questo modo. Sia $n = \text{Dom}(g)$. 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 $h(g) = g(n - 1) + g(n - 2)$ ^a.

^aAbbiamo quindi ottenuto h come funzione di funzioni con dominio in ω e in particolare più piccolo di n , dunque per il teorema tale h definisce univocamente $f(n)$, a partire da $f|_n \in A^*$.

Abbiamo ora 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 4.41. Dimostra commutatività, associatività, etc. di $+$ e \cdot .

§5 Cardinalità

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

Definizione 5.1 (Equipotenza/Cardinalità). Dati due insiemi A e B :

$$|A| = |B| \stackrel{\text{def}}{=} \exists f \in {}^A B \text{ "f è bigettiva } A \rightarrow B\text{"}$$

diciamo anche che “ A ha la stessa **cardinalità** di B ” o che “ A e B sono **equipotenti**”. Poniamo inoltre:

$$|A| \leq |B| \stackrel{\text{def}}{=} \exists B' \subseteq B \ |A| = |B'|$$

ossia $\exists f \in {}^A B$ “ f è iniettiva” (la definizione ci dice proprio che esiste un sottoinsieme di B che è in biuzione con A , e per definizione di iniettività, si ha proprio che $A \hookrightarrow B$)³⁹.

Nota 5.2 (Sulla notazione per le cardinalità) — Osserviamo che:

- La scrittura $|A| = |B|$ suggerisce che esistono insiemi - o oggetti di qualche genere - denotati $|A|$ e $|B|$ di cui si predica l'uguaglianza. Effettivamente costruiamo questi oggetti, ma, per ora, la scrittura $|A| = |B|$ è inscindibile, come ♣ $[A, B]$ (nel senso che per ora è solo un'abbreviazione per dire biuzione, pertanto non possiamo separare quei simboli o farci qualcosa).
- 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 $B = \omega$, infatti $A \subsetneq B$, ma $|A| = |B|$.

Osservazione 5.3 (Proprietà formali di una relazione di equivalenza) — La relazione $|\cdot| = |\cdot|$ soddisfa le proprietà formali di una relazione di equivalenza (ma per ora NON lo è^a):

- **riflessività:** $|A| = |A|$.
- **simmetria:** $|A| = |B| \rightarrow |B| = |A|$.
- **transitività:** $|A| = |B| \wedge |B| = |C| \rightarrow |A| = |C|$.

^aPotrebbe tuttavia essere pensata come una relazione di equivalenza su V (la classe di tutti gli insiemi).

Esercizio 5.4. Dimostrare l'osservazione.

Soluzione. Per la riflessività basta osservare che id_A è una biuzione da A in A . Per la simmetria, abbiamo visto che se $f : A \rightarrow B$ è iniettiva, allora ammette inversa $g : \text{Im}(f) \rightarrow A$ a sua volta iniettiva (e surgettiva poiché ha necessariamente come immagine tutto A), inoltre, essendo f bigettiva si ha che $\text{Im}(f) = B$, quindi $g : B \rightarrow A$, e per quanto detto è bigettiva, dunque nel linguaggio della cardinalità $|B| = |A|$.

Infine, $|A| = |B| \iff \exists f : A \rightarrow B$ bigettiva, $|B| = |C| \iff \exists g : B \rightarrow C$ bigettiva, ora

³⁹Tale relazione sarà anche una relazione di ordine tra cardinalità quando queste ultime saranno singoli oggetti della teoria.

è sufficiente osservare che $g \circ f : A \rightarrow C$ è bigettiva in quanto composizione di funzioni biggettive⁴⁰, per avere $|A| = |C|$. \square

Osservazione 5.5 (Proprietà formali [parziali] di una relazione di ordine [largo]) — La relazione $|\cdot| \leq |\cdot|$ soddisfa^a:

- **riflessività:** $|A| \leq |A|$.
- **transitività:** $|A| \leq |B| \wedge |B| \leq |C| \rightarrow |A| \leq |C|$.

^aTali proprietà, unite al teorema di Cantor-Bernstein, che stiamo per vedere, ci danno una relazione di ordine totale su V .

Esercizio 5.6. Dimostrare l'osservazione.

Soluzione. Per la riflessività basta osservare che id_A è in particolare una mappa iniettiva (oppure che A è un sottoinsieme [improprio] di se stesso e quindi l'identità è la bigezione richiesta dalla definizione). Per la transitività $|A| \leq |B| \iff \exists A \hookrightarrow B$, $|B| \leq |C| \iff \exists g : B \hookrightarrow C$, e osservando che la composizione di funzioni iniettive è iniettiva, si ha che $g \circ f : A \rightarrow C$ è iniettiva $\iff |A| \leq |C|$. \square

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

§5.1 Teorema di Cantor-Bernstein

Teorema 5.7 (Cantor-Bernstein)

Se c'è una funzione iniettiva $A \rightarrow B$ e una funzione iniettiva $B \rightarrow A$, allora esiste una bigezione fra A e B .

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

Dimostrazione. Per ipotesi abbiamo quindi $f : A \rightarrow B$ e $g : B \rightarrow A$ iniettive. Il nostro obiettivo è costruire una nuova funzione $h : A \rightarrow B$ bigettiva.

L'idea è che ogni elemento, poniamo, di A , è una tappa di un percorso:

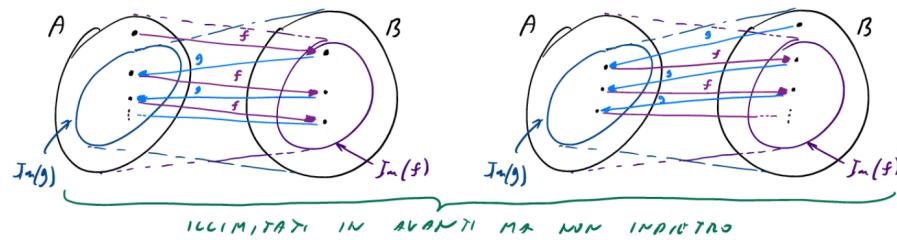
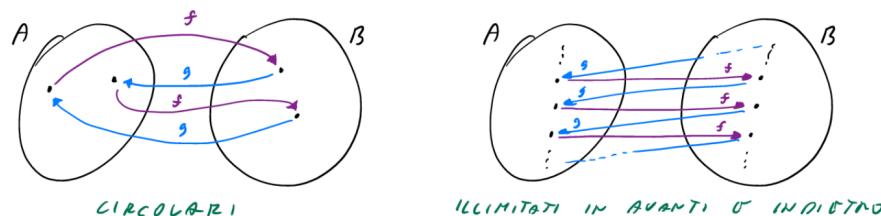
$$a \xrightarrow{f} f(a) \xrightarrow{g} g(f(a)) \xrightarrow{f} f(g(f(a))) \xrightarrow{g} \dots$$

Siccome f e g sono iniettive, questo percorso ha altresì un'unica estensione all'indietro - sappiamo che se le funzioni sono iniettive, allora ammettono un'inversa iniettiva (e surgettiva verso l'insieme di partenza), dunque possiamo sempre tornare indietro in modo unico, estendendo quindi il nostro percorso anche nell'altra direzione:

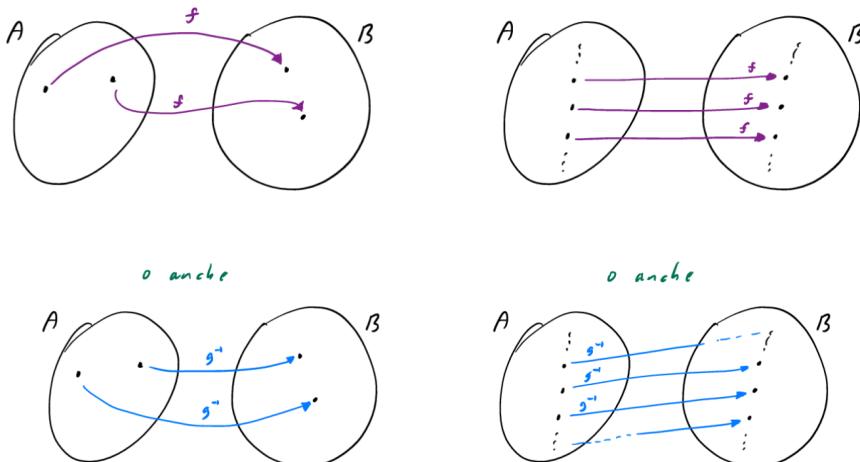
$$\dots \xrightarrow{g} f^{-1}(g^{-1}(a)) \xrightarrow{f} g^{-1}(a) \xrightarrow{g} a \xrightarrow{f} f(a) \xrightarrow{g} g(f(a)) \xrightarrow{f} f(g(f(a))) \xrightarrow{g} \dots$$

a patto che $a \in \text{Im}(g)$ (poiché $g^{-1} : A \supseteq \text{Im}(g) \rightarrow B$ - ed è bigettiva), $g^{-1}(a) \in \text{Im}(f)$, etc. Quando, e se, non possiamo più applicare la funzione inversa, il percorso (all'indietro) si interrompe. Con questa catena di composizioni osserviamo che ci sono quindi solo tre tipi di percorsi possibili:

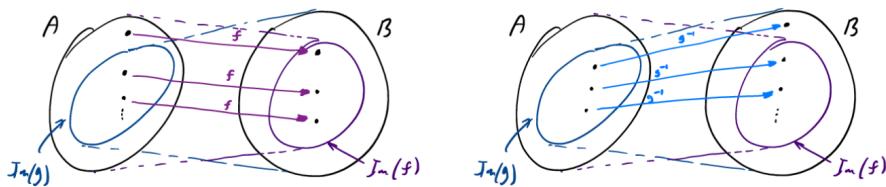
⁴⁰È una semplice verifica.



Per gli elementi che si trovano su un percorso circolare, o su un percorso illimitato avanti e indietro, f fornisce una bigezione, come la fornirebbe anche g^{-1} - la scelta è arbitraria a patto di usare la medesima funzione per l'intero percorso - nel modo seguente⁴¹:



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



⁴¹Informalmente, se siamo in uno dei due casi, allora f è per forza una mappa bigettiva, perché è iniettiva e “prende” tutti gli elementi in arrivo, idem g^{-1} .

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

Formalmente, definiamo per **ricorsione** (prima forma) le seguenti successioni di sottoinsiemi di B e A rispettivamente - ossia, tecnicamente, la funzione $\omega \rightarrow \mathcal{P}(B) \times \mathcal{P}(A) : i \mapsto (B_i, A_i)$, con:

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

Definiamo quindi:

$$B_* = \bigcup_{i \in \omega} B_i \stackrel{\text{def}}{=} \bigcup \{B_i \mid i \in \omega\} \quad A_* = \bigcup_{i \in \omega} A_i$$

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

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

queste mappe coprono tutti i casi possibili, infatti, i percorsi ciclici e illimitati da entrambe le parti sono coperti da $k = f^{-1}$ ed $h = g^{-1}$, mentre nel caso di percorsi che partono da B e sono limitati a sinistra [all'indietro], ovvero con primo elemento in B^* abbiamo che $k(y) = g(y)$, invece nel caso simmetrico, in cui si parte da A con percorso limitato a sinistra (quindi $x \notin A_*$) si ha $h(x) = f(x)$, in tal modo prendiamo tutti gli elementi di entrambi gli insiemi, ed essendo che f e g sono iniettive, per ipotesi, non rischiamo sovrapposizioni ed otteniamo proprio delle bigezioni.

Ci basta quindi dimostrare che h e k sono ben definite, $k \circ h = \text{id}_A$ e $h \circ k = \text{id}_B$, in tal modo avremo la nostra bigezione (e la sua inversa).

h e k 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 $x \in g[B_i] \subseteq \text{Im}(g)$. Nella definizione di k , se $y \notin B_*$, in particolare, $y \notin B_0$, per cui $y \in \text{Im}(f)$.

$k \circ h = \text{id}_A$ 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 $k(h(y)) = k(g^{-1}(x)) = k(y) = g(y) = x$ (abbiamo usato che $y = g^{-1}(x) \in B_*$ per quanto supposto sopra).

Per il caso $x \notin A_*$, osserviamo, intanto, che $x \notin A_* \implies f(x) \notin B_*$. Infatti, se $f(x) \in B_i$, con $i \in \omega$, allora $i \neq 0$, perché $B_0 = B \setminus \text{Im}(f)$, quindi possiamo scrivere $i = s(j)$, e $f(x) \in B_{s(j)} = f[A_j]$. Per l'iniettività di f , abbiamo allora $x \in A_j \not\subseteq A_*$.

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

$h \circ k = \text{id}_B$ 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, perché $f^{-1}(y) \in A_i \rightarrow y = f(f^{-1}(y)) \in A_{s(i)}$. 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.

Definizione 5.8 (Ordinamento stretto fra cardinalità). Dati due insiemi A e B definiamo:

$$|A| < |B| \stackrel{\text{def}}{=} |A| \leq |B| \wedge |A| \neq |B|^{42}$$

⁴²Dove ricordiamo che $|A| \neq |B| \stackrel{\text{def}}{=} \neg(|A| = |B|)$.

§5.2 Teorema di Cantor

Teorema 5.9 (Cantor)

Dato un qualunque insieme A vale:

$$|A| < |\mathcal{P}(A)|$$

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

Dimostrazione. La disegualanza $|A| \leq |\mathcal{P}(A)|$ è facile: basta considerare la funzione iniettiva:

$$A \rightarrow \mathcal{P}(A) : x \mapsto \{x\}$$

(che è iniettiva per [estensionalità](#)). Consideriamo, ora, una qualunque funzione $f : A \rightarrow \mathcal{P}(A)$ iniettiva. Dobbiamo dimostrare che $\text{Im}(f) \subsetneq \mathcal{P}(A)$ (cioè che non è surgettiva). Consideriamo:

$$B = \{x \in A \mid x \notin f(x)\}^{43}$$

Ora $B \subseteq A$, supponendo per assurdo che f sia bigettiva, ovvero che $B = f(a)$ per qualche $a \in A$, avremmo:

$$a \in f(a) \subseteq A \iff a \in B \iff a \notin f(a) \downarrow$$

□

§5.3 Operazioni fra cardinalità

Definizione 5.10 (Somma, prodotto e potenze di cardinalità). Dati A e B possiamo definire somma, prodotto e potenze di cardinalità come segue:

$$\begin{aligned} |A| + |B| &\stackrel{\text{def}}{=} |A \sqcup B| \stackrel{\text{def}}{=} |(A \times \{0\}) \cup (B \times \{1\})| \\ |A| \cdot |B| &\stackrel{\text{def}}{=} |A \times B| \\ |A|^{|B|} &\stackrel{\text{def}}{=} |^B A| \end{aligned}$$

(nella definizione di unione disgiunta abbiamo fatto il prodotto per cose diverse, in modo che gli elementi comuni ai due insiemi sono comunque diversi per la seconda componente, e quindi siano contati due volte.)

Osserviamo che le operazioni fra cardinalità così date sono ben definite.

Proposizione 5.11 (Buona definizione delle operazioni)

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

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

⁴³ $f(x) \in \mathcal{P}(A)$, ovvero è un sottoinsieme di A , quindi stiamo considerando il sottoinsieme degli elementi di A che non stanno nelle loro immagini (dei sottoinsiemi di A).

Dimostrazione. Date $f : A \rightarrow A'$ e $g : B \rightarrow B'$ bigettive, è immediato verificare che le seguenti sono bigezioni:

$$\begin{aligned} A \sqcup B \rightarrow A' \sqcup B' : & (a, 0) \mapsto (f(a), 0) \\ & (b, 1) \mapsto (g(b), 1) \\ A \times B \rightarrow A' \times B' : & (a, b) \mapsto (f(a), g(b)) \\ {}^B A \rightarrow {}^{B'} A' : & h \mapsto f \circ h \circ g^{-1} \end{aligned}$$

44

ed equivalgono alle uguaglianze di cardinalità nella tesi. \square

Notazione 5.12 (Cardinalità finite) — Riferendoci alle cardinalità finite $|\emptyset|, |1|, |2|, \dots$ se non c'è rischio di confusione, scriveremo semplicemente $0, 1, 2, \dots$

Osservazione 5.13 (Teorema di Cantor rivisitato) — $|\mathcal{P}(A)| = 2^{|A|}$, per cui il **teorema di Cantor**, può essere enunciato dicendo che, dato un qualunque A , vale $|A| < 2^{|A|}$.

Verifichiamo che effettivamente ci sia una bigezione tra l'insieme delle parti di A e quello delle funzioni da A in 2.

Dimostrazione. La funzione che ad ogni $B \in \mathcal{P}(A)$ associa la sua **funzione indicatrice** $\chi_B : A \rightarrow 2$ è definita da:

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

ed è una bigezione $\mathcal{P}(A) \rightarrow {}^A 2$ (ovvero $|\mathcal{P}(A)| = |{}^A 2| = |{}^A \{0, 1\}| = |{}^A 2|$ per la nostra codifica dei naturali, e per la definizione data prima la seconda cardinalità corrisponde proprio all'operazione $|2|^{|A|}$). \square

Proposizione 5.14 (Proprietà delle operazioni fra cardinalità)

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

$$\begin{array}{lll} \alpha + 0 = \alpha & \alpha + \beta = \beta + \alpha & \alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma \\ \alpha \cdot 0 = 0 & \alpha \cdot \beta = \beta \cdot \alpha & \alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma \\ \alpha \cdot 1 = \alpha & \alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma & \\ \alpha^0 = 1 & (\alpha^\beta)^\gamma = \alpha^{\gamma \cdot \beta} & (\alpha \cdot \beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma \\ 1^\alpha = 1 & \alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma & \end{array}$$

Dimostrazione. 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 ${}^C({}^B A)$ delle funzioni che ad ogni elemento di C associano una funzione $B \rightarrow A$, e l'insieme ${}^{C \times B} A$, delle funzioni che ad ogni coppia di elementi in $C \times B$ associano un elemento di

A. Associamo a $f \in {}^C({}^B A)$ la funzione $\tilde{f} \in {}^{C \times B} A$ definita da:

$$\tilde{f}(c, b) = (\underbrace{f(c)}_{\in {}^B A})(\underbrace{b}_{\in B}) \text{ } ^{45}$$

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

$$\bar{g}(c) : B \rightarrow A : b \mapsto g(c, b) \text{ } ^{46}$$

La verifica è facilissima, presa $g \in {}^{C \times B} A$ si ha:

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

(quindi $\sim \circ -$ è l'identità). Presa $f \in {}^C({}^B A)$, e fissato un qualunque $c \in C$, si ha:

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

da cui, per l'arbitrarietà di c , $\tilde{f} = f$ (e quindi $- \circ \sim$ è l'identità). \square

⁴⁵Cioè la mappa \sim prende una funzione da C a ${}^B A$ e la manda in un'altra che prende coppie di elementi in $C \times B$, e valuta il primo elemento in f per ottenere una mappa da B a A , che poi valuta in $b \in B$.

⁴⁶Ovvero la mappa $-$ associa una mappa di ${}^{C \times B} A$ con la mappa $\bar{g} \in {}^C({}^B A)$, che valutata in $c \in C$, dà una funzione da B in A , che ad ogni $b \in B$ associa $g(c, b)$.

§6 Cardinalità finite

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

Definizione 6.1 (Insieme finito/infinito). Diciamo che A è **finito** se $\exists n \in \omega |A| = |n|$. Se A non è finito, diciamo che A è **infinito**.

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

Definizione 6.2 (Dedekind-finitezza). Diciamo che A è **Dedekind-finito** se non può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio. Ossia A è Dedekind-finito se:

$$\forall B \subsetneq A |B| < |A|$$

§6.1 Principio dei cassetti

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

Proposizione 6.3 (Principio dei cassetti - ossia finito \rightarrow Dedekind-finito)

Dato A finito e B un sottoinsieme proprio di A , $B \subsetneq A$, vale $|B| < |A|$.

Dimostrazione. Naturalmente $|B| \leq |A|$ vale perché l'identità id_B è una funzione iniettiva $B \rightarrow A$. Occorre quindi dimostrare che $|B| \neq |A|$.

Per ipotesi $|A| = |n|$, per qualche $n \in \omega$, sia $g : A \rightarrow n$ una bigezione, si ha naturalmente che $|B| = |g[B]|$, e $g[B] \subsetneq n$, se verifichiamo che $|g[B]| < |n|$, allora otteniamo in automatico che $|B| < |A|$. Per fare ciò verifichiamo la disegualanza stretta nel caso in cui appunto l'insieme di partenza sia un naturale, dimostriamo per induzione la contronominale di questo fatto, ovvero dimostriamo che ogni sottoinsieme di un naturale con la sua stessa cardinalità è proprio il naturale stesso⁴⁷.

$$\forall n \in \omega \forall B \subseteq n (|B| = |n| \rightarrow B = n)$$

caso $n = \emptyset$ Vera a vuoto perché \emptyset non ha sottoinsiemi.

caso $n = m + 1$ Assumiamo per ipotesi induttiva che $\forall B \subseteq m (|B| = |m| \rightarrow B = m)$, vogliamo dimostrare che $\forall C \subseteq m + 1 (|C| = |m + 1| \rightarrow C = m + 1)$.

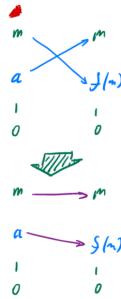
Sia $f : m + 1 \rightarrow C$ una bigezione tra $m + 1$ e C , possiamo assumere, WLOG - vedremo alla fine perché -, che $f(m) = m$ (cioè che $m \in C$ e che è un punto fisso di f), in tal modo $f|_m$ sarà una bigezione tra m e $C \setminus \{m\}$ (che è un suo sottoinsieme), per ipotesi induttiva ciò implica che $C \setminus \{m\} = m$, per cui $C \stackrel{f \text{ bigez.}}{=} \text{Im}(f) = m \cup \{f(m)\} = m \cup \{m\} = m + 1$.



⁴⁷La cui contronominale è appunto che ogni sottoinsieme proprio di n ha cardinalità minore strettamente di quest'ultimo.

Se $f(m) \neq m$ vediamo in primis che esiste sempre $a < m$ tale che $f(a) < m$ e inoltre possiamo sempre costruire una biogezione f' , a partire da f , tale per cui $f'(m) = m$. Se non esistesse $a < m$ tale per cui $f(a) = m$, allora $f|_m$ sarebbe una biogezione tra m e $C \setminus \{f(m)\} \subseteq m$, che per ipotesi induttiva significa $C \setminus \{f(m)\} = m$, per cui $m \cup \{f(m)\} = m + 1 \implies f(m) = m$, contro l'assunto iniziale, per cui assurdo. Abbiamo ora che esiste $a < m$ tale per cui $f(a) = m$, quindi possiamo definire una nuova biogezione f' , che ha m come punto fisso, nella maniera seguente:

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



□

Corollario 6.4 (A finito \implies ha un'unica cardinalità)

Se A è un insieme finito, allora esiste ed è unico un elemento di ω con cui è in biogezione:

$$\exists! n \in \omega \mid |A| = |n|$$

Dimostrazione. Se $|m| = |A| = |n|$, possiamo assumere, senza perdita di generalità $m \leq n$, che corrisponde a $m \subseteq n$, quindi per il principio dei cassetti $m = n$. □

Se adesso volessimo dimostrare il viceversa: [che formulato in versione contronominale è] che un insieme infinito non è Dedekind-finito, quale sarebbe l'ostacolo? Abbiamo già osservato che ω non è finito, perché la funzione successore stabilisce una corrispondenza biunivoca fra ω e $\omega \setminus \{0\} \subsetneq \omega$ (quindi non è Dedekind-finito, e per la contronominale del principio dei cassetti non è finito). Ne segue la seguente osservazione.

Osservazione 6.5 — Se esiste $f : \omega \rightarrow A$ iniettiva, allora A non è Dedekind-finito.^a

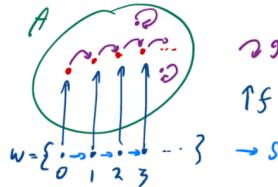
^aE quindi in automatico non è finito.

Dimostrazione. Basta considerare la funzione iniettiva:

$$g : A \rightarrow A : a \mapsto \begin{cases} f \circ s \circ f^{-1}(a) & \text{se } a \in f[\omega] \\ \text{id}_A(a) & \text{altrimenti} \end{cases}$$

È immediato vedere che $\text{Im}(g) = A \setminus \{f(0)\} \subsetneq A$ (l'unico escluso è lo 0, perché non può esserci un elemento che ha come controimmagine un elemento di ω il cui successore sia 0,

perché per quanto visto non esiste), dunque $A \hookrightarrow \text{Im}(g) \subsetneq A$, pertanto è in biiezione con un suo sottoinsieme proprio, per cui non può essere Dedekind-finito.⁴⁸



□

Quindi ci basterebbe dimostrare che ω si immerge in ogni insieme infinito (e dal lemma appena visto avremmo che l'insieme non è Dedekind-finito, completando l'altra freccia del principio dei cassetti). Un tentativo di dimostrazione potrebbe andare come segue.

Dimostrazione. Sia A infinito, costruiamo per ricorsione, seconda forma, una $f : \omega \rightarrow A$ 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 $a \notin \text{Im}(f|_n)$. Pongo $f(n) = a$. □

Dov'è l'errore? Nell'ultima riga! Noi sappiamo che, data $f|_n$, esistono degli $a \in A$ con $a \notin \text{Im}(f|_n)$, questo è corretto. È anche corretto che ci basterebbe porre $f(n) = \text{"uno qualunque di questi } a\text{"}$. Il guaio è che, per applicare il teorema di ricorsione, ci serve una funzione che fissa uno degli a da poter usare come h del teorema di ricorsione (più precisamente, vorremmo definire h come un elemento di $A \setminus \text{Im}(f|_n) \neq \emptyset$, poiché tuttavia dobbiamo ripetere questo procedimento infinite volte - per ogni $n \in \omega$ -, non possiamo fissare infiniti elementi tutti assieme - che è equivalente allo scrivere h come insieme quale è - con gli assiomi attualmente a disposizione, infatti possiamo per ora fissare soltanto un numero finito di cose). 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 $a \notin \text{Im}(f|_n)$ ", 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 immagazzinano tutti i numeri naturali.

Proposizione 6.6 (Tutti i naturali si immagazzinano in un qualsiasi insieme infinito)

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

Dimostrazione. 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, $f = \emptyset$ che va dal vuoto a qualsiasi insieme, va bene.

caso $n = m + 1$ Per ipotesi induttiva esiste $f : m \rightarrow A$ iniettiva. Siccome A è infinito (e m è finito), $A \setminus \text{Im}(f) \neq \emptyset$, quindi esiste $a \in A \setminus \text{Im}(f)$ e possiamo prenderlo (stiamo fissando

⁴⁸È l'argomento dell'[hotel di Hilbert](#).

una sola cose e possiamo farlo). Definiamo la funzione $f' = f \cup \{(n, a)\}$, che è iniettiva in quanto unione di funzioni iniettive su insiemi disgiunti - in arrivo.

□

Corollario 6.7 (Ovvietà)

Un sottoinsieme di un insieme finito è finito.

Dimostrazione. Sia A finito e $B \subseteq A$. Se, per assurdo B fosse infinito, avremmo:

$$|B| \stackrel{B \subseteq A}{\leq} |A| \stackrel{A \text{ finito}}{=} |n| \stackrel{\text{prop. sopra}}{<} |B| \text{ (contradiction)}$$

□

Esercizio 6.8. Dimostrare che:

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

Soluzione. Verifichiamo le due cose separatamente.

- Per ipotesi esiste $f : A \rightarrow n$ iniettiva e non surgettiva, abbiamo quindi $f[A] \subseteq n$, e per il corollario sopra un sottoinsieme di un insieme finito è finito, ovvero $\exists m \in \omega |f[A]| = m$. Osserviamo che necessariamente $m < n$, se fosse $m \geq n$, per la definizione di ordinamento su ω , ciò corrisponde a $m \supseteq n \implies |m| \geq |n|$, per cui:

$$|A| \stackrel{f \text{ iniett.}}{=} |f[A]| = |m| \geq |n| \stackrel{\text{H.p.}}{>} |A| \text{ (contradiction)}$$

- Se verifichiamo che $|f[A]| \leq |A|$, essendo A finito, otteniamo $|f[A]| \leq |n|$, per qualche $n \in \omega$, e, o $|f[A]| = |n|$, oppure $|f[A]| < |n|$ e quindi vale il punto precedente, in ogni caso si ottiene $f[A]$ finito.

Ci resta da verificare l'assunzione iniziale, possiamo farlo sfruttando il buon ordinamento di ω tramite la seguente funzione:

$$g : f[A] \rightarrow A : x \mapsto h^{-1} \left(\min_{<|n|} (h[f^{-1}(x)]) \right)$$

dove $<|n|$ è l'ordine usuale di ω ristretto ad n e h è la bigezione che esiste per ipotesi da A ad n . Si vede facilmente che g è ben definita, verifichiamo che è anche iniettiva:

$$\begin{aligned} g(x) = g(y) &\iff h^{-1} \left(\min_{<|n|} (h[f^{-1}(x)]) \right) = h^{-1} \left(\min_{<|n|} (h[f^{-1}(y)]) \right) \\ &\iff \min_{<|n|} (h[f^{-1}(x)]) = \min_{<|n|} (h[f^{-1}(y)]) \\ &\iff h(a) = h(b) \end{aligned}$$

con $a \in f^{-1}(x)$ e $b \in f^{-1}(y)$ (in altre parole abbiamo dato un nome ai minimi). Ora, essendo h bigettive quanto scritto equivale ad $a = b$, che, applicando f , equivale a:

$$x = f(a) \stackrel{a=b}{=} f(b) = y$$

per cui g è iniettiva e vale la disegualanza iniziale.

□

§6.2 Operazioni fra le cardinalità finite

Proposizione 6.9 (Corrispondenza tra le operazioni su ω e quelle tra cardinalità finite)

Dati $m, n \in \omega$ vale che:

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

ovvero, per gli elementi di ω le operazioni tra cardinalità corrispondono alla cardinalità delle operazioni tra gli elementi, già definite per ricorsione su ω .

Dimostrazione. Dimostriamo, intanto che $|m| + |1| = |s(m)|$. A sinistra abbiamo, infatti la cardinalità di $(m \times \{0\}) \cup \{(0, 1)\}$ ⁴⁹ e a destra abbiamo la cardinalità di $m \cup \{m\}$. Quest'ultimo insieme si mappa bigettivamente nel primo, mandando $x \in m$ in $(x, 0)$ e m in $(0, 1)$. 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 $n = 0$ $|m| + |0| = |(m \times \{0\}) \cup \emptyset| = |m| = |m + 0|$.

caso $n = s(a)$ Per ipotesi induttiva abbiamo $|m| + |a| = |m + a|$, da cui possiamo verificare la tesi come segue:

$$\begin{aligned} |m| + |s(a)| &\stackrel{\text{oss. iniziale}}{=} |m| + (|a| + |1|) \\ &\stackrel{\text{prop. operaz. card.}}{=} (|m| + |a|) + |1| \\ &\stackrel{\text{Hp. indutt}}{=} |m + a| + |1| \\ &\stackrel{\text{oss. iniziale}}{=} |s(m + a)| \\ &\stackrel{\text{def. di +}}{=} |m + s(a)| \end{aligned}$$

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

caso $n = 0$ $|m| \cdot |0| = |m \times \emptyset| = |0| \stackrel{\text{def. di }}{=} |m \cdot 0|$.

caso $n = s(a)$ Per ipotesi induttiva abbiamo $|m| \cdot |a| = |m \cdot a|$, da cui possiamo verificare la tesi come segue:

$$\begin{aligned} |m| \cdot |s(a)| &\stackrel{\text{oss. iniziale}}{=} |m| \cdot (|a| + |1|) \\ &\stackrel{\text{prop. operaz. card.}}{=} |m| \cdot |a| + \underbrace{|m| \cdot |1|}_{|m \times \{0\}|=|m|} \\ &\stackrel{\text{Hp. indutt}}{=} |m \cdot a| + |m| \\ &\stackrel{\text{prop. + card. fin.}}{=} |m \cdot a + m| \\ &\stackrel{\text{def. di }}{=} |m \cdot s(a)| \end{aligned}$$

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

⁴⁹Tipo di Mamino sui suoi appunti in quanto $1 = \{0\}$.

caso $n = 0$ $|m|^{[0]} = |^0 m| = |\{f : 0 \rightarrow m\}| = |\{\emptyset\}| = |1| = |m^0|$ (l'unica funzione possibile dal vuoto a m è $f = \emptyset$ ⁵⁰).

caso $n = s(a)$ Per ipotesi induttiva abbiamo $|m|^{[a]} = |m^a|$, per cui abbiamo:

$$\begin{aligned} |m|^{[s(a)]} &\stackrel{\text{oss. iniziale}}{=} |m|^{[a]+[1]} \\ &\stackrel{\text{prop. operaz. card.}}{=} |m|^{[a]} \cdot |m|^{[1]} = |m| \\ &\stackrel{\text{Hp. indukt}}{=} |m^a| \cdot |m| \\ &\stackrel{\text{caso prec.}}{=} |m^a \cdot m| \\ &\stackrel{\text{def. potenza}}{=} |m^{s(a)}| \end{aligned}$$

(dove $|m|^{[1]} = |m|$ perché $|^1 m| = |\{f : 1 \rightarrow m\}| = |\{(0, 0), (0, 1), (0, 2), \dots, (0, m-1)\}|$, e quest'ultimo insieme è banalmente in biogezione con m).

□

Nota 6.10 — Questa proposizione ci fornisce una dimostrazione delle proprietà aritmetiche elementari delle operazioni su ω [sfruttando le proprietà delle operazioni fra cardinalità], alternativa a quella per induzione (che è stata lasciata per esercizio). Basta, infatti, applicare le corrispondenti proprietà delle operazioni sulle cardinalità^a.

^aE ciò non comporta problemi di circolarità poiché nella dimostrazione della proposizione precedente abbiamo usato **solo** la definizione delle tre operazioni e nessuna delle loro proprietà.

Esercizio 6.11. 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.

I due modi sono sostanzialmente l'induzione ed il principio del minimo (idea la quale sarà riutilizzata in maniera molto simile per dimostrare il lemma di sottrazione ordinale), partiamo da quest'ultimo modo.

Soluzione. Fissati $m, n \in \omega$, con $m \leq n$, dobbiamo verificare esistenza ed unicità di $k \in \omega$ tale che $m + k = n$.

unicità Per l'unicità ci basta osservare che la funzione somma è strettamente crescente in entrambe le componenti⁵¹, dunque qualsiasi $k' \neq k$, per l'ordinamento totale di ω , è necessariamente strettamente maggiore o minore di k , da cui la somma con m è a sua volta strettamente maggiore o minore di n .

esistenza Se $m = n$, allora $k = 0$ e si conclude. Possiamo quindi supporre che $m < n$, sia d il minimo tale per cui $m + d > n$, tale minimo esiste perché $n < s(n) < m + s(n)$, dunque l'insieme in cui è preso è non vuoto e bene ordinato, pertanto d è ben definito. Poiché $m < n$ si ha $d > 0$, dunque $d = b+1$, e per la minimalità di d si ha $m+b \leq n$, dove in particolare, se valesse il $<$, si avrebbe $m+d = m+s(b) = s(m+b) \leq n$, che è assurdo, dunque vale l'uguaglianza e b è il k cercato.

□

⁵⁰E quindi ${}^0 m = \{f : \emptyset \rightarrow m\} = \{\emptyset\} = 1$, o in alternativa si può pensare che $f \subseteq \emptyset \times m = \emptyset \implies f \in \mathcal{P}(\emptyset) = \{\emptyset\}$ e quindi $f = \emptyset \implies {}^0 m = \{f\} = \{\emptyset\} = 1$.

⁵¹Andrebbe verificato per induzione.

Vediamo ora la stessa cosa dimostrata facendo uso dell'induzione numerabile.

Soluzione. Per l'unicità si procede esattamente come sopra, dimostriamo per induzione (su n) che fissati $m, n \in \omega$, con $m \leq n$, esiste $k \in \omega$ tale che $m + k = n$.

caso $n = 0$ In tal caso, o $m < n = 0$, e quindi la tesi è vera a vuoto, oppure $m = n = 0$, ed in questo caso basta prendere $k = 0$.

$n \implies n + 1$ Supponiamo che esista $k \in \omega$ tale che $m + k = n$ e verifichiamo che esista $k' \in \omega$ tale che $m + k' = n + 1$. Dall'ipotesi induttiva:

$$m + k = n \implies m + s(k) = s(m + k) = s(n) = n + 1$$

per cui prendiamo proprio $k' = k + 1$.

□

§7 La cardinalità del numerabile

Definizione 7.1 (Numerabilità). Diciamo che A è **al più numerabile** se $|A| \leq |\omega|$ ed è **numerabile** se $|A| = |\omega|$. Il simbolo \aleph_0 - aleph 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”).

Osservazione 7.2 — In altri termini, dire che A è al più numerabile significa dire che c’è una funzione iniettiva $A \hookrightarrow \omega$. Dire che è numerabile significa dire che c’è una biiezione con ω .

Proposizione 7.3 (Dicotomia della al più numerabilità)

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.

Definizione 7.4 (Buon ordinamento). Un insieme totalmente ordinato $(S, <)$ si dice **bene ordinato** se ogni suo sottoinsieme non vuoto ha un minimo.

$$\forall A \subseteq S \ A \neq \emptyset \rightarrow \exists m \in A \ \forall a \in A \ m \leq a$$

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

Definizione 7.5 (Isomorfismo). Due insiemi (parzialmente⁵²) ordinati $(A, <_A)$ e $(B, <_B)$ sono **isomorfi**, in simboli $(A, <_A) \sim (B, <_B)$ se esiste una biiezione $f : A \rightarrow B$ tale che:

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

cioè se esiste una biiezione che rispetta le relazioni d’ordine.

Osservazione 7.6 (Isomorfismi di ordini totali) — Due insiemi **totalmente** ordinati $(A, <_A)$ e $(B, <_B)$ sono isomorfismi se e solo se esiste una funzione $f : A \rightarrow B$ **surgettiva** e **strettamente crescente** - cioè tale che:

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

(quando entrambi gli ordinamenti sono totali ci basta una sola freccia per avere in automatico l’altra, dunque diciamo che basta solo la stretta crescenza - che tecnicamente è solo la freccia sopra e non anche quella da destra verso sinistra).

⁵²Dove parziale indica l’assenza della proprietà di totalità nella definizione di relazione d’ordine.

Esercizio 7.7. Dimostrare la proposizione enunciata sopra.

Osservazione 7.8 (Ogni insieme finito è isomorfo alla sua cardinalità) — Sia $(A, <_A)$ totalmente ordinato con $|A| = n \in \omega$. Allora $(A, <_A) \sim (n, <)$, dove $<$ denota il buon ordinamento indotto da ω .

Dimostrazione. Procediamo per induzione su n .

caso $n = 0$ $A = \emptyset$, quindi $(A, <_A) \sim (\emptyset, \emptyset)$ tramite la funzione vuota.

caso $n = m + 1$ Se $m = 0$, allora $A = \{a\}$ e $(A, <_A) \sim (1, <)$. Assumiamo quindi $m > 0$, e supponiamo che ogni insieme finito abbia un massimo. Sia N il massimo di A , allora $|A'| = m$, con $A' := A \setminus \{N\}$ (siamo nel caso $m > 0$, quindi è tutto legittimo), per cui per ipotesi induttiva esiste $f : A' \rightarrow m$ isomorfismo e quindi possiamo definire:

$$f' : A \rightarrow m + 1 : x \mapsto \begin{cases} f(x) & \text{se } x \in A' \\ m & \text{se } x = N \end{cases}$$

è banale che questa funzione sia ben definita e strettamente crescente.

Ci resta da verificare l'assunzione iniziale, ovvero che **ogni insieme finito e totalmente ordinato ha un massimo**. Procedendo per induzione, il caso $n = 0$ è banale, supponendo ora che $|A| = n$ ha massimo, vediamo che anche $|B| = n + 1$ ha massimo. Fissata g bigezione tra $n + 1$ e B , abbiamo che $g|_n$ è una bigezione tra n e $B \setminus \{g(m)\}$, pertanto, per ipotesi induttiva, quest'ultimo ammette massimo M . Ora per la totalità dell'ordinamento su B vale esattamente una tra $M > f(m)$ e $M < f(m)$, per cui [si verifica che] nel primo caso M è il massimo di B , nel secondo $f(m)$ è il massimo di B , in ogni caso B ha sempre un massimo, come voluto.

□

Osservazione 7.9 (Ogni ordine totale finito un ha massimo e minimo) — Questa proposizione ci dice che ogni ordine totale finito è isomorfo ad un buon ordine, $n \in \omega$, dunque ogni ordine totale finito ammette sia minimo - perché ω è ben ordinato -, sia massimo - perché l'abbiamo dimostrato nella dimostrazione precedente in generale, o anche come conseguenza della caratterizzazione di $(\omega, <)$ che stiamo per vedere.

Possiamo caratterizzare ω in termini delle proprietà del suo ordinamento naturale, grazie alle proprietà seguenti.

Proposizione 7.10 (Proprietà di $(\omega, <)$ come ordine totale)

Dato $(\omega, <)$ ordine totale allora valgono le seguenti:

- (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:

$$\forall A \subseteq \omega (A \neq \emptyset \wedge (\exists L \in \omega \forall x \in A x \leq L)) \rightarrow (\exists M \in A \forall x \in A x \leq M)$$

Dimostrazione. Abbiamo che (1) è il principio del minimo che abbiamo già dimostrato su ω , per (2) basta prendere $y = s(x)$ (e $x \in s(x) \implies x < y$). Per (3) se A è superiormente limitato da $L \in \omega$, allora $A \subseteq s(L)$, quindi A è finito - perché sottoinsieme di un insieme finito. Siccome A è finito ha un massimo per quanto osservato in precedenza, oppure perché l'ordinamento su A definito da:

$$x \prec y \stackrel{\text{def}}{=} x > y^{53}$$

è totale, per la totalità di $<$, ed è anche buono perché ogni sottoinsieme non vuoto di A è finito, totalmente ordinato, ed ha ha massimo per $<$ per l'osservazione precedente, che è dunque minimo per \prec . Per cui (A, \prec) è un buon ordinamento, quindi ha un minimo per la relazione \prec , che corrisponde ad un massimo per $<$.⁵⁴ \square

Proposizione 7.11 (Caratterizzazione di $(\omega, <)$ come ordine totale)

Sia (A, \prec) , 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 \prec

allora $(A, \prec) \sim (\omega, <)$.^a

^aQuesta proposizione completa la caratterizzazione di $(\omega, <)$ come ordine totale.

Dimostriamo prima un facile lemma.

Lemma 7.12 (Stretta crescenza col successore \implies stretta crescenza)

Sia (A, \prec) un ordine (non necessariamente totale), e sia $f : \omega \rightarrow A$ tale che:

$$\forall n \in \omega \ f(n) \prec f(s(n))^{a}$$

allora f è strettamente crescente, cioè $\forall m, n \in \omega \ m < n \rightarrow f(m) \prec f(n)$.

^aTipo di Mamino nelle dispense su \prec e $<$.

Dimostrazione. 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 $n = n' + 1$, con $m \geq n'$. Nel primo caso $f(m) \overset{\text{Hyp.}}{\prec} f(s(m)) = f(n) \not\prec f(n)$, e analogamente nel secondo:

$$f(m) \overset{n \text{ minimo}}{\preceq} f(n') \overset{\text{Hyp.}}{\prec} f(n) \not\prec f(n)$$

abbiamo quindi in tutti i casi un assurdo. \square

Possiamo ora dimostrare la proposizione.

L'idea è che le proprietà elencate per ipotesi siano il minimo indispensabile che un ordinamento totale deve avere affinché si possa sempre costruire un isomorfismo tra ω e un tale ordinamento totale.

⁵³Noto anche come **ordinamento duale** o **duale** dell'ordinamento $<$.

⁵⁴In ogni caso facciamo sempre affidamento al fatto che ogni insieme finito abbia massimo.

Dimostrazione. Costruiamo per ricorsione prima forma un isomorfismo f da $(\omega, <)$ a (A, \prec) nella maniera seguente:

$$f(0) = \min_{\prec} A \quad f(s(n)) = \min_{\prec} \{a \in A \mid f(n) \prec a\}^{55}$$

dove \min_{\prec} denota il minimo secondo la relazione d'ordine (buona) \prec di A . Verifichiamo che $f : \omega \rightarrow A$ è ben definita, strettamente crescente e surgettiva.

- ◊ f ben definita: il teorema di ricorsione numerabile ci garantisce esistenza ed unicità di f a patto che la $h : A \rightarrow A : x \mapsto \min_{\prec} \{x \in A \mid x \prec a\}$ sia ben definita, in questo caso i minimi sono ben definiti perché per ipotesi (1) A è ben ordinato, nel caso di $f(0)$ naturalmente assumiamo che $A \neq \emptyset$, mentre per il successore osserviamo che $\{a \in A \mid f(n) \prec a\}$ è sempre non vuoto, per ogni $n \in \omega$, perché per ipotesi (2) A è superiormente illimitato - se l'insieme fosse vuoto allora A sarebbe superiormente limitato da un suo elemento.
- ◊ f strettamente crescente: per costruzione $f(n) \prec f(s(n))$ per ogni $n \in \omega$, per cui f soddisfa le ipotesi del lemma precedente ed è strettamente crescente (quindi in particolare iniettiva).
- ◊ f surgettiva: dato $y \in A$ cerchiamo $x \in \omega$ tale che $f(x) = y$. Scegliamo $x := \min_{\prec} \{n \in \omega \mid y \prec f(n)\}$, possiamo farlo perché ω è bene ordinato e se per assurdo $y \succ f(n)$ per ogni $n \in \omega$, allora $f[\omega]$ sarebbe un sottoinsieme di A superiormente limitato e senza massimo - basta prendere f del successore -, contraddicendo (3). Abbiamo quindi $y \prec f(x)$, osserviamo che vale necessariamente anche la disuguaglianza opposta ed abbiamo concluso, distinguiamo due casi.

x = 0 In tal caso $f(x) = \min_{\prec} A$, quindi necessariamente $f(x) \preceq y$.

x = x' + 1 In questo caso, per la minimalità di x , si ha che $f(x') \preceq y$, naturalmente se $f(x') = y$ abbiamo comunque concluso⁵⁶, per cui ci rimane il caso $f(x') \prec y$. Avendo definito $f(x) = f(s(x'))$ come il minimo in A più grande di $f(x')$, segue che $f(x) \preceq y$ - y è nell'insieme in cui prendiamo tale minimo.

□

Tornando alla proposizione iniziale.

Proposizione 7.13 (Dicotomia della al più numerabilità)

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

Dimostrazione. Per ipotesi esiste $f : A \rightarrow \omega$ 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.

Dato un sottoinsieme $B \subseteq \omega$ o è finito o è infinito, nel primo caso abbiamo già concluso, nel secondo mostriamo che $(B, <_{|B}) \sim (\omega, <)$, e di conseguenza $|B| = \aleph_0$.

Naturalmente $(B, <_{|B})$ continua ad essere un buon ordinamento e qualsiasi sottoinsieme superiormente limitato continua ad avere massimo grazie alle proprietà di ω ⁵⁷ - i sottoinsiemi di B sono in particolare sottoinsiemi di ω -, per dimostrare che vale (2) dobbiamo invece verificare che B non ha massimo elemento. Se per assurdo $M := \max B$ allora $B \subseteq s(M)$, ma $s(M)$ è finito, per cui anche B lo sarebbe, che è contro l'ipotesi. □

⁵⁵Cioè la funzione prende ogni volta l'elemento più piccolo non ancora nell'immagine, come vedremo questo è l'unico isomorfismo sensato - e possibile - tra buoni ordinamenti.

⁵⁶Typo (?), Mamino questo caso l'ha saltato.

⁵⁷Typo di Mamino che scambia 2 e 3 nella dimostrazione.

Esercizio 7.14 (Disuguaglianza con la surgettività senza AC). Dimostra che se $|A| \leq \aleph_0$ e $f : A \rightarrow B$ è surgettiva, allora $|B| \leq \aleph_0$.

Soluzione. Mostriamo che sotto queste ipotesi esiste $h : B \hookrightarrow \omega$ - iniettiva. Sia $g : A \hookrightarrow \omega$ e poniamo:

$$h(b) = \min_{<} (g[f^{-1}(b)])$$

$f^{-1}(b) \neq \emptyset$ per ogni $b \in B$ poiché f è surgettiva, per cui il minimo è ben definito, e quindi lo è h . Vediamo l'iniettività, se $h(b) = h(b')$, allora i minimi, siano $g(a)$ e $g(a')$, sono uguali, ma a e a' sono elementi nelle controimmagini rispettivamente di b e b' , cioè tali che $f(a) = b$ e $f(a') = b'$. Sappiamo quindi per ipotesi che $g(a) = g(a')$ e per l'iniettività di g segue $a = a'$, da cui $f(a) = f(a')$, da cui $b = f(a) = f(a') = b'$. \square

§7.1 Insiemi numerabili in pratica

Sapere che, se $|A| \leq \aleph_0$, allora o A è finito o è numerabile, ci fornisce lo strumento essendo 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.

Osservazione 7.15 (Compatibilità tra operazioni e “ordinamento” fra cardinalità) —

Dati gli insiemi A, B, C con $|B| \leq |C|$ allora vale:

$$\begin{aligned} |A| + |B| &\leq |A| + |C| & |A|^{|B|} &\leq |A|^{|C|} \\ |A| \cdot |B| &\leq |A| \cdot |C| & |B|^{|A|} &\leq |C|^{|A|} \end{aligned}$$

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

Dimostrazione. Detta $f : B \rightarrow C$ la funzione iniettiva che testimonia che $|B| \leq |C|$ e detto $B' = f[B]$ abbiamo che $|B| = |B'|$, quindi basta dimostrare le disuguaglianze asserite con B' al posto di B ⁵⁸. Ora, poiché $B' \subseteq C$ otteniamo facilmente:

$$B' \subseteq C \xrightarrow{\text{ovvio}} (A \times \{0\}) \cup (B' \times \{1\}) \subseteq (A \times \{0\}) \cup (C \times \{1\}) = A \sqcup B' \subseteq A \sqcup C$$

$$\xrightarrow{\text{id}_A \times \text{id}_{B'}} |(A \times \{0\}) \cup (B' \times \{1\})| \leq |(A \times \{0\}) \cup (C \times \{1\})|$$

$$\xleftarrow{\text{def}} |A| + |B'| \leq |A| + |C|$$

Le altre si ottengono allo stesso modo. \square

Osservazione 7.16 (Disuguaglianza di inclusione-esclusione) — $|A \cup B| \leq |A| + |B|$.

Dimostrazione. Basta osservare che la seguente funzione è iniettiva:

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

\square

⁵⁸Oppure potevamo assumere WLOG che B fosse proprio contenuto in C e che la mappa fosse proprio id_B , in ogni caso è solo una questione di nomi.

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.

Proposizione 7.17 (Operazioni aritmetiche con \aleph_0)

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

Dimostrazione. Supponiamo di sapere già che $\aleph_0 \cdot \aleph_0 = \aleph_0$, allora possiamo formare la catena di diseguaglianze:

$$\aleph_0 \stackrel{\text{op. card.}}{=} \aleph_0 + 0 \stackrel{\text{oss. sopra}}{\leq} \aleph_0 + \aleph_0 \stackrel{\text{op. card.}}{=} \aleph_0 \cdot 2 \stackrel{\text{oss. sopra}}{\leq} \aleph_0 \cdot \aleph_0 \stackrel{\text{ipotesi}}{=} \aleph_0$$

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 $n \in \omega \setminus \{0\} \rightarrow \aleph_0^n = \aleph_0$, infatti $\aleph_0^1 = \aleph_0$ [e $\aleph_0^2 = \aleph_0 \cdot \aleph_0 = \aleph_0$], quindi $\aleph_0^{n+1} = \aleph_0^n \cdot \aleph_0 \stackrel{\text{H.p. indutt.}}{=} \aleph_0 \cdot \aleph_0 = \aleph_0$. \square

Per concludere la dimostrazione precedente, resta da dimostrare il lemma seguente.

§7.2 Prodotto di numerabili è numerabile

Lemma 7.18 ($\aleph_0 \cdot \aleph_0 = \aleph_0$)

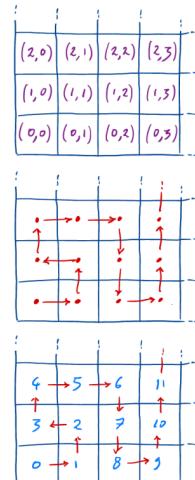
$\aleph_0 \cdot \aleph_0 = \aleph_0$, ossia esiste una bigezione fra $\omega \times \omega$ e ω .

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 disegnare un percorso che pare visitare tutte le maglie della griglia, con sufficiente apparenza di regolarità, probabilmente, 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 del disegno.

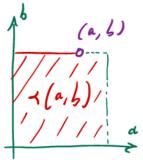
Altrimenti, è possibile esibire delle bigezioni esplicite, per esempio:

$$f(x, y) = 2^x \cdot (2y + 1) - 1 \quad g(x, y) = \frac{(x + y)^2 + 3x + y}{2}$$

È possibile anche scrivere i due numeri della coppia in base 10 a cifre alternate, tipo: $(64, 4096) \mapsto 400906644$.



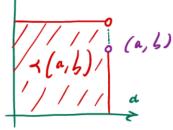
Dimostrazione. Innanzitutto definiamo su $\omega \times \omega$ un ordinamento come segue:



$$(a, b) \prec (a', b') \stackrel{\text{def}}{=} \max(a, b) < \max(a', b')$$

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

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



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 queste coincidono, allora si confrontano b e b' . L'idea è che le coppie \prec di una certa (a, b) fissata sono tutte contenute nel quadrato $\{0, \dots, \max(a, b)\} \times \{0, \dots, \max(a, b)\}$, per cui sono in numero finito, e quindi si ha $(\omega \times \omega, \prec)$ isomorfo a $(\omega, <)$.

Formalmente, iniziamo col verificare che \prec sia effettivamente un ordine stretto e totale.

- irriflessività: immediata dal fatto che confrontare (a, b) con se stessa da un OR con tre alternative tutte necessariamente false a causa dell'irriflessività di $<$.
- transitività: data $(a, b) \prec (a', b') \prec (a'', b'')$ vogliamo ottenere che $(a, b) \prec (a'', b'')$. Dalle disuguaglianze precedenti segue $\max(a, b) \leq \max(a', b') \leq \max(a'', b'')$, se una di queste disuguaglianze è stretta allora $(a, b) \prec (a'', b'')$ e si conclude, altrimenti $\max(a, b) = \max(a', b') = \max(a'', b'')$, e segue dalla definizione di \prec che $a \leq a' \leq a''$. Nuovamente, se una delle disuguaglianze è strette abbiamo concluso, altrimenti per definizione abbiamo $b \leq b' \leq b''$, e necessariamente una delle disuguaglianze deve essere stretta, altrimenti all'inizio avremmo avuto un'uguaglianza, che è assurdo, per cui si conclude necessariamente.
- totalità: basta osservare che se per (a, b) ed (a', b') non vale nessuna delle due fra \prec e \succ , allora necessariamente $a = a'$ e $b = b'$, che rende anche in questo caso vera la definizione di ordinamento totale.

Ora vogliamo dire che $(\omega \times \omega, \prec) \sim (\omega, <)$, in tal modo, avendo un'isomorfismo di ordini, avremmo in particolare una biogezione tra ω e $\omega \times \omega$. Partiamo dall'osservazione che se $(a, b) \in \omega \times \omega$ allora possiamo definire:

$$(\omega \times \omega)_{(a,b)} \stackrel{\text{def}}{=} \{(x, y) \in \omega \times \omega \mid (x, y) \prec (a, b)\}$$

detto il “**segmento iniziale**” determinato da (a, b) su $(\omega \times \omega, \prec)$. Tale segmento iniziale è finito, infatti $(\omega \times \omega)_{(a,b)} \subseteq s(\max(a, b)) \times s(\max(a, b))$, dove il RHS è un insieme finito e quindi tutti i suoi sottoinsiemi sono finiti.

Ci serve dire: 1. $(\omega \times \omega, \prec)$ è bene 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 $A \neq \emptyset$, possiamo fissare $a \in A$ e considerare $(\omega \times \omega)_a \cap A$. Se tale intersezione è vuota allora si vede banalmente che a è il minimo di A . Se l'intersezione è non vuota, allora è un sottoinsieme di un insieme finito e totalmente ordinato, dunque ha minimo $m \in A$ e tale minimo lo è proprio per tutti gli elementi di A , infatti, preso $x \in A \setminus ((\omega \times \omega)_a \cap A)$, si ha $m < a \leq x$.
2. Dato $(a, b) \in \omega \times \omega$, $(a, b) \prec (s(a), s(b))$, dunque $\omega \times \omega$ è illimitato.
3. Dato $A \subseteq \omega \times \omega$ non vuoto e superiormente limitato da $(a, b) \in \omega \times \omega$, abbiamo che $A \subseteq (\omega \times \omega)_{(a+1,b+1)}$, dunque è finito, e quindi ammette massimo perché \prec è totale e valgono le osservazioni fatta in precedenza.

□

§7.3 Numeri interi e razionali

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 - [esercizio](#) - una relazione di equivalenza induce un insieme di classi di equivalenza.

Definizione 7.19 (\mathbb{Z}). Definiamo \mathbb{Z} come l'insieme delle classi di equivalenza su $\omega \times \omega$ indotte dalla relazione:

$$(a, b) \sim_{\mathbb{Z}} (a', b') \stackrel{\text{def}}{=} a + b' = b + a' \text{ } ^{59}$$

Esercizio 7.20. Dimostrare che $\sim_{\mathbb{Z}}$ è una relazione di equivalenza.

Esempio 7.21 (Operazioni su \mathbb{Z})

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

$$\begin{aligned} [(a, b)]_{\mathbb{Z}} + [(a', b')]_{\mathbb{Z}} &\stackrel{\text{def}}{=} [(a + a', b + b')]_{\mathbb{Z}} \\ -[(a, b)]_{\mathbb{Z}} &\stackrel{\text{def}}{=} [(b, a)]_{\mathbb{Z}} \\ [(a, b)]_{\mathbb{Z}} \cdot [(a', b')]_{\mathbb{Z}} &\stackrel{\text{def}}{=} [(a \cdot a' + b \cdot b', a \cdot b' + a' \cdot b)]_{\mathbb{Z}} \end{aligned}$$

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

Definizione 7.22 (\mathbb{Q}). Definiamo \mathbb{Q} come l'insieme delle classi di equivalenza su $\mathbb{Z} \times (\omega \setminus \{0\})$ indotte dalla relazione:

$$(n, d) \sim_{\mathbb{Q}} (n', d') \stackrel{\text{def}}{=} n \cdot d' = n' \cdot d \text{ } ^{60}$$

Esercizio 7.23. Dimostrare che $\sim_{\mathbb{Q}}$ è una relazione di equivalenza.

Esercizio 7.24 (Operazioni su \mathbb{Q}). Definisci $+, -, \cdot$ e \square^{-1} su \mathbb{Q} nella maniera ragionevole e dimostra che \mathbb{Q} è un campo.

Esercizio 7.25 (Ordinamento su \mathbb{Q}). 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:

$$\forall a, b \in \mathbb{Q} \quad a < b \rightarrow \exists c \in \mathbb{Q} \quad a < c < b \text{ } ^a$$

^aTipo di Mamino.

⁵⁹Moralmente: “ $(a, b) = a - b$ ”.

⁶⁰Moralmente: “ $(n, d) = \frac{n}{d}$ ”.

Nota 7.26 — Gli esercizi precedenti sono tediosi, ma non sono difficili. Nel resto del corso daremo per scontate le proprietà aritmetiche elementari di \mathbb{Z} e \mathbb{Q} . D'ora innanzi scriveremo:

$$a - b \stackrel{\text{def}}{=} [(a, b)]_{\mathbb{Z}} \quad \frac{n}{d} \stackrel{\text{def}}{=} [(n, d)]_{\mathbb{Q}}$$

Per dimostrare la numerabilità di \mathbb{Z} e \mathbb{Q} , è comodo richiamare ancora un [esercizio](#), però, questa volta, lo risolviamo⁶¹.

Corollario 7.27 (Caratterizzazione della al più numerabilità)

Un insieme $A \neq \emptyset$ è al più numerabile se e solo se esiste $f : \omega \rightarrow A$ surgettiva.⁶²

⁶¹D'ora in avanti le disuguaglianze che danno al più numerabile ottenute mediante mappe surgettive saranno quindi legittime.

Dimostrazione. La freccia \Leftarrow deriva dall'esercizio citato prima. Per l'inverso, supponiamo A al più numerabile e mostriamo che c'è sempre una mappa surgettiva tra ω ed A . Per ipotesi esiste $g : A \hookrightarrow \omega$ - iniettiva -, essendo $A \neq \emptyset$ possiamo fissare $a \in A$ e definire la seguente mappa:

$$f : \omega \rightarrow A : x \mapsto \begin{cases} g^{-1}(x) & \text{se } x \in \text{Im}(g) \\ a & \text{altrimenti} \end{cases}$$

tal mappa è naturalmente ben definita ed è surgettiva in quanto stiamo semplicemente estendendo la mappa bigettiva $g^{-1} : \omega \supseteq \text{Im}(g) \rightarrow A$. \square

Notazione 7.28 (Successione - enumerazione) — Con **successione** (numerabile) intendiamo semplicemente una funzione con dominio ω , per cui:

$$\alpha = \{\alpha_i\}_{i \in \omega} \stackrel{\text{def}}{=} \alpha : \omega \rightarrow \dots : i \mapsto \alpha_i$$

cioè α è un “elenco numerabile” - non necessariamente esaustivo - degli elementi dell'insieme di arrivo. Per **enumerazione** intendiamo una successione (numerabile) surgettiva, tale per cui, detto A l'insieme di arrivo, si ha $\text{Im}(\alpha) = A$, o - informalmente - $A = \{\alpha_i | i \in \omega\}$.

Il corollario sopra, quindi, non ci dice altro che $A \neq \emptyset$ è al più numerabile se e solo se ha almeno un'enumerazione.

Esempio 7.29 (L'insieme dei numeri interi è numerabile)

\mathbb{Z} è numerabile.

Dimostrazione. La funzione $\omega \times \omega \rightarrow \mathbb{Z} : (a, b) \mapsto a - b$ è surgettiva per definizione (è la proiezione al quoziente di $\omega \times \omega$ modulo $\sim_{\mathbb{Z}}$, che sappiamo essere sempre surgettiva, in questo caso stiamo indicando le classi $[(a, b)]_{\mathbb{Z}}$ con $a - b$, ma sono sempre classi di equivalenza), e $\omega \times \omega$ è numerabile⁶² dunque $|\mathbb{Z}| \leq \aleph_0$.

D'altro canto, la funzione $\omega \rightarrow \mathbb{Z} : n \mapsto [(n, 0)]_{\mathbb{Z}}$ è iniettiva, infatti $[(n, 0)]_{\mathbb{Z}} =$

⁶¹La soluzione riportata all'esercizio di riferimento è quella di Mamino.

⁶² $|\omega \times \omega| = \aleph_0 \cdot \aleph_0 = \aleph_0$.

$[(m, 0)]_{\mathbb{Z}} \iff (n, 0) \sim (m, 0) \iff n = m$ (per definizione di $\sim_{\mathbb{Z}}$), dunque $\aleph_0 \leq |\mathbb{Z}|$, pertanto - per [Cantor-Bernstein](#) - $|\mathbb{Z}| = \aleph_0$. \square

Esempio 7.30 (L'insieme dei numeri razionali è numerabile)

\mathbb{Q} è numerabile.

Dimostrazione. Come nell'esempio precedente, la proiezione al quoziante $\mathbb{Z} \times (\omega \setminus \{0\}) \rightarrow \mathbb{Q} : (n, d) \mapsto \frac{n}{d}$ (dove la frazione è un'abbreviazione per la classe di equivalenza $[(n, d)]_{\mathbb{Q}}$), è surgettiva per costruzione, inoltre $|\mathbb{Z} \times (\omega \setminus \{0\})| = |\mathbb{Z}| \cdot |\omega \setminus \{0\}| = \aleph_0 \cdot \aleph_0 = \aleph_0$, dunque vale il [corollario](#) sulla disuguaglianza tra cardinalità, pertanto $\aleph_0 \geq |\mathbb{Q}|$.

Viceversa, la funzione $\omega \rightarrow \mathbb{Q} : n \mapsto \frac{n}{1}$ è iniettiva, infatti $\frac{n}{1} = \frac{m}{1} \iff n \cdot 1 = m \cdot 1 \iff n = m$, dunque per definizione si ha $\aleph_0 \leq |\mathbb{Q}|$. Da cui per [Cantor-Bernstein](#) $|\mathbb{Q}| = \aleph_0$. \square

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 - ovvero un'unione al più numerabile di insiemi al più numerabili è a sua volta 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 di a_i , cioè esiste:

$$\alpha_i : \omega \rightarrow a_i : j \mapsto \alpha_i(j) = \alpha_{i,j}$$

tale per cui $a_i = \text{Im}(\alpha_i) = \{\alpha_{i,j}\}_{j \in \omega}$, allora possiamo mandare surgettivamente - cioè enumerare - $\omega \times \omega$ in $\bigcup A$ mandando ogni coppia (i, j) nel j -esimo elemento dell' i -esimo elemento di A , $(i, j) \mapsto \alpha_{i,j}$, e, siccome $\omega \times \omega$ numerabile, allora per il [corollario](#) $|\bigcup A| \leq \aleph_0$. L'[errore](#) è credere di poter fissare una enumerazione α_i di 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 che associa ogni naturale ad una enumerazione dell'elemento di A da lui indicizzato, $i \mapsto \alpha_i$. Possiamo però assumere di averla, così si corregge il ragionamento impreciso di prima.

Proposizione 7.31 ($|A| \leq \aleph_0 \implies |\bigcup A| \leq \aleph_0$)

Sia $A = \{a_i \in A | i \in \omega\}$ e sia $\{\alpha_i\}_{i \in \omega}$ una successione di funzioni^a tali per cui, per ogni $i \in \omega$, si ha che $\alpha_i : \omega \rightarrow a_i$ è una enumerazione di a_i , allora $|\bigcup A| \leq \aleph_0$.

^aChe stiamo appunto assumendo di avere già, altrimenti serve AC.

Dimostrazione. Basta osservare che la funzione:

$$f : \omega \times \omega \rightarrow \bigcup A : (i, j) \mapsto \alpha_i(j) = \alpha_{i,j}$$

è surgettiva e vale quindi il solito [corollario](#). Infatti, dato $a \in \bigcup A$, poiché $A = \{a_i\}_{i \in \omega}$, allora $a \in a_i$, per qualche $i \in \omega$, e poiché $a_i = \text{Im}(\alpha_i)$ - qui stiamo usando che gli elementi di A sono a loro volta al più numerabili -, allora esiste $j \in \omega$ tale per cui $\alpha_i(j) = a$. \square

Notazione 7.32 — Data una funzione $f : I \rightarrow S$ definiamo:

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

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

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

Definizione 7.33 (Parti finite). Definiamo le **parti finite** di un insieme A come:

$$\mathcal{P}^{\text{fin.}}(A) \stackrel{\text{def}}{=} \{X \in \mathcal{P}(A) : |X| < \aleph_0\}$$

Proposizione 7.34 (Insieme al più numerabile \implies parti finite al più numerabile)

$$|A| \leq \aleph_0 \rightarrow |\mathcal{P}^{\text{fin.}}(A)| \leq \aleph_0.$$

Dimostrazione. Il caso $A = \emptyset$ è immediato. Assumiamo $A \neq \emptyset$, sia:

$$\mathcal{P}^{\leq n} = \{X \in \mathcal{P}(A) : |X| \leq n\}$$

siccome $\mathcal{P}^{\text{fin.}}(A) = \bigcup_{n \in \omega} \mathcal{P}^{\leq n}(A)$, basta esibire una successione di enumerazioni $n \mapsto (\alpha_n \rightarrow \mathcal{P}^{\leq n}(A))$, per poter usare il corollario sull'unione - così da evitare AC.

Essendo $|\omega \times A| = \aleph_0$ dall'ipotesi, possiamo fissare $f : \omega \rightarrow \omega \times A : x \mapsto (f_1(x), f_2(x))$ ⁶³ surgettiva (in realtà anche bigettiva). A questo punto possiamo costruire la successione di enumerazioni $(\alpha_n)_{n \in \omega}$ - con α_n enumera $\mathcal{P}^{\leq n}(A)$ per ogni $n \in \omega$ - per ricorsione numerabile prima forma come segue:

$m = 0$ In questo caso $\mathcal{P}^{=0}(A) = \{\emptyset\}$, dunque α_0 è la funzione che mappa tutti i naturali in 0, cioè $\alpha_0 = \{(n, 0)\}_{n \in \omega}$.

$m \implies m + 1$ Data un'enumerazione α_m di $\mathcal{P}^{\leq m}(A)$, definiamo l'enumerazione α_{m+1} di $\mathcal{P}^{\leq m+1}(A)$ nella maniera seguente:

$$\alpha_{m+1} : \omega \rightarrow \mathcal{P}^{\leq m+1} : x \mapsto \begin{cases} \emptyset & \text{se } x = 0 \\ \underbrace{\alpha_m(f_1(x-1))}_{\in \mathcal{P}^{\leq m}(A)} \cup \underbrace{\{f_2(x-1)\}}_{\in A} & \neq \emptyset \text{ altrimenti} \end{cases}$$

di fatto - a parte lasciare un insieme vuoto - stiamo prendendo tutti gli insiemi in $\mathcal{P}^{\leq m}(A)$ e ci stiamo aggiungendo un elemento di A ⁶⁴ - va verificato che questa costruzione mantenga la surgettività e lo faremo a breve.

Verifichiamo ora per induzione che la successione che abbiamo costruito ricorsivamente $(\alpha_n)_{n \in \omega}$ di enumerazioni dei $\mathcal{P}^{\leq n}(A)$ sia effettivamente tale, ovvero che α_n sia una mappa surgettiva da ω in $\mathcal{P}^{\leq n}(A)$ per ogni $n \in \omega$.

$m = 0$ La successione costante $\alpha_0 = \{(n, 0)\}_{n \in \omega}$ è banalmente surgettiva.

⁶³Avendo fissato una f a caso f_1 ed f_2 sono di fatto funzioni surgettive - entrambe da ω al rispettivo insieme - a caso.

⁶⁴Una sorta di shift per la cardinalità.

$m \implies m+1$ Per ipotesi induttiva la successione $\alpha_m : \omega \twoheadrightarrow \mathcal{P}^{\leq m}(A)$ è surgettiva, vogliamo verificare che anche $\alpha_{m+1} : \omega \twoheadrightarrow \mathcal{P}^{\leq m+1}(A)$ lo è. Dato $Y \in \mathcal{P}^{\leq s(m)}(A)$ si danno due casi. Se $Y = \emptyset$, allora per costruzione $Y = \alpha_{s(m)}(0) = \emptyset$. Altrimenti siamo nel caso in cui esiste almeno un elemento $y \in Y$.

In questo caso necessariamente $|Y \setminus \{y\}| \leq m$, quindi per ipotesi induttiva - cioè α_m surgettiva - $Y \setminus \{y\} = \alpha_m(t)$ per qualche $t \in \omega$. Per la surgettività di $f : \omega \twoheadrightarrow \omega \times A$, la coppia (t, y) è immagine di qualche $x \in \omega$, cioè $f(x) = (f_1(x), f_2(x)) = (t, y)$. Segue quindi che proprio $x + 1$ è una controimmagine di Y :

$$\begin{aligned} \alpha_{m+1}(x+1) &= \alpha_m(f_1(x)) \cup \{f_2(x)\} && (\text{definizione } \alpha_{m+1}) \\ &= \alpha_m(t) \cup \{y\} && (f(x) = (t, y)) \\ &= (Y \setminus \{y\}) \cup \{y\} = Y && (\text{Hp. induttiva}) \end{aligned}$$

□

Applicazione

Dimostriamo che l'insieme dei numeri reali algebrici $\mathbb{A}_{\mathbb{R}}^{65}$ è numerabile. Per questa applicazione, assumiamo le proprietà 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 a coefficienti razionali:

$$\mathbb{A}_{\mathbb{R}} \stackrel{\text{def}}{=} \{x \in \mathbb{R} \mid \exists p(x) \in \mathbb{Q}[x] \setminus \{0\} \ p(x) = 0\}$$

I numeri reali che non sono algebrici si dicono **trascendenti** ($= \mathbb{R} \setminus (\overline{\mathbb{Q}} \cap \mathbb{R})$), 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 coefficienti razionali nella indeterminata x , è numerabile. Possiamo identificare un polinomio:

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

con l'insieme dei suoi monomi:

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

e ciascun monomio con la coppia (grado, coefficiente):

$$p(x) = \{(0, a_0), (1, a_1), \dots, (d, a_d)\}^{66}$$

Formalmente, come accade per i numeri, le coppie ordinate, le funzioni, etc., 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:

$$\mathbb{Q}[x] \subseteq \mathcal{P}^{\text{fin.}}(\omega \times \mathbb{Q})^{67}$$

per cui, essendo che $|\omega \times \mathbb{Q}| = \aleph_0 \implies |\mathcal{P}^{\text{fin.}}(\omega \times \mathbb{Q})| = \aleph_0$, si ha $|\mathbb{Q}[x]| \leq \aleph_0$. Inoltre è elementare che $\mathbb{Q} \hookrightarrow \mathbb{Q}[x]$ (ad esempio $q \mapsto \{(0, q)\}$ è una mappa iniettiva che dà tutti i polinomi di grado 0), in tal modo si ha anche l'altra diseguaglianza di cardinalità e

⁶⁵Sarebbe $\overline{\mathbb{Q}} \cap \mathbb{R}$.

⁶⁶Può essere pensata come funzione da d in \mathbb{Q} , o come una funzione da ω a \mathbb{Q} a supporto finito.

⁶⁷Più precisamente $\mathbb{Q}[x] = \bigcup_{n \in \omega} n \times \mathbb{Q} \subseteq \mathcal{P}^{\text{fin.}}(\omega \times \mathbb{Q})$.

quindi - come al solito per **Cantor-Bernstein** - $|\mathbb{Q}[x]| = \aleph_0$. Venendo ad $\mathbb{A}_{\mathbb{R}}$ abbiamo una facile surgettione:

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

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

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

$$\text{"}\alpha \text{ è la } i\text{-esima radice di } p\text{"} \equiv p(\alpha) = 0 \wedge |\{x \in \mathbb{R} | x \leq \alpha \wedge p(x) = 0\}| = |i|$$

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

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

Per separazione esiste, quindi, f , e, di conseguenza $|\mathbb{A}_{\mathbb{R}}| \leq \aleph_0$. La diseguaglianza opposta è immediata perché $\mathbb{Q} \subseteq \mathbb{A}_{\mathbb{R}}$ - è facile scrivere un polinomio in $\mathbb{Q}[x]$ che abbia come radice un qualsiasi $q \in \mathbb{Q}$ fissato.

Esercizio 7.35 (Ogni gruppo finitamente generato è al più numerabile). Dato un insieme X , una funzione $f : X \times X \rightarrow X$, e un sottoinsieme $A \subseteq X$ al più numerabile, dimostra che esiste un $\bar{A} \subseteq X$ al più numerabile tale che $A \subseteq \bar{A}$ e $f[\bar{A} \times \bar{A}] \subseteq \bar{A}$. Concludi che un gruppo finitamente generato è al più numerabile.

"Typo di Mamino, questa ipotesi manca nelle dispense, ma c'è scritta nel 2021."

Soluzione. [DA COMPLETARE] L'idea per risolvere la prima parte è ottenere \bar{A} come unione numerabile di una successione che parta da A e che ad ogni passaggio nel faccia l'immagine via f , in modo tale che l'unione rispetti poi tutte le proprietà volute. Per questa ragione definiamo per ricorsione numerabile prima forma la seguente successione:

$$A_n : \omega \rightarrow \mathcal{P}(X) : \begin{cases} A_0 = 0 \\ A_{n+1} = f[A_n \times A_n] \cup A_n \end{cases}$$

e quindi $\bar{A} := \bigcup_{n \in \omega} A_n$. Naturalmente, essendo $A_n \subseteq X$ per ogni $n \in \omega$ - per definizione di f - , si ha che $\bar{A} \subseteq X$; inoltre, presi $x, y \in \bar{A}$ si ha $x \in A_i$ e $y \in A_j$, per $i, j \in \omega$, poiché $A_n \subseteq A_{n+1}$, cioè la successione è crescente, si ha $x, y \in A_{\max(i,j)}$, per cui per definizione di f si conclude $f(x, y) \in A_{\max(i,j)+1} \subseteq \bar{A}$.

Ci rimane da verificare che $|\bar{A}| \leq \aleph_0$, per fare ciò vogliamo usare il corollario dell'unione - che evita AC -, dobbiamo quindi procurarci una successione di enumerazioni $n \mapsto \alpha_n$, con $\alpha_n : \omega \rightarrow A_n$. Definiamo la successione per ricorsione numerabile.

$n = 0$ Per ipotesi $A_0 = A$ è al più numerabile quindi possiamo fissare una sua enumerazione ed usare quella come α_0 .

$n \implies n + 1$ Supponiamo di avere per ipotesi induttiva $\alpha_n : \omega \rightarrow A_n$ e costruiamo $\alpha_{n+1} : \omega \rightarrow A_{n+1}$

Dimostriamo ora per induzione che la successione così definita è effettivamente una successione di enumerazione per gli A_n ⁶⁸.

⁶⁸Come nella proposizione sulle parti finite, non solo la successione di enumerazioni ci permette di applicare il corollario sull'unione, ma ha come conseguenza - cosa che stiamo per dimostrare per induzione - che $\forall n \in \omega |A_n| \leq \aleph_0$, che a priori non sapevamo.

$n = 0$ Abbiamo preso già α_0 enumerazione nelle costruzione per ricorsione, quindi non c'è altro da dimostrare.

$n \implies n + 1$ Supponiamo che α_n sia surgettiva e dimostriamo che lo è $\alpha_{n+1} : \omega \rightarrow A_{n+1}$. Dato $y \in A_{n+1} = f[A_n \times A_n] \cup A_n$, ci sono tre possibilità:

- se $y \in A_n \setminus f[A_n \times A_n]$: in tal caso, essendo α_n surgettiva esiste $x \in \omega$ tale per cui $\alpha_n(x) = y$
- se $y \in A_n \cap f[A_n \times A_n]$: in tal caso $y = f(z)$, con $z = (a, b) \in A_n \times A_n$, e di nuovo, per surgettività di α_n esistono $a', b' \in A_n$, per cui $\alpha_n(a') = a$ e $\alpha_n(b') = b$
- se $y \in f[A_n \times A_n] \setminus A_n$:

Per la seconda parte, dato un gruppo G e $S \subseteq G$, tale che $|S| < \aleph_0$ e $\langle S \rangle = G$, consideriamo la funzione:

$$f : G \times G \rightarrow G : (x, y) \mapsto xy^{-1}$$

per quanto dimostrato nella prima parte esiste $\bar{S} \subseteq G$ tale che $S \subseteq \bar{S}$ e $|\bar{S}| \leq \aleph_0$. Essendo ora G non vuoto e finitamente generato si ha $S \neq \emptyset$, per cui $\bar{S} \neq \emptyset$, verifichiamo dunque che \bar{S} è un sottogruppo di G .

- Essendo $\bar{S} \neq \emptyset$ esiste $g \in \bar{S}$, e per ipotesi $e_G = gg^{-1}f(g, g) \in \bar{S}$.
- Dal primo punto segue facilmente che $\forall g \in \bar{S} \quad g^{-1} = e_G \cdot g^{-1} = f(e_G, g) \in \bar{S}$.
- Infine $\forall g, h \in \bar{S}$, per il punto precedente vale sempre che $h^{-1} \in \bar{S}$, e per ipotesi $gh = f(g, h^{-1}) \in \bar{S}$.

Abbiamo quindi che \bar{S} è un sottogruppo di G che contiene S , per cui è proprio tutto il gruppo, $\bar{S} = G$, e quindi vale $|G| = |\bar{S}| \leq \aleph_0$. \square

§7.4 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.

Definizione 7.36 (Densità). Sia $(A, <)$ totalmente ordinato, e $B \subseteq A$, diciamo che B è **denso in** $(A, <)$ se:

$$\forall x, y \in A \quad x < y \rightarrow \exists z \in B \quad x < z < y$$

cioè tra due elementi di A c'è sempre un elemento di B .

Inoltre diciamo che $(A, <)$ è **denso**, cioè è denso in se stesso, se:

$$\forall x, y \in A \quad x < y \rightarrow \exists z \in A \quad x < z < y$$

cioè tra due elementi di A c'è sempre qualche elemento di A .

Esempio 7.37 $((\mathbb{Q}, <)$ è denso in se stesso)

Abbiamo già osservato, in un esercizio, che \mathbb{Q} è denso, infatti:

$$x < y \rightarrow x < \frac{x+y}{2} < y$$

cioè presi due qualsiasi elementi di \mathbb{Q} , la loro media aritmetica è sempre in mezzo e sta in \mathbb{Q} (formalmente le due diseguaglianze si giustificano con le operazioni di \mathbb{Q} + l'ordinamento totale + le proprietà di compatibilità tra operazioni e ordinamento).

NON ESEMPIO 7.38 $((\omega, <)$ non è denso in se stesso)

L'insieme ω con il suo ordinamento naturale non è denso, perché $\nexists z \in \omega \text{ } 0 < z < 1$.

Teorema 7.39 (Teorema di isomorfismo di Cantor)

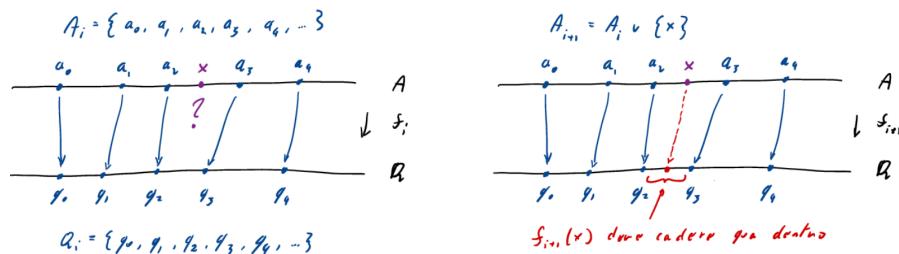
Sia $(A, <)$ un insieme totalmente ordinato tale che:

1. $|A| = \aleph_0$
2. $(A, <)$ è denso
3. $(A, <)$ non ha **estremi**, ossia non ha né massimo né minimo elemento

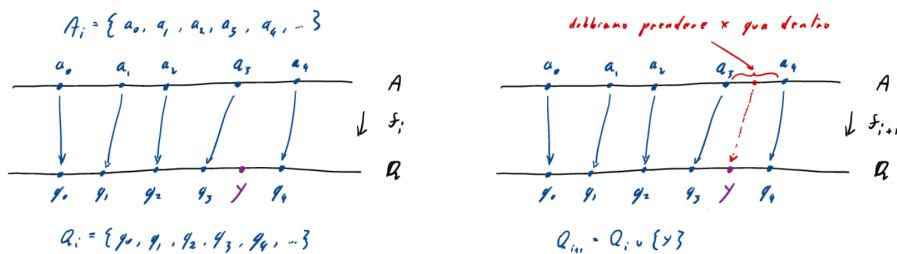
allora $(A, <) \sim (\mathbb{Q}, <)$.^a

^aNotare che le proprietà elencate sono cose che abbiamo già verificato che valgono per \mathbb{Q} , quindi questo teorema è la caratterizzazione di $(\mathbb{Q}, <)$ come ordine totale.

L'idea è di costruire l'isomorfismo per ricorsione. Ad ogni passo della ricorsione avremo $f_i : A_i \rightarrow Q_i$ 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 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 $y \in \text{Im}(f_{i+1})$.



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 farà comodo la seguente osservazione.

Osservazione 7.40 (L'unione di un insieme di funzioni compatibili è una funzione) —
Sia $F \subseteq \mathcal{P}(A \times B)$ un insieme di funzioni. Se vale che:

$$\forall f_1, f_2 \in F \quad f_1|_{\text{Dom}(f_1) \cap \text{Dom}(f_2)} = f_2|_{\text{Dom}(f_1) \cap \text{Dom}(f_2)}$$

cioè se le funzioni da A a B coincidono sull'intersezione dei domini a due a due, $\forall x \in \text{Dom}(f_1) \cap \text{Dom}(f_2) \quad f_1(x) = f_2(x)$, allora $\bigcup F$ è ancora una funzione dall'unione dei domini a B :

$$\bigcup F : \bigcup \{\text{Dom}(f) | f \in F\} \rightarrow B$$

Dimostrazione. Bisogna verificare che vale la proprietà fondamentale delle funzioni, ovvero che, se $(x, y_1) \in \bigcup F$ e $(x, y_2) \in \bigcup F$, allora $y_1 = y_2$.

Dalla prima cosa abbiamo che esiste $f_1 \in \bigcup F$ tale che $f_1(x) = y_1$ e, dalla seconda, sappiamo che esiste $f_2 \in \bigcup F$ tale che $f_2(x) = y_2$, ma questo significa - per definizione di dominio - che $x \in \text{Dom}(f_1) \cap \text{Dom}(f_2)$, dunque dall'ipotesi si ha che:

$$y_1 = f_1(x) \stackrel{\text{H.p.}}{=} f_2(x) = y_2$$

□

Siamo ora pronti per dimostrare formalmente il teorema.

Dimostrazione. Per l'ipotesi 1 possiamo fissare un'enumerazione di A e \mathbb{Q} rispettivamente:

$$A = \{a_i | i \in \omega\} \quad \mathbb{Q} = \{q_i | i \in \omega\}$$

vogliamo costruire una successione di funzioni $(f_i)_{i \in \omega}$ tale per cui, per ogni $i \in \omega$:

- (1) $f_i : A_i \rightarrow Q_i$ con $|A_i| = |Q_i| < \aleph_0$.
- (2) f_i è un isomorfismo di ordini fra A_i e Q_i .
- (3) $f_i \subseteq f_{s(i)}$ - ossia $f_{s(i)}$ estende f_i .
- (4) $\forall j < i \quad a_j \in A_i \wedge q_j \in Q_i$, ossia il dominio e l'immagine contengono sempre almeno i primi i elementi delle rispettive enumerazioni (poi possono contenere anche altro come vedremo dopo nella costruzione):

$$\{a_0, \dots, a_{i-1}\} \subseteq \text{Dom}(f_i) = A_i \quad Q_i = \{q_0, \dots, q_{i-1}\} \subseteq \text{Im}(f_i) = Q_i$$

Dando per buona l'esistenza e l'unicità della successione sopra, possiamo definire:

$$f := \bigcup_{i \in \omega} f_i$$

- ◊ f è una funzione: da (3) segue, facilmente per induzione, che $\forall i < j \quad f_i \subseteq f_j$, quindi è una successione di funzioni ciascuna che estende la precedente, per cui sono compatibili e l'unione è ancora una funzione.
- ◊ $f : A \rightarrow \mathbb{Q} = \text{Im}(f)$: da (4) vale che $\text{Dom}(f) = \bigcup_{i \in \omega} \text{Dom}(f_i) = \bigcup_{i \in \omega} A_i = A$ e $\text{Im}(f) = \bigcup_{i \in \omega} \text{Im}(f_i) = \bigcup_{i \in \omega} Q_i = \mathbb{Q}$ - dove abbiamo appunto usato che dominio e immagine i -esimi, A_i e Q_i , per (4) contengono i primi i -termini della enumerazione. Poiché abbiamo preso come codominio proprio l'immagine f è automaticamente surgettiva.

- ◊ f strettamente crescente: dati $x, y \in A$ tali per cui $x < y$, si ha che $x \in A_i$ e $y \in A_j$, per $i, j \in \omega$, ora detta $t := \max(i, j)$ si ha che $x, y \in A_t$ e, per (4), $A_t \subseteq f(t)$, con f_t isomorfismo - per (2), segue quindi:

$$x < y \leftrightarrow f(x) = f_t(x) < f_t(y) = f(y)$$

Non ci resta altro da fare che costruire la successione $(f_i)_{i \in \omega}$ per ricorsione numerabile - prima forma. Poniamo $f_0 = \emptyset$, per costruire $f_{s(i)}$ definiamo prima un passo intermedio $f_{i+0.5}$ - nel primo passo, $f_{i+0.5}$, estendiamo la funzione aggiungendo a_i al dominio (se non ci fosse già), nel secondo passo, f_{i+1} , analogamente, aggiungiamo q_i all'immagine (se non ci fosse già). Data quindi $f_i : A_i \rightarrow Q_i$, distinguiamo due casi:

- se $a_i \in \text{Dom}(f_i)$: allora $f_{i+0.5} = f_i$.
- altrimenti: detto $\bar{j} := \min\{j \in \omega \mid f_i \cup \{(a_i, q_j)\} \text{ è un isomorfismo}\}$ (teoricamente basta strettamente crescente visto che l'immagine è il codominio), poniamo $f_{i+0.5} = f_i \cup \{(a_i, q_{\bar{j}})\}$.

Ora possiamo fare il secondo passo di estensione e definire f_{i+1} :

- se $q_i \in \text{Im}(f_{i+0.5})$: allora $f_{i+1} = f_{i+0.5}$.
- altrimenti: detto $\bar{\iota} := \min\{\iota \in \omega \mid f_{i+0.5} \cup (a_{\bar{\iota}}, q_i) \text{ è un isomorfismo}\}$ (come prima basta strettamente crescente).⁶⁹

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 seguente proposizione:

$$\forall i \in \omega \text{ "la costruzione di } f_i \text{ è ben posta e valgono (1), ..., (4)"}$$

Naturalmente il nel caso $f_0 = \emptyset$ la proposizione è vera a vuoto, vediamo il passo induttivo, ma solo per la buona definizione.

Per verificare che la definizione di f_{i+1} sia ben posta, supponendo per ipotesi induttiva che f_i lo sia e che valgano per lei le proprietà (1), ..., (4), bisogna verificare dunque che i minimi esistano in entrambi i passaggi di estensione, e qui entrano in gioco le ipotesi 2 e 3 del teorema. Vediamo che esiste il minimo nel primo passaggio di estensione (sarà analogo verificarlo nel secondo). Consideriamo:

$$\bar{j} = \min\{j \in \omega \mid f_i \cup \{(a_i, q_j)\} \text{ è un isomorfismo}\}$$

Per ipotesi induttiva, vale (1) per f_i , per cui A_i è finito. Detto $n = |A_i|$ (avendo già fatto il caso $i = 0$ sappiamo che $i > 0$ e dalla costruzione $|i| \leq |A_i|$), sfruttando il fatto visto che un ordine totale finito è isomorfismo ad un numero naturale possiamo bene ordinare A_i nella maniera seguente:

$$A_i = \{\alpha_0, \dots, \alpha_{n-1}\} \quad \text{con } \alpha_0 < \dots < \alpha_{n-1}$$

Ora, siamo naturalmente nel caso in cui $a_i \notin \text{Dom}(f_i)$, quindi o $a_i < \alpha_0$, o $\alpha_k < a_i < \alpha_{k+1}$ per qualche k , o $a_{n-1} < a_i$. Nel primo e terzo caso, rispettivamente, siccome \mathbb{Q} non ha estremi, c'è un $q_j < f_i(\alpha_0)$, o $q_j > f_i(\alpha_n)$, per cui $f_{i+0.5} \cup \{(a_i, q_j)\}$ è un isomorfismo. Nel secondo caso, per la densità di \mathbb{Q} , esiste q_j con $f_i(\alpha_k) < q_j < f_i(\alpha_{k+1})$ e quindi di nuovo $f_{i+0.5} \cup \{(a_i, q_j)\}$ è un isomorfismo. Nella verifica del secondo passo dell'estensione faremo lo stesso identico ragionamento con Q_i usando questa volta densità ed illimitatezza di A , per trovare gli elementi. □

⁶⁹Notare che la costruzione sarebbe stata simmetrica e funzionante nel caso avessimo voluto costruire $f : \mathbb{Q} \rightarrow A$.

Corollario 7.41 (Ogni ordine al più numerabile è isomorfo ad un sottoinsieme di \mathbb{Q})

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 7.42 — 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.

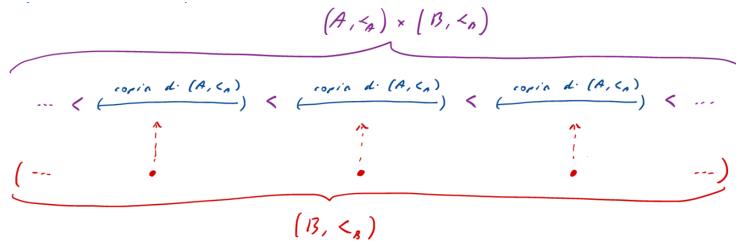
Definizione 7.43 (Prodotto lessicografico di ordini). Dati $(A, <_A)$ e $(B, <_B)$ definiamo il **prodotto lessicografico** di ordini come:

$$(A, <_A) \times (B, <_B) \stackrel{\text{def}}{=} (A \times B, <_{A \times B})$$

dove $(a, b) <_{A \times B} (a', b') \stackrel{\text{def}}{=} (b <_B b') \vee (b = b' \wedge a <_A a')$.

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 il prodotto lessicografico $(A, <_A) \times (B, <_B)$ come “ $(A, <_A)$ ripetuto $(B, <_B)$ volte”.

**Osservazione 7.44** (Il prodotto lessicografico grafico di ordini totali è un ordine totale)

— Se $(A, <_A)$ e $(B, <_B)$ sono ordini totali, allora anche $(A, <_A) \times (B, <_B)$ lo è.^a

^aÈ una facile verifica che usa appunto la totalità di $<_A$ e $<_B$.

Esercizio 7.45 (Associatività del prodotto lessicografico). Dati $(A, <_A)$, $(B, <_B)$ e $(C, <_C)$ dimostra che:

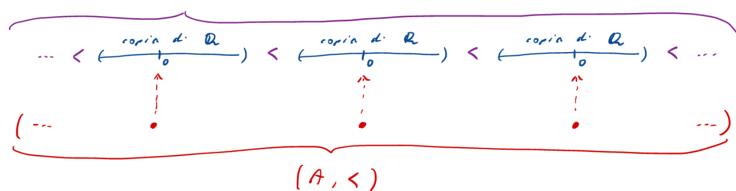
$$((A, <_A) \times (B, <_B)) \times (C, <_C) \sim (A, <_A) \times ((B, <_B) \times (C, <_C))$$

ossia che il prodotto lessicografico di ordini è associativo a meno di isomorfismi.

Veniamo ora alla dimostrazione del corollario

Dimostrazione. Se $A = \emptyset$ è banale, supponiamo quindi $A \neq \emptyset$ e consideriamo:

$$(S, <) \stackrel{\text{def}}{=} (\mathbb{Q}, <) \times (A, <)$$



L'insieme $S = \mathbb{Q} \times A$ 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 - né superiori né inferiori. Per verificare che è denso, consideriamo $(q_1, a_1) < (q_2, a_2)$ e verifichiamo che in ogni caso c'è sempre un altro elemento di S strettamente nel mezzo.

- Se $a_1 < a_2$, allora $(q_1, a_1) < (q_1 + 1, a_1) < (q_2, a_2)$ - e funziona per la definizione di ordinamento nel prodotto lessicografico.
- Se $a_1 = a_2$ - per cui siamo nella stessa copia di \mathbb{Q} -, si ha che $(q_1, a_1) < \left(\frac{q_1+q_2}{2}, a_1\right) < (q_2, a_2) = (q_2, a_1)$.

quindi $(S, <)$ è denso e per il **teorema di isomorfismo di Cantor** si ha $(S, <) \sim (\mathbb{Q}, <)$. Infine $A \hookrightarrow \mathbb{Q} \times A : a \mapsto (0, a)$, quindi, componendo l'immersione (strettamente crescente) con l'isomorfismo trovato, abbiamo che $(A, <)$ è isomorfo ad un sottoinsieme di $(\mathbb{Q}, <)$. \square

Esercizio 7.46 (Isomorfismo di Cantor senza l'ipotesi di illimitatezza). Dimostra che se $(A, <)$ è denso (ma non necessariamente senza estremi) e $2 \leq |A| \leq \aleph_0$, allora $(A, <)$ è isomorfismo a uno dei seguenti intervalli di \mathbb{Q} :

$$[0, 1]_{\mathbb{Q}} \quad]0, 1]_{\mathbb{Q}} \quad [0, 1[_{\mathbb{Q}} \quad]0, 1[_{\mathbb{Q}}$$

Soluzione. Osserviamo che per l'ipotesi di densità $2 \leq |A| \leq \aleph_0 \implies |A| = \aleph_0$ ⁷⁰. A questo punto, se A è senza estremi si ha:

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

($]0, 1[_{\mathbb{Q}}$ è totalmente ordinato [ereditariamente dall'ordine di \mathbb{Q}], senza estremi, numerabile [sottoinsieme di \mathbb{Q} e c'è la mappa $n \mapsto \frac{1}{n}$] e denso [basta prendere la media di due elementi e osservare che sta sempre in mezzo per le proprietà algebriche di \mathbb{Q}]).

Negli altri casi si osserva che:

$$[0, 1]_{\mathbb{Q}} =]0, 1]_{\mathbb{Q}} \cup \{0, 1\} \quad]0, 1]_{\mathbb{Q}} =]0, 1[_{\mathbb{Q}} \cup \{1\} \quad [0, 1[_{\mathbb{Q}} =]0, 1[_{\mathbb{Q}} \cup \{0\}$$

vediamo, ad esempio, nel caso di A con entrambi gli estremi, che, detti questi a e b , si ha:

$$(A \setminus \{a, b\}, <_{|A \setminus \{a, b\}}) \sim (\mathbb{Q}, <) \sim]0, 1[_{\mathbb{Q}}, <)$$

e analogamente negli altri due casi. Fissiamo un isomorfismo f tra $A \setminus \{a, b\}$ e $]0, 1[_{\mathbb{Q}}$ ed estendiamolo all'isomorfismo voluto:

$$f' : A \rightarrow [0, 1]_{\mathbb{Q}} : x \mapsto \begin{cases} 0 & \text{se } x = a \\ 1 & \text{se } x = b \\ f(x) & \text{altrimenti} \end{cases}$$

si verifica facilmente che è effettivamente un isomorfismo e negli altri casi si procede in maniera analoga. \square

⁷⁰Stiamo escludendo l'insieme denso con un solo elemento grazie all'ipotesi che $|A| \geq 2$.

§7.5 Il grafo random

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.

Cogliamo questa occasione per suggerire un esercizio di applicazione della medesima tecnica che è un po' complicato. Si tratta di definire il **grafo random** o **grafo di Rado**.

Definizione 7.47 (Grafo). Un **grafo** (V, e) sull'insieme di vertici V è dato da una relazione e simmetrica $(\forall x, y \in V (x, y) \in e \leftrightarrow (y, x) \in e)$ e irriflessiva $(\forall x \in V (x, x) \notin e)$.

L'idea è che V può essere immaginato come un insieme di punti che possono essere connessi da archi. Dire che c'è un arco fra x e y equivale a $(x, y) \in e$.

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 $i < j$ - cioè la seconda componente è sempre strettamente più grande della prima - lanciamo una moneta che fa testa con probabilità p - tutte queste monete indipendentemente - 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 isomorfismi⁷¹, dove, per essere precisi dobbiamo definire cosa sia un isomorfismo tra grafi.

Definizione 7.48 (Isomorfismo fra grafi). I grafi (V_1, e_1) e (V_2, e_2) sono **isomorfi** se esiste una bigezione $f : V_1 \rightarrow V_2$ tale che:

$$\forall v, w \in V_1 (v, w) \in e_1 \leftrightarrow (f(v), f(w)) \in e_2$$

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 $p^{|X|} \cdot (1-p)^{|Y|}$ ⁷² - come che sia, è un certo numero > 0 - e, avendo preso X ed Y finiti, ci sono infiniti $v \in \omega \wedge v \notin X \cup Y$.

Si capisce, quindi, che con probabilità 1 - ossia certamente - almeno uno di questi v vincerà questa lotteria (ne abbiamo infiniti in fondo), ossia sarà connesso a tutti gli X e a nessuno degli Y . Usiamo l'esistenza di questo v per definire un grafo random.

Definizione 7.49 (Grafo random). Il grafo (ω, e) ⁷³ è un **grafo random** se:⁷⁴

$$\forall X, Y \subseteq \omega \wedge X \cap Y = \emptyset \wedge |X|, |Y| < \aleph_0 \exists v \in \omega \setminus (X \cup Y) \underbrace{X \times \{v\} \subseteq e}_{\forall x \in X (x, v) \in e} \wedge \underbrace{(Y \times \{v\}) \cap e = \emptyset}_{\exists y \in Y (y, v) \in e}$$

cioè se per ogni coppia di sottoinsiemi finiti di vertici disgiunti esiste un vertice fuori dall'unione di questi ultimi, connesso a tutti i vertici di uno ed a nessuno dei vertici dell'altro.

⁷¹A meno di rinominare i vertici, che è quello che diremo nella definizione di isomorfismo.

⁷²Eventi indipendenti: v è connesso ad un vertice di X con probabilità p , ed è connesso a tutti i vertici di X con probabilità $p^{|X|}$, viceversa non è connesso ad alcun vertice di Y con probabilità $(1-p)^{|Y|}$.

⁷³Questa definizione è per ω , ma la definizione generale di grafo random è data dalla stessa proprietà per un generico grafo (numerabile) (G, e) .

⁷⁴Tipo di Mamino, manca ipotesi di finitezza.

Esercizio 7.50 (Esistenza e unicità del grafo random). Dimostra che esiste un grafo random, ed è unico a meno di isomorfismi - cioè indipendentemente da $p \in]0, 1[$ viene sempre lo stesso grafo.^a

^aHint: Usare la tecnica del back-and-forth per l'unicità.

Soluzione. Vediamo separatamente esistenza ed unicità.

esistenza Per l'esistenza dobbiamo definire una relazione su ω ⁷⁵ che rispetti la proprietà che definisce un grafo random. Per fare ciò ci serviremo per comodità del **predicato BIT** definito come segue:

$$\text{BIT}(i, j) = \left\lfloor \frac{i}{2^j} \right\rfloor \mod 2$$

cioè $\text{BIT}(i, j) = 1$ se la j -esima cifra di i espresso in base 2 è 1, altrimenti è 0. A questo punto possiamo definire la seguente relazione:

$$\forall i, j \in \omega \ i \sim y \equiv \text{BIT}(i, j) \vee \underbrace{\text{BIT}(j, i)}_{=\text{BIT}(i, j)^\top}$$

ovvero la simmetrizzazione della relazione BIT. Questa relazione è appunto simmetrica e rispetta la proprietà del grafo random, dati infatti $X, Y \subseteq \omega$ finiti e disgiunti, consideriamo:

$$x := 2^{\max(X, Y)+1} + \sum_{i \in X} 2^i$$

cioè ci assicura che $x \equiv 1 \pmod{2^i}$ per ogni $i \in X$, per cui $\forall i \in X (x, i) \in e$, ed al contempo $x \equiv 0 \pmod{2^j}$ per ogni $j \in \omega \setminus (X \cup \{\max(X, Y) + 1\}) \supseteq Y$, cioè $(x, j) \notin e$ per ogni $j \in Y$. Naturalmente non vale nemmeno che $(j, x) \in e$ per $j \in Y$ in quanto $x > j$, dunque la cifra x -esima di j in base 2 è necessariamente 0 ($j < x < 2^x \implies \left\lfloor \frac{j}{2^x} \right\rfloor = 0$).

unicità Siano (S, s) e (R, r) due grafi random, verifichiamo che sono isomorfi. Fissiamo due enumerazioni di S ed R :

$$S = \{s_i | i \in \omega\} \quad R = \{r_i | i \in \omega\}$$

e costruiamo una successione di funzioni $(f_i)_{i \in \omega}$ tale che:

- (1) $f_i : S_i \rightarrow R_i$ con $|S_i|, |R_i| < \aleph_0$.
- (2) f_i è un isomorfismo di grafi.
- (3) $\forall i \in \omega f_i \subseteq f_{i+1}$.
- (4) $\forall i \in \omega \{s_0, \dots, s_{i-1}\} \subseteq \text{dom}(S_i) = S_i \wedge \{r_0, \dots, r_{i-1}\} \subseteq \text{Im}(f_i) = R_i$.

Data quindi $(f_i)_{i \in \omega}$, possiamo definire $f := \bigcup_{i \in \omega} f_i$, con $\text{dom}(f) = \bigcup_{i \in \omega} S_i = S$ - il contenimento dal basso c'è per (4), quello dall'alto perché come vedremo nella costruzione della successione $\forall i \in \omega S_i \subseteq S$. Osserviamo ora che:

◊ f è ben definita e surgettiva: per (3) l'unione delle funzioni f_i è una funzione, inoltre, come per il dominio $\bigcup_{i \in \omega} R_i = R$, per cui $f : S \rightarrow R$ è surgettiva.

⁷⁵Come per la definizione di grafo random, l'esistenza la si può dimostrare più in generale per un qualsiasi insieme numerabile.

\diamond f è un isomorfismo: presi $x, y \in S$ vogliamo verificare che valga $(x, y) \in s \leftrightarrow (f(x), f(y)) \in r$. Dato che $x \in S_i$ e $y \in S_j$, per $i, j \in \omega$, preso WLOG $j > i$, abbiamo $x, y \in S_j$, per cui:

$$(x, y) \in s \leftrightarrow (f(x), f(y)) = (f_j(x), f_j(y)) \stackrel{f_j \text{ isomorfismo}}{\in} R$$

Non ci resta altro che costruire $(f_i)_{i \in \omega}$ per ricorsione numerabile. Poniamo $f_0 = \emptyset$, ora dato f_i definiamo f_{i+1} mediante due passi di estensione come segue. Definiamo prima $f_{i+0.5}$ a partire da f_i nella maniera seguente:

- se $s_i \in \text{dom}(f_i)$, allora $f_{i+0.5} = f_i$.
- altrimenti sia $\bar{j} := \min\{j \in \omega | f_i \cup \{(s_i, r_j)\} \text{ è un isomorfismo}\}$, poniamo $f_{i+0.5} = f_i \cup \{(s_i, r_{\bar{j}})\}$.

Ora definiamo f_{i+1} a partire da $f_{i+0.5}$:

- se $r_i \in \text{Im}(f_i)$, allora $f_{i+1} = f_{i+0.5}$.
- altrimenti sia $\bar{\iota} := \min\{\iota \in \omega | f_{i+0.5} \cup \{(s_{\iota}, r_i)\} \text{ è un isomorfismo}\}$, poniamo $f_{i+1} = f_{i+0.5} \cup \{(s_{\bar{\iota}}, r_i)\}$.

A questo punto dimostriamo per induzione che la costruzione sopra sia ben posta in ogni passaggio e che valgano le proprietà (1), ..., (4). Per $f_0 = \emptyset$ è banale, assumiamo ora che f_i sia ben definita e che valgano le proprietà (1), ..., (4) e verifichiamo che vale la stessa cosa per f_{i+1} . Per la buona definizione dobbiamo verificare che nei passaggi di estensione i minimi esistano sempre, dunque, nel caso in cui $s_i \notin \text{dom}(f_i)$ verifichiamo che l'insieme $\{j \in \omega | f_i \cup \{(s_i, r_j)\} \text{ è un isomorfismo}\}$ è non vuoto, per fare ciò dobbiamo verificare che esiste $r_j \in R$ tale che $\forall x \in S_i \text{ se } (x, s_i) \in s \text{ allora si ha } (f_i(x), r_j) \in r$. Essendo S_i finito, l'insieme degli elementi con cui s_i è in relazione è finito, e quindi a sua volta lo sarà l'insieme delle immagini via f_i di tali elementi, chiamiamolo U , ora poiché (R, r) soddisfa la proprietà del grafo random esiste almeno un elemento u in relazione con tutti gli elementi di U e con nessun elemento del vuoto (basta un qualunque sottoinsieme di R finito e disgiunto da U), a questo punto ci basta prendere $r_j = u$.

Analogamente, nel secondo passaggio di estensione, nel caso in cui $r_i \notin \text{Im}(f_{i+0.5})$, dobbiamo verificare che l'insieme $\{\iota \in \omega | f_{i+0.5} \cup \{(s_{\iota}, r_i)\} \text{ è un isomorfismo}\}$ sia non vuoto, ovvero trovare un $s_{\iota} \in S$ tale che $\forall y \in R$ per cui $(y, r_i) \in R$, si abbia $(f_{i+0.5}^{-1}(y), s_{\iota}) \in s^{76}$. Come prima, l'insieme degli elementi di $R_{i+0.5}$ in relazione con r_i è finito, e così sarà anche la sua controimmagine via $f_{i+0.5}^{-1}$, chiamiamola V , a questo punto, essendo (S, s) un grafo random, esiste un elemento $v \in S$ in relazione con tutti gli elementi di V e nessuno del vuoto, ci basta dunque prendere $s_{\iota} = v$. Verifichiamo ora che valgano le proprietà (1), ..., (4) per f_{i+1} . È immediato osservare che $f_i \subseteq f_{i+0.5} \subseteq f_{i+1}$ per costruzione, e, sempre per costruzione, $s_i \in \text{dom}(f_{i+1})$ e $r_i \in \text{Im}(f_i + 1)$, in tal modo abbiamo verificato (3) e (4). In entrambi i passaggi della costruzione aggiungiamo al più un elemento, dunque S_{i+1} e R_{i+1} sono finiti, per cui abbiamo (1), infine, $f_{i+0.5}$ è un isomorfismo per costruzione e da questo segue che per costruzione lo è anche f_{i+1} , dunque abbiamo anche (2).

□

⁷⁶Tecnicamente stiamo già assumendo di aver verificato che $f_{i+0.5}$ è un isomorfismo, ma questo segue banalmente dall'ipotesi induttiva e dalla costruzione.

§8 \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 le verifiche.

Definizione 8.1 (Maggiorante, insieme superiormente limitato ed estremo superiore). Sia $(A, <)$ un ordine totale, allora:

- $m \in A$ 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 con $\sup B$ - se s è il minimo dei maggioranti di B .

Nota 8.2 — Non sempre gli estremi superiori esistono, e, se B ha un estremo superiore, questo è unico^a.

^aSegue dall'unicità del minimo di un insieme ordinato.

Definizione 8.3 (Ordine totale completo). Un ordine totale $(A, <)$ è **completo** se ogni $B \subseteq A$ superiormente limitato ha un estremo superiore $\sup B \in A$.⁷⁷

Esercizio 8.4 (\mathbb{Q} non è completo). Dimostra, usando solo le proprietà di \mathbb{Q} , che l'insieme $\{x \in \mathbb{Q} | x^2 < 2\}$ non ha estremo superiore in \mathbb{Q} .

Lemma 8.5 (\mathbb{Q} è archimedeo)

Diciamo che un campo ordinato K soddisfa la **proprietà archimedea** se, dati $x, y \in K$, con $0 < x < y$, esiste $n \in \mathbb{N}$ tale che $nx > y$.^a $(\mathbb{Q}, 0, 1, +, \cdot, \leq)$ è un campo ordinato archimedeo.

^aO equivalentemente dato $x \in K$, con $x > 0$, esiste $n \in \mathbb{N}$ tale che $n > x$.

Soluzione.

□

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.

Definizione 8.6 (Segmento iniziale). Sia $(A, <)$ un ordine totale. $B \subseteq A$ è un **segmento iniziale** di A se $\forall x \in B \forall y \in A$ $y < x \rightarrow y \in B$ - cioè se contiene un punto, contiene tutti i precedenti, strettamente.

Ossia B è un segmento iniziale di A se, ognualvolta B contiene un elemento, B contiene altresì tutti gli elementi minori di questo. Un segmento iniziale B di A si dice **proprio** se $B \neq A$.

⁷⁷Questa per la precisione è la definizione di **Dedekind-completezza**.

Esempio 8.7 (Segmento iniziale principale)

Dato $(A, <)$ ordine totale, A stesso e \emptyset sono segmenti iniziali di A . Dato $x \in A$, l'insieme:

$$A_x \stackrel{\text{def}}{=} \{y \in A \mid y < x\}$$

è un segmento iniziale proprio di A - detto **segmento iniziale principale** determinato da x . Ad esempio $\{x \in \mathbb{Q} \mid x < 0 \vee x^2 < 2\}$ è un segmento iniziale - proprio - di \mathbb{Q} che non è principale.

Nota 8.8 — 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} .

Definizione 8.9 (Sezioni di Dedekind). Una **sezione** sull'insieme totalmente ordinato $(A, <)$ è un segmento iniziale **proprio** e **non vuoto** di A che **non ha un massimo elemento** - per convenzione sceglieremo di non metterci massimo elemento.

Ossia B segmento iniziale di A è una sezione se $B \neq A$, $B \neq \emptyset$ e $\forall x \in B \exists y \in B \ x < y$.

Definizione 8.10 (Insieme ordinato dei numeri reali). Definiamo l'insieme dei **numeri reali** come l'insieme delle sezioni di Dedekind di \mathbb{Q} :

$$\mathbb{R} \stackrel{\text{def}}{=} \{x \in \mathcal{P}(\mathbb{Q}) \mid x \text{ è una sezione su } \mathbb{Q}\}^{78}$$

con l'ordinamento dato da:

$$\forall x, y \in \mathbb{R} \ x \leq y \stackrel{\text{def}}{=} x \subseteq y^{79}$$

poiché il contenimento come relazione su $\mathcal{P}(\mathbb{Q})$ è un ordinamento parziale, allora anche \leq lo è in automatico.

Proposizione 8.11 (\mathbb{R} è completo)

$(\mathbb{R}, <)$ è un ordine totale completo.

Prima della dimostrazione, isoliamo un semplice lemma.

Lemma 8.12 (L'unione di segmenti iniziali è un segmento iniziale)

Sia $(A, <)$ un ordine totale e X un insieme di segmenti iniziali di A . Allora $\bigcup X$ è un segmento iniziale di A .

Dimostrazione. Sia $\alpha \in \bigcup X$ e sia $\beta \in A$, con $\beta < \alpha$, vogliamo verificare che $\beta \in \bigcup X$. Poiché $\alpha \in \bigcup X$, allora $\alpha \in B$, con B segmento iniziale di A e $B \in X$, a questo punto è ovvio per la proprietà dei segmenti iniziali che $\beta < \alpha \rightarrow \beta \in B \subseteq \bigcup X$. \square

Ora possiamo dimostrare la proposizione come segue.

⁷⁸Moralmente: sono tutti i modi di prendere \mathbb{Q} , tagliarlo in due e prendere la cosa a sinistra (per le nostre convenzioni).

⁷⁹Era equivalente definire il $<$ a partire da \subset , avremmo ottenuto comunque lo stesso ordine su \mathbb{R} .

Dimostrazione. Abbiamo detto che (\mathbb{R}, \leq) , con \leq definito come il contenimento tra le sezioni di Dedekind di \mathbb{Q} è già un ordinamento parziale, dobbiamo quindi verificarne la totalità. Dati $x, y \in \mathbb{R}$, supponiamo per assurdo che non valga né $x \subseteq y$ né $y \subseteq x$, allora, essendo $x, y \neq \emptyset$ - per definizione di sezioni -, si ha che esistono $a, b \in \mathbb{Q}$ tali che $a \in x \setminus y$ e $b \in y \setminus x$. A questo punto, visto che l'ordinamento su \mathbb{Q} è totale, vale necessariamente una tra $a < b$ e $b < a$ (non può valere l'uguale sennò l'elemento starebbe nell'intersezione di x e y). Nel primo caso, poiché $b \in y$ - ed y è un segmento iniziale - si avrebbe $a \in y \downarrow$, analogamente, nel secondo caso, $b \in x \downarrow$.

Verifichiamo ora la completezza, dato $A \subseteq \mathbb{R}$ non vuoto e superiormente limitato, cioè ammette un maggiorante $m \in \mathbb{R}$, dimostriamo che $\sup A = \bigcup A \in \mathbb{R}$.

Per il lemma precedente $\bigcup A$, essendo unione di reali, è ancora un segmento iniziale - di \mathbb{Q} -, e, siccome A non è vuoto, allora $\bigcup A \neq \emptyset$. Poiché m è un maggiorante di A , si ha $\forall x \in A x \leq m \equiv x \subseteq m \implies \bigcup A \leq m \in \mathbb{R}$, per cui $\bigcup A \neq \mathbb{R}$ ⁸⁰, quindi è un segmento iniziale non vuoto e proprio, inoltre, non ha massimo, perché se lo avesse sarebbe massimo per una delle sezioni dell'unione cosa che non può avvenire. Abbiamo quindi che $\bigcup A$ è una sezione di Dedekind di \mathbb{Q} e quindi $\bigcup A \in \mathbb{R}$.

Verifichiamo che $\bigcup A$ è il minore dei maggioranti di A . Se $x \in A$, allora $x \subseteq \bigcup A$, e, per la definizione di ordinamento data, ciò equivale a $x \leq \bigcup A$. Ora, se m è un altro maggiorante di A , allora per definizione $\forall x \in A x \leq m \equiv x \subseteq m$, ma ciò significa che $\bigcup A \subseteq m \equiv \bigcup A \leq m$, ovvero $\bigcup A$ è il minimo tra i maggioranti. \square

Osservazione 8.13 (\mathbb{Q} si immerge in maniera ordinata e densa in \mathbb{R}) — La funzione $\iota : \mathbb{Q} \hookrightarrow \mathbb{R} : a \mapsto \mathbb{Q}_a = \{x \in \mathbb{Q} | x < a\}$, cioè la funzione che manda ogni razionale nella sua sezione di Dedekind principale, immerge \mathbb{Q} in \mathbb{R} in maniera strettamente crescente e densa - ossia $\iota[\mathbb{Q}]$ è densa in \mathbb{R} .

Dimostrazione. Osserviamo in primis che ι è ben definita in quanto \mathbb{Q}_a è un segmento iniziale di \mathbb{Q} , proprio e non vuoto, per cui è una sezione di Dedekind di \mathbb{Q} , cioè un elemento di \mathbb{R} . Vediamo ora che dati $a, b \in \mathbb{Q}$, con $a < b$, si ha che $\mathbb{Q}_a \subsetneq \mathbb{Q}_b$, infatti:

$$x \in \mathbb{Q}_a \iff x < a < b \implies x < b \iff x \in \mathbb{Q}_b$$

e $a \notin \mathbb{Q}_a \wedge a \in \mathbb{Q}_b$ per cui $\iota(a) < \iota(b)$. Infine, dati $x, y \in \mathbb{R}$, con $x < y$, vediamo che contenuto strettamente nel mezzo c'è un elemento di $\text{Im}(\iota)$. Poiché $x < y \equiv x \subsetneq y \implies y \setminus x \neq \emptyset$, e per definizione $y \setminus x \subseteq \mathbb{Q}$, per cui possiamo prendere $b \in y \setminus x$ e, siccome y non ha massimo, abbiamo $b < q \in y \setminus x$, verifichiamo che $x < \iota(q) = \mathbb{Q}_q < y$. Infatti, poiché $q \in y$ - e y è una sezione - allora $\forall c \in \mathbb{Q}_q \equiv c < q \wedge q \in y \implies c \in y$, e naturalmente $q \notin \mathbb{Q}_q$ ma $q \in y$ per cui $\mathbb{Q}_q \subsetneq y \equiv \iota(q) < y$. Analogamente, poiché $a, b \notin x$, allora $\forall z \in x z \leq a < b \equiv x \subseteq \mathbb{Q}_a \subsetneq \mathbb{Q}_b$, dove non c'è l'ultima uguaglianza perché $a < b \rightarrow a \in \mathbb{Q}_b$ e $a \notin \mathbb{Q}_a$. \square

Notazione 8.14 (Abuso di immersioni) — 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

⁸⁰Tipo Mamino

abusare della notazione immaginando che queste siano vere e proprie inclusioni:

$$\omega \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

In realtà non è vero: per esempio è $\iota[\mathbb{Q}]$, non \mathbb{Q} , a 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.

Corollario 8.15 (\mathbb{R} è più che numerabile)

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

Dimostrazione. Dall'osservazione sulla notazione di sopra, abbiamo visto che $\mathbb{Q} \hookrightarrow \mathbb{R}$, da cui $\aleph_0 = |\mathbb{Q}| \leq |\mathbb{R}|$, inoltre \mathbb{Q} è denso in \mathbb{R} , pertanto \mathbb{R} è denso in se stesso. Si vede facilmente che \mathbb{R} non ha massimo né minimo, quindi se \mathbb{R} fosse numerabile sarebbe isomorfo, per l'[isomorfismo di Cantor](#), a \mathbb{Q} . D'altro canto \mathbb{R} è completo e \mathbb{Q} no - per l'[esercizio](#) visto -, dunque non possono essere isomorfi, e quindi necessariamente non vale l'ipotesi 1 del teorema di isomorfismo di Cantor che avevamo assunto, dunque non può esserci una biiezione $\implies \aleph_0 < |\mathbb{R}|$. \square

§8.1 Caratterizzazione dei reali come ordine

Abbiamo stabilito che $(\mathbb{R}, <)$ è un ordine totale, completo e 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.

Proposizione 8.16 (Caratterizzazione di $(\mathbb{R}, <)$)

Sia $(A, <)$ un ordine totale, se:

1. $(A, <)$ è completo
2. $(A, <)$ è senza estremi
3. esiste $B \subseteq A$ numerabile e denso in A^{a}

allora $(A, <) \sim (\mathbb{R}, <)$.

^aSi dice anche che A è **separabile**.

Dimostrazione. Denotiamo con \tilde{A} l'insieme delle sezioni di Dedekind su B , cioè $\tilde{A} = \{x \in \mathcal{P}(B) | x \text{ è una sezione di } \mathbb{Q}\}$. Osserviamo che $(A, \leq) \sim (\tilde{A}, \subseteq)$ - cioè un ordine totale con le proprietà sopra è necessariamente isomorfo alle sezioni di Dedekind del suo denso numerabile. L'isomorfismo è infatti dato da:

$$f : A \rightarrow \tilde{A} : a \mapsto B_a = \{x \in B | x < a\}$$

la cui inversa è:

$$g : \tilde{A} \rightarrow A : Y \mapsto \sup Y$$

Verifiche: dobbiamo mostrare in primis che le mappe sono l'una l'inversa dell'altra.

$g \circ f = \text{id}_A$ Dato $a \in A$, osserviamo che $g(f(a)) = \sup B_a = \sup\{x \in B \mid x < a\}$, e che il sup di tale insieme è proprio a . Infatti, è banale che a è un maggiorante, preso $b < a$ maggiorante per B_a , essendo B denso, esiste $b < b' < a$, e dall'ultima diseguaglianza $b' \in B_a$, per cui b non può essere un maggiorante, dunque a è proprio il minimo dei maggioranti.

$f \circ g = \text{id}_{\tilde{A}}$ Data una sezione di B , $X \in \tilde{A}$, osserviamo che $f(g(X)) = B_{\sup X}$, mostriamo che $B_{\sup X} = X$. È ovvio che $\forall x \in X \ x < \sup X$ - ricordiamo che le sezioni non hanno massimo, quindi non c'è l'uguale -, per cui $x \in B_{\sup X}$ e quindi $X \subseteq B_{\sup X}$. Viceversa, dato $x \in B_{\sup X}$, ciò equivale a $x < \sup X$, e, per definizione di sup, esiste necessariamente $x' \in X$ tale che $x < x' < \sup X$, ed essendo X un segmento iniziale segue $x \in X$, per cui $B_{\sup X} \subseteq X$.

Osserviamo infine che naturalmente f è strettamente crescente (si può usare g), dati $a, a' \in A$, segue $B_a \subsetneq B_{a'}$ (e naturalmente \tilde{A} è totalmente ordinato con la stessa dimostrazione di \mathbb{R}).

Ora per il teorema di isomorfismo di Cantor abbiamo che $(B, <|_B) \sim (\mathbb{Q}, <)$, infatti è numerabile e denso per 3 - se è denso in A lo è in particolare in se stesso -, inoltre, poiché A è illimitato e B è denso in lui, allora anche B è illimitato.

A questo punto, è facile osservare che fissato un isomorfismo tra $(B, <|_B)$ e $(\mathbb{Q}, <)$ questo preserva le sezioni di Dedekind, per cui induce un isomorfismo tra le sezioni di Dedekind dei rispettivi due insiemi, e unendo ciò alla prima osservazione si ha $(\tilde{A}, <) \sim (A, <) \sim (\mathbb{R}, <)$. \square

Per completezza, definiamo ora la struttura di campo di \mathbb{R} . Non verificheremo le proprietà, e neanche la correttezza di queste definizioni.

Definizione 8.17 (Campo ordinato). $(F, 0, 1, +, \cdot, \leq)$ è un **campo ordinato** se:

- $(F, 0, 1, +, \cdot)$ è un campo
- $(F, <)$ è un'ordine totale ⁸¹
- $\forall x, y, z \in F \ x < y \rightarrow x + z < y + z$ (**compatibilità con la somma**)
- $\forall x, y \in F (0 < x \wedge 0 < y) \rightarrow 0 < x \cdot y$ (**compatibilità con il prodotto**)

(le ultime due richieste sono le proprietà di **compatibilità** della struttura di campo [= compatibilità delle operazioni] con l'ordinamento $<$ di F).

Definizione 8.18 (Somma su \mathbb{R}). Dati $x, y \in \mathbb{R}$ definiamo la **somma di numeri reali**:

$$x + y \stackrel{\text{def}}{=} \{a + b \in \mathbb{Q} \mid a \in x \wedge b \in y\}$$

cioè la sezione di \mathbb{Q} che ha come elementi i razionali somme di elementi di x e y .

Definizione 8.19 (Prodotto su \mathbb{R}). Dati $x, y \in \mathbb{R}$ con $x > 0$ e $y > 0$ definiamo il **prodotto di numeri reali**:

$$x \cdot y \stackrel{\text{def}}{=} \{q \in \mathbb{Q} \mid q \leq 0\} \cup \{a \cdot b \in \mathbb{Q} \mid a \in x \wedge b \in y \wedge a > 0 \wedge b > 0\}$$

cioè l'unione di $\mathbb{Q}_0 \cup \{0\}$ con la sezione di \mathbb{Q} che ha come elementi i razionali prodotti di elementi **positivi** di x e y .

Definiamo quindi $-x$ tramite l'inverso additivo ed il prodotto nei casi $x < 0$, $y > 0$ etc. tramite l'uso della regola dei segni.

⁸¹Come ribadito più volte è indifferente usare $<$ o \leq .

Teorema 8.20 (Unicità di $(\mathbb{R}, 0, 1, +, \cdot, \leq)$)

\mathbb{R} dotato delle operazioni definite, è l'unico campo ordinato completo a meno di isomorfismo.

La dimostrazione di questo teorema, talvolta, si vede nei corsi di analisi 1, noi non la studieremo, Per chi fosse interessato: LIBRO DI TESTO [2], capitolo 10; NOTE DEL PROF. Di Nasso, fascicolo 4 [3]; LEZIONE 16 dell'a.a. 2020-21 [4].

§8.2 La cardinalità del continuo è 2^{\aleph_0}

Torniamo ad una questione più strettamente insiemistica.

Teorema 8.21 (Cardinalità del continuo)

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

Questo teorema ci dice, in un modo ancora diverso, che \mathbb{R} è più che numerabile - poiché $\aleph_0 < 2^{\aleph_0}$ (per Cantor) - ma, in più, caratterizza anche esattamente la cardinalità di \mathbb{R} .

Prima della dimostrazione formale, vediamo intuitivamente perché il risultato è vero. Per definizione $\mathbb{R} \subseteq \mathcal{P}(\mathbb{Q})$, quindi si immerge nelle parti, da cui $|\mathbb{R}| \leq 2^{\aleph_0}$, mentre la disegualanza da dimostrare è $2^{\aleph_0} \leq |\mathbb{R}|$. Esibiamo quindi una funzione iniettiva $\mathcal{P}(\omega) \rightarrow \mathbb{R}$ come segue:

$$f : \mathcal{P}(\omega) \rightarrow \mathbb{R} : S \mapsto 0.a_0^S a_1^S a_2^S a_3^S \dots \quad \text{con } a_i^s = \begin{cases} 0 & \text{se } i \notin S \\ 1 & \text{se } i \in S \end{cases}$$

per esempio $S = \{2, 3, 5, 7, 11, \dots\}$ dà $f(S) = 0.001101010001\dots$ è chiaro che:

$$f(S) = f(T) \stackrel{\text{def}}{\iff} \forall i \in \omega \ a_i^S = a_i^T \stackrel{\text{def}}{\iff} \forall i \in \omega \ i \in S \leftrightarrow i \in T \stackrel{\text{estensionalità}}{\iff} S = T$$

Non è difficile formalizzare questa dimostrazione⁸². Basterebbe definire $0.a_1 a_2 a_3 \dots$ come $\sum_{i=0}^{\infty} a_i 10^{-(i+1)}$, poi $\sum_{i=0}^{\infty}$ come $\sup_{n \in \omega} \sum_{i=0}^n$, 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.

§8.3 Operazioni che coinvolgono la cardinalità del continuo

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.

Osservazione 8.22 — $(2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0}$.

Dimostrazione. Basta osservare che per le proprietà delle operazioni sulla cardinalità $(2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$, e, ricordando che prodotto di numerabili è numerabile, si ottiene $2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$. \square

⁸²L'unica cosa a cui stare attenti è fissare una sola rappresentazione binaria nel caso di periodicità.

Lema 8.23 (Assorbimento della cardinalità al più continua)

Siano α, β abbreviazioni per o “finito” o \aleph_0 o 2^{\aleph_0} , allora:

$$\alpha + \beta = \alpha \cdot \beta = \max(\alpha, \beta)$$

eccetto il caso $\alpha \cdot 0 = 0 \cdot \beta = 0$.

Dimostrazione. Somme e prodotti di cardinalità finite sono finite (per il [teorema](#), e in questo caso l'enunciato del lemma è già soddisfatto perché nel caso di entrambe le cose finite ci interessa soltanto che tutte e tre le operazioni sopra diano cose finite, pertanto da ora possiamo assumere che una delle due abbreviazioni non sia finita e procedere con la dimostrazione). Supponiamo quindi $\aleph_0 \leq \beta$ e, senza perdita di generalità, $\alpha < \beta$. Abbiamo:

$$\begin{aligned} \beta &= \beta + 0 & \stackrel{\text{compatib. op. cardin.}}{\leq} & \alpha + \beta & \stackrel{\text{compatib. op. cardin. + Hp.}}{\leq} & 2\beta = \beta \\ \beta &= \beta \cdot 1 & \stackrel{\text{compatib. op. cardin.}}{\leq} & \alpha \cdot \beta & \stackrel{\text{compatib. op. cardin. + Hp.}}{\leq} & \beta^2 = \beta \end{aligned}$$

dove l'ultima uguaglianza nel prodotto vale perché $\aleph_0^2 = \aleph_0$, e $2^{\aleph_0} \leq (2^{\aleph_0})^2 \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0}$ (quindi la cosa accade per entrambi i possibili valori di β). Nel caso di 2β , si osserva che $\aleph_0 \leq 2 \cdot \aleph_0 \leq \aleph_0 \cdot \aleph_0 = \aleph_0$ e $2^{\aleph_0} \leq 2 \cdot 2^{\aleph_0} \leq 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0}$ (come al solito per le proprietà di compatibilità e dando per buone le disuguaglianze iniziali, che possono essere verificate scrivendo semplici mappe).

Pertanto si conclude l'enunciato usando Cantor-Bernstein nella serie di disuguaglianze sopra, che ci danno proprio la tesi (ricordando che avevamo scelto WLOG β come massimo). \square

Lema 8.24 ($\alpha^{\aleph_0} = 2^{\aleph_0}$)

Se $2 \leq \alpha \leq 2^{\aleph_0}$ ^a allora $\alpha^{\aleph_0} = 2^{\aleph_0}$.

^aPer la disuguaglianza di [Cantor](#) nel mezzo c'è anche \aleph_0 , dunque vale anche che $\aleph_0^{\aleph_0} = 2^{\aleph_0}$

Dimostrazione. È sufficiente osservare che:

$$2^{\aleph_0} \leq \alpha^{\aleph_0} \leq (2^{\aleph_0})^{\aleph_0} \stackrel{\text{ooss. sopra}}{=} 2^{\aleph_0}$$

dove le disuguaglianze sono semplicemente l'ipotesi + [l'osservazione sulla compatibilità](#) tra ordinamento e operazioni fra cardinalità (si conclude come al solito per [Cantor-Bernstein](#)). \square

§8.4 Sottrarre un numerabile dal continuo

Ricordiamo un'osservazione riguardo al numerabile.

Osservazione 8.25 (Numerabile - finito = numerabile) — Sia $|A| = \aleph_0$ e $B \subseteq A$ con $|B| < \aleph_0$. Allora $|A \setminus B| = \aleph_0$.

Dimostrazione. Siccome $A \setminus B \subseteq A$, per la dicotomia vista, o $|A \setminus B| = \aleph_0$ o $|A \setminus B| < \aleph_0$. Escludiamo che valga la seconda possibilità, infatti se così fosse:

$$A = B \cup (A \setminus B)$$

cioè un insieme numerabile è unione di insiemi finiti, dunque è finito - ad esempio per inclusione-esclusione $\aleph_0 = |A| = |A \cup A \setminus B| \leq |A| + |A \setminus B| = n + m \in \omega$ - che è assurdo. \square

Vale una proposizione analoga per 2^{\aleph_0} .

Lemma 8.26 (Continuo - al più numerabile = continuo)

Sia $|A| = 2^{\aleph_0}$ e $B \subseteq A$ con $|B| \leq \aleph_0$, allora $|A \setminus B| = 2^{\aleph_0}$.

Nota 8.27 (Continuo - al più continuo (escluso) = continuo) — Il lemma varrebbe anche rimpiazzando $|B| \leq \aleph_0$ con $|B| < 2^{\aleph_0}$, però, per ora, possiamo dimostrare solo l'asserto più debole sopra.

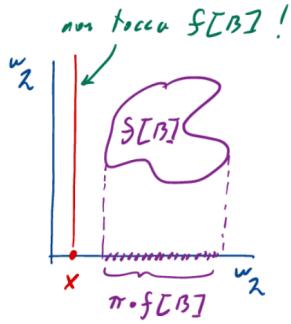
Dimostrazione. Chiaramente $A \setminus B \subseteq A \implies |A \setminus B| \leq |A| = 2^{\aleph_0}$, basta quindi dimostrare la diseguaglianza opposta. Siccome $2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0}$, esiste una bigezione:

$$f : A \rightarrow {}^\omega 2 \times {}^\omega 2$$

sia $\pi : {}^\omega 2 \times {}^\omega 2 \rightarrow {}^\omega 2 : (x, y) \mapsto x$ - è surgettiva ma non iniettiva. Siccome B è al più numerabile, per un esercizio visto:

$$|f[B]| \leq |B| \leq \aleph_0 < 2^{\aleph_0}$$

in particolare $|f[B]| = |B|$ perché f bigezione, inoltre, essendo $f[B]$ al più numerabile e π surgettiva, $|\pi[f[B]]| \leq |f[B]|$ - come visto nell'[esercizio⁸³](#).



Quindi, in particolare $\pi \circ f[B] \neq {}^\omega 2$. Possiamo quindi prendere $x \in {}^\omega 2 \setminus \pi \circ f[B]$. Dire che $x \notin \pi \circ f[B]$ significa che le coppie con prima componente x nel prodotto sono disgiunte da $f[B]$, cioè $(\underbrace{\{x\} \times {}^\omega 2}_{=\pi^{-1}(x)}) \cap f[B] = \emptyset$.

E nuovamente, tornando indietro ad A via f^{-1} , troviamo $f^{-1}(\{x\} \times {}^\omega 2) \cap B = \emptyset$, 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 bigettiva:

$$|f^{-1}(\{x\} \times {}^\omega 2)| \stackrel{f \text{ bigett.}}{=} |\{x\} \times {}^\omega 2| = 1 \cdot 2^{\aleph_0} = 2^{\aleph_0}$$

dunque abbiamo anche la diseguaglianza dal basso e quindi $|A \setminus B| = 2^{\aleph_0}$. \square

Siamo finitamente pronti per dimostrare che $|\mathbb{R}| = 2^{\aleph_0}$.

⁸³ $|f[B]| \leq \aleph_0$, $f[B] \xrightarrow{\pi} \pi[f[B]]$, quindi $|\pi[f[B]]| \leq \aleph_0$.

Dimostrazione. ($|\mathbb{R}| = 2^{\aleph_0}$)

Siccome $\mathbb{R} \subseteq \mathcal{P}(\mathbb{Q})$, la disegualanza $|\mathbb{R}| \leq 2^{\aleph_0}$ è immediata. Per dimostrare la disegualanza opposta definiamo:

$$A \stackrel{\text{def}}{=} \{X \in \mathcal{P}(\omega) | X \neq \emptyset \wedge |\omega \setminus X| \geq \aleph_0\}$$

ossia i sottoinsiemi di ω non vuoti e **coinfiniti**.

Intuitivamente: $X \in A$ rappresenta lo sviluppo in notazione binaria di un $x \in]0, 1[$ - $x = 0.a_1a_2a_3\dots$, $a_i = 1 \leftrightarrow i \in X$ - la condizione $X \neq \emptyset$ serve a escludere lo 0, la condizione di infinitezza a escludere l'uno periodico.⁸⁴

Ci basta dimostrare che $|A| = 2^{\aleph_0}$ e che esiste $f : A \rightarrow \mathbb{R}$ iniettiva. La prima cosa è facile, infatti gli insiemi coinfiniti si ottengono togliendo dalle parti quelli cofiniti (e il vuoto):

$$A = \mathcal{P}(\omega) \setminus (\{\emptyset\} \cup \underbrace{\{X \in \mathcal{P}(\omega) : |\omega \setminus X| < \aleph_0\}}_{=:S})$$

E l'insieme S dei sottoinsiemi di ω cofiniti è in corrispondenza biunivoca con $\mathcal{P}^{\text{fin.}}(\omega)$, semplicemente prendendo effettivamente il complementare:

$$\overline{\square} : S \rightarrow \mathcal{P}^{\text{fin.}}(\omega) : X \mapsto \overline{X} = \omega \setminus X$$

Quindi $|S| = |\mathcal{P}^{\text{fin.}}(\omega)| = \aleph_0$, e, di conseguenza $|A| = |\mathcal{P}(\omega) \setminus (\{\emptyset\} \cup S)| = 2^{\aleph_0}$, grazie al lemma precedente. Resta da costruire $f : A \rightarrow \mathbb{R}$ iniettiva.

Cominciamo col definire un ordine totale su A . Dati $X, Y \in A$ definiamo:

$$X <_A Y \stackrel{\text{def}}{=} \exists i \in \omega \underbrace{(i \cap X = i \cap Y)}_{\forall j < i \ j \in X \leftrightarrow j \in Y} \wedge \underbrace{(i \in Y \setminus X)}_{i \in Y \wedge i \notin X}$$

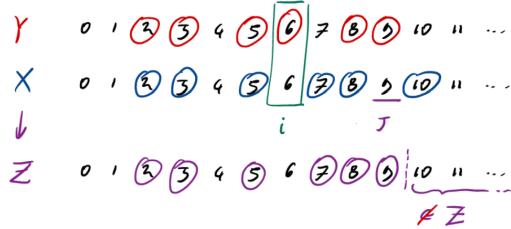
in altri termini, detto i il minimo elemento della differenza simmetrica $X \Delta Y \stackrel{\text{def}}{=} (X \setminus Y) \cup (Y \setminus X)$ - che è ben definito perché sono sottoinsiemi di ω -, se $i \in Y$ - per cui, chiaramente, $i \notin X$ - allora $X < Y$, se, invece $i \in X$ - per cui $i \notin Y$ - allora $Y < X$. La verifica che un ordine così definito è totale è immediata.

Sia $B \stackrel{\text{def}}{=} \mathcal{P}^{\text{fin.}}(\omega) \setminus \{\emptyset\} \subseteq A$, chiaramente $|B| = \aleph_0$, dimostriamo che B è denso in A - cioè i sottoinsiemi finiti di ω sono densi in quelli coinfiniti.

Dati $X, Y \in A$, con $X < Y$, e, per definizione, sia $i := \min X \Delta Y$, consideriamo $j := \min\{x \in \omega | x > i \wedge x \notin X\}$ - dove l'insieme è non vuoto in quanto X è coinfinito. Ora, dato l'insieme finito $Z := (X \cap j) \cup \{j\}$, verifichiamo che $X < Z < Y$, in questo modo abbiamo che B è denso in A . **Di fatto,abbiamo mantenuto l'intersezione comune tra X e Z fino a j , dopodiché $j \in Z \wedge j \notin Z$,** per cui $X < Z$. Analogamente, avendo preso $j > i$ e gli stessi elementi di X fino a j , accade che $i = \min Z \Delta Y$, per cui $Z < Y$.

⁸⁴Cioè codificando un sottoinsieme di ω con una stringa binaria, un insieme che da un certo punto in poi prende tutti i naturali è una stringa binaria con tutti 1 da un certo punto, e quindi il corrispondente numero $0.a_1a_2\dots$ ad un certo punto ha un 1 periodico - e questa cosa è problematica perché ad esempio $0,1 = 0,01111\dots$, e ciò fa perdere l'iniettività alla mappa che vogliamo costruire. Tuttavia, imponendo che il sottoinsieme sia coinfinito, abbiamo o che è finito (e quindi da un certo punto in poi c'è 0 definitivamente), oppure è infinito, ma nel contempo ha infiniti punti che non stanno in lui, quindi la stringa non può avere un 1 periodico.

⁸⁵Cioè gli elementi più piccoli di i sono nell'intersezione di X e Y , per cui i è il più piccolo elemento non comune e $X < Y$ significa che sta in Y .



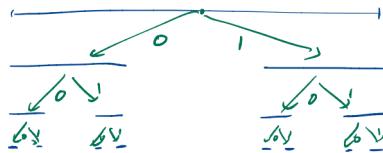
Stabilito che B è denso in A , allora, in particolare, B è denso in se stesso, dunque valgono le ipotesi del **isomorfismo di Cantor** e quindi c'è $g : B \rightarrow \mathbb{Q}$, isomorfismo di ordini. Ora, siccome B è denso in A , la funzione:

$$h : A \rightarrow \{\text{sezioni su } B\} : X \mapsto B_X = \{Y \in B | Y < X\}$$

è - banalmente ben definita - e iniettiva (perché strettamente crescente). Quindi la mappa $f : A \rightarrow \mathbb{R} : X \mapsto g[h(X)]$, che prende un insieme coinfinito, lo manda nella sezione di Dedekind da lui generata su B , e infine nella corrispettiva sezione su \mathbb{Q} , è una funzione - ben posta e - iniettiva da A ad \mathbb{R} , infatti è composizione di due mappe iniettive. \square

§8.5 (*) Alternativa per la cardinalità di \mathbb{R}

Vediamo un modo alternativo di stimare dal basso la cardinalità di \mathbb{R} sfruttando l'insieme di Cantor. L'idea è che ad successione binaria possiamo associare un punto dell'insieme di Cantor scegliendo semplicemente il percorso sui rami dell'albero della costruzione, dopodiché - poiché intersechiamo una successione decrescente di compatti - otteniamo un insieme non vuoto da cui prendere il punto di C da far corrispondere alla sequenza binaria.



In tal modo avremo $2^{\aleph_0} = |2^\omega| \leq |C| \leq |\mathbb{R}|$.

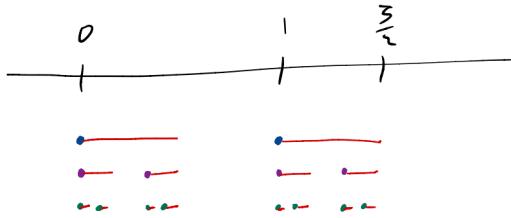
Dimostrazione. Definiamo la seguente funzione:

$$f : {}^\omega 2 \rightarrow \mathbb{R} : (a_i)_{i \in \omega} \mapsto \sum_{i=0}^{\infty} \frac{a_i}{3^i} = a_1 \cdot 3^{-1} + a_2 \cdot 3^{-2} + \dots$$

- sarebbe una scrittura in base 3 senza la cifra 2^{86} , cioè una cosa del tipo $0.01011100\dots$, dove non abbiamo problemi di ambiguità a causa di periodicità, dati da $0,1 = 0,02222\dots$, poiché abbiamo tolto il 2 e quindi usiamo solo la prima scrittura. In particolare è come elencare i punti del Cantor fatto in $[0, \frac{3}{2}]$.⁸⁷

⁸⁶Potremmo anche fare la stessa cosa buttando via 1 anziché 2, ma convenzionalmente si sceglie che è meglio avere 0.1 che 0.0222.... Potremmo altresì usare una base diversa ottenendo la stessa cosa, purché non sia due, in tal caso si procede come la prima dimostrazione vista.

⁸⁷Infatti si poteva procedere anche usando il Cantor solito e definendo la mappa da $\{0,2\}^\omega$ a \mathbb{R} , che manda una successione in $\sum_{i=1}^{\infty} \frac{a_i}{3^i} = \frac{1}{3} \sum_{i=0}^{\infty} \frac{a_i}{3^i}$, e in particolare, questa si ottiene dalla funzione precedente moltiplicata per $\frac{2}{3}$ (notare che questa cosa cambia l'insieme numerico da $\{0,1\}$ a $\{0,2\}$ e sistema l'indice per il primo termine della scrittura decimale).



Dove naturalmente la sommatoria è definita per ricorsione numerabile come funzione da $\omega \rightarrow \mathbb{R}$ nella maniera seguente:

$$\sum_{i=0}^0 \square_i = \square_0 \quad \sum_{i=0}^{n+1} \square_i = \left(\sum_{i=0}^n \square_i \right) + \square_{n+1}$$

e la serie è ben definita come:

$$\sum_{i=0}^{\infty} \square_i = \sup_{n \in \omega} \left(\sum_{i=0}^n \square_i \right)$$

Occorre quindi verificare che f è ben definita ed iniettiva.

\diamond f ben definita: cioè la serie in arrivo è un elemento di \mathbb{R} , ossia $\sup_{n \in \omega} \left(\sum_{i=0}^n \frac{a_i}{3^i} \right)$ esiste, e, come sappiamo, ciò è equivalente a chiedere che $\left\{ \sum_{i=0}^n \frac{a_i}{3^i} \right\}_{n \in \omega}$ ha un maggiorante. Vediamo per induzione che:

$$\sum_{i=0}^n \frac{a_i}{3^i} \leq \frac{3}{2} - \frac{1}{2 \cdot 3^n}$$

fatto questo il RHS si può stimare a sua volta con $\frac{3}{2}$ - sarebbe la somma della serie -, che costituisce un upper bound per ogni $n \in \omega$, quindi per tutti gli elementi dell'insieme.

$n = 0$ Banalmente $\sum_{i=0}^0 \frac{a_i}{3^i} = \frac{a_0}{3^0} = \frac{a_1}{3} \leq \frac{1}{3} < \frac{4}{3} = \frac{3}{2} - \frac{1}{2 \cdot 3^1}$.

$n \implies n+1$ Supponiamo $\sum_{i=0}^n \frac{a_i}{3^i} \leq \frac{3}{2} - \frac{1}{2 \cdot 3^n}$ e dimostriamo $\sum_{i=0}^{n+1} \frac{a_i}{3^i} \leq \frac{3}{2} - \frac{1}{2 \cdot 3^{n+1}}$.

$$\begin{aligned} \sum_{i=0}^{n+1} \frac{a_i}{3^i} &= \left(\sum_{i=0}^n \frac{a_i}{3^i} \right) + \frac{a_{n+1}}{3^{n+1}} && (\text{def. ricorsiva}) \\ &\leq \frac{3}{2} - \frac{1}{2 \cdot 3^n} + \frac{a_{n+1}}{3^{n+1}} && (\text{hp. induttiva}) \\ &\leq \frac{3}{2} - \frac{1}{2 \cdot 3^n} + \frac{1}{3^{n+1}} && (a_{n+1} \in \{0, 1\}) \\ &= \frac{3}{2} - \frac{1}{3^n} \cdot \frac{1}{6} = \frac{3}{2} - \frac{1}{2 \cdot 3^{n+1}} \end{aligned}$$

\diamond f iniettiva: date due successioni binarie distinte, $(a_i)_{i \in \omega}$ e $(b_i)_{i \in \omega}$, sia $i_0 \in \omega$ il minimo per cui $a_{i_0} \neq b_{i_0}$. Assumiamo WLOG di essere nel caso $a_{i_0} = 0$ e $b_{i_0} = 1$ e verifichiamo che $f(b) > f(a)$ - stiamo proprio verificando la stretta crescenza. In particolare dimostriamo che:

$$f(a) < f(a) + \frac{1}{2 \cdot 3^{i_0}} \leq f(b)$$

Per verificare la seconda disuguaglianza osserviamo che:

$$\begin{aligned}
 f(a) &= \sup_{n \in \omega} \left(\sum_{i=0}^n \frac{a_i}{3^i} \right) \\
 &= \sup_{n \in \omega} \left(\sum_{i < i_0} \frac{a_i}{3^i} + \sum_{i=i_0+1}^n \frac{a_i}{3^i} \right) && (a_{i_0+1} = 0) \\
 &= \sup_{n \in \omega} \left(\sum_{i < i_0} \frac{b_i}{3^i} + \sum_{i=i_0+1}^n \frac{a_i}{3^i} \right) && (\forall i < i_0 \ a_i = b_i) \\
 &= \sup_{n \in \omega} \left(\sum_{i < i_0} \frac{b_i}{3^i} + \frac{1}{3^{i_0+1}} \sum_{j=0}^{n-i_0-1} \frac{a_{j+i_0+1}}{3^j} \right) && (j = i - i_0 - 1) \\
 &\leq \sup_{n \in \omega} \left(\sum_{i < i_0} \frac{b_i}{3^i} + \frac{1}{3^{i_0+1}} \cdot \frac{3}{2} \right) && (\text{dalla stima sopra}) \\
 &= \sum_{i < i_0} \frac{b_i}{3^i} + \frac{1}{2 \cdot 3^{i_0}}
 \end{aligned}$$

Ora, dato che:

$$f(b) \geq \sum_{i < i_0} \frac{b_i}{3^i} + \frac{1}{3^{i_0}} \implies \sum_{i < i_0} \frac{b_i}{3^i} \leq f(b) - \frac{1}{3^{i_0}} \quad (b_{i_0} = 1)$$

possiamo concludere la stima sopra:

$$f(a) \leq \sum_{i < i_0} \frac{b_i}{3^i} + \frac{1}{2 \cdot 3^{i_0}} \leq f(b) - \frac{1}{3^{i_0}} + \frac{1}{2 \cdot 3^{i_0}} = f(b) - \frac{1}{2 \cdot 3^{i_0}}$$

che è equivalentemente alla seconda disuguaglianza voluta.

□

§8.6 (*) $(F, 0, 1, +, \cdot, \leq)$

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 [all'interno della teoria che stiamo costruendo]:

$$\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \dots\}$$

$$\{\omega, s(\omega), s(s(\omega)), s(s(s(\omega))), \dots\}$$

Però gli assiomi 1-7 non bastano 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 solo 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 farebbe comodo escludere l'esistenza di qualcosa del tipo $Y = \{\{\{\{\dots\}\}\}\}$ 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 identificabile dalla sua struttura**. Mi spiego, per esempio \emptyset è identificato dal fatto di non avere elementi, $\{\emptyset\}$ è identificato dal fatto di avere un solo elemento che non ha elementi etc. 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.

§9 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.

Teorema 9.1 (Tutti i buoni ordini sono “totalmente ordinati” fra loro)

Siano $(A, <_A)$ e $(B, <_B)$ ^a 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 di $(A, <_A)$

^aNel seguito scriveremo semplicemente $(A, <)$ e $(B, <)$ per comodità.

Di fatto stiamo creando un'ordinamento totale tra buoni ordini con questo teorema, se definiamo:

$$(A, <_A) \prec (B, <_B) \stackrel{\text{def}}{=} \exists C \text{ segmento iniziale proprio di } (B, <_B) \text{ e } (A, <_A) \sim C$$

allora \prec soddisfa le **proprietà formali di un ordinamento totale fra le classi di isomorfismo di buoni ordini**. Definiamo altresì l'ordine largo associato:

$$(A, <_A) \preceq (B, <_B) \stackrel{\text{def}}{=} ((A, <_A) \prec (B, <_B)) \vee ((A, <_A) \sim (B, <_B))$$

ossia “ $(A, <_A)$ è isomorfo a un segmento iniziale [proprio o meno] di $(B, <_B)$ ”. Richiamiamo le definizioni fondamentali.

Definizione 9.2 (Buon ordinamento). $(A, <)$ è un **buon ordinamento** se ogni $B \subseteq A$ non vuoto ha un minimo elemento.

Definizione 9.3 (Segmento iniziale). Dato un ordine totale $(A, <)$, $B \subseteq A$ è un **segmento iniziale** se [assorbe gli elementi più piccoli] $\forall b \in B \forall x \in A \ x < b \rightarrow x \in B$.

Definizione 9.4 (Segmenti iniziali propri e principali). Il segmento iniziale B è **proprio** se $B \neq A$. Il segmento iniziale B è **principale** se è della forma:

$$B = A_a \stackrel{\text{def}}{=} \{x \in A \mid x < a\}$$

per qualche $a \in A$, e, in questo caso, si dice che è un **segmento iniziale principale determinato da a** .

È chiaro che un segmento iniziale principale, A_a , è **sempre** proprio, perché $a \notin A_a$, e nel caso dei buoni ordini questa è una doppia implicazione (quindi se è proprio è anche principale).

Proposizione 9.5 (proprio \implies principale nei buoni ordini)

Ogni segmento iniziale proprio di un buon ordine è principale.

Dimostrazione. Sia $(A, <)$ ben ordinato e $I \subsetneq A$ un segmento iniziale proprio. Consideriamo $a := \min_{<} (A \setminus I)$ (per l'ipotesi di buon ordinamento il minimo c'è). Allora $I = A_a$ (ovvero il nostro segmento iniziale proprio è principale determinato da a).

Verifiche: vediamo i due contenimenti, $x \in A_a \stackrel{\text{def}}{\implies} x < a \stackrel{a \text{ min. in } A \setminus I}{\implies} x \notin A \setminus I \implies x \in I$ (cioè se $x < a$, poiché a è il minimo che sta nel complementare di I rispetto ad A , x che è più piccolo non può soddisfare la proprietà e quindi non sta nel complementare aka sta in I), dunque $A_a \subseteq I$.

Viceversa, supponiamo per assurdo $x \in I$ e $x \notin A_a$, la seconda equivale ad $a \leq x$ (per definizione di segmento iniziale principale), ma allora, siccome $x \in I$, per definizione di segmento iniziale $a \in I$, ma per definizione a era il minimo in $A \setminus I \implies$ non poteva essere in I , dunque assurdo, quindi $x \in I \implies x \in A_a$, da cui $I \subseteq A_a$. \square

Esercizio 9.6 (Buon ordine \iff (proprio \implies principale)). 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 bene ordinato da $<$.

Soluzione. La proposizione appena vista ci fornisce già \implies , dunque non ci resta che dimostrare la freccia opposta, ovvero se vale la proposizione su un ordine totale $(A, <)$, allora questo è un buon ordine. Sia $B \subseteq A$, $B \neq \emptyset$, vogliamo vedere che ha un minimo, $\forall x \in B$ sia B_x il segmento iniziale principale determinato da un elemento di B , consideriamo:

$$\bigcap_{x \in B} B_x$$

osserviamo che l'intersezione di segmenti iniziali è ancora un segmento iniziale [ogni x nell'intersezione sta in tutti i segmenti iniziali, quindi vale la solita proprietà], inoltre, tale segmento iniziale è necessariamente proprio (infatti, se ci sono almeno due elementi in B l'intersezione dei segmenti iniziali principali taglia fuori l'elemento più grande), dunque per ipotesi, l'intersezione è un segmento iniziale principale. Sia $m \in B$ l'elemento tale che:

$$B_m = \{x \in B \mid x < m\} = \bigcap_{x \in B} B_x$$

verifichiamo che m è il minimo di B (ciò significherebbe che $B_m = \emptyset$). Supponiamo per assurdo che esista $y < m$, ovvero $y \in B_m = \bigcap_{x \in B} B_x$, ciò equivale a $y < x$, $\forall x \in B$, compreso y stesso, si ottiene cioè $y < y \not\in$. Dunque m è il minimo e $B_m = \emptyset$. \square

Osservazione 9.7 (Finto buon ordine) — In \mathbb{Z} ogni segmento iniziale proprio è principale, come accade in ω , tuttavia \mathbb{Z} non è buon ordine. Ciò apparentemente contraddirebbe quanto appena dimostrato, tuttavia non è così, infatti, come visto nella dimostrazione sopra il vuoto è un segmento iniziale proprio, che in ω è principale (e corrisponde a ω_0), mentre in \mathbb{Z} non c'è un elemento che lo determini come segmento iniziale principale (pur essendo proprio), da ciò si vede che l'implicazione proprio \implies principale, non si verifica in \mathbb{Z} , che quindi non è un buon ordine, come già sapevamo.

Lema 9.8 (Le funzioni crescenti di un buon ordine stanno sopra la diagonale)

Sia $(A, <)$ un buon ordinamento e $f : A \rightarrow A$ una funzione **strettamente** crescente - $\forall x, y \in A \ x < y \rightarrow f(x) < f(y)$ -, allora $\forall x \in A \ x \leq f(x)$.^a

^aQuesto risultato vale in maniera analoga per classi ben ordinate.

Dimostrazione. Per assurdo, assumiamo la negazione della tesi, $\exists x \in A \ x > f(x)$. Quindi l'insieme $B = \{x \in A | f(x) < x\}$ non è vuoto. Sia $k := \min B$. Allora $f(k) < k$ (perché elemento di B), e, siccome f è crescente $f(f(k)) < f(k)$, per cui $f(k) \in B$ a sua volta (è strettamente più grande della sua immagine), e, ricordando che per ipotesi $f(k) < k$, contraddice la minimalità di k e ci dà un assurdo. \square

Corollario 9.9 (Proprietà degli isomorfismi tra buoni ordinamenti)

Valgono le seguenti:

- (1) Un buon ordinamento **non** è isomorfo a un suo segmento iniziale proprio. (**irriflessività**).
- (2) L'identità è il solo isomorfismo fra un buon ordinamento e se stesso.
- (3) Se $(A, <)$ e $(B, <)$ ^a sono buoni ordini isomorfi allora esiste un unico isomorfismo fra di essi.

^aRicordare che quelli sono $<_A$ e $<_B$.

Dimostrazione. Dimostriamo singolarmente gli enunciati:

- (1) Supponiamo che $(A, <)$ sia isomorfo al suo segmento iniziale proprio A_a , ordinato - si intende - dalla restrizione di $<$, e sia $f : A \rightarrow A_a$ un isomorfismo. Allora f è crescente per definizione di isomorfismo. Tuttavia $f(a) < a$, poiché in arrivo $f(a) \in A_a$, contraddicendo il lemma sopra, quindi abbiamo un assurdo.
- (2) Sia $f : A \rightarrow A$ un automorfismo del buon ordine $(A, <)$, dobbiamo dimostrare che $f = \text{id}_A$. Se così non fosse, ci sarebbe almeno un $x \in A$ tale che $f(x) \neq x$. Se $f(x) < x$ stiamo contraddicendo il lemma perché f deve essere crescente (in quanto isomorfismo di ordini). Se $x < f(x)$, vale la stessa considerazione di prima con f^{-1} , e quindi di nuovo un assurdo.
- (3) Se $f : A \rightarrow B$ e $g : B \rightarrow C$ fossero due isomorfismi diversi, allora $g^{-1} \circ f : A \rightarrow C$ sarebbe un automorfismo di A diverso dall'identità, contraddicendo il punto (2).

\square

Osservazione 9.10 (Transitività della “relazione d’ordine” tra buoni ordini) — Siano $(A, <)$, $(B, <)$, $(C, <)$ buoni ordinamenti, allora:

$$(A, <) \preceq (B, <) \wedge (B, <) \preceq (C, <) \rightarrow (A, <) \preceq (C, <)$$

Dimostrazione. Siano $f : A \rightarrow B$ e $g : B \rightarrow C$ isomorfismi fra A e un segmento iniziale di B e fra B e un segmento iniziale di C rispettivamente. Dimostriamo che $g \circ f : A \rightarrow C$ è un isomorfismo fra A e un segmento iniziale di C . Naturalmente $g \circ f$ è crescente in

quanto composizione di funzioni crescenti, dunque occorre solo verificare che $g \circ f[A]$ è un segmento iniziale di C .

Verifica: sia $g(f(a))$ un qualunque elemento di $g \circ f[A]$, e sia $x \in C$ tale che $x < g(f(a))$, dobbiamo verificare, per avere la definizione di segmento iniziale, che $x \in g \circ f[A]$. Naturalmente $g(f(a)) \in g[B]$ e per ipotesi $g[B]$ è segmento iniziale di C , quindi $x \in g[B]$ e possiamo scrivere $x = g(y)$. Ora, siccome g è un isomorfismo, da $x < g(f(a))$ deduciamo $y < f(a)$, inoltre per ipotesi $f[A]$ è un segmento iniziale di B , pertanto $y \in f[A]$, ovvero $y = f(z)$ per $z \in A$. Abbiamo quindi $x = g(f(z)) \in g \circ f[A]$. \square

Osservazione 9.11 (Antisimmetria della “relazione d’ordine” sui buoni ordini) — Siano $(A, <)$ e $(B, <)$ buoni ordini, allora:

$$(A, <) \preceq (B, <) \wedge (B, <) \preceq (A, <) \rightarrow (A, <) \sim (B, <)$$

dunque vale la proprietà antisimmetrica.^a

^aI buoni ordini sono una classe, non un’insieme, dunque la relazione \preceq (o \prec), volendo, è una relazione d’ordine su una classe, non su un insieme.

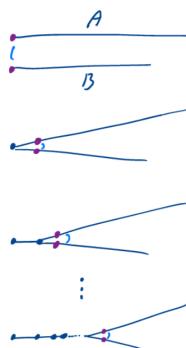
Dimostrazione. Siano $f : A \rightarrow B$ e $g : B \rightarrow A$ isomorfismi fra A e un segmento iniziale di B e fra B e un segmento iniziale di A . Ricordando la dimostrazione dell’osservazione precedente, $g \circ f$ è un isomorfismo fra A e un segmento iniziale $g \circ f[A]$ di A , ma per l’(1) del corollario $g \circ f[A]$ non può essere un segmento iniziale proprio di A , quindi deve essere proprio tutto A , $g \circ f[A] = A$. segue quindi, per il (2) del medesimo corollario, che $g \circ f = \text{id}_A$. Ragionando simmetricamente si ottiene $f \circ g = \text{id}_B$, pertanto f è proprio un isomorfismo fra A e B con inversa g , da cui $(A, <) \sim (B, <)$. \square

Possiamo finalmente passare alla dimostrazione d’ordine del teorema.

Teorema 9.12 (Totalità della “relazione d’ordine” sui buoni ordini)

Siano $(A, <)$ e $(B, <)$ insiemi ben ordinati, allora vale **una e una sola** delle seguenti:

$$(A, <) \prec (B, <) \quad (A, <) \sim (B, <) \quad (B, <) \prec (A, <)$$



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 , etc. 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 il procedimento? Solo se, ad un certo punto, abbiamo identificato interamente uno dei due insiemi, con un segmento iniziale dell’altro - perché 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.

Questa 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 permetterebbero di numerare i passaggi della costruzione, gli **ordinali**, sono appunto l’oggetto che stiamo tentando di costruire.

Dimostrazione. Per il corollario visto prima, si può verificare al più una delle tre condizioni, altrimenti avremmo un assurdo, verifichiamo dunque che se ne verifichi almeno una. Consideriamo f definita come segue:

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

Vogliamo dimostrare che f è una funzione crescente, che $\text{Dom}(f)$ è un segmento iniziale di A , e che $\text{Im}(f)$ è un segmento iniziale di B , da cui f manda segmenti iniziali in segmenti iniziali. Quindi f è un isomorfismo fra un segmento iniziale di A e uno di B . Infine dimostriamo che necessariamente $\text{Dom}(f) = A$ o $\text{Im}(f) = B$, e questo conclude la dimostrazione perché se si verifica una delle due o tutte e due, abbiamo ottenuto la tesi del teorema. Procediamo ora con tutte le verifiche.

f è una funzione Supponiamo per assurdo $(a, b) \in f$ e $(a, b') \in f$ con $b \neq b'$. Senza perdita di generalità supponiamo $b < b'$ (quindi B_b s.i. proprio di $B_{b'}$), e, per la definizione data di f ciò corrisponde a:

$$B_b \sim A_a \sim B_{b'}$$

dunque $B_{b'}$ sarebbe isomorfo al suo segmento iniziale proprio B_b \sharp .

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:

$$A_{a'} \sim B_{f(a')} \preceq B_{f(a)} \sim A_a$$

dove i due isomorfismi, vengono semplicemente dalla definizione di f , e $B_{f(a')} \preceq B_{f(a)}$ segue da $B_{f(a')} \subseteq B_{f(a)}$, che vale perché stiamo supponendo $f(a') \leq f(a)$ per ipotesi assurda. Abbiamo quindi ottenuto che $A_{a'} \preceq A_a$, ovvero $A_{a'} \subseteq A_a \implies a' \leq a$, che è assurdo perché avevamo per ipotesi $a < a'$.

$\text{Dom}(f)$ è s.i. di A Sia $a \in \text{Dom}(f)$ e $a' < a$, vogliamo dimostrare che $a' \in \text{Dom}(f)$. L'ipotesi $a \in \text{Dom}(f)$ equivale a dire che $A_a \sim B_b$, per qualche $b \in B$, inoltre, essendo $a' < a$ si ha $A_{a'} \subsetneq A_a \rightarrow A_{a'} \prec A_a$, per cui $A_{a'} \prec B_b$. A questo punto esiste $b' \in B_b \subsetneq B$ tale che $A_{a'} \sim (B_b)_{b'}$, per definizione di \prec , e, osservando che $(B_b)_{b'} = B_{b'}$, si ha proprio $A_{a'} \sim B_{b'} \implies (a', b') \in f$, per cui $a' \in \text{Dom}(f)$.

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

**$\text{Dom}(f) = A$
o $\text{Im}(f) = B$** Se così non fosse, per la terza e quarta verifica, avremmo contemporaneamente

$\text{Dom}(f) = A_a$ e $\text{Im}(f) = B_b$ ⁸⁸, per opportuni $a \in A$ e $b \in B$. Per la seconda verifica f è crescente, quindi è un isomorfismo fra $\text{Dom}(f) = A_a$ e $\text{Im}(f) = B_b$, pertanto, si ottiene proprio $A_a \sim B_b$, e quindi, per definizione di f , $(a, b) \in f$, da cui $a \in \text{Dom}(f) = A_a \sharp$ (oppure $b \in \text{Im}(f) = B_b \sharp$). Segue quindi che almeno una delle due condizioni è sempre vera.

□

Esercizio 9.13 (Sottoinsiemi propri e buoni ordinamenti). Sia $(A, <)$ un buon ordine e sia $B \subsetneq A$. Dimostra che $B \preceq A$, ma non necessariamente $B \prec A$.

⁸⁸Stiamo negando un OR quindi l'unica possibilità è che siano entrambe false.

Soluzione. In primis osserviamo che non può valere $A \prec B$, infatti, se A fosse isomorfo ad un segmento iniziale proprio di B , sia B_b , per $b \in B$, allora $b \leq f(b)^{89} \in B_b \implies b \leq f(b) < b \notin$. Per il teorema appena dimostrato sappiamo che la classe dei buoni ordini è totalmente ordinata, per cui vale necessariamente $B \preceq A$.

Per avere un controsenso di $B \subsetneq A \not\Rightarrow B \prec A$ ci basta considerare $(\omega, <)$ e il sottoinsieme proprio 2ω dei numeri pari, in questo caso infatti abbiamo $(2\omega, <|_{2\omega}) \sim (\omega, <)$, che è dato dalla funzione che mappa $i \mapsto n_i$ (l' i -esimo numero pari preso in ordine strettamente crescente). \square

Esercizio 9.14 (Unione di buoni ordinamenti). Sia $(A, <_A)$ un ordine totale con $A = \bigcup S$. Supponiamo che:

1. ogni $X \in S$ è un buon ordine con la restrizione $<_{A|X}$
2. per ogni $X, Y \in S$, o X è segmento iniziale di Y o Y è segmento iniziale di X

Dimostra che allora $(A, <_A)$ è un buon ordine. Esibisci inoltre un controsenso alla tesi eliminando la condizione 2 dalle ipotesi.

Soluzione. Dato $B \subseteq A$ diverso dal vuoto, allora, detto $Z = \{X \in S \mid X \cap B \neq \emptyset\}$, possiamo considerare $\bigcap Z$ ed osservare che $\bigcap Z = X \in Z$, infatti, se per assurdo ci fosse almeno un elemento di un altro insieme, $y \in \bigcap Z$, con $y \in Y \in S \wedge y \notin X$, allora, essendo che per ipotesi o X è segmento iniziale di Y o viceversa, si ha: nel primo caso y non può stare nell'intersezione perché non appartiene ad X , per cui abbiamo un assurdo, nel secondo - se Y segmento iniziale di X - avremmo che $y \in X$ e quindi ancora un assurdo. Abbiamo quindi che $\emptyset \neq \bigcap Z = X \in Z$, per cui $X \cap B \neq \emptyset$, ed è ben definito $b = \min_{<_{A|X}}(X \cap B) = \min_{<_{A|X}}(\bigcap Z \cap B)$.

Non resta che osservare che b è il minimo anche per gli elementi di $B \setminus X$. Dato $b' \in B \setminus X$, allora $b' \in Y \in Z$, con $Y \neq X$, osserviamo ora che X è segmento iniziale di Y (deve valere una delle due cose per ipotesi, ed essendo $X = \bigcap Z \subseteq Y$, siamo necessariamente in questo caso), per cui $X = Y_c$ (siamo in un buon ordinamento), per qualche $c \in Y$, e in particolare si ha proprio $b < c \leq b'$, infatti la prima disegualanza è banale, mentre la seconda deriva dal fatto che $b' \in B \setminus X$ e per la proprietà dei segmenti iniziali se fosse $b' < c$ allora $b' \in Y_c = X$ che è assurdo.

Per il controsenso alla tesi nel caso in cui manchi la seconda condizione, consideriamo l'insieme $\mathbb{Q} = \{q_n \mid n \in \omega\}$ di cui abbiamo fissato un'enumerazione, detto $Q_n = \{q_i \mid i < n\}$, naturalmente si ha:

$$\mathbb{Q} = \bigcup_{n \in \omega} Q_n$$

dove $(\mathbb{Q}, <)$ è totalmente ordinato e i $(Q_n, <|_{Q_n})$ sono bene ordinati dalla restrizione dell'ordinamento di \mathbb{Q} essendo insiemi finiti, inoltre non è vero che presi Q_n e Q_m uno non è necessariamente segmento iniziale dell'altro, perché nell'enumerazione possiamo (e necessariamente dovrà accadere) aggiungere anche elementi più piccoli. Siamo pertanto nelle condizioni dell'esercizio tranne che per 2., e quindi naturalmente non si ottiene che $(\mathbb{Q}, <)$ è bene ordinato. \square

⁸⁹Notare che la disegualanza continua a valere solo perché $B \subseteq A$, in generale se i buoni ordinamenti sono diversi non vale.

§9.1 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 versatili di quelli ottenibili con queste operazioni.

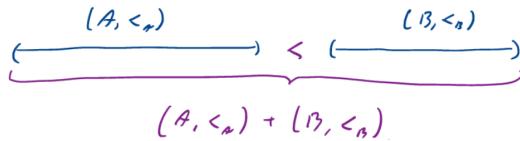
Definizione 9.15 (Somma di ordini totali). Dati $(A, <_A)$ e $(B, <_B)$ ordini totali. Definiamo la **somma di ordini totali** come:

$$(A, <_A) + (B, <_B) \stackrel{\text{def}}{=} (A \sqcup B, <_+)$$

dove, ricordiamo che $A \sqcup B = (A \times \{0\}) \cup (B \times \{1\})$, e $<_+$ è definito da:

$$\begin{aligned} (x, y) <_+ (x', y') &\stackrel{\text{def}}{=} (y = 0 \wedge y' = 1) \\ &\vee (y = 0 \wedge y' = 0 \wedge x <_A x') \\ &\vee (y = 1 \wedge y' = 1 \wedge x <_B x') \end{aligned}$$

L'idea è che $(A, <_A) + (B, <_B)$ si ottiene attaccando $(B, <_B)$ in coda a $(A, <_A)$.



Riproponiamo, per completezza, la definizione di prodotto lessicografico.

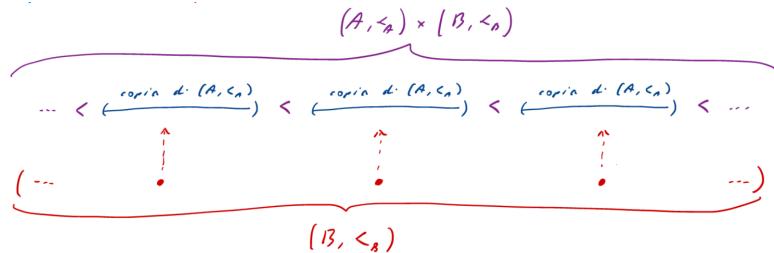
Definizione 9.16 (Prodotto di lessicografico). Siano $(A, <_A)$ e $(B, <_B)$ ordini totali. Definiamo il **prodotto del lessicografico**:

$$(A, <_A) \cdot (B, <_B) \stackrel{\text{def}}{=} (A \times B, <_\times)$$

dove $<_\times$ è definito da:

$$(x, y) <_\times (x', y') \stackrel{\text{def}}{=} (y <_B y') \vee (y = y' \wedge x <_A x')$$

L'idea di confrontare prima la seconda componente, deriva dal fatto che $(A, <_A) \cdot (B, <_B)$ sono tante copie di $(A, <_A)$ giustapposte, quanti sono gli elementi di B (e quindi associate nello stesso ordine).



Per definire l'esponentiale ci serve la nozione di supporto.

Definizione 9.17 (Supporto di una funzione da un insieme a un buon ordine). Dato un buon ordine $(B, <)$ e $f : A \rightarrow B$, il **supporto** di f è:

$$\text{supp}_B(f) \stackrel{\text{def}}{=} \{x \in A | f(x) \neq \min_{<_B} B\}$$

(mitteremo il pedice B quando è chiaro cosa sia B).

Il supporto è quindi il sottoinsieme dei punti sull'insieme di partenza, sui quali f non assume il minimo del buon ordinamento in arrivo quest'ultimo.

Definizione 9.18 (Esponenziali di ordini totali). Dati $(A, <_A)$ e $(B, <_B)$ ordini totali, definiamo l'**esponenziale di ordini totali**:

$$(A, <_A)^{(B, <_B)} \stackrel{\text{def}}{=} (\{f \in {}^B A : |\text{supp}_A f| < \aleph_0\}, <_{\exp})$$

dove l'insieme è quello delle funzioni a supporto finito (quindi che su un numero finito di punti non assumono il valore $\min_{<_B} B$), e l'ordine $<_{\exp}$ è definito da:

$$f <_{\exp} g \stackrel{\text{def}}{=} (f \neq g) \wedge (f(m) <_A g(m))$$

dove m è il massimo valore in B su cui f e g sono diverse, cioè non sono entrambe $\min A$, $m := \max_{<_B} \{x \in B | f(x) \neq g(x)\}$.

L'idea è che una funzione $B \rightarrow A$ può essere vista come una specie di tupla con tante componenti quanti sono gli elementi di B^{90} . Ordinare queste tuple lessicograficamente significa (generalizzando l'idea usata per il prodotto lessicografico) che vince la componente diversa più a destra, e se definitivamente c'è il minimo in entrambe le tuple, per la finitezza del supporto, basta confrontare l'ultima componente dove sono diverse, ossia la componente corrispondente all'elemento di B più grande su cui le funzioni sono diverse.

Esercizio 9.19. Verificare che $(\omega, <)^{(\omega, <)} \sim (\mathbb{N}[x], \prec)$, dove $\mathbb{N}[x]$ denota l'insieme dei polinomi a coefficienti in \mathbb{N} , e definiamo:

$$p \prec q \stackrel{\text{def}}{=} \exists N \in \mathbb{N} \forall x \in \mathbb{N} x > N \rightarrow p(x) < q(x)$$

ossia $p \prec q$ se $p(x) < q(x)$ definitivamente.

Soluzione. Possiamo scrivere esplicitamente l'isomorfismo come segue:

$$(\omega, <)^{(\omega, <)} \rightarrow (\mathbb{N}[x], \prec) : f \mapsto \sum_{i=0}^{\infty} f(i)x^i$$

osserviamo in primis che la sommatoria è in realtà una somma di un numero finito di termini in quanto f ha supporto finito, dunque ciò che otteniamo è un polinomio e quindi la mappa è ben definita. Si vede facilmente che è surgettiva, infatti, dato $p(x) = \sum_{i=0}^n a_i x^i$, è sufficiente considerare:

$$f : \omega \rightarrow \omega : i \mapsto \begin{cases} a_i & \text{se } 0 \leq i \leq n \\ 0 & \text{altrimenti} \end{cases}$$

che è naturalmente una funzione a supporto finito dai naturali ai naturali. Infine, verifichiamo la stretta crescenza, date $f < g$, abbiamo $f(m) < g(m)$, per m massimo valore in ω per cui sono distinte; si danno due casi, o $f(m) = 0$ e quindi $g(m) > 0$, in questo caso a g corrisponde un polinomio $q(x)$ di grado più grande strettamente, dunque,

⁹⁰D'altronde abbiamo visto che $|{}^B A| = |A|^{|B|}$, il che ci fa notare che la definizione data di insieme di funzioni come una sorta di esponenziazione di un insieme ad un altro, è coerente con quella di esponenziazione come prodotto cartesiano ripetuto un numero di volte pari alla cardinalità dell'esponente, da qui l'identificazione di ${}^B A$ con $\underbrace{A \times \dots \times A}_{|B| \text{ volte}}$, che ci dà l'intuizione descritta (e che formalmente si traduce nell'insieme di funzioni, che sarà poi la vera definizione di prodotto cartesiano).

se f corrisponde a $p(x)$, si ha $q(x) = o(p(x))$ per $x \rightarrow +\infty$, per cui $\lim_{x \rightarrow +\infty} \frac{q(x)}{p(x)} = +\infty$, che equivale alla definizione data di $p \prec q$. Nel caso in cui $f(m) > 0$, allora $p(x)$ e $q(x)$ sono polinomi dello stesso grado, ma $q(x)$ ha coefficiente di testa maggiore strettamente di quello di $p(x)$, per cui $\lim_{x \rightarrow +\infty} \frac{q(x)}{p(x)} > 0 \implies p \prec q$. \square

Proposizione 9.20 (Somma, prodotto ed esponenziale di buoni ordini è un buon ordine)

Se $(A, <_A)$ e $(B, <_B)$ sono buoni ordini, allora anche:

$$(A, <_A) + (B, <_B) \quad (A, <_A) \cdot (B, <_B) \quad (A, <_A)^{(B, <_B)}$$

sono buoni ordini.

Dimostrazione. Si tratta di banali verifiche, **eccetto la terza**.

La relazione $<_{\exp}$ è irriflessiva per definizione richiede $f \neq g$, dunque se sono uguali non sono in relazione. Occorre quindi verificare la transitività. Assumiamo $f <_{\exp} g$ e $g <_{\exp} h$, dove naturalmente $f, g, h \in {}^B A$, e poniamo:

$$\begin{aligned} m_1 &= \max_{<_B} \{x \in B \mid f(x) \neq g(x)\} \\ m_2 &= \max_{<_B} \{x \in B \mid g(x) \neq h(x)\} \\ m_3 &= \max_{<_B} \{x \in B \mid f(x) \neq h(x)\} \end{aligned}$$

detto $m := \max(m_1, m_2)$, abbiamo $f(m) \leq_A g(m) \leq_A h(m)$, dove la prima disegualanza è stretta se $m = m_1$, e la seconda lo è se $m = m_2$, in ogni caso, almeno una delle due disegualanze è sempre stretta per cui abbiamo $f(m) <_A h(m)$. Osserviamo inoltre che se $x > m$ allora necessariamente $f(x) = g(x) = h(x)$ perché avremmo in questo caso che $x > m_1, m_2$, che sono i massimi su cui si hanno le disegualanze, per cui $m = m_3$.

Mostriamo ora che $<_{\exp}$ è un ordine totale, se $f \neq g$ allora è ben definito $m := \max_{<_B} \{x \in B \mid f(x) \neq g(x)\}$, infatti le funzioni sono a supporto finito per ipotesi dunque stiamo prendendo il massimo su un insieme finito e non vuoto essendo le funzioni diverse, si conclude per la totalità di $<_A$ che vale necessariamente o $f(m) <_A g(m)$ o $g(m) <_A f(m)$, nel primo caso $f <_{\exp} g$, nel secondo $g <_{\exp} f$.

Resta da verificare che l'ordine ottenuto esponenziando è buono. Chiamiamo S l'insieme delle funzioni a supporto finito da B ad A e supponiamo per assurdo che non sia bene ordinato, cioè:

$$\exists f \in S \underbrace{\exists A \subseteq S (f \in A \wedge \forall g \in A \exists h \in A h <_{\exp} g)}_{\text{c'è un } A \subseteq S \text{ non vuoto}} \underbrace{\text{che non ha minimo}}$$

Da quanto appena scritto possiamo fissare una $f \in S$ tale che $\exists A \subseteq S$ etc. con queste proprietà: che il massimo del suo supporto sia il minimo possibile, $m := \max_{<_B} (\text{supp}_A(f))$, e che, a parità di m , il valore di $f(m)$ sia minimo. Fissata f come scritto, possiamo fissare ora anche A nella formula in modo tale che $f \in A$ ed A sia un sottoinsieme senza minimo. Il nostro obiettivo ora è costruire $\tilde{A} \subseteq S$ che non abbia minimo e contenga una funzione \tilde{f} con $\tilde{m} := \max_{<_B} (\text{supp}_A(f)) <_B m$, in questo modo neghiamo la minimalità di m ed otteniamo la contraddizione voluta. Osserviamo innanzitutto che A può essere

ripartito in generale come:

$$\begin{aligned} A_1 &= \{g \in A \mid \max_{<_B}(\text{supp}_A(g)) <_B m\} \\ A_2 &= \{g \in A \mid \max_{<_B}(\text{supp}_A(g)) = m \wedge g(m) = f(m)\} \\ A_3 &= \{g \in A \mid \max_{<_B}(\text{supp}_A(g)) = m \wedge f(m) <_A g(m)\} \\ A_4 &= \{g \in A \mid m <_B \max_{<_B}(\text{supp}_A(g))\} \end{aligned}$$

e segue dalla definizione che le funzioni in A_1 , sono $<_{\exp}$ di quelle in A_2 , che sono $<_{\exp}$ etc. fino ad A_4 - è sufficiente pensare alle definizioni che abbiamo dato -. Però A_1 è vuoto, perché altrimenti, presa $f' \in A_1$, abbiamo $f' \in A$ e $\max(\text{supp}_A(f')) < m$ contro la minimalità di m . Abbiamo invece che A_2 non è vuoto perché contiene f , e non ha minimo, infatti, se avesse minimo, questo dovrebbe essere anche minimo di A - per la minimalità di m , avremmo preso la f che fa meno su m e quindi necessariamente la più piccola di tutte -, che non ha minimo per ipotesi.

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 perché $<_{\exp}$ confronta la massima componente in cui sono diverse, per cui la funzione:

$$H : A_2 \rightarrow S : g \mapsto \widehat{g} \quad \text{con} \quad \widehat{g}(x) = \begin{cases} \min A & \text{se } x = m \\ g(x) & \text{altrimenti} \end{cases}$$

è strettamente crescente, poiché dove le funzioni sono uguali poniamo semplicemente il loro valore uguale a $\min A$, cosa ininfluente per $<_{\exp}$, mentre dove vale la disegualanza continua a valere nell'immagine poiché non modifichiamo nulla in tal caso. Per cui $\widetilde{A} := H[A_2]$ non ha minimo, altrimenti, essendo H strettamente crescente, tornando indietro anche A lo avrebbe. Ora, però, segue dalla definizione di H , che, fissata $g \in A_2$, $\text{supp}(\widehat{g}) = \text{supp}(g) \setminus \{m\}$ (lo abbiamo rimosso "a mano" con H), quindi, ponendo $\widetilde{f} := \widehat{g}$, abbiamo $\max(\text{supp}(\widetilde{f})) < m$ (prima m era il massimo valore del supporto e non dava $\min A$, ora che l'abbiamo rimosso dal supporto, avendolo preso come il max del precedente supporto, ciò che rimane è necessariamente strettamente minore), e questo contraddice la minimalità di m .⁹¹ \square

Proposizione 9.21 (Buona definizione delle operazioni tra "classi di isomorfismo")

Le operazioni aritmetiche sui buoni ordini **passano al quoziente modulo isomorfismi**. Ossia, dati due buoni ordinamenti $\mathcal{A} = (B, <_A)$ e $\mathcal{B} = (B, <_B)$, e dati $\mathcal{A}' = (A', <_{A'}) \sim \mathcal{A}$ e $\mathcal{B}' = (B', <_{B'}) \sim \mathcal{B}$, si ha:

$$\mathcal{A} + \mathcal{B} \sim \mathcal{A}' + \mathcal{B}' \quad \mathcal{A} \cdot \mathcal{B} \sim \mathcal{A}' \cdot \mathcal{B}' \quad \mathcal{A}^{\mathcal{B}} \sim \mathcal{A}'^{\mathcal{B}'}$$

quindi le operazioni fra buoni ordini sono equivalenti modulo l'essere isomorfi.^a

^aIn altre parole le operazioni tra buoni ordini sono definite sulle classi di equivalenza di buoni ordini isomorfi, e la proposizione mostra che queste operazioni sono ben definite.

⁹¹Cose che andrebbero verificate per rendere precisa questa dimostrazione: perché posso fissare A e f tali che..., in altre parole perché esistono A ed f tali per cui...; perché si può partizionare A in quei 4 insiemi; fare le verifiche delle disegualanze tra gli elementi dei 4 insiemi; precisare meglio i dettagli della parte finale.

Dimostrazione. Fissati gli isomorfismi $f : A \rightarrow A'$ e $g : B \rightarrow B'$, 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:

$${}^B A \rightarrow {}^{B'} A' : h \mapsto f \circ h \circ g^{-1}$$

in altre parole, l'isomorfismo richiesto per dimostrare la tesi, che è quello scritto sopra, è quello che manda h nella mappa che fa commutare il seguente diagramma:

$$\begin{array}{ccc} B & \xrightarrow{h} & A \\ g^{-1} \uparrow & & \downarrow f \\ B' & \longrightarrow & A' \end{array}$$

andrebbe verificato che anche la nuova funzione $f \circ h \circ g^{-1}$ sia a supporto finito, ma questo segue dal fatto che f e g sono isomorfismi di ordini, in particolare vale che $g^{-1}[\text{supp}_{A'}(f \circ h \circ g^{-1})] = \text{supp}_A(h)$ (va verificato il doppio contenimento e può essere fatto facilmente tenendo conto e seguendo il diagramma sopra), da cui la bigezione e quindi la finitezza di $\text{supp}_{A'}(f \circ h \circ g^{-1})$. \square

Esercizio 9.22 (Buona definizione delle operazioni tra buoni ordini). Fare le altre verifiche della proposizione sopra.

Proposizione 9.23 (Proprietà delle operazioni sui buoni ordini)

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

associatività: $(\mathcal{A} + \mathcal{B}) + \mathcal{C} \sim \mathcal{A} + (\mathcal{B} + \mathcal{C}) \quad (\mathcal{A} \cdot \mathcal{B}) \cdot \mathcal{C} \sim \mathcal{A} \cdot (\mathcal{B} \cdot \mathcal{C})$

distributività a sinistra: $\mathcal{A} \cdot (\mathcal{B} + \mathcal{C}) \sim \mathcal{A} \cdot \mathcal{B} + \mathcal{A} \cdot \mathcal{C}$

proprietà delle potenze: $\mathcal{A}^{\mathcal{B}+\mathcal{C}} \sim \mathcal{A}^{\mathcal{B}} \cdot \mathcal{A}^{\mathcal{C}} \quad (\mathcal{A}^{\mathcal{B}})^{\mathcal{C}} \sim \mathcal{A}^{\mathcal{B} \cdot \mathcal{C}}$

^aValgono in realtà anche l'esistenza e le proprietà degli elementi neutri per \cdot e $+$.

Dimostrazione. Facili verifiche. \square

Esercizio 9.24 (Proprietà delle operazioni tra buoni ordini). Fare qualcuna delle verifiche delle proprietà sopra.

Non tutte le proprietà delle operazioni aritmetiche su ω valgono per i buoni ordini.

Esercizio 9.25 (Proprietà **false** delle operazioni tra buoni ordini). Esibire controesempi alle seguenti:

$$\mathcal{A} + \mathcal{B} \sim \mathcal{B} + \mathcal{A}$$

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

$$\mathcal{A} \cdot \mathcal{B} \sim \mathcal{B} \cdot \mathcal{A}$$

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

ovvero non valgono: commutatività, distributività a destra e potenza di un prodotto.

Soluzione. Vediamo controesempi caso per caso.

commutatività + Basta considerare $1 + \omega$ e $\omega + 1$ (sia 1 che ω sono buoni ordini), infatti abbiamo che:

$$1 + \omega = (1 \sqcup \omega, <_+) \quad \omega + 1 = (\omega \sqcup 1, <_+)$$

dove $1 \sqcup \omega = (1, 0) \cup (\omega \times \{1\}) = \{(1, 0), (0, 1), (1, 1), (2, 1), \dots\}$, con $<_+$ che è l'ordine dato dalla somma di buoni ordini, dunque $(1, 0) <_+ (n, 1), \forall n \in \omega$. Si vede facilmente quindi che $1 + \omega$ (oltre ad essere un buon ordine in quanto somma di buoni ordini) è superiormente illimitato e vale il principio del massimo, dunque $1 + \omega \sim \omega$. Viceversa, dove $\omega \sqcup 1 = (\omega \times \{0\}) \cup \{(1, 1)\} = \{(1, 1), (0, 0), (1, 0), (2, 0), \dots\}$, con $<_+$ che è sempre l'ordine dato dalla somma di buoni ordini, ma in questo caso si ha $(n, 0) <_+ (1, 1), \forall n \in \omega$, dunque $\omega + 1$ è superiormente limitato, pertanto non può essere isomorfo ad ω , dunque $1 + \omega \neq \omega + 1$.

commutatività · È sufficiente considerare $2 \cdot \omega$ e $\omega \cdot 2$, infatti in questo caso i buoni ordinamenti sono:

$$(2 \times \omega, <_\times) \quad (\omega \times 2, <_\times)$$

Si osserva che $(2 \times \omega, <_\times) \sim (\omega, <)$, infatti, detto n_i l' i -esimo numero pari e $m_i = n_i + 1$ l' i -esimo numero dispari, la mappa $(0, i) \mapsto n_i$ e $(1, i) \mapsto m_i$ è l'isomorfismo cercato. D'altra parte, per le proprietà sopra, si ha $\omega \cdot 2 = \omega \cdot (1 + 1) = \omega + \omega$, e non si può avere isomorfismo in quanto ω è naturalmente isomorfo al segmento iniziale proprio $(\omega, <) \prec \omega + \omega = (\omega \sqcup \omega, <_+)$.

□

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, dove le operazioni di ω coincidono con quelle cardinali e ordinali, e anche in generale per somma e prodotto - come è ovvio dalla definizione - ma fallisce per l'esponenziazione quando consideriamo buoni ordinamenti infiniti.

Esercizio 9.26 (Cardinalità dell'esponenziazione ordinale). 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 $|C| = \aleph_0$.^a

Hint: ricordare che $\mathcal{P}^{\text{fin}}(\omega) = \aleph_0$ e pensare a come si possa identificare ciò con ω^ω .

Soluzione. A meno di bigezioni, vogliamo dimostrare che $|\omega^\omega| = \aleph_0$, per fare ciò osserviamo che data $f \in \omega^\omega$, essa è a supporto finito, quindi come insieme la si può identificare univocamente come un insieme finito - cioè lasciando solo le coppie corrispondenti a elementi che non danno $\min \omega = 0$ tramite f - per cui si ha che $\{f \in \omega^\omega : |\text{supp}_\omega(f)| < \aleph_0\} \hookrightarrow \mathcal{P}^{\text{fin}}(\omega \times \omega) : f \mapsto f|_{\text{supp}_\omega(f)}$ è ben definita, e iniettiva (per tornare indietro basta estendere il dominio a tutto ω ed associare ai nuovi elementi 0). Abbiamo quindi $|\omega^\omega| \leq \aleph_0$. Viceversa è ovvio che $\omega \hookrightarrow \omega^\omega : n \mapsto f_n$, ovvero la funzione tale che $f_n(n) = 1$ e $f_n(m) = 0$, per ogni $m \in \omega \setminus \{n\}$, che è ovviamente a supporto finito, per cui abbiamo facilmente l'iniettività e quindi la disuguaglianza dal basso. □

§9.2 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 l'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.

Definizione 9.27 (Insieme transitivo). L'insieme α è **transitivo** se $\forall x \in \alpha x \subseteq \alpha$, o equivalentemente, se $\forall x \in \alpha \forall y \in x y \in \alpha$ (da cui il termine transitivo).

Ossia: diciamo che α è transitivo se gli elementi degli elementi di α sono, a loro volta, elementi di α , cioè se gli elementi sono a loro volta sottoinsiemi dell'insieme insieme (si pensi ad esempio a ω).

Definizione 9.28 (Ordinali di Von Neumann). L'insieme α è un **ordinale** se è **transitivo e bene ordinato dalla relazione di appartenenza**. Formalmente, l'insieme transitivo α è un ordinale se $(\alpha, <_\alpha)$ è un buon ordine, con:

$$<_\alpha \stackrel{\text{def}}{=} \{(x, y) \in \alpha \times \alpha \mid x \in y\}^{92}$$

Denotiamo con **Ord** la classe degli ordinali⁹³, per cui:

$$\alpha \in \text{Ord} \stackrel{\text{def}}{=} \text{"}\alpha\text{ è transitivo e ben ordinato da } \in\text{"}$$

Esempio 9.29 (Esempi di ordinali)

Alcuni esempi di ordinali già incontrati:

- ω è un ordinale
- gli elementi di ω sono ordinali
- $s(\omega) = \omega \cup \{\omega\}$ è un ordinale

Osservazione 9.30 (Ord è una classe transitiva) — Se $\alpha \in \text{Ord}$ e $\beta \in \alpha$, allora $\beta \in \text{Ord}$ e $\beta = \alpha_\beta$, ovvero β è un ordinale ed è il segmento iniziale principale di α , determinato da β . In particolare la classe degli ordinali Ord è transitiva.^a

^aCioè tutti gli ordinali sono a loro volta insiemi di ordinali di più piccoli.

Dimostrazione. Siccome $\beta \in \alpha$, per la transitività di α , $\beta \subseteq \alpha$, quindi β è un sottoinsieme bene ordinato dalla restrizione di $<_\alpha$, ovvero sempre l'appartenenza \in . La transitività di β segue dalla transitività della relazione di ordine $<_\alpha$. Prendiamo, infatti, $\delta \in \gamma \in \beta$, vogliamo verificare che $\delta \in \beta$, per fare ciò osserviamo che per la transitività di α si ha:

$$\gamma \in \beta \in \alpha \implies \gamma \in \alpha \quad \delta \in \gamma \in \alpha \implies \delta \in \alpha$$

⁹²Esattamente come accade su ω : $x < y \leftrightarrow x \in y \leftrightarrow (x, y) \in <$.

⁹³Tale classe contiene un elemento per ciascun buon ordinamento, ad esempio, preso $(\omega, <)$, come rappresentante della sua classe di isomorfismo, prendiamo ω stesso - inteso come buon ordinamento transitivo e ordinato dall'appartenenza - come rappresentante della "classe di equivalenza" nella classe dei buoni ordini (attenzione a non confondere i due significati del termine classe).

ora abbiamo quindi $\delta, \gamma, \beta \in \alpha$ e sappiamo che $\delta <_{\alpha} \gamma \wedge \gamma <_{\alpha} \beta$, per cui, essendo $<_{\alpha}$ transitivo, si ottiene $\delta <_{\alpha} \beta \equiv \delta \in \beta$, per cui β è transitivo. Resta da dire che $\beta = \alpha_{\beta}$:

$$x \in \alpha_{\beta} \stackrel{\text{def. s.i.}}{\iff} x \in \alpha \wedge x <_{\alpha} \beta \stackrel{\text{def. } \leq^{\alpha}}{\iff} x \in \alpha \wedge x \in \beta$$

Ora, essendo che per transitività vale $x \in \beta \rightarrow x \in \alpha$, possiamo quindi eliminare dall'AND il primo termine e ottenere:

$$x \in \alpha \wedge x \in \beta \iff x \in \beta$$

ovvero $x \in \alpha_{\beta} \leftrightarrow x \in \beta$, dunque per estensionalità $\alpha_{\beta} = \beta$. \square

La proposizione che stiamo per vedere ci dice che due ordinali non possono essere nella stessa classe di isomorfismo di buoni ordini, cioè **per ogni classe di isomorfismo di buoni ordinamenti c'è al più un ordinale**. Vorremmo poi dimostrare che ogni classe di isomorfismo contiene almeno un ordinale, in modo da poter dire che in ogni classe ce n'è esattamente uno. Vediamo prima della proposizione una semplice osservazione.

Osservazione 9.31 (Gli isomorfismi tra ordini totali mantengono i s.i. principali) —

Se $f : A \rightarrow B$ è un isomorfismo fra $(A, <_A)$ e $(B, <_B)$, allora preso un qualunque $a \in A$ abbiamo $f[A_a] = B_{f(a)}$.

Dimostrazione. Basta semplicemente osservare che:

$$\begin{aligned} x \in B_{f(a)} &\iff x <_B f(a) \\ &\iff f^{-1}(x) <_A a \\ &\iff f^{-1}(x) \in A_a \\ &\iff x \in f[A_a] \end{aligned}$$

e si conclude per estensionalità. \square

Proposizione 9.32 (Gli ordinali isomorfi sono proprio uguali)

Dati $\alpha, \beta \in \text{Ord}$, se $(\alpha, <_{\alpha}) \sim (\beta, <_{\beta})$, cioè $\alpha \sim \beta$, allora $\alpha = \beta$.^a

^aLa proposizione ha come conseguenza che per ogni classe di isomorfismo di buoni ordinamenti, c'è **al più** un ordinale, perché se ce ne fosse più di uno - posto che per ora non sappiamo nemmeno se ce ne sia uno - sarebbero esattamente uguali.

Dimostrazione. Sia $f : \alpha \rightarrow \beta$ un isomorfismo, ci basta dimostrare che $\forall \gamma \in \alpha \ f(\gamma) = \gamma$, cioè che $f = \text{id}_{\alpha}$. Sia, per assurdo, γ il minimo elemento di α tale che $f(\gamma) \neq \gamma$, allora:

$$\gamma \stackrel{\text{Oss.}}{=} \alpha_{\gamma} \stackrel{(*)}{=} f[\alpha_{\gamma}] \stackrel{\text{Oss. sopra}}{=} \beta_{f(\gamma)} \stackrel{\text{Oss.}}{=} f(\gamma) \not=$$

dove $(*)$ è vero in quanto, abbiamo preso γ come il più piccolo ordinale per cui f non è l'identità, e α_{γ} è fatto da cose strettamente più piccole di γ , dunque $f[\alpha_{\gamma}] = \alpha_{\gamma}$. \square

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.

Teorema 9.33 (Gli ordinali sono totalmente ordinati dalla “relazione” di appartenenza)

Dati $\alpha, \beta \in \text{Ord}$, vale **una e una sola** delle seguenti:^a

$$\alpha < \beta = \alpha \in \beta \text{ che vale se e solo se } (\alpha, <_\alpha) \prec (\beta, <_\beta)$$

$$\alpha = \beta \text{ che vale se e solo se } (\alpha, <_\alpha) \sim (\beta, <_\beta)$$

$$\alpha < \beta = \beta \in \alpha \text{ che vale se e solo se } (\beta, <_\beta) \prec (\alpha, <_\alpha)$$

^aEssendo gli ordinali una classe propria, come stiamo per vedere, questo teorema ci dice che tale classe è totalmente ordinata.

Notazione: nella dimostrazione porremo per comodità $\alpha \prec \beta \stackrel{\text{def}}{=} (\alpha, <_\alpha) \prec (\beta, <_\beta)$, e analogamente $\alpha \sim \beta$ e $\beta \prec \alpha$.

Dimostrazione. La tricotomia vale già sull’ordinamento \preceq per il teorema visto sui buoni ordinamenti, per cui verificando i se e solo se la si ottiene anche su $<$, in tal modo otteniamo che tutti gli ordinali sono totalmente ordinati da $<$. Inoltre, nella proposizione precedente abbiamo già verificato che se due ordinali sono isomorfi allora sono proprio uguali - ed il viceversa è triviale -, per cui ora vediamo solo la prima equivalenza essendo la terza perfettamente simmetrica.

- ◀ Se $\alpha \prec \beta$, allora per definizione α è isomorfo ad un segmento iniziale proprio - cioè principale - di β , $\alpha \sim \beta_\gamma$, per qualche $\gamma \in \beta$, e, per l’osservazione fatta prima, $\beta_\gamma = \gamma$. Per cui $\alpha \sim \gamma$ e dalla proposizione precedente otteniamo proprio che $\alpha = \gamma$, quindi si conclude che $\alpha \in \beta$.
- ▶ Se $\alpha \in \beta$, allora, per l’osservazione solita, sappiamo che $\alpha = \beta_\alpha$, e quindi banalmente, cioè via id_α , si ha $\alpha \prec \beta$.

□

Notazione 9.34 (Ordine della classe degli ordinali) — Dati $\alpha, \beta \in \text{Ord}$, avendo dimostrato che l’appartenenza è una “relazione di ordine totale” per gli ordinali, quando si parla di ordinali useremo la notazione:

$$\alpha < \beta \stackrel{\text{def}}{=} \alpha \in \beta$$

Infatti il teorema precedente ci dice che la relazione $<$ gode delle proprietà di un ordine totale stretto sulla classe degli ordinali.

Esercizio 9.35 (Gli ordinali finiti sono tutti e soli quelli di ω). Dimostra che α è un ordinale finito se e solo se $\alpha \in \omega$.

Soluzione. Sappiamo già che dato $n \in \omega$, $(n, <_{|n})$ è un buon ordinamento transitivo con l’ordine dato dall’appartenenza, e per definizione è finito, pertanto è banale osservare che tutti gli elementi di ω sono ordinali finiti.

Viceversa, dato α ordinale finito, poiché è finito è in biogezione con un certo naturale $n \in \omega$, che, come ricordato sopra, è un ordinale a sua volta con l’ordinamento indotto, otteniamo che $n \sim \alpha$. Infatti essendo n ed α buoni ordinamenti esiste un unico isomorfismo tra loro - ed è dato da $f(i) = \min(\alpha \setminus f[i])$ per $i = 0, \dots, n-1$, che è surgettivo poiché gli insiemi

sono equipotenti e finiti⁹⁴ -, quindi per la proposizione vista, essendo α ed n ordinali, $\alpha \sim n \implies \alpha = n \implies \alpha \in \omega$. \square

Proposizione 9.36 (Ordine largo sulla classe degli ordinali)

Siano $\alpha, \beta \in \text{Ord}$, allora:

$$\alpha \leq \beta \leftrightarrow \alpha \subseteq \beta$$

$$\text{con } \alpha \leq \beta \stackrel{\text{def}}{=} \alpha < \beta \vee \alpha = \beta.$$

Dimostrazione. Vediamo le due implicazioni:

- Si danno due casi, se $\alpha = \beta$, allora naturalmente ciò vale anche come insiemi per estensionalità. Se $\alpha < \beta$, per definizione $\alpha \in \beta$, e poiché β è transitivo $\alpha \subseteq \beta$.
- ← Dato $\alpha \subseteq \beta$, supponiamo per assurdo che $\beta < \alpha$, allora $\beta \in \alpha \subseteq \beta$, per cui $\beta \in \beta$ (contraddizione), infatti $\beta \in \beta \equiv \beta < \beta$, ed avendo dimostrato che $<$ corrisponde a \prec , che è un ordine totale, allora naturalmente lo è anche $<$, e quindi in particolare è una relazione d'ordine irriflessiva.⁹⁵

\square

Ricordiamo che $s(\alpha) \stackrel{\text{def}}{=} \alpha \cup \{\alpha\}$. La proposizione seguente ci dice che $s(\alpha)$ è, a buon diritto, il successore di α , anche quando α è un ordinale.

Proposizione 9.37 (Il successore è un ordinale)

Dato $\alpha \in \text{Ord}$, $s(\alpha)$ è il minimo ordinale $> \alpha$.

Dimostrazione. Occorre inizialmente verificare che $s(\alpha)$ è un ordinale.

transitività Se $\beta \in s(\alpha)$, allora per definizione di successore o $\beta \in \alpha$ o $\beta = \alpha$. Abbiamo naturalmente che $\alpha \subseteq s(\alpha)$, dunque nel primo caso la transitività segue da quella di α , infatti $\gamma \in \beta = \alpha \implies \gamma \in \alpha \subseteq s(\alpha)$, ovvero $\gamma \in s(\alpha)$. Nel secondo caso è proprio banale perché per costruzione appunto $\alpha \subseteq s(\alpha)$.

buon ordine Siccome $s(\alpha)$ è un insieme di ordinali, è un ordine totale su $s(\alpha)$, per quanto già visto. Dato $X \subseteq s(\alpha) = \alpha \cup \{\alpha\}$, con $X \neq \emptyset$, abbiamo due casi, o $X = \alpha$ o $X \cap \alpha \neq \emptyset$. Nel primo caso naturalmente sappiamo che α è bene ordinato e si conclude, nel secondo caso $\min(X) = \min(X \cap \alpha)$, infatti il minimo al RHS è ben definito perché α è ben ordinato ed è minimo anche per $X \setminus (X \cap \alpha) = \{\alpha\}$, in quanto appartiene ad α .

Supponiamo ora per assurdo che $s(\alpha)$ non sia il minimo ordinale $> \alpha$, allora esiste γ tale che $\alpha < \gamma < s(\alpha)$, dalla prima disegualanza segue, per transitività, che $\alpha \subseteq \gamma$, inoltre $\alpha \in \gamma \implies \alpha \subseteq \alpha$, per cui $s(\alpha) \subseteq \gamma \leftrightarrow s(\alpha) \leq \gamma$. \square

⁹⁴Per la precisione stiamo usando il fatto che se $|A| = |B| = n \in \omega$, allora $f : A \rightarrow B$ (o viceversa) è iniettiva se e solo se è surgettiva.

⁹⁵Segnalo l'osservazione ironica di Mamino nelle dispense originali che fa riferimento a buona fondazione.

Corollario 9.38 (Successore del primo termine in una disuguaglianza tra ordinali)

$\forall \alpha, \beta \in \text{Ord} \ \beta \leq \alpha \leftrightarrow \beta < s(\alpha)$.

Dimostrazione. Sono due facili verifiche.

← Da $\beta < s(\alpha)$, deduciamo per la definizione dell'ordinamento sugli ordinali che $\beta \in s(\alpha) = \alpha \cup \{\alpha\}$, che equivale a $\beta \in \alpha$ o $\beta = \alpha$, e, di nuovo per la definizione di ordinamento sugli ordinali, la prima cosa equivale a $\beta < \alpha$, pertanto abbiamo proprio che $\beta \leq \alpha$.

→ Per quanto visto $\beta \leq \alpha \leftrightarrow \beta < \alpha \vee \beta = \alpha$, nel primo caso, per transitività, essendo $\beta < \alpha < s(\alpha)$, si ha $\beta < s(\alpha)$, nel secondo $\beta = \alpha < s(\alpha)$, e la seconda disuguaglianza è vera per la proposizione precedente.

□

Proposizione 9.39 (Proprietà degli insiemi di ordinali)

Dato un insieme di ordinali X :

1. Se $X \neq \emptyset$, allora esiste il minimo di X , detto $\min X$, inoltre $\min X = \bigcap X$.^a
2. Esiste il minimo dei maggioranti di X - gli $\alpha \in \text{Ord}$ tali che $\forall \beta \in X \ \beta \leq \alpha$ -, detto $\sup X$, inoltre $\sup X = \bigcup X$.
3. C'è almeno un ordinale che non appartiene a X .

^aDa cui si deduce anche che la classe Ord è bene ordinata usando la stessa idea di questa dimostrazione.

Dimostrazione. Vediamo singolarmente i vari punti.

1. **Dimostriamo che il minimo esiste.** Essendo $X \neq \emptyset$ possiamo fissare $\alpha \in X$. Consideriamo $\mu := \min_{<_{s(\alpha)}}(X \cap s(\alpha))$. Questo esiste perché $X \cap s(\alpha) \neq \emptyset$ in quanto α vi appartiene, ed è ben definito perché $s(\alpha)$ è un ordinale. Osserviamo ora che è minimo anche per $X \setminus s(\alpha)$ - **di fatto abbiamo tolto da X tutti gli ordinali $\leq \alpha$ -**, preso $\beta \in X \setminus s(\alpha)$ si ha necessariamente che $\beta \geq s(\alpha)$ (altrimenti $\beta < \alpha \equiv \beta \in s(\alpha)$), e poiché $\mu \in s(\alpha)$, si ha $\mu < s(\alpha) \leq \beta$. **Ora verifichiamo che il minimo μ sia uguale a $\bigcap X$.** Per definizione di minimo $\forall \gamma \in X \ \mu \leq \gamma \leftrightarrow \mu \subseteq \gamma$, pertanto $\mu \leq \bigcap X$. D'altro canto $\mu \in X$, quindi $\bigcap X \subseteq \mu \leftrightarrow \bigcap X \leq \mu$.
2. Dimostriamo in primis che $\bigcup X$ è un ordinale.

transitività Dato $\alpha \in \bigcup X$, per definizione, esiste $\beta \in X$ tale che $\alpha \in \beta$. Per transitività di β si ha $\gamma \in \alpha \in \beta \rightarrow \gamma \in \beta$, da cui $\gamma \in \bigcup X$, che quindi è transitivo.

buon ordine Ogni $\alpha \in \bigcup X$ appartiene a qualche ordinale $\beta \in X$, pertanto, per la solita **osservazione sulla transitività di Ord**, α è un ordinale, quindi $\bigcup X$ è un insieme di ordinali - in particolare $\bigcup X \subseteq \text{Ord}$ ed è un insieme per l'assioma dell'unione - ed è bene ordinato per il punto 1. della proposizione.⁹⁶

⁹⁶Questa cosa poteva anche essere dimostrata alternativamente, senza usare il punto 1. facendo invece leva sull'esercizio visto in precedenza dell'unione di buoni ordinamenti che sono uno segmento iniziale dell'altro.

Per ogni $\alpha \in X$ si ha, per definizione di unione, $\alpha \subseteq \bigcup X$, che equivale, per quanto visto, a dire $\alpha \leq \bigcup X$, pertanto $\bigcup X$ è un maggiorante di X . Osserviamo ora che è il più piccolo maggiorante, infatti, dato σ maggiorante di X , per definizione, $\forall \alpha \in X \alpha \leq \sigma \leftrightarrow \alpha \subseteq \sigma$, cioè contiene tutti gli $\alpha \in X$, e quindi in particolare contiene la loro unione, $\bigcup X \subseteq \sigma \leftrightarrow \bigcup X \leq \sigma$.

3. Basta considerare $s(\sup X)$, per il 2. sappiamo che l'estremo superiore di X esiste, e dalle proprietà viste sugli ordinali, sappiamo che il successore di un ordinale è il minimo ordinale più grande, dunque, in questo caso, $s(\sup X)$ è un maggiorante stretto per X , pertanto non sta nell'insieme.

□

Corollario 9.40 (Gli insiemi di ordinali transitivi sono ordinali)

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

Dimostrazione. Per il 2. della proposizione precedente sappiamo che ogni insieme di ordinali è ben ordinato - dall'appartenenza naturalmente -, dunque la definizione di ordinale in questo caso si riduce al richiedere la transitività dell'insieme. □

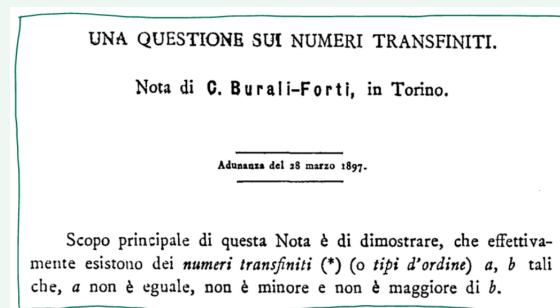
Corollario 9.41 (Paradosso di Burali-Forti)

Ord è una classe propria.

Ossia non esiste l'insieme di tutti gli ordinali.

Dimostrazione. Per il punto 3. della proposizione sulle proprietà degli insiemi di ordinali, se Ord fosse un insieme, esisterebbe un ordinale che non vi appartiene, che è assurdo. □

Nota 9.42 (Cosa c'è di paradossale nel paradosso di Burali-Forti?) — Nel 1897, Cesare Burali-Forti era assolutamente convinto della esistenza dell'insieme di tutti gli ordinali - definiti allora come le classi di isomorfismo dei buoni ordini - quello che non sapeva è se la relazione \prec fosse un ordine totale su queste classi.



Burali-Forti credette di poter negare la totalità dell'ordine \prec ragionando per assurdo. Se \prec fosse un ordine totale, si può dimostrare che è buono esattamente come abbiamo visto sopra, ma allora $\Omega \stackrel{\text{def}}{=} [(\text{Ord}, \prec)]$, la classe di isomorfismo di $(\text{Ord}, \prec)^a$, sarebbe a sua volta una classe di isomorfismo di un buon ordinamento e quindi uno dei membri della classe Ord stessa, e, considerando il suo successore

$s(\Omega)$, avremmo $\Omega \prec s(\Omega)$, ma anche ovviamente $s(\Omega) \prec \Omega$, perché $s(\Omega) \in \text{Ord}$ \notin .

Il guaio è che, nello stesso anno, Cantor pubblicò 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 esiste? **No**. Sfortunatamente Burali-Forti aveva capito male la definizione di buon ordinamento, e ancora così, forse, nessuno se ne sarebbe accorto, ma, quel che è peggio, aveva tentato di correggerla, facendo, in realtà un pasticcio. La contraddizione è stata quindi imputata, da Burali-Forti 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 ordinamento, e fu così che il paradosso di Burali-Forti acquisì il suo nome. E tutti vissero felici e contenti.

^aPer la precisione stiamo prendendo l'ordinale associato, cosa che non sappiamo ancora fare ma che si può fare come vedremo a breve.

§9.3 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:

$$\text{Ord} \stackrel{?}{=} \underbrace{\{\emptyset, s(\emptyset), \dots, s^n(\emptyset), \dots, \omega, s(\omega), \dots, s^n(\omega), \dots\}}_{\text{in realtà, questo si chiamerà } \omega + \omega}$$

la classe degli ordinali raggiungibili a partire da \emptyset o da ω con un numero finito di applicazioni della mappa successore.

Esercizio 9.43. Dimostra che la classe descritta sopra è effettivamente una classe, ossia è definita da una formula.

Soluzione. Chiamiamo $O = \{\emptyset, s(\emptyset), \dots, s^n(\emptyset), \dots, \omega, s(\omega), \dots, s^n(\omega), \dots\}$, allora la formula insiemistica che descrive O è:

$$x \in O \stackrel{\text{def}}{=} (x = \emptyset) \vee (x = \omega) \vee (\exists n \in \omega (\underbrace{x = s^n(\emptyset)}_{x=n} \vee \underbrace{x = s^n(\omega)}_{x=\omega+n}))$$

avendo una formula insiemistica ben posta, abbiamo che O è una classe. \square

Se vogliamo poter rispondere alla domanda “quanti 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 avvarremo dell’concetto di funzione classe.

Definizione 9.44 (Funzione classe). 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 9.45 (Funzione classe) — Possiamo denotare una funzione classe $\varphi(x, y)$ da A a B mediante la notazione più familiare:

$$F : A \rightarrow B$$

In questo caso, la scrittura $y = F(x)$ è una semplice abbreviazione:

$$y = F(x) \stackrel{\text{def}}{=} y \in B \wedge \varphi(x, y)$$

Esempio 9.46 (Esempi di funzioni classe)

Le seguenti sono funzioni classe $V \rightarrow V$:

$$F_1(x) = x \quad F_2(x) = \{x\} \quad F_3(x) = \mathcal{P}(x) \quad F_4(x) = s(x)$$

La funzione classe $F_5(x) = \sup(x \cap \text{Ord})$, con $x \cap \text{Ord} \stackrel{\text{def}}{=} \{\alpha \in x \mid \alpha \in \text{Ord}\}$, è $V \rightarrow \text{Ord}$.

Assioma 9.47 (Assioma del rimpiazzamento)

Se A è un insieme e $F : V \rightarrow V$ è una funzione classe, allora $F[A] \stackrel{\text{def}}{=} \{F(x) \mid x \in A\}$ è un insieme.^a

$$\forall A \exists B \forall y y \in B \leftrightarrow \exists x \in A y = F(x)$$

cioè per ogni insieme esiste un insieme i cui elementi sono immagini di quelli di A per mezzo della funzione classe F .

^aCome per la separazione, anche questo è uno schema di assiomi, uno per ogni possibile (formula insiemistica) funzione classe F .

Proposizione 9.48 (Unicità del rimpiazzamento)

Data una funzione classe $F : V \rightarrow V$ vale che:

$$\forall A \exists ! B \forall y y \in B \leftrightarrow \exists x \in A y = F(x)$$

Dimostrazione. Estensionalità. □

Osservazione 9.49 (Rimpiazzamento da insieme a classe) — Dato un insieme A e una funzione classe $G : A \rightarrow V$, esiste ed è unico l'insieme $G[A]$ tale che:

$$\forall y y \in G[A] \leftrightarrow \exists x \in A y = G(x)$$

in altre parole, l'assioma del rimpiazzamento vale anche con una funzione classe che va da un insieme ad una classe.

Dimostrazione. Ci basta semplicemente applicare l'assioma del rimpiazzamento appena enunciato, applicato alla funzione classe $F : V \rightarrow V$ definita come:

$$y = F(x) \stackrel{\text{def}}{=} (x \in A \wedge y = G(x)) \vee (x \notin A \wedge y = \emptyset)$$

ossia:

$$F(x) \stackrel{\text{def}}{=} \begin{cases} G(x) & \text{se } x \in A \\ \emptyset & \text{altrimenti} \end{cases}$$

infatti se $x \in A$ si ha $G(x) = F(x)$, altrimenti c'è il vuoto, per cui $G[A] = F[A]$ è un insieme grazie al rimpiazzamento. \square

Esercizio 9.50 (Esistenza del prodotto cartesiano via rimpiazzamento). 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**.

Soluzione. L'idea è quella di creare l'insieme di tutti gli insiemi del tipo $\{\{a\}, \{a, b\}\}$, per tutti gli $a \in A$ e $b \in B$. Per fare questo, fissato $b \in B$ definiamo la funzione classe:

$$H : V \rightarrow V : x \mapsto \{x, b\}$$

che è ben definita per l'assioma del paio. Ora per rimpiazzamento $H[A] = A_b$ è un insieme - ed è in particolare l'insieme di tutte le coppie $\{a, b\}$ al variare di $a \in A$ -, ora possiamo definire la funzione classe:

$$G : A_b \rightarrow V : \{a, b\} \mapsto \{\{a\}, \{a, b\}\}$$

che è ben definita perché di fatto stiamo facendo $\{\{a, b\} \cap A\} \cup \{\{a, b\}\}$, che è ancora un insieme per gli assiomi di singoletto e unione. A questo punto $E_b = G[A_b]$ è un insieme per rimpiazzamento - ed è proprio l'insieme di tutti gli insiemi $\{\{a\}, \{a, b\}\}$ per b fissato e a che varia in A , cioè è proprio $A \times \{b\}$ -. A questo punto possiamo definire la funzione classe:

$$F : B \rightarrow V : b \mapsto E_b$$

che è ben definita per quanto osservato e $F[B] = C$ che ci dà l'insieme $\{E_b\}_{b \in B} = \{\{A \times \{b\}\}\}_{b \in B}$, da cui:

$$\bigcup C$$

è l'insieme, per l'assioma dell'unione, di tutte le coppie ordinate (a, b) per $a \in A$ e $b \in B$, ed è quindi proprio $A \times B$. \square

Teorema 9.51 (Ogni buon ordine è isomorfo ad un unico ordinale)

Dato un buon ordine $(A, <)$, esiste un unico ordinale α tale che $(A, <) \sim \alpha$.

Dimostrazione. L'unicità segue per quanto abbiamo già visto, cioè $\alpha \sim \alpha' \rightarrow \alpha = \alpha'$. Basta quindi da dimostrare l'esistenza di almeno un ordinale α per ogni classe di isomorfismo di un buon ordinamento. Sia:

$$A' = \{x \in A \mid \exists \gamma \in \text{Ord} \quad A_x \sim \gamma\}$$

ovvero l'insieme degli elementi nel buon ordinamento che determinano segmenti iniziali isomorfi ad un qualche ordinale. Consideriamo la funzione classe $F : A' \rightarrow \text{Ord}$:

$$F(x) = \text{l'unico } \gamma \in \text{Ord} \text{ tale che } A_x \sim \gamma$$

l'unicità segue dalla solita proposizione e ci garantisce che la funzione classe sia ben definita:

$$A_x \sim \gamma \wedge A_x \sim \gamma' \implies \gamma \sim \gamma' \implies \gamma = \gamma'$$

Vogliamo dimostrare che l'insieme $\alpha := F[A'] \sim (A, <)$ - che esiste per rimpiazzamento - è proprio un ordinale isomorfo a $(A, <)$. Dimostriamo dunque che α è un ordinale, A' è un segmento iniziale di A , $\alpha \sim A'$, e infine che $A' = A$.

α è un ordinale α è definito come l'insieme degli ordinali isomorfi ai segmenti iniziali corrispondenti agli elementi di A' , dunque, per un fatto visto, ci basta dimostrare che è transitivo affinché sia un ordinale a sua volta.

Sia $\gamma \in \beta \in \alpha$, con β che è per definizione un ordinale isomorfo ad un qualche segmento iniziale principale di A , $\beta \sim A_a$, vediamo che anche γ è isomorfo ad un segmento iniziale principale di A e quindi $\gamma \in \alpha$. Fissato un isomorfismo $f : \beta \rightarrow A_a$, possiamo considerarne la restrizione a γ , che è ancora un isomorfismo, $f|_\gamma : \gamma \rightarrow (A_a)_{f(\gamma)} = A_{f(\gamma)}$, dove abbiamo usato che gli isomorfismi mandano s.i. in s.i., $f[\gamma] = f[\beta_\gamma] = (A_a)_{f(\gamma)}$, abbiamo quindi ottenuto che $\gamma = F(f(\gamma))$.

A' s.i. di A Sia $y < x \in A'$, vogliamo verificare che $y \in A'$, poiché $x \in A'$ esiste $\gamma \in \text{Ord}$ tale che $A_x \sim \gamma$, e naturalmente $A_y \subsetneq A_x$. Fissato $f : A_x \rightarrow \gamma$ isomorfismo, se verifichiamo che $f[A_y]$ è un ordinale abbiamo concluso poiché si avrebbe $A_y \sim f[A_y] \in \text{Ord}$ e quindi $y \in A'$. A questo punto dati $\beta \in \alpha \in f[A_y]$, poiché A_y è un isomorfismo, tornando indietro si ha $f^{-1}(\beta) < f^{-1}(\alpha) \in A_y$, ma poiché A_y è un segmento iniziale, allora $f^{-1}(\beta) \in A_y \iff \beta \in f[A_y]$.

Alternativa: Fissato $f : A_x \rightarrow \gamma$ isomorfismo, allora $f|_{A_y} : A_y \rightarrow \gamma_{f(y)}$ è un isomorfismo perché restrizione di un isomorfismo e sappiamo che gli isomorfismi mandano segmenti iniziali principali in segmenti iniziali principali per un'osservazione vista in precedenza, dunque l'immagine è proprio $\gamma_{f(y)}$, inoltre $\gamma_{f(y)} = f(y) \in \text{Ord}$, quindi evitiamo la verifica diretta che l'immagine sia un ordinale.

$A' \sim \alpha$ Sia $f : A' \rightarrow \alpha = F[A'] : x \mapsto F(x)$ la funzione tra insiemi, definita per separazione in $A' \times \alpha = A' \times F[A']$ - quindi abbiamo prima ottenuto l'insieme di arrivo con rimpiazzamento e poi ci siamo ristretti a quest'ultimo per avere una funzione -. Dimostriamo che f è un isomorfismo di ordini.

La surgettività è immediata perché, per costruzione, abbiamo che $\alpha = F[A'] \stackrel{\text{def. } f}{=} f[A']$. Osserviamo ora che la stretta crescenza deriva dall'ordinamento dei segmenti iniziali:

$$x <_A y \implies f(x) \sim A_x \prec A_y \sim f(y)$$

dove gli isomorfismi sono per definizione di f , e la disuguaglianza tra i segmenti iniziali come buoni ordinamenti deriva banalmente da $x < y$. Segue quindi che $f(x) \prec f(y)$, ed essendo ordinali ciò significa proprio che $f(x) \in f(y) \equiv f(x) < f(y)$.

$A' = A$ Se $A' \neq A$, cioè se $A' \subsetneq A$, avendo visto che A' è un segmento iniziale, abbiamo che è principale, quindi $A' = A_k$, per $k \in A$. Ma allora $A_k \sim \alpha \in \text{Ord}$ per i punti 1. e 3., per cui $k \in A' = A_k \not\in \alpha$.

□

Una conseguenza del risultato precedente è che possiamo definire le operazioni sugli ordinali come semplice riflesso di quelle sui buoni ordini - avendo a questo punto una corrispondenza esatta tra classi di isomorfismo di buoni ordini e ordinali -.

Definizione 9.52 (Operazioni sugli ordinali - v.1). Dati $\alpha, \beta \in \text{Ord}$, definiamo $\alpha + \beta$, $\alpha \cdot \beta$, α^β come, rispettivamente, l'unico ordinale tale che:

$$\begin{aligned} \alpha + \beta &\sim (\alpha, <_\alpha) + (\beta, <_\beta) & \alpha \cdot \beta &\sim (\alpha, <_\alpha) \cdot (\beta, <_\beta) \\ \alpha^\beta &\sim (\alpha, <_\alpha)^{(\beta, <_\beta)} \end{aligned}$$

Esercizio 9.53. Dimostra che l'insieme introdotto all'inizio della sezione è effettivamente $\omega + \omega$, ossia, più precisamente:

$$\forall x \ x \in \omega + \omega \leftrightarrow (\exists m \in \omega \ x = m) \vee (\exists n \in \omega \ x = \omega + n)$$

Soluzione.

□

§9.4 Induzione e ricorsione transfinita

Il piatto forte di questa sezione è una seconda applicazione dell'assioma del rimpiazzamento: il teorema di ricorsione transfinita. Questo risultato sarà più chiaro a chi ha, in precedenza, risolto il seguente esercizio.

Esercizio 9.54. Dimostra che esiste un insieme A tale che:

$$\forall x \ x \in A \leftrightarrow x = \emptyset \vee \exists y \in A \ x = \{y\}$$

ossia, in sostanza dimostra che esiste:

$$\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \dots\}$$

ovvero un insieme che contiene \emptyset e tale per cui qualsiasi altro elemento diverso dal vuoto che contiene è il singoletto di un altro suo elemento.

L'idea 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 dire alla situazione dell'esercizio - perché non abbiamo un insieme in arrivo -.

Soluzione. Vorremmo definire la funzione classe $F : \omega \rightarrow V$ data da:

$$F(n) = \text{singoletto } n \text{ volte di } \emptyset$$

a questo punto potremmo verificare che $A = F[\omega]$ 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 $n \in \omega$ abbiamo:

$$y = F(n) := \exists f \text{ tale che } \begin{cases} f \text{ è una funzione} \\ \text{Dom}(f) = s(n) \\ f(0) = \emptyset \\ \forall i \in n \ f(s(i)) = \{f(i)\} \\ f(n) = y \end{cases}$$

(notare che le tre richieste nel mezzo sono identiche alla definizione di n -approssimazione, nonché $f(n) = y$ è proprio il modo in cui dalle approssimazioni passiamo alla ricorsione nel teorema di ricorsione numerabile) cioè fissato $n \in \omega$, dire $y = F(n)$, vuol dire che esiste una funzione f con le proprietà richieste sopra, che calcolata in n dà appunto y (cioè il vuoto con n parentesi).

Proprio come nel teorema di ricorsione numerabile, per dimostrare che F è una funzione classe, ci basta dimostrare che $\forall n \in \omega \ \exists! f$ che soddisfa le tre richieste centrali, fatto ciò f sarà ben definita ed unica - per cui sarà ben definito anche $f(n) = y$ -, e quindi anche F è ben posta - **in pratica esistono e sono uniche le approssimazioni finite anche in questo caso, e come nel teorema di ricorsione numerabile possiamo costruire una funzione (classe in questo caso) che unisce le approssimazioni finite.**

esistenza Procediamo per induzione numerabile. Il caso $n = 0$ è immediato, basta considerare $f = \{(0, \emptyset)\}$ e tale f rispetta tutte le richieste.

Nel caso $n = s(m)$, per ipotesi induttiva, abbiamo una funzione f' con $\text{Dom}(f') = n$, $f'(0) = \emptyset$ e $\forall i < n \ f'(s(i)) = \{f'(i)\}$. Poniamo quindi $f = f' \cup \{(n, \{f'(m)\})\}$ ed otteniamo che $\text{Dom}(f) = \text{Dom}(f') \cup \{n\} = s(n)$, $f(0) = f'(0) = \emptyset$ e, preso $i < n = s(m)$, o $i < m$ o $i = n$; nel primo caso abbiamo che $f(s(i)) = f'(s(i)) = \{f'(i)\} = \{f(i)\}$, nel secondo $f(s(i)) = f(n) = \{f'(m)\} = \{f(m)\} = \{f(i)\}$.

unicità Date f_1 e f_2 che soddisfano le condizioni: $\text{Dom}(f_*) = s(n)$, $f_*(0) = \emptyset$ e $\forall i < n \ f_*(s(i)) = \{f_*(i)\}$, dimostriamo per induzione su i che $\forall i \in \omega \ i \leq n \rightarrow f_1(i) = f_2(i)$.

- Caso $i = 0$: $f_1(0) = \emptyset = f_2(0)$.
- Caso $i = s(j)$: $f_1(i) = \{f_1(j)\} \stackrel{\text{Hyp. indutt.}}{=} \{f_2(j)\} = f_2(i)$.

Ora che abbiamo la funzione classe F - abbiamo verificato che l'immagine della formula insiemistica data esiste ed è unica - è immediato verificare che $F(0) = \emptyset$. Inoltre, dato $n \in \omega$, $F(s(n)) = \{F(n)\}$, infatti, detto $y = F(s(n))$, per definizione esiste ed è unica f la funzione con $\text{Dom}(f) = s(s(n)), \dots$ tale che $F(s(n)) = f(s(n))$, osserviamo che $f|_{s(n)}(n) = F(n)$ (si verifica facilmente che $f|_{s(n)}$ rispetta tutte le richieste della definizione di $y = F(n)$, e quindi è proprio l'unica funzione che esiste per tale definizione). Abbiamo quindi:

$$F(s(n)) = f(s(n)) \stackrel{\text{def. } f}{=} \{f(n)\} = \{F(n)\}$$

Abbiamo quindi che F - oltre ad essere ben definita ed unica - soddisfa anche le richieste che volevamo per poter dire “singoletto di \emptyset n volte”, a questo punto possiamo quindi considerare $A := F[\omega]$ ed osservare che è proprio l'insieme che stavamo cercando. Infatti $\emptyset = F(0) \in A$, e, preso $y \in A = F[\omega]$ che non sia il vuoto, abbiamo $y = F(n)$, con $n \neq 0$, per cui $n = s(m)$, per qualche $m \in \omega$, allora detto $x = F(m) \in A$, si ha $y = F(s(m)) \stackrel{\text{oss. prima}}{=} \{F(m)\} = \{x\}$, pertanto qualsiasi elemento non sia il vuoto è il singoletto di qualche altro elemento dell'insieme, proprio come richiesto dalla formula nella richiesta. \square

Proposizione 9.55 (Induzione transfinita - v.1)

Data una formula insiemistica $\varphi(x)$. Se vale [l'ipotesi dell'induzione]^a:

$$\forall \alpha \in \text{Ord} (\forall \beta < \alpha \varphi(\beta)) \rightarrow \varphi(\alpha)$$

ovvero se per ogni ordinale, sapere che la formula è vera per gli ordinali più piccoli, rende vera la formula per l'ordinale stesso, allora la formula vale per tutti gli ordinali $\forall \alpha \in \text{Ord} \ \varphi(\alpha)$.

^aCome nell'induzione normale, il difficile sta nel mostrare che vale il passo induttivo, rappresentato dall'implicazione nell'ipotesi, poi il teorema assicura la veridicità dell'enunciato.

In termini di classi, rappresentando con C la classe definita dalla formula $\varphi(x)$, abbiamo che se vale $\forall \alpha \in \text{Ord} (\forall \beta < \alpha \varphi(\beta)) \rightarrow \alpha \in C$, allora $\forall \alpha \in \text{Ord} \ \alpha \in C$, cioè $\text{Ord} \subseteq C$.

Dimostrazione. Per assurdo, neghiamo la tesi $\neg(\forall \alpha \in \text{Ord} \ \varphi(\alpha)) \equiv \exists \alpha \in \text{Ord} \ \neg\varphi(\alpha)$. Possiamo quindi fissare un α per cui la formula $\varphi(\alpha)$ è falsa, a questo punto, applicando l'ipotesi ad α , dovendo essere l'implicazione sempre vera, ed avendo conseguente falso - ovvero $\varphi(\alpha)$ -, allora anche l'antecedente deve essere falso, ovvero deve necessariamente valere che $\neg(\forall \beta < \alpha \varphi(\beta)) \equiv \exists \beta < \alpha \neg\varphi(\beta)$.

Reiterando lo stesso identico ragionamento con β , otteniamo che esiste almeno un $\gamma < \beta$ tale che è vera $\neg\varphi(\gamma)$, per cui possiamo considerare $\beta_0 := \min\{\gamma \in \beta \mid \neg\varphi(\gamma)\}$ ⁹⁷ Reiterando di nuovo il ragionamento iniziale con β_0 otteniamo che esiste almeno un $\delta < \beta_0$ tale che è vera $\neg\varphi(\delta)$, contro la minimalità di β_0 . \square

⁹⁷Ora possiamo scrivere un insieme per separazione in β - prima non potevamo essendo $\alpha \in \text{Ord}$ - non vuoto per quanto visto, e quindi con un minimo per le proprietà degli insiemi di ordinali.

Nota 9.56 (L'induzione transfinita è uno schema di teoremi) — Il principio di induzione transfinita non è, letteralmente, un teorema della teoria degli insiemi, quanto piuttosto uno scherma di teoremi - o metateorema - che ci permette di costruire un diverso teorema per ogni possibile formula φ nel linguaggio della teoria degli insiemi - non essendo le classi oggetti della teoria degli insiemi, esse non possono essere quantificate con i quantificatori soliti, quindi l'induzione può essere enunciata solo per una formula fissata ogni volta, e non per tutte le formule -.

C'è una chiara analogia fra la forma precedente del principio di induzione transfinita e la forma forte dell'induzione aritmetica. A volte, però, è comodo esprimere l'induzione transfinita in una forma che meglio ricorda il principio di induzione di Peano.

Definizione 9.57 (Ordinali successori e limiti). Diciamo che $\alpha \in \text{Ord}$ è un **ordinale successore** se $\exists \beta \in \text{Ord} \ \alpha = s(\beta)$. Un ordinale $\alpha > 0$ che non è successore è detto **ordinale limite**.

Osservazione 9.58 (Caratterizzazione degli ordinali successori) — Un ordinale α è successore se e solo se ha un massimo.^a

^aPiù precisamente, un insieme di ordinali è un ordinale successore se e solo se è transitivo ed ha un massimo. Equivalentemente un ordinale che non ha massimo è limite.

Dimostrazione. Ci basta osservare che vale la seguente catena di equivalenze:

$$\beta \text{ è il massimo di } \alpha \iff \alpha \text{ è il minimo ordinale } > \beta \iff s(\beta) = \alpha$$

la seconda equivalenza l'abbiamo già vista in precedenza, dimostriamo quindi la prima.

- \Leftarrow Se β non fosse il massimo di α , allora esisterebbe un ordinale γ tale che $\alpha > \gamma > \beta$, che è contro la minimalità di α .
- \Rightarrow Se esistesse un ordinale γ più grande di β e più piccolo di α , $\beta < \gamma < \alpha$, si avrebbe che $\gamma \in \alpha$ supera β che quindi non può essere il massimo di α .

□

Proposizione 9.59 (Induzione transfinita - v.2)

Sia $\varphi(x)$ una formula insiemistica, se vale:

- (i) $\varphi(0)$ (**caso base**)
- (ii) $\forall \gamma \in \text{Ord} \ \varphi(\gamma) \rightarrow \varphi(s(\gamma))$ (**caso successore**)
- (iii) per ogni ordinale limite λ si ha $(\forall \beta < \lambda \varphi(\beta)) \rightarrow \varphi(\lambda)$ ^a (**caso limite**)

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

^aCioè vale anche un passo induttivo - forte - per gli ordinali che non sono successori.

Dimostrazione. Basta verificare l'ipotesi della prima forma dell'**induzione transfinita**, per avere in automatico la veridicità della formula in generale. Fissato quindi $\alpha \in \text{Ord}$ bisogna mostrare che vale la formula:

$$(\forall \beta < \alpha \varphi(\beta)) \rightarrow \varphi(\alpha)$$

Se α è limite o 0 abbiamo questa formula tout court - nel caso di 0 la formula sopra è vera a vuoto, nel caso degli ordinali limite abbiamo assunto che la formula sopra è vera come ipotesi -. Verifichiamo che la formula sopra è vera anche nel caso in cui $\alpha = s(\gamma)$:

$$\forall \beta < \alpha = s(\gamma) \varphi(\beta) \xrightarrow{\gamma < s(\gamma)} \varphi(\gamma) \xrightarrow{\text{H.p. (ii)}} \varphi(s(\gamma)) = \varphi(\alpha)$$

dunque anche in questo caso vale l'ipotesi della prima forma dell'induzione transfinita, che quindi vale proprio $\forall \alpha \in \text{Ord}$. Pertanto la prima forma dell'induzione transfinita ci garantisce che $\varphi(\alpha)$ vale per tutti gli $\alpha \in \text{Ord}$. \square

Ora possiamo finalmente dimostrare il teorema di ricorsione transfinita.

Notazione 9.60 (Restrizione di una funzione classe a funzione) — Data una funzione classe $F : A \rightarrow B$ e un insieme $X \subseteq A$ esiste la funzione tra insiemi:

$$f = F|_X : X \rightarrow F[X] : a \mapsto F[a]$$

che è ottenuta per separazione in $X \times F[X]$ - il secondo è un insieme per rimpiazzamento -, ed è in automatico una funzione surgettiva.

Teorema 9.61 (Ricorsione transfinita - v.1)

Data una funzione classe $G : V \rightarrow V$ esiste un'unica^a funzione $F : \text{Ord} \rightarrow V$ tale che:

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

^aDove l'unicità va intesa nel senso seguente: date F_1, F_2 come sopra, vale $\forall \alpha \in \text{Ord} \quad F_1(\alpha) = F_2(\alpha)$.

L'idea è di costruire una funzione classe $H : \text{Ord} \rightarrow V$ - la successione delle troncate di G - in maniera tale che, a posteriori, avremo $F_\alpha = H(\alpha)$. Poi semplicemente porremo $F(\alpha) := H(s(\alpha))(\alpha)$. $H(\alpha)$ è l'analogo transfinito di una α -approssimazione nella dimostrazione del teorema di ricorsione numerabile -nel senso della seconda forma più che della prima⁹⁸ -.

Dimostrazione. Definiamo la funzione classe $H : \text{Ord} \rightarrow V$ con:

$$f = H(\alpha) := \begin{cases} f \text{ è una funzione} \\ \text{Dom}(f) = \alpha \\ \forall \beta \in \alpha \quad f(\beta) = G(f|_\beta) \end{cases}$$

Verifichiamo, per induzione transfinita su α , che H sia realmente una funzione classe $\text{Ord} \rightarrow V$, ossia che sia effettivamente una funzione:

$$\forall \alpha \in \text{Ord} \quad \exists ! f \quad f = H(\alpha)$$

caso 0 $f = H(0) \iff f = \emptyset$, quindi f esiste ed è unica quando si valuta H in 0.

caso $\alpha = s(\gamma)$ Per ipotesi induttiva esiste ed è unica $f = H(\gamma)$, dunque possiamo definire $f' = f \cup \{(\gamma, G(f))\}$ e verificare che f' rispetta le condizioni ed è unica. Si vede immediatamente che $\text{Dom}(f') = \text{Dom}(f) \cup \{\gamma\} = \gamma \cup \{\gamma\} = s(\gamma) = \alpha$, inoltre, preso $\beta \in \alpha = s(\gamma)$ si hanno due casi:

⁹⁸Anzi, di fatto, questa dimostrazione rimaneggiata ci dà una dimostrazione del secondo teorema di ricorsione numerabile usando le approssimazioni finite.

- $\diamond \underline{\text{se } \beta \in \gamma:}$ allora $f'(\beta) \stackrel{\text{def.}}{=} f(\beta) \stackrel{\text{Hp. indutt.}}{=} G(f|_\beta) \stackrel{\text{def.}}{=} G(f'_\beta)$
- $\diamond \underline{\text{se } \beta = \gamma:}$ allora $f'(\gamma) \stackrel{\text{def.}}{=} G(f) = G(f|_\gamma) \stackrel{\text{def.}}{=} G(f'_\gamma)$, dove l'uguaglianza al centro vale poiché banalmente $f = f|_\gamma$ essendo $\text{Dom}(f) = \gamma$.

Verifichiamo ora l'unicità di f' , data $g = H(\alpha)$ - cioè un'altra funzione che rispetta le condizioni iniziali -, siccome $\text{Dom}(f') = \text{Dom}(g) = \alpha$, ci basta verificare che le due funzioni coincidono su α . Per definizione $g|_\gamma = H(\gamma)$ e per l'unicità di f si ha che $g|_\gamma = f = f'_\gamma$, l'unico caso che resta da verificare è quindi γ stesso:

$$g(\gamma) \stackrel{\text{def.}}{=} G(g|_\gamma) \stackrel{\text{Hp. indutt.}}{=} G(f) = G(f'_\gamma) \stackrel{\text{def.}}{=} f'(\gamma)$$

caso $\alpha = \lambda$ Sia λ limite, per ipotesi induttiva abbiamo che $\forall \beta < \lambda \exists! f f = H(\beta)$ tale che $\text{Dom}(f) = \beta$ e $\forall \gamma < \beta f(\gamma) = G(f|_\gamma)$, dobbiamo dimostrare che $\exists! g g = H(\lambda)$, con $\text{Dom}(g) = \lambda$ e $\forall \beta < \lambda g(\beta) = G(g|_\beta)$.

Per rimpiazzamento esiste l'insieme $H[\lambda]$, poniamo $h := \bigcup H[\lambda] = \bigcup_{\beta < \lambda} H(\beta)$, vogliamo dimostrare che $g = H(\lambda) \leftrightarrow g = h$. Per cominciare dimostriamo che $h = H(\lambda)$.

$\diamond \underline{h \text{ è una funzione:}}$ Dobbiamo dire che date $f_1, f_2 \in H[\lambda]$, queste coincidono sull'intersezione dei loro domini. Siano $f_1 = H(\beta_1)$ e $f_2 = H(\beta_2)$, assumiamo WLOG che $\beta_1 < \beta_2$, segue quindi che $f_2|_{\beta_1} = H(\beta_1)$ - per definizione la restrizione di f_2 rispetta le proprietà di una β_2 -approssimazione, e per ipotesi induttiva è unica (ed è proprio $H(\beta_2)$), quindi $f_2|_{\beta_1} = H(\beta_1) = f_2$.

$\diamond \underline{\text{Dom}(h) = \lambda:}$ Segue banalmente che:

$$\text{Dom}(h) = \bigcup_{\beta \in \lambda} \text{Dom}(H(\beta)) = \bigcup_{\beta \in \lambda} \beta = \lambda$$

$\diamond \underline{\forall \beta < \lambda h(\beta) = G(h|_\beta):}$ Dato $\beta < \lambda$, essendo λ limite, $s(\beta) < \lambda$, quindi, detta $f = H(s(\beta))$ - di fatto è la più piccola funzione che calcola $f(\beta)$ e le altre che lo calcolano nell'unione sono sue estensioni -, abbiamo $h(\beta) \stackrel{\text{def. } h}{=} f(\beta) \stackrel{\text{Hp. indutt.}}{=} G(f|_\beta) \stackrel{\text{def. } h}{=} G(h|_\beta)$.

Abbiamo quindi che h è una λ -approssimazione, verifichiamo l'unicità. Detta $g = H(\lambda)$, dobbiamo dimostrare che $g = h$. Dato $\beta < \lambda$, abbiamo per definizione $g|_\beta = h|_\beta = H(\beta)$, e per l'unicità di $H(\beta)$ - che abbiamo per ipotesi induttiva - segue:

$$\forall \beta < \lambda g(\beta) = G(g|_\beta) = G(H(\beta)) = G(h|_\beta) = h(\beta) \implies g = h$$

Abbiamo stabilito che H è una funzione classe ben posta. Definiamo ora:

$$y = F(\alpha) := \exists f f = H(s(\alpha)) \wedge y = f(\alpha)$$

e per quanto abbiamo appena visto F è ben definita poiché $H(s(\alpha))$ esiste ed è unica per ogni $\alpha \in \text{Ord}$ - in pratica H è la successione delle troncate come nel secondo teorema di ricorsione numerabile -, dobbiamo quindi mostrare che $F(\alpha) = G(F|_\alpha)$, infatti come nella ricorsione numerabile v.2, $F(\alpha) = f(\alpha) = (H(s(\alpha)))(\alpha) = G(f|_\alpha)$, dunque ci basta solo verificare che $F|_\alpha = f|_\alpha$ per concludere l'esistenza.

Preso $\beta < \alpha$ e $f' = H(s(\beta))$, per definizione che $F(\beta) \stackrel{\text{def. } F}{=} f'(\beta) = G(f'_\beta) = G(f|_\beta) =$

$f(\beta)$ dove l'uguaglianza in rosso vale perché le funzioni date da $H(\cdot)$ coincidono sull'intersezione dei loro domini per l'unicità delle approssimazioni vista sopra - fondamentalmente ciò ci dice che le approssimazioni estendono ciascuna le altre⁹⁹ -, pertanto $\forall \beta < \alpha F(\beta) = f(\beta) \implies F_{\alpha|} = f_{|\alpha}$. A questo punto si ha proprio $F(\alpha) = f(\alpha) = G(f_{|\alpha}) = G(F_{|\alpha})$. Resta da dimostrare l'unicità di F . Ossia che date F_1 e F_2 tali che:

$$\begin{aligned}\forall \alpha \in \text{Ord } F_1(\alpha) &= G(F_{1|\alpha}) \\ \forall \alpha \in \text{Ord } F_2(\alpha) &= G(F_{2|\alpha})\end{aligned}$$

allora $\forall \alpha \in \text{Ord } F_1(\alpha) = F_2(\alpha)$. Per [induzione transfinita v.1](#) possiamo assumere che $\forall \beta < \alpha F_1(\beta) = F_2(\beta)$, ma questo equivale proprio a dire $F_{1|\alpha} = F_{2|\alpha}$, quindi:

$$F_1(\alpha) \stackrel{\text{def.}}{=} G(F_{1|\alpha}) \stackrel{\text{Hyp. induttiva}}{=} G(F_{2|\alpha}) \stackrel{\text{def.}}{=} F_2(\alpha)$$

□

Come per l'induzione, possiamo esprimere la ricorsione transfinita separando i casi zero, successore e limite.

Definizione 9.62 (Prodotto cartesiano di classi). Date due classi A, B definiamo la **classe prodotto cartesiano** $A \times B$ come:

$$x \in A \times B \stackrel{\text{def.}}{=} \exists a \in A \exists b \in B x = (a, b)$$

Corollario 9.63 (Ricorsione transfinita - v.2)

Date le funzioni classe $G_1 : \text{Ord} \times V \rightarrow V$ e $G_2 : V \rightarrow V$ e dato $x_0 \in V$, esiste un'unica funzione classe $F : \text{Ord} \rightarrow V$ tale che:

$$\forall \alpha \in \text{Ord } F(\alpha) := \begin{cases} F(0) = x_0 \\ \forall \alpha \in \text{Ord } F(s(\alpha)) = G_1(\alpha, F(\alpha)) \\ \forall \lambda \in \text{Ord } \lambda \text{ limite} \rightarrow F(\lambda) = G_2(F_{|\lambda}) \end{cases}$$

Dimostrazione. Ci basta applicare il [teorema di ricorsione transfinita v.1](#), e per farlo, non dobbiamo far altro che definire una funzione classe $G : \text{Ord} \rightarrow \text{Ord}$, rispetto a cui $F(\alpha) = G(F_{|\alpha})$, ed il teorema ci assicura esistenza ed unicità. Possiamo esibire G nel modo seguente:¹⁰⁰

$$G(f) = \begin{cases} \emptyset & \text{se } f \text{ NON è una funzione con } \text{Dom}(f) \in \text{Ord} \\ x_0 & \text{se } f = \emptyset \text{ (o } \text{Dom}(f) = \emptyset\text{)} \\ G_1(\alpha, f(\alpha)) & \text{se } \text{Dom}(f) = \alpha + 1 \text{ per qualche } \alpha \in \text{Ord} \\ G_2(f) & \text{altrimenti} \end{cases}$$

□

⁹⁹Per la precisione $f_{|\beta} = H(\alpha)_{|\beta} = \text{unica } \beta\text{-approssimazione} = H(\beta) = H(s(\beta))_{|\beta} = f'_{|\beta}$ (poiché le restrizioni soddisfano ancora le proprietà delle approssimazioni).

¹⁰⁰Il caso $f = \emptyset$ corrisponderebbe alla troncata 0-esima della ricorsione - come nella ricorsione numerabile $f'(0) = 0, f'(s(n)) = f'(n) \cup \{(n, h(f'(n)))\}$ e $f(0) = f'(s(0))(0) = h(0)$ -, per in maniera simile abbiamo $F(0) = G(F_{|0}) = G(\emptyset) = x_0$.

§9.5 Operazioni fra gli ordinali

Definizione 9.64 (Operazioni sugli ordinali - v.2). Esistono le funzioni classe di somma, prodotto e potenza di ordinali, così definite:

$$\alpha + \beta := \begin{cases} \alpha + 0 = \alpha \\ \alpha + s(\beta) = s(\alpha + \beta) \\ \alpha^\lambda = \sup\{\alpha + \beta \mid \beta < \lambda\} \end{cases} \quad \alpha \cdot \beta := \begin{cases} \alpha \cdot 0 = 0 \\ \alpha \cdot s(\beta) = \alpha \cdot \beta + \alpha \\ \alpha \cdot \lambda = \sup\{\alpha \cdot \beta \mid \beta < \lambda\} \end{cases}$$

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

Ossia, le operazioni aritmetiche sugli ordinali si possono definire in modo analogo alle operazioni aritmetiche su ω nei casi 0 e successore, e **estendendole con continuità** nel caso limite.

Definizione 9.65 (Continuità). Una funzione classe $F : \text{Ord} \rightarrow \text{Ord}$ mai decrescente - $\alpha < \beta \rightarrow F(\alpha) \leq F(\beta)$ - si dice **continua** se, per ogni ordinale limite λ vale $F(\lambda) = \sup F[\lambda] = \sup_{\alpha < \lambda} F(\alpha)$.¹⁰¹

Nota 9.66 (Sulle definizioni ricorsive delle funzioni aritmetiche degli ordinali) — Sarebbe corretto osservare che, letteralmente, il teorema di ricorsione transfinita non pare sufficiente a garantire l'esistenza, per esempio, della funzione classe $+ : \text{Ord} \times \text{Ord}$. Il problema è che, fissato α , possiamo costruire ricorsivamente la funzione classe " $\alpha+$ " : $\text{Ord} \rightarrow \text{Ord}$, ma abbiamo, a quanto pare, una diversa funzione per ogni possibile α . Ci sono due vie d'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 abbastanza complicata.

La seconda strada è 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.

¹⁰¹L'idea è la stessa dell'estensione continua di una funzione reale ad di fuori del suo dominio, ovvero quella di far valere la funzione appena fuori l'estremo superiore dell'immagine dell'insieme non esteso.

Proposizione 9.67 (Equivalenza delle definizioni delle operazioni ordinali)

Vale che:

$$\begin{aligned}\alpha + \beta &\sim (\alpha, <_\alpha) + (\beta, <_\beta) & \alpha \cdot \beta &\sim (\alpha, <_\alpha) \cdot (\beta, <_\beta) \\ \alpha^\beta &\sim (\alpha, <_\alpha)^{(\beta, <_\beta)}\end{aligned}$$

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.

Dimostrazione. Si procede sempre per [induzione transfinita v.2](#) su β in modo da sfruttare la continuità delle operazioni a destra nei casi limiti.

$$\alpha + \beta \sim (\alpha, <_\alpha) + (\beta, <_\beta)$$

$\beta = 0$ Consideriamo $\alpha + 0$ e $(\alpha, <_\alpha) + (0, <_0)$, per la definizione ricorsiva sappiamo che $\alpha + 0 = \alpha$, mentre, per la definizione di somma sui buoni ordini abbiamo che:

$$(\alpha, <_\alpha) + (0, <_0) = (\alpha \sqcup 0, <_+) = ((\alpha \times \{0\}) \cup (\underbrace{\emptyset \times \{1\}}_{=\emptyset}, <_+) = (\alpha \times \{0\}, <_+)$$

A questo punto è facile osservare che $\alpha \sim (\alpha \times \{0\}, <_+)$.

$\beta = s(\gamma)$ Assumiamo come ipotesi induttiva che $\alpha + \beta \sim (\alpha, <_\alpha) + (\beta, <_\beta)$ e dimostriamo che $\alpha + s(\beta) \sim (\alpha, <_\alpha) + (s(\beta), <_{s(\beta)})$. Sia $f : \alpha + \beta \rightarrow \alpha \sqcup \beta$ un isomorfismo, osserviamo che $\alpha \sqcup s(\beta) = (\alpha \sqcup \beta) \cup (\beta, 1)$, dunque possiamo considerare $\tilde{f} = f \cup \{(\alpha + \beta, (\beta, 1))\}$, ed osservare che \tilde{f} è un isomorfismo tra $\alpha + s(\beta)$ e $\alpha \sqcup s(\beta)$, infatti, iniettività e surgettività sono banali per costruzione, per la stretta crescenza è sufficiente osservare che $\alpha + \beta$ è il massimo di $\alpha + s(\beta) = s(\alpha + \beta)$, ed al contempo che $(\beta, 1)$ è il massimo di $\alpha \sqcup s(\beta)$ - infatti ha seconda componente 1, dunque il confronto è sempre vinto contro un elemento di α , ed al contempo β è il massimo di $s(\beta)$, dunque è proprio il massimo di questo buon ordinamento -, segue che la monotonia è rispettata e quindi \tilde{f} è un isomorfismo.

$\beta = \lambda$ limite Dato $\gamma \sim (\alpha, <) + (\lambda, <)$, cioè $\gamma \sim \alpha \sqcup \lambda$ con l'ordinamento dato da $<_+$, vogliamo dimostrare che $\alpha + \lambda = \gamma$, avendo come ipotesi induttiva che $\alpha + \beta \sim \alpha \sqcup \beta$, per $\beta < \lambda$. Fissiamo f isomorfismo tra $\alpha \sqcup \lambda$ e γ , siccome $\alpha \sqcup \beta$ è un segmento iniziale proprio di $\alpha \sqcup \lambda$ l'isomorfismo lo preserva e, tenendo conto dell'ipotesi induttiva, lo manda in $\alpha + \beta$ ¹⁰², inoltre osserviamo che $\bigcup_{\beta < \lambda} \alpha \sqcup \beta = \bigcup_{\beta < \lambda} (\alpha \times \{0\}) \cup (\beta \times \{1\}) = (\alpha \times \{0\}) \cup \bigcup_{\beta < \lambda} (\beta \times \{1\}) = (\alpha \times \{0\}) \cup \left(\left(\bigcup_{\beta < \lambda} \beta \right) \times \{1\} \right) = (\alpha \times \{0\}) \cup (\lambda \times \{1\}) = \alpha + \lambda$, segue quindi:

$$\begin{aligned}\gamma &= f[\alpha \sqcup \lambda] \\ &= f \left[\bigcup_{\alpha < \beta} \alpha \sqcup \beta \right] \\ &\stackrel{(*)}{=} \bigcup_{\beta < \lambda} f[\alpha \sqcup \beta] \\ &= \bigcup_{\beta < \lambda} \alpha + \beta = \alpha + \lambda\end{aligned}$$

¹⁰²In altre parole c'è un solo isomorfismo tra i buoni ordinamenti $\alpha \sqcup \beta$ e $\alpha + \beta$, ed essendo la restrizione di f ancora un isomorfismo deve coincidere con quell'unico isomorfismo, che per ipotesi induttiva sappiamo esattamente cosa fa.

dove (\star) vale in generale - cioè l'immagine di un'unione di insiemi è sempre l'unione delle immagini degli insiemi - in quanto stiamo considerando gli ordinali come sottoinsiemi del dominio e non come elementi - in questo caso la scambio avrebbe richiesto f continua -.

Per le altre verifiche, che seguono circa lo stesso schema, riportiamo solo il caso limite.

$$\alpha \cdot \beta \sim (\alpha, <_\alpha) \cdot (\beta, <_\beta)$$

$\beta = \lambda$ limite Si procede come prima, sia $\gamma \sim (\alpha, <_\alpha) \cdot (\lambda, <_\lambda)$ e $f : \alpha \times \lambda \rightarrow \gamma$ isomorfismo, vogliamo dimostrare che $\gamma = \alpha \cdot \lambda$. Per ipotesi induttiva abbiamo che $\alpha \times \beta \sim \alpha \cdot \beta$, per cui come prima $\alpha \times \beta$ è un segmento iniziale proprio di $\alpha \times \lambda$, e per l'unicità degli isomorfismi tra buoni ordinamenti, si ha $f[\alpha \times \beta] = \alpha \cdot \beta$. Inoltre, come prima, vale che $\bigcup_{\beta < \lambda} \alpha \times \beta = \alpha \times \left(\bigcup_{\beta < \lambda} \beta \right) = \alpha \times \lambda$, segue quindi:

$$\begin{aligned} \gamma &= f[\alpha \times \lambda] \\ &= f \left[\bigcup_{\beta < \lambda} \alpha \times \beta \right] \\ &\stackrel{(\star)}{=} \bigcup_{\beta < \lambda} f[\alpha \times \beta] \\ &= \bigcup_{\beta < \lambda} \alpha \cdot \beta = \alpha \cdot \lambda \end{aligned}$$

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

$\beta = \lambda$ limite In questo caso, si ripropone il ragionamento dei due casi precedente, con un leggero problema tecnico. Dato $\beta < \lambda$, nei due casi precedente, abbiamo usato il fatto che $\alpha \sqcup \beta$ e $\alpha \times \beta$ sono, rispettivamente, segmenti iniziali di $\alpha \sqcup \lambda$ e $\alpha \times \lambda$, che poi scriviamo come unione, appunto, di questi sottoinsiemi.

Il guaio, adesso, è che l'insieme delle funzioni $\beta \rightarrow \alpha$ a supporto finito non è neppure sottoinsieme dell'insieme delle funzioni $\lambda \rightarrow \alpha$ a supporto finito. La soluzione è semplice, detti:

$$SF(\square \rightarrow \alpha) \equiv \{g : \square \rightarrow \alpha \text{ a supporto finito}\}$$

$$EXT_\beta^\alpha : SF(\beta \rightarrow \alpha) \rightarrow SF(\lambda \rightarrow \alpha) : g \mapsto h \quad \text{con } h|_\beta = g \text{ e } \forall \delta \in \lambda \setminus \beta \ h(\delta) = 0$$

ossia EXT è l'operatore che estende una funzione a supporto finito $g : \beta \rightarrow \alpha$ a una funzione da λ ad α ponendo 0 su $\alpha \setminus \beta$.

È chiaro che $EXT_\beta^\alpha [SF(\beta \rightarrow \alpha)] \sim SF(\beta \rightarrow \alpha)$ - via $h \mapsto h|_\beta$ -, perché l'ordine $g_1 <_{\exp} g_2$ su $SF(\square \rightarrow \alpha)$ è definito confrontando le immagini del massimo x tale che $g_1(x) \neq g_2(x)$, e, su $x \in \lambda \setminus \beta$, le funzione nell'immagine di EXT_β^α sono identicamente 0, quindi la mappa naturale tra i due insiemi è strettamente crescente - e banalmente surgettiva -. Inoltre $EXT_\beta^\alpha [SF(\beta \rightarrow \alpha)]$ è un segmento iniziale di $SF(\lambda \rightarrow \alpha)$ ¹⁰³. Possiamo quindi replicare l'argomento usato negli altri casi limite: fissiamo $\gamma \sim (\alpha, <_\alpha)^{(\lambda, <_\lambda)}$ e l'isomorfismo $f : SF(\lambda \rightarrow \alpha) \rightarrow \gamma$, e per ipotesi induttiva abbiamo:

$$EXT_\beta^\alpha [SF(\beta \rightarrow \alpha)] \sim SF(\beta \rightarrow \alpha) \stackrel{\text{Hyp. indutt.}}{\sim} \alpha^\beta$$

¹⁰³Tipo Mamino, è λ non β

quindi, sfruttando il fatto che $EXT_{\beta}^{\alpha}[SF(\beta \rightarrow \alpha)]$ è un segmenti iniziale di $SF(\beta \rightarrow \alpha)$, la restrizione di f a lui lo manda esattamente in α^{β} - poiché sopra abbiamo visto che sono buoni ordinamenti isomorfi, grazie alla transitività di \sim e naturalmente c'è un solo isomorfismo -, abbiamo dunque:

$$f[EXT_{\beta}^{\alpha}[SF(\beta \rightarrow \alpha)]] = \alpha^{\beta}$$

L'ultima osservazione che ci resta da fare è che, data $g \in SF(\lambda \rightarrow \alpha)$, detto $\delta := \max(\text{supp}(g))$, siccome λ è limite $\delta < s(\delta) < \lambda$, allora g è proprio l'estensione di una qualche funzione a supporto finito da $s(\delta)$ ad α , ovvero $g \in EXT_{s(\delta)}^{\alpha}[SF(s(\delta) \rightarrow \alpha)]$, pertanto vale:

$$SF(\lambda \rightarrow \alpha) = \bigcup_{\beta < \alpha} EXT_{\beta}^{\alpha}[SF(\beta \rightarrow \alpha)]$$

di conseguenza funziona il solito ragionamento:

$$\begin{aligned} \gamma &= f[SF(\lambda \rightarrow \alpha)] \\ &= f \left[\bigcup_{\beta < \alpha} EXT_{\beta}^{\alpha}[SF(\beta \rightarrow \alpha)] \right] \\ &\stackrel{(*)}{=} \bigcup_{\beta < \alpha} f[EXT_{\beta}^{\alpha}[SF(\beta \rightarrow \alpha)]] \\ &= \bigcup_{\beta < \alpha} \alpha^{\beta} = \alpha^{\lambda} \end{aligned}$$

□

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 inteso - 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 definendo esiste, con le definizioni estensionali è, invece, ricavarne le proprietà.

§10 Aritmetica ordinale e 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 $\beta_1 > \beta_2 > \dots > \beta_n$ (ordinali). Con queste forme normali di Cantor è possibile calcolare le operazioni aritmetiche in modo esplicito.

Nota 10.1 — Per procederemo con ordine, assumeremo la definizione ricorsiva delle operazioni ordinali e procederemo unicamente da quella.

Proposizione 10.2 (Monotonia delle operazioni fra ordinali)

Le funzioni $(\alpha, \beta) \mapsto \alpha + \beta$, $(\alpha, \beta) \mapsto \alpha \cdot \beta$ e $(\alpha, \beta) \mapsto \alpha^\beta$ sono **strettamente crescenti nel secondo argomento** - per $\alpha \cdot \beta$ assumendo $\alpha \neq 0$, per α^β assumendo $1 < \alpha$ - e **mai decrescenti [o crescenti debolmente] nel primo argomento**.

Per dimostrare la proposizione ci serviranno queste note.

Nota 10.3 (Condizione sufficiente per la disuguaglianza tra gli estremi superiori) — Dati due insiemi di ordinali X, Y non vuoti vale che:^a

$$\forall \alpha \in X \exists \beta \in Y \alpha \leq \beta \rightarrow \sup X \leq \sup Y$$

^aMoralmente: se posso dominare ogni elemento di X con un elemento di Y , allora vale la disuguaglianza tra gli estremi superiori.

Dimostrazione. Basta osservare che ogni maggiorante di Y è un maggiorante di X , e quindi in particolare si ottiene, dalla definizione di sup di X che $\sup X \leq \sup Y$.

Preso $\alpha \in X$, per ipotesi, esiste $\beta \in Y$ con $\alpha \leq \beta$, e, dato γ maggiorante di Y , si ha $\alpha \leq \beta \leq \gamma \rightarrow \alpha \leq \gamma$, per l'arbitrarietà di α abbiamo quindi che γ è un maggiorante di X , pertanto varrà in particolare che $\sup Y$ è un maggiorante di X e si conclude. \square

Nota 10.4 (Il successore è strettamente crescente) — La funzione classe $\alpha \mapsto s(\alpha)$ è una mappa strettamente crescente.

Dimostrazione. $\alpha < \beta \leftrightarrow s(\alpha) \leq \beta \leftrightarrow s(\alpha) < s(\beta)$, dove entrambe le equivalenze corrispondono alle osservazioni sul successore di uno dei due termini di una disuguaglianza. \square

Possiamo quindi dimostrare la proposizione.

Dimostrazione. Vediamo le due richieste nel caso della somma separatamente.

$\beta \mapsto \alpha + \beta$ è strettamente crescente

Dobbiamo dire che dati $\beta < \gamma$, vale che $\alpha + \beta < \alpha + \gamma$. Procediamo per **induzione transfinita v.2** γ (cioè quello a più a destra della somma, così da poter usare bene la definizione dell'operazione nel caso limite).

caso $\gamma = 0$ Vera a vuoto, poiché $\beta < 0 \leftrightarrow \beta \in \emptyset$.

caso $\gamma = s(\delta)$ Per ipotesi induttiva abbiamo che $\beta < \delta \rightarrow \beta + \alpha < \beta + \delta$. Preso $\beta < s(\delta)$, questo è equivalente a $\beta \leq \delta$, da cui, unendo entrambi i casi assieme, si ha:

$$\alpha + \beta \leq \alpha + \delta < s(\alpha + \delta) \stackrel{\text{def. ric.}}{=} \alpha + s(\delta) = \alpha + \gamma$$

dove la prima disegualanza si ha perché o $\beta = \delta$ o $\beta < \delta$, e quindi in un caso vale l'ipotesi induttiva, nell'altro c'è uguaglianza; la disegualanza stretta deriva invece dal fatto visto che il successore è strettamente crescente.

caso $\gamma = \lambda$ limite Dato $\beta < \lambda$, abbiamo $s(\beta) < \lambda$ (se così non fosse λ sarebbe successore), dunque, possiamo applicare l'ipotesi induttiva a β ed a $s(\beta)$, ottenendo:

$$\alpha + \beta < s(\alpha + \beta) = \alpha + s(\beta) \leq \sup\{\alpha + \delta | \delta < \lambda\} = \alpha + \lambda$$

dove per la seconda disegualanza è semplicemente la definizione di sup sull'insieme di tutte le possibili somme con secondo termine $< \lambda$, mentre l'ultima uguaglianza è la continuità della somma.

$\alpha \mapsto \alpha + \beta$ è non decrescente

Dobbiamo dire che $\alpha < \gamma$, allora $\alpha + \beta \leq \gamma + \beta$. Procediamo questa volta per [induzione transfinita v.2](#) su β (che è il termine più a destra della somma).

caso $\beta = 0$ Banale per la definizione ricorsiva della somma.

caso $\beta = s(\delta)$ Per ipotesi induttiva, vale che $\alpha < \gamma \rightarrow \alpha + \delta \leq \gamma + \delta$ e vogliamo dimostrare che $\alpha < \gamma \rightarrow \alpha + s(\delta) \leq \gamma + s(\delta)$. Usando l'osservazione sulla monotonia del successore fatta prima, e la definizione della somma nel caso successore, si ha:

$$\alpha + s(\delta) = s(\alpha + \delta) \stackrel{\text{Hp. indutt. + monoton.}}{\leq} s(\gamma + \delta) = \gamma + s(\delta)$$

caso $\beta = \lambda$ limite Per ipotesi induttiva, se $\delta < \lambda$, allora $\alpha < \gamma \rightarrow \alpha + \delta \leq \gamma + \delta$, dobbiamo verificare che quest'ultima implicazione vale con λ stesso al posto di δ

$$\alpha + \lambda \stackrel{(*)}{=} \sup\{\alpha + \delta | \delta < \lambda\} \leq \sup\{\gamma + \delta | \delta < \lambda\} \stackrel{(*)}{=} \gamma + \lambda$$

dove $(*)$ vale per la continuità della somma ordinale e la disegualanza larga al centro è il lemma della disegualanza dei sup, la cui ipotesi è soddisfatta dall'ipotesi induttiva.

Le dimostrazioni per il prodotto e l'esponenziale ripetono pedissequamente 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. \square

Esercizio 10.5. Le ipotesi che $\alpha \neq 0$ per il prodotto e $1 < \alpha$ per l'esponenziale dove sono usate?

Soluzione. Le ipotesi vengono usate nei casi successori rispettivamente del prodotto e della somma nel caso della monotonia stretta nella seconda componente (nel caso della monotonia debole sulla prima non ci sono particolari problemi). \square

Osservazione 10.6 (Controesempio alla stretta crescenza della prima componente) —

Basta considerare $0 + \omega$ e $1 + \omega$, infatti, ω è ordinale limite, dunque:

$$0 + \omega = \sup\{0 + n \mid n < \omega\} = \sup\{n \mid n < \omega\} = \bigcup\{n \mid n < \omega\} = \omega$$

$$1 + \omega = \sup\{1 + n \mid n < \omega\} = \sup\{s(n) \mid n < \omega\} = \bigcup\{s(n) \mid n < \omega\} = \omega$$

quindi la somma con ω dà lo stesso risultato, ma $0 < 1$, dunque la somma non è strettamente crescente nella prima componente.^a

^aUn controesempio per il prodotto può essere visto ad esempio con $1 \cdot \omega = 2 \cdot \omega = \omega$, e per l'esponenziale, come vedremo nella sezione dedicata alle regole di calcolo in forma normale, lo si può fare con $1^\omega = 2^\omega = \omega^\omega$.

Proposizione 10.7 (Proprietà delle operazioni fra ordinali)

Dati $\alpha, \beta, \gamma \in \text{Ord}$ valgono le seguenti proprietà:

associatività:

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \quad (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

distributività a sinistra:

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

proprietà delle potenze:

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

Nota 10.8 — Abbiamo già asserito la proposizione corrispondente per i buoni ordinamenti (notare gli uguali al posto dei simboli di isomorfismo in questo caso), ma lasciando la dimostrazione per esercizio. Lasceremo comunque parte della dimostrazione per esercizio, ma non invano: è un esercizio più facile.

Osservazione 10.9 ($\sup X \notin X \implies \sup X$ ordinale limite) — Dato X un insieme di ordinali, sappiamo che è sempre ben definito $\sup X \in \text{Ord}$, se vale che $\sup X \notin X$, allora si ha che $\sup X$ è limite.^a

^aNotare che la freccia opposta non è in generale vera, ad esempio prendendo $X = \{\omega\}$, si ha che $\sup X = \omega \in X$.

Dimostrazione. Se per assurdo $\sup X = \alpha + 1$, siccome $\sup X$ non è elemento di X ed è un suo maggiorante, si ha $\forall \beta \in X \ \beta < \alpha + 1$, cioè $\forall \beta \in X \ \beta \leq \alpha$, ovvero α è un maggiorante di X strettamente più piccolo di $\alpha + 1 = \sup X$. \square

Osservazione 10.10 (Le operazioni tra ordinali commutano col sup) — Dato X un insieme di ordinali e $\alpha \in \text{Ord}$ vale che le tre operazioni tra gli ordinali definite per ricorsione transfinita commutano col sup a destra:^a

$$\alpha + \sup X = \sup\{\alpha + \beta \mid \beta \in X\} \quad \alpha \cdot \sup X = \sup\{\alpha \cdot \beta \mid \beta \in X\}$$

$$\alpha^{\sup X} = \sup\{\alpha^\beta \mid \beta \in X\}$$

^aD'altronde abbiamo appena visto che se $\sup X \notin X$ il sup è un ordinale limite, e noi abbiamo costruito le operazioni per essere continue a destra, quindi questo fatto risulta una conseguenza abbastanza naturale.

Dimostrazione. Le dimostrazioni sono uguali. Vediamo la prima.

Se $\sup X \in X$, poiché abbiamo visto che la funzione $\beta \mapsto \alpha + \beta$ è strettamente crescente, segue facilmente che $\alpha + \sup X$ è un maggiorante di $\alpha + \beta$, con $\beta \in X$, in quanto $\beta \leq \sup X$, in particolare, sempre per monotonia è proprio il minore dei maggioranti.

Se $\lambda := \sup X \notin X$ (in questo caso è facile dire che la somma è un maggiorante, ma difficile dire che è il minimo), per quanto visto nell'osservazione sopra sappiamo che λ è limite, per cui:

$$\alpha + \lambda \stackrel{\text{def. } +}{=} \sup \underbrace{\{\alpha + \gamma \mid \gamma < \lambda\}}_{=:A} \stackrel{(*)}{=} \sup \underbrace{\{\alpha + \beta \mid \beta \in X\}}_{=:B}$$

per dimostrare $(*)$, osserviamo in primis che $\alpha + \lambda$ è un maggiorante [stretto] di $\{\alpha + \beta \mid \beta \in X\}$ per la monotonia della somma nella seconda componente, in quanto $\lambda > \beta$. Per la disegualianza opposta, data la minimalità di λ , si che $\forall \gamma < \lambda \exists \beta \in X \beta \geq \lambda$, da cui per monotonia, $\alpha + \gamma \leq \alpha + \beta$, dunque per il lemma sulla disegualianza del sup, si conclude che $\sup\{\alpha + \beta \mid \beta \in X\} \geq \alpha + \lambda$. \square

Possiamo quindi dimostrare la proposizione sulle proprietà delle operazioni tra ordinali.

Dimostrazione. Sono tutte facili induzioni su γ^{104} . 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 $\gamma = 0$ Si vede immediatamente $(\alpha + \beta) + 0 \stackrel{\text{def. ricors.}}{=} \alpha + \beta \stackrel{\text{def. ricors.}}{=} \alpha + (\beta + 0)$.

caso $\gamma = s(\delta)$ Segue dall'ipotesi induttiva e dalla definizione ricorsiva della somma ordinale:

$$\begin{aligned} (\alpha + \beta) + s(\delta) &\stackrel{\text{def. ricors.}}{=} s((\alpha + \beta) + \delta) \\ &\stackrel{\text{Hyp. indutt.}}{=} s(\alpha + (\beta + \delta)) \\ &\stackrel{\text{def. ricors.}}{=} \alpha + s(\beta + \delta) \\ &\stackrel{\text{def. ricors.}}{=} \alpha + (\beta + s(\delta)) \end{aligned}$$

caso $\gamma = \lambda$ limite Ancora una volta segue dall'ipotesi induttiva e dalla definizione ricorsiva della somma nel caso limite:

$$\begin{aligned} (\alpha + \beta) + \lambda &\stackrel{\text{def. ricors.}}{=} \sup\{(\alpha + \beta) + \delta \mid \delta < \lambda\} \\ &\stackrel{\text{Hyp. indutt.}}{=} \sup\{\alpha + (\beta + \delta) \mid \delta < \lambda\} \\ &\stackrel{\text{Oss. sopra}}{=} \alpha + (\sup\{\beta + \delta \mid \delta < \lambda\}) \\ &\stackrel{\text{def. ricors.}}{=} \alpha + (\beta + \lambda) \end{aligned}$$

\square

¹⁰⁴Come sempre l'ordinale più a destra, per poter sfruttare la continuità.

§10.1 Sottrazione e divisione euclidea

Introduciamo, ora, due lemmi che serviranno per calcolare la formale normale di Cantor: la sottrazione e la divisione di ordinali.

Lemma 10.11 (Sottrazione ordinale)

Dati $\alpha, \gamma \in \text{Ord}$, con $\alpha \leq \gamma^a$, esiste un unico $\beta \in \text{Ord}$ tale che $\alpha + \beta = \gamma$.

^aNaturalmente non può accadere che $\gamma < \alpha \leq \alpha + \gamma'$.

Intuitivamente $\gamma \sim \alpha \sqcup (\gamma \setminus \alpha)$, penando alla somma ordinale come somma buoni ordini, dove abbiamo proprio che $\gamma \setminus \alpha = \{\delta \in \gamma \mid \delta \notin \alpha\}$.



Vediamo ora una dimostrazione formale.

Dimostrazione. Vediamo esistenza e unicità separatamente.

unicità Abbiamo l'unicità perché la funzione $+$ è strettamente crescente nel secondo argomento, come visto in precedenza, dunque se ci fosse un altro ordinale diverso da β , per la totalità dell'ordinamento sugli ordinali, sarebbe $<$ o $>$ di β , da cui anche la somma sarebbe strettamente minore o maggiore e quindi diversa da γ , pertanto β è unico.

esistenza Se $\alpha = \gamma$ è sufficiente prendere $\beta = 0$. Possiamo quindi supporre che $\alpha < \gamma$ e consideriamo il minimo δ tale che la somma supera γ , $\gamma < \alpha + \delta - \delta$ esiste poiché $\gamma < s(\gamma) \leq \alpha + s(\gamma)$ e quindi l'insieme degli ordinali la cui somma con α a sinistra è maggiore strettamente di γ è non vuoto.

Se δ è successore, $\delta = \beta + 1$, allora, per la minimalità di δ , si ha $\alpha + \beta \leq \gamma < s(\alpha + \beta) = \alpha + s(\beta) = \alpha + \delta$, pertanto nella prima disegualanza non può valere il minore stretto, perché se così fosse si avrebbe che $\gamma \geq s(\alpha + \beta) = \alpha + \delta$, che è assurdo, quindi abbiamo proprio che $\alpha + \beta = \gamma$.

Osserviamo ora che δ non può essere limite e così abbiamo concluso. Se δ fosse limite avremmo:

$$\gamma \stackrel{\text{def. } \delta}{<} \alpha + \delta \stackrel{\text{def. } +}{=} \sup_{\varepsilon < \delta} (\alpha + \varepsilon)$$

ma allora, dovendo essere il sup di un insieme non vuoto, ciò vuol dire, affinché la disegualanza scritta sia vera, che esiste $\varepsilon < \delta$ tale che $\gamma < \alpha + \varepsilon$, contro la minimalità di δ , che è assurdo. Alternativamente, ci bastava osservare che, per la minimalità di δ , $\alpha + \varepsilon \leq \gamma$, per ogni $\varepsilon < \delta$, per cui passando la disegualanza al sup, avremmo ottenuto $\sup_{\varepsilon < \delta} (\alpha + \varepsilon) \leq \gamma$, che unito alla catena sopra ci dà ancora una volta un assurdo.^{105 106}

□

¹⁰⁵Il passaggio delle disegualanze larghe al sup è conseguenza del lemma visto ad inizio capitolo sulle disegualanze tra sup.

¹⁰⁶L'esistenza può essere dimostrata in modo equivalente per induzione transfinita.

Lemma 10.12 (Divisione euclidea di ordinali)

Dati $\alpha, \gamma \in \text{Ord}$, con $\alpha \neq 0$, esistono e sono unici $\beta, \rho \in \text{Ord}$ tali che $\rho < \alpha$ e $\alpha \cdot \beta + \rho = \gamma$.

Dimostrazione. Verifichiamo esistenza e unicità separatamente.

unicità Fissato β, ρ è unico, o per monotonia stretta nella seconda componente della somma o per il lemma sulla sottrazione visto sopra¹⁰⁷. Dobbiamo quindi dimostrare solo l'unicità di β . Supponiamo per assurdo di avere $\beta \neq \beta'$, e WLOG $\beta < \beta'$, con relativamente resti $\rho, \rho' < \alpha$, per cui $\alpha \cdot \beta + \rho = \alpha \cdot \beta' + \rho'$, allora sfruttando la monotonia si ottiene:

$$\begin{aligned} \alpha \cdot \beta + \rho &< \alpha \cdot \beta + \alpha \\ &= \alpha \cdot s(\beta) && (\text{def. ricorsiva } \cdot) \\ &\leq \alpha \cdot \beta' && (\beta < \beta') \\ &\leq \alpha \cdot \beta' + \rho' && (\rho' \geq 0) \\ &= \alpha \cdot \beta + \rho && \text{(Hyp. assurda)} \end{aligned}$$

esistenza Procediamo come nella dimostrazione del lemma di sottrazione, e consideriamo il minimo δ tale che $\gamma < \alpha \cdot \delta$ - tale δ esiste, cioè l'insieme è non vuoto, in quanto $\gamma = 1 \cdot \gamma \leq \alpha \cdot \gamma < \alpha \cdot s(\gamma)$. Assumiamo che δ sia successore, $\delta = s(\beta)$, allora per la minimalità di δ , si ha $\alpha \cdot \beta \leq \gamma$ ¹⁰⁸, possiamo quindi applicare il lemma di sottrazione ordinale ed ottenere l'unico ρ per cui:

$$\alpha \cdot \beta + \rho = \gamma$$

Osserviamo ora che $\rho < \alpha$, infatti, se per assurdo fosse $\rho \geq \alpha$, avremmo:

$$\begin{aligned} \gamma &< \alpha \cdot \delta \\ &= \alpha \cdot s(\beta) \\ &= \alpha \cdot \beta + \alpha \\ &\leq \alpha \cdot \beta + \rho = \gamma \end{aligned}$$

Infine dobbiamo verificare che δ non sia limite, se per assurdo lo fosse, avremmo:

$$\gamma < \alpha \cdot \delta = \sup_{\varepsilon < \delta} (\alpha \cdot \varepsilon)$$

dove, affinché la disegualanza sia valida, il sup al RHS deve essere ben definito, e per un insieme di ordinali lo è, come abbiamo visto, quando l'insieme è non vuoto, per cui esiste $\varepsilon < \delta$ tale per cui $\gamma < \alpha \cdot \varepsilon$, contro la minimalità di δ , che è assurdo. Alternativamente si può osservare che, per la minimalità di δ , $\forall \varepsilon < \delta \alpha \cdot \varepsilon \leq \gamma$, tale disegualanza passa al sup, ed aggiunta in fondo alla catena scritta sopra ci dà nuovamente un assurdo.

□

¹⁰⁷Di fatto, essendo che l'unicità nella sottrazione la si ha come conseguenza della monotonia stretta nella seconda componente, il motivo per cui si ha unicità è sempre la monotonia della somma.

¹⁰⁸Notare che non vale necessariamente l'uguale come nella dimostrazione del lemma di sottrazione perché, supponendo il minore stretto, qui avremmo $\gamma \geq s(\alpha \cdot \beta) \neq \alpha \cdot \beta + \beta = \alpha \cdot s(\beta) = \alpha \cdot \delta$.

§10.2 La forma normale di Cantor

Teorema 10.13 (Forma normale di Cantor - CNF)

Ogni ordinale α può essere espresso in maniera unica come somma finita del tipo:

$$\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n$$

con $\beta_1 > \beta_2 > \dots > \beta_n$ ordinali, $k_1, k_2, \dots, k_n \in \omega \setminus \{0\}$ e $n \in \omega$.

Dimostrazione. Dividiamo la dimostrazione in esistenza ed unicità.

esistenza Procediamo per induzione transfinita, supponiamo che ogni ordinale strettamente più piccolo di α abbia una forma normale e verifichiamo che anche α la abbia. Sia γ il minimo tale che $\alpha < \omega^\gamma$ - che esiste in quanto $\alpha \leq \omega_\alpha < \omega^{s(\alpha)}$, dove la prima disegualanza è il fatto che $x \mapsto \omega^x$ è una funzione strettamente crescente tra buoni ordini. Come nei lemmi precedenti, diamo per buono che γ sia successore, $\gamma = s(\beta)$, allora abbiamo che $\omega^\beta \leq \alpha$, possiamo fare la divisione euclidea di α per ω^β e ottenere:

$$\alpha = \omega^\beta \cdot k + \rho \quad \rho < \omega^\beta \leq \alpha$$

con k e ρ unici. A questo punto vale l'ipotesi induttiva per ρ e lo si può scrivere in CNF, per verificare che allora anche α sia scritto in CNF è necessario osservare due cose. In primis che $0 < k < \omega$, infatti:

- $k = 0$: in questo caso $\alpha = \rho < \alpha \not\models$.
- $k \geq \omega$: in questo caso $\alpha < \omega^\gamma = \omega^{s(\beta)} = \omega^\beta \cdot \omega \leq \omega^\beta \cdot k \leq \omega^\beta \cdot k + \rho = \alpha \not\models$.

Osserviamo inoltre che, dato che $\rho < \omega^\beta$, scrivendo, con l'ipotesi induttiva, $\rho = \omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n$, si ha $\beta_2 < \beta$, infatti, se così non fosse, cioè se fosse che $\beta_2 \geq \beta$, avremmo:

$$\omega^\beta \leq \omega^{\beta_2} \leq \omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n = \rho < \omega^\beta \not\models$$

pertanto la scrittura ottenuta dalla divisione di α per ω^β è effettivamente una scrittura di α in forma normale di Cantor.

Ci resta soltanto da verificare che il γ usato all'inizio non è limite, se per assurdo lo fosse, avremmo:

$$\alpha < \omega^\gamma = \sup_{\delta < \gamma} \omega^\delta$$

e affinché la disegualanza sia vera il sup al RHS deve essere ben definito, e lo è a condizione che l'insieme di ordinali su cui è preso è non vuoto, ovvero a condizione che esista $\delta < \gamma$ tale che $\alpha < \omega^\delta$, contro la minimalità di γ .¹⁰⁹

unicità Sia α minimo ordinale che non ha un'unica forma normale¹¹⁰, per cui abbiamo che α si può scrivere in almeno due forme normali di Cantor distinte:

$$\begin{aligned} \alpha &= \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n \\ &= \omega^{\beta'_1} \cdot k'_1 + \omega^{\beta'_2} \cdot k'_2 + \dots + \omega^{\beta'_{n'}} \cdot k'_{n'} \end{aligned}$$

¹⁰⁹Come al solito si può osservare alternativamente anche che la disegualanza $\omega^\delta \leq \alpha$, valida per la minimalità di γ , passa al sup generando ancora una volta un assurdo.

¹¹⁰Lo possiamo prendere perché abbiamo visto che la classe degli ordinali è bene ordinata.

dove n' non è necessariamente uguale ad n , per cui le scritture possono avere lunghezza diversa. Ci basta dimostrare che $\beta_1 = \beta'_1$ e $k_1 = k'_1$, infatti in tal caso, per la stretta monotonia otteniamo:

$$\omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n = \omega^{\beta'_2} \cdot k'_2 + \dots + \omega^{\beta'_{n'}} \cdot k'_{n'} < \omega^{\beta_1}, \omega^{\beta'_1}$$

dunque avremmo trovato un ordinale strettamente più piccolo di α con almeno due scritture distinte in CNF e quindi avremmo un assurdo.

Se abbiamo che $\beta_1 = \beta'_1$, allora necessariamente anche $k_1 = k'_1$, infatti in questo caso possiamo scrivere:

$$\alpha = \omega^{\beta_1} \cdot k_1 + \underbrace{\dots}_{<\omega^{\beta_1}} = \omega^{\beta_1} \cdot k'_1 + \underbrace{\dots}_{<\omega^{\beta_1}}$$

cioè nella forma della divisione euclidea, e quindi otteniamo $k_1 = k'_1$, per unicità della scrittura in questa forma¹¹¹.

Ci resta quindi solo da verificare che $\beta_1 = \beta'_1$, se per assurdo supponessimo, WLOG, che $\beta_1 < \beta'_1$, dunque $s(\beta_1) \leq \beta'_1$, avremmo:

$$\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n < \omega^{s(\beta_1)} \leq \omega^{\beta'_1} \cdot k'_1 + \dots = \alpha \text{ f}$$

□

Esercizio 10.14. Dimostrare le diseguaglianze in viola (sono tutte uguali).

Soluzione. Per l'ultima diseguaglianza basta osservare che per monotonia:

$$\omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n \leq \omega^{\beta_1} \cdot k_1 + \omega^{\beta_1} \cdot k_2 + \dots + \omega^{\beta_1} \cdot k_n = \omega^{\beta_1} \cdot (\underbrace{k_1 + \dots + k_n}_{=:k})$$

e a questo punto $\omega^{\beta_1} \cdot k < \omega^{\beta_1} \cdot \omega = \omega^{s(\beta_1)}$. Per le prime tre diseguaglianze, basta ragionare in maniera identica con $\omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n$ (analogamente con la versione con i'), ottenendo $\omega^{\beta_2} \cdot k < \omega^{\beta_2} \cdot (k+1) \leq \omega^{s(\beta_2)} \leq \omega^{\beta_1}$. □

§10.3 Punti fissi e ε -numbers

Si potrebbe credere che il teorema precedente, applicato ricorsivamente agli esponenti β_1, \dots, β_n , implichi che ogni ordinale si possa scrivere sotto forma di un'espressione finita composta di somme, prodotti e potenze delle costanti $0, 1, 2, \dots, \omega$. Tipo questa:

$$\omega^{\omega^4 \cdot 7 + \omega^2 \cdot 1} \cdot 9 + \omega^{75} + 9$$

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 $\varepsilon_0 = \omega^{\varepsilon_0}$ ¹¹². La forma normale di Cantor di ε_0 è quindi, chiaramente, ω^{ε_0} , e procedere ricorsivamente sull'esponente $\omega^{\varepsilon_0}, \omega^{\omega^{\varepsilon_0}}, \text{etc.}$ non conduce ad un'espressione finita, intuitivamente verrebbe una cosa del tipo:

$$\varepsilon_0 = \underbrace{\omega^{\omega^{\omega^{\dots}}}}_{\omega \text{ volte}}$$

La proposizione seguente è interessante di per sé, ma, in particolare, ci permetterà di dimostrare l'esistenza degli ε -numbers.

¹¹¹Inoltre otterremo anche che le code sono uguali, ma di nuovo ciò è di fatto sempre una conseguenza della monotonia stretta sulla seconda componente.

¹¹²Notare che in questo caso non vale che $\alpha > \beta_1$, e quindi ε_0 non può essere scritto nella forma sopra.

Proposizione 10.15 (Ogni funzione normale ha una classe propria di punti fissi)

Sia $F : \text{Ord} \rightarrow \text{Ord}$ una funzione classe **strettamente** crescente e continua^a - ossia $F(\lambda) = \sup F[\lambda] = \sup_{\alpha < \lambda} F(\alpha)$ per λ limite. Allora, per ogni $\alpha \in \text{Ord}$, F ha un punto fisso $\geq \alpha$, ossia vale che:

$$\exists \pi \in \text{Ord} \quad \alpha \leq \pi \wedge F(\pi) = \pi$$

^aTali funzioni prendono il nome di **funzioni normali**.

Dimostrazione. Fissato $\alpha \in \text{Ord}$ costruiamo un punto fisso di F che sia maggiore o uguale ad α . Definiamo per ricorsione numerabile:

$$\pi_n := \begin{cases} \pi_0 = \alpha \\ \pi_{n+1} = F(\pi_n) \end{cases}$$

se $F(\alpha) = \alpha$ allora $\pi_n = \alpha$ ed abbiamo il punto fisso voluto, altrimenti, essendo F strettamente crescente, si ha $\alpha < F(\alpha)$, cioè $\pi_0 < \pi_1$ ¹¹³, da cui si verifica per induzione che π_n è strettamente crescente¹¹⁴, $\forall n \in \omega \quad \pi_n < \pi_{n+1}$, di conseguenza, detto:

$$\pi \stackrel{\text{def}}{=} \sup_{n \in \omega} \pi_n$$

abbiamo che π è un ordinale limite, poiché $\pi \notin \{\pi_n | n \in \omega\}$ (altrimenti non sarebbe il sup), inoltre naturalmente $\pi > \pi_0 = \alpha$, per cui:

$$F(\pi) \stackrel{F \text{ continua}}{=} \sup_{n \in \omega} F(\pi_n) \stackrel{\text{def}}{=} \sup_{n \in \omega} \pi_{n+1} = \pi$$

□

Osservazione 10.16 (I punti fissi sono una classe propria di ordinali) — Abbiamo dimostrato che per ogni ordinale c'è un punto fisso di F (sotto opportune ipotesi) che è maggiore di tale ordinale, pertanto i punti fissi di F non possono formare un insieme di ordinali perché non esiste un estremo superiore, dunque formano una (sotto)classe propria di Ord .

Esempio 10.17 ($x \mapsto \omega^x$)

La mappa $x \mapsto \omega^x$ è strettamente crescente, per la monotonia stretta dell'esponenziale nella seconda componente, ed è continua in quanto abbiamo definito l'esponenziale di ordinali infiniti estendendo per continuità la definizione dal caso finito, pertanto per il teorema sopra tale mappa ha una classe propria di punti fissi, che sono appunto tali per cui $\varepsilon = \omega^\varepsilon$.

¹¹³Type Mamino scrive ovunque 0 al posto di α .

¹¹⁴Per ipotesi induttiva $\pi_{n-1} < \pi_n$, e poiché F è strettamente crescente, applicandola alla diseguaglianza si ottiene $\pi_n < \pi_{n+1}$, quindi il passo induttivo.

Esercizio 10.18. Sia $\varepsilon_0 = \sup\{1, \omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \dots\}$. Formalmente definiamo per ricorsione numerabile $\alpha_0 = 1$, $\alpha_{n+1} = \omega^{\alpha_n}$, allora $\varepsilon_0 = \sup\{\alpha_n \mid n \in \omega\}$. Dimostrare che ε_0 è il più piccolo punto fisso della funzione $x \mapsto \omega^x$.

Soluzione. Osserviamo in primis che ε_0 è un ordinale limite, per farlo ci basta osservare che $\varepsilon_0 \notin \{\alpha_n \mid n \in \omega\}$, infatti la successione α_n è strettamente crescente, dunque se fosse che $\varepsilon_0 = \alpha_m$, per $m \in \omega$, allora $\alpha_{m+1} > \varepsilon_0$ e quindi quest'ultimo non sarebbe il sup, che è assurdo, segue quindi che ε_0 è limite per un lemma visto.¹¹⁵

Verifichiamo ora che ε_0 è un punto fisso di $x \mapsto \omega^x$:

$$\varepsilon_0 \stackrel{\text{def}}{=} \sup_{n \in \omega} \alpha_n \stackrel{(*)}{=} \sup_{n \in \omega} \omega^{\alpha_n} \stackrel{\text{lemma}}{=} \omega^{\sup_{n \in \omega} \alpha_n} \stackrel{\text{def}}{=} \omega^{\varepsilon_0}$$

dove (*) vale per il lemma della disuguaglianza dei sup applicato in ambo i versi, infatti dato α_n , è sufficiente prendere ω^{α_n} nel secondo insieme per avere la prima disuguaglianza, viceversa, preso ω^{α_n} nel secondo, basta osservare che $\alpha_{n+1} = \omega^{\alpha_n}$ è nel primo.

Infine osserviamo che ε_0 è il più piccolo punto fisso di $x \mapsto \omega^x$, infatti, se esistesse $y < \varepsilon_0$ punto fisso di $x \mapsto \omega^x$, allora avremmo:

$$\alpha_n \leq y < \alpha_{n+1} \quad 116$$

infatti $y \in \bigcup_{n+1} \alpha_n$, dunque y è almeno in un α_n che è successore (altrimenti basta prendere il successivo), e ci basta prendere il minimo successore a cui appartiene per avere la disuguaglianza sopra (se il termine di testa di y in CNF non fosse $\geq \alpha_n$, allora α_{n+1} non sarebbe il minimo a cui appartiene y). Dalle disuguaglianze sopra segue che:

$$\alpha_{n+1} = \omega^{\alpha_n} \leq \omega^y \leq \omega^{\alpha_{n+1}} = \alpha_{n+2}$$

per cui se y fosse un punto fisso, si avrebbe $y < \alpha_{n+1} \leq \omega^y = y$. \square

Esercizio 10.19 (Lista dei punti fissi di una funzione normale). Sia $F : \text{Ord} \rightarrow \text{Ord}$ crescente e continua, allora esiste $G : \text{Ord} \rightarrow \text{Ord}$ strettamente crescente tale che:

$$\forall \alpha \in \text{Ord} \quad F(\alpha) = \alpha \leftrightarrow \exists \beta \in \text{Ord} \quad \alpha = G(\beta)$$

Soluzione. Dalla proposizione sopra abbiamo visto che i punti fissi di $F : \text{Ord} \rightarrow \text{Ord}$ sono una classe propria C_F , dunque possiamo definire per ricorsione transfinita:

$$G(\alpha) = \min\{x \in C_F : \forall y \in G[\alpha] \quad x > y\} \quad 117$$

che è ben definita per il teorema di ricorsione transfinita, ed è strettamente crescente per costruzione. Verifichiamo inoltre che $\text{Im}(G) = C_F$, preso $\beta \in C_F$, si ha che:

$$\beta < s(\beta) \leq G(s(\beta))$$

ed essendo $G(s(\beta))$ il più piccolo ordinale in C più grande di tutti gli ordinali di $G[s(\beta)]$, per minimalità, si ha che esiste $\gamma \in G[s(\beta)]$ tale che $\gamma \geq \beta$, da cui $\beta \in G[s(\beta)]$, e quindi $\beta \in \text{Im}(G)$. Segue quindi che G è un isomorfismo tra Ord e $C_F \subseteq \text{Ord}$, ed in tal modo soddisfa la tesi, infatti $\forall \alpha \in \text{Ord} \quad F(\alpha) = \alpha \iff \alpha \in C_F \stackrel{G \text{ surg.}}{\iff} \exists \beta \in C_F \quad G(\beta) = \alpha$. \square

¹¹⁵In realtà non serve osservarlo per poter applicare il lemma di commutazione tra potenze e sup di insiemi di ordinali, ma è comunque interessante notarlo.

¹¹⁶Il caso $y \in \omega$ andrebbe fatto a parte per essere precisi, ma è molto facile osservare che anche in questo caso segue la tesi.

¹¹⁷Non stiamo usando separazione, è solo una formula insiemistica, e il minimo è sempre ben definito perché la classe C_F è una sottoclasse di Ord che è bene ordinata, e C_F è sempre non vuota perché è una classe propria.

Esercizio 10.20 (Unicità della lista). La G dell'esercizio precedente è univocamente determinata da F ed è una funzione classe continua.

Soluzione. Verifichiamo che data $H : \text{Ord} \rightarrow C_F \subseteq \text{Ord}$ strettamente crescente e che soddisfi la proprietà $\forall \alpha \in \text{Ord} \ F(\alpha) = \alpha \leftrightarrow \exists \beta \in \text{Ord} \ \alpha = H(\beta)$ (che equivale al fatto che $\text{Im}(H) = C_F$, ovvero H isomorfismo tra Ord e C_F , la classe propria dei punti fissi di F), allora soddisfa la definizione ricorsiva di G data nell'esercizio precedente, e quindi coincide proprio con quest'ultima per il teorema di ricorsione transfinita, da cui segue quindi l'unicità della lista dei punti fissi G .

Poiché H è strettamente crescente per ipotesi, naturalmente $H(\alpha)$ è più grande di tutti gli elementi di $H[\alpha]$, inoltre, se esistesse $\gamma \in C_F$, tale che $\gamma < H(\alpha)$ e maggiore di tutti gli $H[\alpha]$, allora $\gamma > F(\delta)$ per $\delta < \alpha$, per la monotonia di H , e $\gamma < F(\delta)$ per $\delta \geq \alpha$, dunque $\gamma \notin \text{Im}(H)$, che è per ipotesi contro la surgettività di $H : \text{Ord} \rightarrow C_F$, dunque $H(\alpha)$ è proprio il più piccolo ordinale di C_F più grande di tutti gli ordinali in $H[\alpha]$, pertanto H soddisfa la relazione ricorsiva di G e quindi coincide con quest'ultima.

La continuità di G segue banalmente dalla definizione ricorsiva che abbiamo dato, infatti:

$$G(\lambda) = \min\{x \in C_F : \forall y \in G[\lambda] \ x > y\} = \sup_{\alpha < \lambda} G[\lambda] = \sup_{\alpha < \lambda} G(\alpha)$$

□

Osservazione 10.21 (Derivata di funzioni ordinali) — Data una funzione $F : \text{Ord} \rightarrow \text{Ord}$ normale la proposizione iniziale ci dice che F ha una classe propria di punti fissi, e gli ultimi due esercizi ci dicono che tali punti fissi possono essere elencata in modo unico e strettamente crescente da una nuova funzione $G : \text{Ord} \rightarrow \text{Ord} : \alpha \mapsto \alpha\text{-esimo punto fisso di } F$, tale funzione prende talvolta in letteratura il nome di **derivata** di F . Notare infine che G , per quanto abbiamo visto, è, per costruzione, a sua volta normale, dunque può essere “derivata” a sua volta, dandoci nuovamente un'unica lista dei suoi punti fissi.

Definizione 10.22 (ε -numbers). Definiamo l'unica funzione che elenca i punti fissi di $x \mapsto \omega^x$, ovvero la sua derivata, ε_α , i cui valori prendono il nome di **epsilon-numbers** e sono appunto i punti fissi di $x \mapsto \omega^x$ elencati in maniera ordinata dagli ordinali.

Definizione 10.23 (ζ -numbers). Definiamo l'unica funzione che elenca i punti fissi della funzione ε_α , ovvero la sua derivata¹¹⁸, ζ_α , i cui valori prendono il nome di **zeta-numbers** e sono appunto i punti fissi di ζ_α elencati in maniera ordinata dagli ordinali.

I primi due esercizi seguenti saranno assai più facili quando, usando l'assioma della scelta, dimostreremo che un insieme numerabile di insiemi numerabili è numerabile.¹¹⁹

Esercizio 10.24 (★ Difficile senza leggere l'idea sotto). $|\varepsilon_0| = \aleph_0$.^a

^a**Idea:** dimostrare che $\alpha \in \varepsilon_0$ 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.

Soluzione. Per definizione $\varepsilon_0 = \sup\{\alpha_n \mid n \in \omega\}$, dove $\alpha_0 = 1$ e $\alpha_{n+1} = \omega^{\alpha_n}$, si ha che $\varepsilon_0 \geq \alpha_1 = \omega$, dunque $\omega \subseteq \varepsilon_0 \rightarrow \aleph_0 \leq |\varepsilon_0|$.¹²⁰ Per la diseguaglianza opposta □

¹¹⁸Sarebbe la derivata seconda di $x \mapsto \omega^x$.

¹¹⁹Ricordare che l'avevamo già dimostrato dando per buono di avere una successione di enumerazioni, ma anche il quel caso l'enumerazione ce la si può procurare solo con scelta.

¹²⁰Se avessimo AC potremmo concludere immediatamente l'altra diseguaglianza dimostrando per induzione che $|\alpha_n| = \aleph_0$, da cui $|\varepsilon_0| = |\sup_{n \in \omega} \alpha_n| = |\bigcup_{n \in \omega} \alpha_n| \stackrel{\text{AC}}{\leq} \aleph_0$.

Esercizio 10.25 (★ Ostico). Sia ζ_0 minimo tale che $\varepsilon_{\zeta_0} = \zeta_0$, allora $|\zeta_0| = \aleph_0$.

Soluzione. Per gli esercizi sopra, sappiamo che ζ_α è la funzione che elenca i punti fissi di ε_α in maniera strettamente crescente, dunque ζ_0 è il più piccolo punto fisso di ε_α per definizione. Dallo stesso teorema, sappiamo che ε_α , essendo a sua volta successione crescente di punti fissi di $x \mapsto \omega^x$, è strettamente crescente, per cui $\varepsilon_0 \leq \varepsilon_{\zeta_0}$, da cui otteniamo la disegualanza dal basso $\aleph_0 = |\varepsilon_0| \leq |\zeta_0|$.

Per il viceversa \square

Esercizio 10.26 (Teorema di scrittura in base ordinale). Sia γ un qualunque ordinale ≥ 2 . Ogni ordinale α si scrive in modo unico come somma finita:

$$\alpha = \gamma^{\beta_1} \cdot k_1 + \dots + \gamma^{\beta_n} \cdot k_n$$

con $\beta_1 > \beta_2 > \dots > \beta_n$ ordinali, $k_1, \dots, k_n \in \gamma \setminus \{0\}$ e $n \in \omega$.

Soluzione. Dividiamo esistenza ed unicità della scrittura in base γ .

esistenza Procediamo per induzione transfinita forte, dunque supponiamo che tutti gli ordinali minori strettamente di α si possano scrivere in base γ come sopra, e dimostriamo che anche α si può scrivere in tale forma.

Sia δ il minimo ordinale tale che $\alpha < \gamma^\delta$ - che esiste in quanto $x \mapsto \gamma^x$ è strettamente crescente tra classi bene ordinate, per cui $\alpha \leq \gamma^\alpha < \gamma^{s(\alpha)}$, e quindi la sottoclasse di Ord da cui prendiamo il minimo è non vuota. Assumiamo che $\delta = \beta + 1$, e per minimalità di δ si ha $\gamma^\beta \leq \alpha$ e applichiamo il lemma di divisione euclidea per ottenere:

$$\alpha = \gamma^\beta \cdot k + \rho \quad \rho < \gamma^\beta \leq \alpha$$

con k e ρ unici. Possiamo applicare l'ipotesi induttiva a ρ e scrivere $\rho = \gamma^{\beta_2} \cdot k_2 + \dots + \gamma^{\beta_n} \cdot k_n$, a questo punto, per dire che la scrittura trovata dalla divisione sostituendo ρ con la sua scrittura in base γ , è effettivamente una scrittura in base γ per α , dobbiamo verificare due cose. In primis osserviamo che $0 < k < \gamma$:

- $k = 0$: in tal caso $\alpha = \rho < \alpha \cancel{<} \alpha$.
- $k \geq \gamma$: in questo caso $\gamma^\delta = \gamma^{\beta+1} = \gamma^\beta \cdot \gamma \leq \gamma^\beta \cdot k \leq \gamma^\beta \cdot k + \rho = \alpha < \gamma^\delta \cancel{<} \alpha$.

Osserviamo inoltre che $\beta > \beta_2$, infatti, se fosse $\beta_2 \geq \beta$ si avrebbe:

$$\gamma^\beta \leq \gamma^{\beta_2} \leq \gamma^{\beta_2} \cdot k_2 + \dots + \gamma^{\beta_n} \cdot k_n = \rho < \gamma^\beta \cancel{<} \alpha$$

quindi abbiamo ottenuto che esiste almeno una scrittura in base γ per α . Ci resta soltanto da verificare l'assunzione iniziale che δ sia successore e non limite, se δ fosse limite si avrebbe:

$$\alpha < \gamma^\delta = \sup_{\varepsilon < \delta} \gamma^\varepsilon$$

affinché la disegualanza sia vera l'insieme di ordinali su cui si prende il sup al RHS deve essere non vuoto, cioè deve esistere $\varepsilon < \delta$ tale che $\alpha < \gamma^\varepsilon$, contro la minimalità di δ . Alternativamente si può osservare che, per la minimalità di δ , si ha $\forall \varepsilon < \delta \gamma^\varepsilon \leq \alpha$, e, passando questa disegualanza al sup - cosa che si può fare per il lemma sulla disegualanza dei sup - si ottiene $\gamma^\delta = \sup_{\varepsilon < \delta} \gamma^\varepsilon \leq \alpha \cancel{<} \alpha$.

unicità Sia α il minimo ordinale che non si scrive in modo unico in base γ - se la sottoclasse di tali ordinali fosse vuota avremmo già la tesi - ovvero:

$$\begin{aligned}\alpha &= \gamma^{\beta_1} \cdot k_1 + \dots + \gamma^{\beta_n} \cdot k_n \\ &= \gamma^{\beta'_1} \cdot k'_1 + \dots + \gamma^{\beta'_n} \cdot k'_n\end{aligned}$$

Osserviamo che se $\beta_1 = \beta'_1$ e $k_1 = k'_1$, allora per la stretta monotonia della somma sulla seconda componente si ottiene:

$$\gamma^{\beta_2} \cdot k_2 + \dots + \gamma^{\beta_n} \cdot k_n = \gamma^{\beta_2} \cdot k_2 + \dots + \gamma^{\beta_n} \cdot k_n < \alpha$$

ovvero che esiste un ordinale più piccolo di α che ammette due scritture in base γ , contro la minimalità di α . Osserviamo inoltre che se $\beta_1 = \beta'_1$, allora necessariamente $k_1 = k'_1$, infatti:

$$\alpha = \gamma^{\beta_1} \cdot k_1 + \underbrace{\dots}_{<\gamma^{\beta_1}} = \gamma^{\beta'_1} \cdot k'_1 + \underbrace{\dots}_{<\gamma^{\beta'_1}}$$

dunque $k_1 = k'_1$ e c'è uguaglianza delle code per unicità data dal lemma di divisione. Verifichiamo infine che necessariamente $\beta_1 = \beta'_1$, infatti, se fosse WLOG $\beta_1 < \beta'_1$, cioè si avrebbe:

$$\alpha = \gamma^{\beta_1} \cdot k_1 + \dots + \gamma^{\beta_n} \cdot k_n \leq \gamma^{\beta_1} \cdot k \stackrel{k < \gamma}{<} \gamma^{s(\beta_1)} \leq \gamma^{\beta'_1} \leq \gamma^{\beta'_1} \cdot k'_1 + \dots + \gamma^{\beta'_n} \cdot k'_n = \alpha \text{ f}$$

dove abbiamo posto $k = k_1 + \dots + k_n$.

□

§10.4 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 un'idea del loro aspetto. Il lemma seguente è un caso particolare, ma è semplice e vale la pena ricordarlo.

Lemma 10.27 (Assorbimento a sinistra da parte dell'ordinale più grande)

Siano $\alpha, \beta, \gamma \in \text{Ord}$ tali che $\alpha < \omega^\beta \leq \gamma$, allora:

$$\alpha + \gamma = \gamma$$

Ciò calcolare $\alpha + \gamma$ assorbe tutti gli α abbastanza piccoli, ossia quelli minori di qualche potenza di ω che sia a sua volta minore o uguale a γ .

Dimostrazione. Naturalmente si ha che $\gamma \leq \alpha + \gamma$ (debole monotonia sulla prima componente) dunque ci basta dimostrare che $\alpha + \gamma \leq \gamma$. Scrivendo α in forma normale di Cantor abbiamo:

$$\alpha = \omega^{\beta_1} \cdot k_1 + \dots + \omega^{\beta_n} \cdot k_n$$

con $\beta_1 > \beta_2 > \dots > \beta_n$. Quindi possiamo ottenere che $\alpha \leq \omega^{\beta_1} \cdot k$, per qualche $k \in \omega$, infatti, sostituendo tutti gli esponenti $\alpha_2, \dots, \alpha_n$ con α_1 , ed usando la debole monotonia, si ottiene:

$$\alpha = \omega^{\beta_1} \cdot k_1 + \dots + \omega^{\beta_n} \cdot k_n \leq \alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_1} \cdot k_2 + \dots + \omega^{\beta_1} \cdot k_n = \omega^{\beta_1} \cdot (k_1 + \dots + k_n)$$

per cui poniamo $k := k_1 + \dots + k_n$ ¹²¹. Osserviamo che β_1 è il più piccolo esponente per cui si ha tale disegualanza (qualsiasi cosa più piccola ci dà per monotonia $\alpha < \alpha$), mettendo assieme ciò con l'ipotesi $\alpha < \omega^\beta$, deduciamo $\beta_1 < \beta$, da cui quindi $\beta_1 + 1 \leq \beta$. Usando il lemma della sottrazione, possiamo sottrarre ω^{β_1+1} a γ e ottenere $\gamma = \omega^{\beta_1+1} + \gamma' = \omega^{\beta_1} \cdot \omega + \gamma'$, con γ' unico per il lemma. Da cui:

$$\alpha + \gamma \stackrel{\text{sopra + monotonia}}{\leq} \omega^{\beta_1} \cdot k + \omega^{\beta_1} \cdot \omega + \gamma' = \omega^{\beta_1}(k + \omega) + \gamma' = \omega^{\beta_1} \cdot \omega + \gamma' = \gamma$$

dove l'uguaglianza in rosso segue deriva dal fatto che:

$$k + \omega = \sup\{k + n \mid n < \omega\} = \omega$$

□

Proposizione 10.28 (Regole di calcolo in forma normale di Cantor)

Per le somme ($c \neq 0, d \neq 0$) vale che:

$$\omega^\alpha \cdot c + \omega^\beta \cdot d = \begin{cases} \omega^\beta \cdot d & \text{se } \alpha < \beta \\ \omega^\alpha \cdot (c + d) & \text{se } \alpha = \beta \\ \omega^\alpha \cdot c + \omega^\beta \cdot d & \text{se } \beta < \alpha \end{cases}$$

Per i prodotti si applica la proprietà distributiva, e poi le regole seguenti:

$$\begin{aligned} \beta > 0 &\rightarrow (\omega^{\alpha_1} \cdot k_1 + \dots + \omega^{\alpha_2} \cdot k_2 + \dots) \cdot \omega^\beta = \omega^{\alpha_1+\beta} \\ n \in \omega \setminus \{0\} &\rightarrow (\omega^{\alpha_1} \cdot k_1 + \dots + \omega^{\alpha_2} \cdot k_2 + \dots) \cdot n = \omega^{\alpha_1} \cdot k_1 n + \dots + \omega^{\alpha_2} \cdot k_2 + \dots \end{aligned}$$

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

$$\begin{aligned} k \in \omega \setminus \{0\} &\quad k^{\omega^{1+\alpha}} = \omega^{\omega^\alpha} \\ \beta > 0 \wedge \alpha_1 > 0 &\rightarrow (\omega^{\alpha_1} \cdot k_1 + \dots + \omega^{\alpha_2} \cdot k_2 + \dots)^{\omega^\beta} = \omega^{\alpha_1 \cdot \omega^\beta} \end{aligned}$$

Dimostrazione. La regole per la somma sono immediate: la prima è il lemma precedente, infatti se $\alpha < \beta$, allora $\omega^\alpha \cdot c < \omega^\alpha \cdot \omega = \omega^{s(\alpha)} \leq \omega^\beta \cdot d$, e il termine di sinistra viene assorbito nella somma; la seconda è la proprietà distributiva a sinistra valida per il prodotto di ordinali in generale, e la terza è la scrittura stessa in forma normale di Cantor, che per ipotesi non può essere semplificata ulteriormente. Per dimostrare che:

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

osserviamo preliminarmente il caso particolare $n \cdot \omega = \omega$ per $n \in \omega \setminus \{0\}$:

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

dove la prima disegualanza è la solita debole monotonia sulla prima componente del prodotto, la seconda disegualanza è il lemma sulla disegualanza dei sup e vale perché l'insieme di destra contiene tutti i naturali e quindi tutti i prodotti, infine, l'ultima uguaglianza è semplicemente il fatto che ω è limite e quindi uguale al sup dei suoi

¹²¹Una volta viste le regole per la somma in forma normale anziché questa stima sarà più comoda e veloce sommare ω^{α_1} in fondo ed ottenere la stima $\alpha \leq \omega^\alpha \cdot (k_1 + 1)$, che è anche migliore.

elementi. Ora possiamo scrivere $\beta = 1 + \gamma$ (volendo è il lemma della sottrazione ordinale, ma può essere giustificato in tanti altri modi), per cui si ha:¹²²

$$\begin{aligned} \omega^{\alpha_1+\beta} &= \omega^{\alpha_1}\omega^\beta \\ &\leq (\omega^{\alpha_1} \cdot k_1 + \omega^{\alpha_2} \cdot k_2 + \dots) \cdot \omega^\beta \\ &\leq (\omega^{\alpha_1} \cdot k_1 + \omega^{\alpha_2} \cdot k_2 + \dots + \omega^{\alpha_1}) \cdot \omega^\beta \\ &= \omega^{\alpha_1}(k_1 + 1) \cdot \omega^\beta \\ &= \omega^{\alpha_1} \underbrace{(k_1 + 1)\omega}_{=\omega} \omega^\gamma \\ &= \omega^{\alpha_1} \cdot \omega \cdot \omega^\gamma = \omega^{\alpha_1+\beta} \end{aligned}$$

dove: la prima uguaglianza sono le proprietà delle potenze degli ordinali; la seconda disuguaglianza è la debole monotonia della prima componente del prodotto; nella terza abbiamo aggiunto ω^{α_1} alla fine, ed è la stretta monotonia sulla seconda componente della somma, essendo $0 < \omega^{\alpha_1}$, unita alla debole monotonia sulla prima componente del prodotto totale, da cui la disuguaglianza larga; la quarta uguale è la regola della somma, infatti per l'ipotesi sulla forma normale di Cantor, avendo aggiunto ω^{α_1} alla fine, i termini vengono cancellati, si ottiene $\omega^{\alpha_1} \cdot k_1 + \omega^{\alpha_1}$ e infine si usa la distributività a sinistra; per la quinta uguaglianza stiamo usando che $\beta = 1 + \gamma$ e le solite proprietà delle potenze; la sesta uguaglianza è il caso particolare visto sopra $n \cdot \omega = \omega$, e naturalmente $k_1 + 1 \in \omega$; infine, nell'ultima uguaglianza usiamo ancora che $\beta = 1 + \gamma$.

La seconda regola, del prodotto di un ordinale in forma normale e un naturale:

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

si ottiene per induzione su n . La prima per il prodotto invece è immediata:

$$\begin{aligned} k^{\omega^{1+\alpha}} &= k^{\omega \cdot \omega^\alpha} \\ &= (k^\omega)^{\omega^\alpha} \\ &= (\sup\{k^n | n \in \omega\})^{\omega^\alpha} \\ &= \omega^{\omega^\alpha} \end{aligned}$$

sono solo la definizione ricorsiva della potenza nel caso limite e le proprietà delle potenze degli ordinali, l'unica cosa degna di nota da osservare è che l'estremo superiore di quell'insieme, per il solito lemma, maggiora $\{n | n \in \omega\}$, e contemporaneamente ω è un suo maggiorante per questo motivo si vede che è ω stesso.

Per dimostrare infine l'ultima regola sulle potenze di ordinali in forma normale:

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

partiamo dal caso particolare $(\omega^\alpha \cdot k)^\omega = \omega^{\alpha \cdot \omega}$:

$$\begin{aligned} \omega^{\alpha \cdot \omega} &\leq (\omega^\alpha \cdot k)^\omega \\ &= \sup\{(\omega^\alpha \cdot k)^n | n \in \omega\} \\ &= \sup\{\omega^{\alpha \cdot n} \cdot k^n | n \in \omega\} \\ &\leq \sup\{\omega^{\alpha \cdot (n+1)} | n \in \omega\} \leq \omega^{\alpha \cdot \omega} \end{aligned}$$

dove: la prima disuguaglianza è la solita monotonia, applicata al prodotto interno; la seconda uguaglianza è la definizione ricorsiva di potenza di un ordinale nel caso limite; la

¹²²Typo Mamino, c'è proprio uguaglianza al quarto passaggio.

terza uguaglianza sono le proprietà delle potenze; la quarta disuguaglianza è la monotonia sulla seconda componente del prodotto data da $k^n \leq \omega^n$, e poi sono semplicemente le proprietà delle potenze; infine si ha che $\omega^{\alpha \cdot \omega}$ è un maggiorante dell'insieme.

Siccome $\beta > 0$, possiamo scrivere, come nel caso del prodotto, $\beta = 1 + \gamma$, dunque abbiamo $\omega^\beta = \omega \cdot \omega^\gamma$ ¹²³, da cui:

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

dove: la prima disuguaglianza è debole monotonia sulla base della potenza; per la seconda ci basta aggiungere ai termini della somma ω^{α_1} alla fine, come fatto per il prodotto e poi usare la regola per la somma; la terza uguaglianza sono le proprietà delle potenze; la quarta uguaglianza è il caso particolare che abbiamo visto prima; la quinta sono di nuovo le proprietà delle potenze di ordinali, e, infine la sesta era il fatto che $\omega^\beta = \omega^{1+\gamma}$. \square

¹²³Tipo di Mamino (ha scritto γ anziché di ω^γ) che si porta dietro tutto il conto.

Esempio 10.29 (Operazioni tra ordinali in forma normale di Cantor)

Elenchiamo alcuni esempi usando le proprietà appena viste:

- $(\omega + 1)^2 = (\omega + 1)(\omega + 1) = (\omega + 1) \cdot \omega + (\omega + 1) \cdot 1 = \omega^2 + \omega + 1$, le uniche cose usate sono la distributività a sinistra del prodotto di ordinali, la prima regola per il prodotto di ordinali e volendo la seconda nel caso di prodotto per 1 [che in teoria abbiamo già gratis come elemento neutro dalle regole generali per gli ordinali].
- $(\omega + 1)^2 \cdot n = (\omega^2 + \omega + 1) \cdot n = \omega^2 \cdot n + \omega + 1$, dove $n \in \omega \setminus \{0\}$. In questo caso abbiamo combinato semplicemente il risultato sopra con la seconda regola per il prodotto di ordinali in forma normale.
- $(\omega + 1)^2 \cdot \omega = (\omega^2 + \omega + 1) \cdot \omega = \omega^3$, come sopra, ma usando la prima regola per il prodotto.
- $(\omega + 1)^3 = (\omega^2 + \omega + 1) \cdot (\omega + 1) = (\omega^2 + \omega + 1) \cdot \omega + \omega^2 + \omega + 1 = \omega^3 + \omega^2 + \omega + 1$, abbiamo usato distributività e seconda regola per il prodotto.
- $(\omega + 1)^n = \omega^n + \omega^{n-1} + \dots + 1 = \sum_{i=n}^0 \omega^{i\text{a}}$, $n \in \omega$. Lo si vede per induzione, i casi base sono fatti sopra (il caso 0 è il caso base della definizione ricorsiva di potenza ordinale), dunque possiamo procedere per induzione e fare il passo induttivo:

$$(\omega + 1)^{n+1} = (\omega + 1)^n \cdot (\omega + 1) \stackrel{\text{Hyp. indutt.}}{=} \left(\sum_{i=n}^n \omega^i \right) \cdot (\omega + 1) = \left(\sum_{i=n}^n \omega^i \right) \cdot \omega + \sum_{i=n}^n \omega^i$$

e usando la prima regola per il prodotto si ottiene:

$$\omega^{n+1} + \sum_{i=n}^n \omega^i = \sum_{i=n+1}^n \omega^i$$

che è proprio la tesi nel caso successore.

- $(\omega + 1)^\omega = \omega^\omega$, usando la seconda regola per le potenze.
- $(2 \cdot \omega^2 + \omega \cdot 3 + 7)^3$ ^b, osserviamo che $2 \cdot \omega^2 = 2 \cdot \omega \cdot \omega = (2 \cdot \omega) \cdot \omega = \omega \cdot \omega = \omega^2$, per l'osservazione fatta prima, secondo cui $n \cdot \omega = \omega$, per $n \in \omega \setminus \{0\}$. Da qui si può procedere con le regole che conosciamo, calcoliamo per comodità prima il quadrato:

$$\begin{aligned} (\omega^2 + \omega \cdot 3 + 7)^2 &= (\omega^2 + \omega \cdot 3 + 7) \cdot (\omega^2 + \omega \cdot 3 + 7) \\ &= (\omega^2 + \omega \cdot 3 + 7) \cdot \omega^2 + (\omega^2 + \omega \cdot 3 + 7) \cdot \omega \cdot 3 \\ &\quad + (\omega^2 + \omega \cdot 3 + 7) \cdot 7 \\ &= \omega^4 + \omega^3 \cdot 3 + \omega^2 \cdot 7 + \omega \cdot 3 + 7 \end{aligned}$$

iterando ancora una volta la distributività, le regole per il prodotto [e ricordando che quest'ultimo è associativo], si ottiene il risultato:

$$(\omega^2 + \omega \cdot 3 + 7)^3 = \omega^6 + \omega^5 \cdot 3 + \omega^4 \cdot 7 + \omega^3 \cdot 3 + \omega^2 \cdot 7 + \omega \cdot 3 + 7$$

^aNotare la somma al contrario, perché l'ordine conta in forma normale di Cantor.

^bDall'esame del 27-1-2020.

§11 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 infinita¹²⁴. Definiremo la scrittura $|X| = \aleph_\alpha$, come $|X| = |\omega_\alpha|$. Indagheremo inoltre 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 farlo occorre l'assioma della scelta. Le cardinalità degli ordinali fanno comodo, per esempio, perché sono confrontabili.

Osservazione 11.1 (Tutte le cardinalità degli ordinali sono confrontabili) — Dati $\alpha, \beta \in \text{Ord}$, o $|\alpha| < |\beta|$ o $|\alpha| = |\beta|$ o $|\beta| < |\alpha|$.

Dimostrazione. Basta osservare che, data la totalità della relazione d'ordine tra gli ordinali, o $\alpha \subseteq \beta$ o $\beta \subseteq \alpha$, quindi per l'inclusione, si ha o $|\alpha| \leq |\beta|$ o $|\beta| \leq |\alpha|$. \square

Ad ogni cardinalità di un ordinale, associamo un rappresentante canonico: il minimo ordinale di quella cardinalità.

Definizione 11.2 (Ordinale iniziale). Dato $\alpha \in \text{Ord}$, diciamo che è un **ordinale iniziale** se $\forall \beta < \alpha \ |\beta| < |\alpha|$.

Esercizio 11.3. Dimostrare che se α è un ordinale infinito e iniziale, allora α è limite.

Soluzione. Supponiamo per assurdo che α sia successore, $\alpha = \beta + 1$, allora $\beta < \beta + 1$, e, poiché è per ipotesi iniziale, si ha:

$$|\beta| < |\beta + 1| = |\beta \cup \{\beta\}| = |\beta| + 1$$

Mostriamo ora che $|\beta| = |\beta \cup \{\beta\}|$ in modo da avere un assurdo e concludere. In primis osserviamo che non può essere che $\beta < \omega$, in quanto ciò implicherebbe, essendo ω iniziale, $|\beta| < \aleph_0$, e per una proposizione precedente, ciò implicherebbe β finito, che è assurdo. Poiché tutti gli ordinali sono confrontabili, si ha quindi $\omega \leq \beta \leftrightarrow \omega \subseteq \beta$, per cui possiamo definire la funzione seguente.¹²⁵

$$\beta \rightarrow \beta \cup \{\beta\} : x \mapsto \begin{cases} \beta & \text{se } x = 0 \\ 0 & \text{se } x = 1 \\ x - 1 & \text{se } x \in \omega \setminus \{0, 1\} \\ x & \text{altrimenti} \end{cases}$$

che è ben definita perché tutti i naturali meno lo zero sono successori, ed è banalmente iniettiva e surgettiva, dunque possiamo concludere. \square

¹²⁴In realtà, senza scelta non lo possiamo ancora dire per tutti gli insiemi, ma sarà a prescindere vero relativamente a tutte le cardinalità degli ordinali.

¹²⁵Scritta con un piccolo abuso di notazione ma non cambia nulla.

§11.1 Teorema di Hartogs

Il nostro scopo è, ora, dimostrare che gli ordinali **iniziali** sono una classe propria, e quindi enumerarli per mezzo di una funzione classe $\text{Ord} \rightarrow \text{Ord} : \alpha \mapsto \omega_\alpha$. Quello che segue è lo strumento tecnico fondamentale.

Teorema 11.4 (Teorema di Hartogs)

Dato un insieme X esiste un ordinale α che non è equipotente (cioè non è in biogezone) ad alcun sottoinsieme di X , ossia $|\alpha| \not\leq |X|$.

Moralmente: esiste sempre un ordinale che non si immerge in X , dunque esiste sempre un'ordinale con una cardinalità più grande di qualunque insieme.

Dimostrazione. Consideriamo il sottoinsieme delle relazioni di buon ordinamento su qualche sottoinsieme di X :

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

Sia F la funzione classe che associa, ad ogni buon ordine, l'unico ordinale a lui isomorfo¹²⁶. Per **rimpiazzamento**, esiste l'insieme di ordinali $F[Y]$ e naturalmente c'è almeno un ordinale che non vi appartiene; il nostro obiettivo è dimostrare che c'è almeno un ordinale che non è in biogezone con alcun sottoinsieme di X .

Sia $\alpha \notin F[Y]$, mostriamo che tale ordinale non è in biogezone ad alcun sottoinsieme di X , ovvero $|\alpha| \not\leq |X|$. Se per assurdo, $|\alpha| \leq |X'|$, allora α sarebbe isomorfo a qualche $X' \subseteq X$, e quest'ultimo sarebbe ben ordinabile in maniera indotta - ponendo $x <_{X'} y \stackrel{\text{def}}{=} f(x) <_\alpha f(y)$ - da cui automaticamente $(X', <_{X'}) \sim \alpha \implies \alpha \in F[Y]$, che è assurdo per come abbiamo preso α . \square

Definizione 11.5 (Numero di Hartogs). Dato un insieme X , il **numero di Hartogs** di X , che indichiamo con $H(X)$, è il più piccolo ordinale che non si immerge in X [o non è equipotente ad alcun sottoinsieme di X] - ossia $H(X) \in \text{Ord}$ è minimo tale che $|H(X)| \not\leq |X|$.

Osservazione 11.6 (Buona definizione del numero di Hartogs) — Il teorema di Hartogs ci garantisce che ce n'è sempre almeno uno, per ogni insieme X , dunque la **classe** degli ordinali non equipotenti ad alcun sottoinsieme di X è non vuota ed è una sottoclasse di Ord , che è bene ordinata, pertanto ammette un minimo, e di conseguenza il numero di Hartogs di un insieme è sempre ben definito.

Osservazione 11.7 ($H(X)$ è un ordinale iniziale) — Dato un insieme X , osserviamo che il suo numero di Hartogs $H(X)$ è un ordinale iniziale.

Dimostrazione. Per assurdo, se esistesse $\beta < H(X)$ tale che $|\beta| \geq |H(X)|$, avremmo, per minimalità di $H(X)$ che $|\beta| \geq |X|$, e quindi $|H(X)| \leq |\beta| \leq |X| \nleq$. \square

¹²⁶Cioè $F : Y \rightarrow \text{Ord} : R \mapsto \gamma$, tale che $\gamma \sim (X', R)$, e da quanto sappiamo γ esiste ed è unico quindi la funzione classe F è ben definita.

Corollario 11.8 (Gli ordinali iniziali sono una classe propria)

La classe degli ordinali iniziali è una classe propria.^a

^aLa stessa dimostrazione ci dà il medesimo risultato anche limitandoci agli ordinali iniziali infiniti.

Moralmente staremmo escludendo dalla classe degli ordinali iniziali un insieme di ordinali iniziali finiti, ma togliere un insieme di cose da una classe non è sufficiente a renderla non propria.

Dimostrazione. Se, per assurdo, esistesse l'insieme X degli ordinali iniziali, allora per ogni $\alpha \in X$ si avrebbe, per definizione di unione, $\alpha \subseteq \bigcup X$, da cui per ogni ordinale iniziale, si avrebbe $|\alpha| \leq |\bigcup X|$, in particolare, essendo $H(\bigcup X)$ un ordinale iniziale, si ottiene $|H(\bigcup X)| \leq |\bigcup X| \not\leq$, perché contro la definizione di Hartogs. \square

Osservazione 11.9 ($\alpha \hookrightarrow H(\alpha)$) — Dato $\alpha \in \text{Ord}$, $H(\alpha)$ è il più piccolo ordinale tale che $|\alpha| < |H(\alpha)|$. Cioè $H(\alpha)$ è il più piccolo ordinale in cui si immerge α .

Dimostrazione. Siccome le cardinalità degli ordinali sono tutte confrontabili:

$$|\alpha| < |H(\alpha)| \leftrightarrow |H(\alpha)| \not\leq |\alpha|$$

ed essendo l'Hartogs, per definizione, l'ordinale più piccolo per cui è vero il RHS, è anche automaticamente il più piccolo per cui è vero il LHS.

Alternativamente, supponendo per assurdo che esista $\beta < H(\alpha)$ tale che $|\alpha| < |\beta|$, per la minimalità di $H(\alpha)$, si ha anche che $|\beta| \leq |\alpha|$, dunque si otterebbe $|\alpha| = |\beta|$, contraddicendo che $|\alpha| < |\beta|$. \square

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 11.10. Cosa c'è di **Sbagliato** nella dimostrazione seguente dell'esistenza di un $\alpha \in \text{Ord}$ più che numerabile?

Sia $\alpha \stackrel{\text{def}}{=} \sup\{\beta \in \text{Ord} : |\beta| \leq \aleph_0\}$. Se per assurdo $|\alpha| \leq \aleph_0$, allora $|s(\alpha)| = |\alpha| + 1 \leq \aleph_0$, quindi, essendo α il sup si avrebbe $s(\alpha) \leq \alpha \not\leq$.

Soluzione. Osserviamo che $\{\beta \in \text{Ord} : |\beta| \leq \aleph_0\} = H(\omega)$, infatti dato $x \in H(\omega) \rightarrow x < H(\omega)$ e per la minimalità di quest'ultimo, si ha $|x| \leq |\omega| = \aleph_0$, cioè $x \in \{\beta \in \text{Ord} : |\beta| \leq \aleph_0\}$. Viceversa, dato $x \in \{\beta \in \text{Ord} : |\beta| \leq \aleph_0\}$, se fosse $x \geq H(\omega)$, allora $H(\omega) \subseteq x$, da cui $|H(\omega)| \leq |x| \leq |\omega| \not\leq$, pertanto vale $x < H(\omega) \leftrightarrow x \in H(\omega)$, e quindi $\{\beta \in \text{Ord} : |\beta| \leq \aleph_0\} \subseteq H(\omega)$.

A questo punto l' α della dimostrazione sopra è proprio $H(\omega)$ come ordinale, e quindi il problema della dimostrazione precedente, cioè il motivo per cui non l'abbiamo usata ed abbiamo introdotto l'Hartogs è che l'insieme di cui si prende il sup è proprio $H(\omega)$, della cui esistenza non siamo certi fino al teorema di Hartogs, per cui la dimostrazione sopra sarebbe stata sbagliata, ed una volta definito l'Hartogs ne è un'idea equivalente. \square

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**, vale infatti il lemma seguente.

Lemma 11.11 ($F : \text{Ord} \rightarrow C$)

Sia C una classe **propria** di ordinali, allora esiste un'unica funzione classe $F : \text{Ord} \rightarrow C$ strettamente crescente e biunivoca.

Dimostrazione. Sia $G : \text{Ord} \rightarrow C$ definita per ricorsione transfinita forte da:

$$G(\alpha) = \text{il minimo } \beta \in C \text{ maggiore di tutti gli elementi di } G[\alpha]^{127}$$

Per costruzione G è strettamente crescente, dunque iniettiva. Per verificare la surgettività consideriamo $\beta \in C$, siccome G è crescente vale che $\beta < s(\beta) \leq G(s(\beta))$ (le funzioni crescenti di buoni ordini stanno sopra le diagonali¹²⁸). Per la minimalità di $G(s(\beta))$, si ha che, essendo $\beta \in C$, $\beta \in G[s(\beta)]$, cioè β è in $\text{Im}(G)$, pertanto G è anche surgettiva. Ci resta da dimostrare che G è unica, nel senso delle funzioni classe, cioè se F soddisfa le ipotesi, allora soddisfa necessariamente la definizione ricorsiva di G , e quindi per il teorema di ricorsione transfinita vale che $F(\alpha) = G(\alpha)$, $\forall \alpha \in \text{Ord}$.

Data $F : \text{Ord} \rightarrow C$ strettamente crescente e bigettiva, si ha naturalmente che $F(\alpha)$ è maggiore di tutti gli elementi di $F[\alpha]$, affinché soddisfi la definizione ricorsiva di G dobbiamo verificare che effettivamente $F(\alpha)$ è il minimo maggiore di tutti gli elementi di $F[\alpha]$. Supponiamo per assurdo che esista $\beta \in C$ tale che $\beta < F(\alpha)$ ed al contempo maggiore strettamente di tutti gli elementi di $F[\alpha]$, per la surgettività di F si ha $\beta = F(\gamma)$, per $\gamma \in \text{Ord}$. Per monotonia, essendo β più grande di ciascun elemento di $F[\alpha]$, si ha naturalmente che $\beta > F(\gamma)$ se $\gamma < \alpha$, e al contempo, poiché $\beta < F(\alpha)$, sempre per monotonia, si ha $\beta < F(\gamma)$, $\forall \gamma \geq \alpha$, per cui $\beta \neq F(\gamma)$ per ogni $\gamma \in \text{Ord}$. \square

Definizione 11.12 (Funzione degli aleph). La **funzione classe dagli ordinali agli ordinali iniziali infiniti** $\alpha \mapsto \omega_\alpha$ è definita come l'**unica crescente e biunivoca** fra queste classi, che esiste ed è unica per il lemma appena visto.

Proposizione 11.13 (Definizione ricorsiva della funzione degli aleph)

Definiamo per ricorsione transfinita v.2 la funzione ω_α come segue:

$$\begin{aligned}\omega_0 &= \omega \\ \omega_{\alpha+1} &= H(\omega_\alpha) \\ \omega_\lambda &= \sup\{\omega_\alpha \mid \alpha \in \lambda\} \text{ per } \lambda \text{ limite}\end{aligned}$$

ed osserviamo che tale funzione è proprio la funzione degli aleph definita sopra.^a

^aNotare che da questa definizione abbiamo che è anche continua, dunque ha una classe propria di punti fissi per un teorema visto.

Dimostrazione. Per verificare che la funzione sopra sia effettivamente l'unica funzione strettamente crescente e bigettiva tra Ord e la classe propria degli ordinali iniziali è sufficiente far vedere che soddisfa la definizione ricorsiva di quella sopra e concludere con il teorema di ricorsione transfinita.¹²⁹

¹²⁷Stiamo semplicemente scrivendo un predicato per indicare una funzione classe, che quindi è ben definita perché il predicato è sempre decidibile.

¹²⁸Questo fatto visto solo tra insiemi bene ordinati, vale, con una dimostrazione analoga anche tra classi bene ordinate, quindi lo possiamo usare anche per funzioni classe.

¹²⁹Potremmo anche, al contrario, mostrare che la funzione che abbiamo definito è strettamente crescente e surgettiva da Ord a C , e per il lemma sopra concludere che è effettivamente l'unica possibile, ma ciò risulta più difficile rispetto al far vedere che soddisfa direttamente la definizione ricorsiva dell'unica che sappiamo rispettare tali ipotesi.

Per il caso 0 si ha banalmente che ω è un ordinale iniziale e $\omega_0 = \emptyset$, dunque la definizione ricorsiva è verificata. Nel caso successore si ha che $H(\omega_\alpha)$ è un ordinale iniziale ed è per definizione il minimo che non si immerge in ω_α , dunque è anche il minimo maggiore strettamente di $H(x)$, con $x \in \omega_\alpha$ (poiché $H(\omega_\alpha) > \omega_\alpha > x$ e $H(x) \leq \omega_\alpha$). Nel caso limite verifichiamo innanzitutto che la funzione sia ben definita e quindi ω_λ sia un ordinale iniziale, per fare ciò consideriamo $\beta < \omega_\lambda$ (dunque $|\beta| \leq |\omega_\lambda|$ per transitività) e supponiamo per assurdo che $|\beta| = |\omega_\lambda|$, essendo $\beta < \omega_\lambda = \bigcup_{\alpha < \lambda} \omega_\alpha \rightarrow \beta \leq \omega_\lambda \rightarrow \beta \subseteq \omega_\alpha$, per cui si ha:

$$|\beta| \leq |\omega_\alpha| < |\omega_{\alpha+1}| \leq |\omega_\lambda| = \beta \not\subseteq \omega_\lambda$$

Inoltre ω_λ rispetta la definizione ricorsiva perché abbiamo costruito la funzione estendendola per continuità al caso limite, dunque ω_λ è proprio il più piccolo ordinale iniziale maggiore o uguale a $\omega_{|\lambda|}$, ed in particolare vale il maggiore stretto perché per ogni $x < \lambda$, $\omega_x < \omega_{x+1} \leq \omega_\lambda$. O anche perché abbiamo visto che ordinale iniziale \implies limite, dunque ω_λ ordinale limite e per la caratterizzazione di questi non appartiene all'insieme di cui è sup, pertanto è maggiore strettamente di tutti i suoi elementi. \square

Notazione 11.14 ($|\omega_\alpha| = \aleph_\alpha$) — Usiamo il simbolo \aleph_α come abbreviazione per $|\omega_\alpha|$. Così, per esempio, X è numerabile $\equiv |X| = |\omega_0| \equiv |X| = \aleph_0$.

§11.2 Somme e prodotti di aleph

Proposizione 11.15 (Somme e prodotti di aleph)

Dati \aleph_α , \aleph_β e $n \in \omega \setminus \{0\}$ vale che:

$$\begin{aligned}\aleph_\alpha + \aleph_\beta &= \aleph_\alpha \cdot \aleph_\beta = \max(\aleph_\alpha, \aleph_\beta) = \aleph_{\max(\alpha, \beta)} \\ \aleph_\alpha + |n| &= \aleph_\alpha \cdot |n| = \aleph_\alpha\end{aligned}$$

Assumiamo per un istante il seguente lemma.

Lemma 11.16 ($\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$)

$$\forall \alpha \in \text{Ord } \aleph_\alpha^2 = \aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha.$$

^aSi verifica per induzione allora che $\aleph_\alpha^n = \aleph_\alpha$, $\forall n \in \omega \setminus \{0\}$.

Ora dimostriamo la proposizione assumendo il lemma.

Dimostrazione. Supponiamo WLOG che $\aleph_\beta \geq \aleph_\alpha$ (per quanto visto tutte le cardinalità degli ordinali sono confrontabili, in particolare quanto scritto equivale proprio a $\alpha \subseteq \beta$), e osserviamo che:

$$\aleph_\beta = \aleph_\beta + 0 \leq \aleph_\beta + \aleph_\alpha \leq \aleph_\beta \cdot 2 \leq \aleph_\beta \cdot \aleph_\beta \stackrel{\text{assunto}}{=} \aleph_\beta$$

dunque $\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \aleph_\beta$ ovvero sono entrambi uguali a $\max(\aleph_\alpha, \aleph_\beta) = \aleph_{\max(\aleph_\alpha, \aleph_\beta)}$. Analogamente, nel caso di cardinalità finite vale:

$$\begin{aligned}\aleph_\alpha &= \aleph_\alpha + 0 \leq \aleph_\alpha + |n| \leq \aleph_\alpha + \aleph_0 \stackrel{\text{sopra}}{=} \aleph_\alpha \\ \aleph_\alpha &= \aleph_\alpha \cdot 1 \leq \aleph_\alpha \cdot |n| \leq \aleph_\alpha \cdot \aleph_0 \stackrel{\text{sopra}}{=} \aleph_\alpha\end{aligned}$$

dove abbiamo usato che $\aleph_0 \leq \aleph_\alpha$, per la definizione ricorsiva della funzione degli aleph. \square

Osservazione 11.17 (Ogni cardinalità infinita \leq un aleph è un aleph) — Se $|X| = \aleph_\alpha$ e $\aleph_0 \leq |Y| \leq |X|$, allora $|Y| = \aleph_\beta$, per qualche $\beta \leq \alpha$.^a

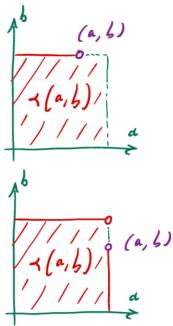
^aPer ora sappiamo che $\aleph_0 \leq |X| \rightarrow X$ infinito, ma non il viceversa, per cui serve AC.

Dimostrazione. Senza perdita di generalità possiamo assumere $X = \omega_\alpha$ e $Y \subseteq X$ ¹³⁰. Allora Y è bene ordinato dall'ordinamento indotto e possiamo definire γ il minimo ordinale tale che $|\gamma| = |Y|$ (c'è almeno un ordinale infinito isomorfo a $(Y, <_{|Y})$ perché Y è bene ordinato dall'ordine indotto, dunque si può scrivere per separazione nel suo Hartogs l'insieme degli ordinali equipotenti e minori o uguali e prenderne il minimo, che sarà un ordinale iniziale infinito, e questi li abbiamo elencati prima), per cui $\gamma = \omega_\beta$, con $\omega_\beta \leq \omega_\alpha$ e, per la monotonia di $x \mapsto \omega_x$ si ha $\beta \leq \alpha$. \square

Ora dimostriamo finalmente il lemma.

Dimostrazione. Procediamo per induzione transfinita in forma forte, dunque possiamo assumere che $\forall \beta < \alpha \aleph_\beta^2 = \aleph_\beta$ e dimostrare che $\aleph_\alpha^2 = \aleph_\alpha$. La strategia è costruire un buon ordine \prec su $\omega_\alpha \times \omega_\alpha$, tale che si abbia un'isomorfismo con ω_α stesso, $(\omega_\alpha \times \omega_\alpha, \prec) \sim \omega_\alpha$. Definiamo:

$$\begin{aligned} (a, b) \prec (a', b') &\stackrel{\text{def}}{=} \max(a, b) < \max(a', b') \\ &\vee ((\max(a, b) = \max(a', b')) \wedge a < a') \\ &\vee ((\max(a, b) = \max(a', b')) \wedge (a = a') \wedge b < b') \end{aligned}$$



Che è lo stesso ordinamento che abbiamo usato per dimostrare che il prodotto di numerabili è numerabile. In pratica, per confrontare (a, b) con (a', b') , si confrontano prima $\max(a, b)$ e $\max(a', b')$; a parità si confrontano a e 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 sono identiche¹³¹). Resta da verificare che vale proprio:

$$X \stackrel{\text{def}}{=} (\omega_\alpha \times \omega_\alpha, \prec) \sim \omega_\alpha$$

Sia β l'ordinale corrispondente a X , dobbiamo mostrare, per avere l'isomorfismo di buoni ordinamenti, che i cardinali sono uguali, ovvero $\beta = \omega_\alpha$. Siccome $|\omega_\alpha| \leq |\omega_\alpha \cdot \omega_\alpha| = |\beta|$, e ω_α è iniziale, per la contronominale della definizione di ordinali iniziale otteniamo che $\beta \geq \omega_\alpha$, dunque non dobbiamo far altro che escludere che $\omega_\alpha < \beta$, ovvero che ω_α non è isomorfo ad un segmento iniziale proprio di X .

Fissiamo un segmento iniziale proprio $X_{(a,b)}$ di X e dimostriamo che $|X_{(a,b)}| < \aleph_\alpha$, cioè si avrebbe che $|X_{(a,b)}| < |\omega_\alpha|$ e quindi non può accadere che $X_{(a,b)} \sim \omega_\alpha$.

Sia $\mu := \max(a, b)$, essendo $a, b \in \omega_\alpha$, si ha naturalmente che $\mu < \omega_\alpha$ e ω_α è iniziale, quindi limite, si ha $s(\mu) < \omega_\alpha$, e di nuovo $|s(\mu)| < \aleph_\alpha$. Di conseguenza, per la monotonia della funzione degli aleph, $|s(\mu)| = \aleph_\gamma$, per qualche $\gamma < \alpha$, oppure $s(\mu) \in \omega$.

- Nel primo caso $|s(\mu) \times s(\mu)| = \aleph_\gamma^2 \stackrel{\text{Hyp. indutt.}}{=} \aleph_\gamma$.
- Nel secondo caso $s(\mu) \times s(\mu)$ è finito, e quindi $|s(\mu) \times s(\mu)| < \aleph_0$.

¹³⁰Quindi la dimostrazione varrà a meno di bigezioni e di indurre [buoni] ordinamenti sugli altri insiemi tramite queste ultime.

¹³¹Tranne nel caso del buon ordinamento in cui bisogna fare un'induzione transfinita su α per coprire il caso di intersezione non vuota.

In ogni caso $|s(\mu) \times s(\mu)| < \aleph_\alpha$ e, siccome vale che $X_{(a,b)} \subseteq s(\mu) \times s(\mu)$, abbiamo allora $|X_{(a,b)}| \leq |s(\mu) \times s(\mu)| < \aleph_\alpha$, come voluto. \square

Esercizio 11.18. Per $n \in \omega$ sia $\mathcal{P}^n(X) \stackrel{\text{def}}{=} \{Y \in \mathcal{P}(X) : |Y| = n\}$, dimostrare che $\forall n \in \omega$ si ha che $|\mathcal{P}^n(\omega_\alpha)| = \aleph_\alpha$.

Soluzione. Possiamo definire la seguente mappa:

$$\omega_\alpha \hookrightarrow \mathcal{P}^n(\omega_\alpha) : x \mapsto \text{Im}(f_x)$$

dove:

$$f_x : n \rightarrow \omega_\alpha : i \mapsto f_x(i) = \begin{cases} x & \text{se } i = 0 \\ x + i & \text{se } 1 \leq i \leq n - 1 \end{cases}$$

Osserviamo in primis che f_x è iniettiva per ogni $x \in \omega_\alpha$, dunque $n = |\text{Im}(f_x)| \in \mathcal{P}^n(\omega_\alpha)$, e quindi la mappa sopra è ben definita, infatti $f_x(i) = f_x(j) \rightarrow x + i = x + j$, e per la stretta monotonia nella seconda componente della somma ordinale si ha $i = j$. Da quanto appena detto segue anche che le funzioni f_x sono strettamente crescenti, dunque se $\text{Im}(f_x) = \text{Im}(f_y)$, poiché sono insiemi finiti, per cui bene ordinati, ed isomorfi a n , l'isomorfismo possibile è uno solo, per un fatto noto, ed è quello definito ricorsivamente che manda ogni volta un elemento nel minimo elemento dell'insieme d'arrivo più grande di tutti quelli dell'immagine ristretta, per cui si ha proprio $f_x = f_y$, da cui $x = f_x(0) = f_y(0) = y$. Abbiamo quindi ottenuto che $\aleph_\alpha = |\omega_\alpha| \leq |\mathcal{P}^n(\omega_\alpha)|$.

Viceversa, possiamo definire la mappa:

$$\mathcal{P}^n(\omega_\alpha) \rightarrow \omega_\alpha^n : A \mapsto (a_0, \dots, a_{n-1})$$

con a_i , i -esimo elemento di A , ordinato secondo l'ordine di ω_α ristretto ad A . Naturalmente tale mappa è ben definita, visto che ogni insieme produce esattamente una n -upla, ed è iniettiva in quanto due n -uple uguali implicano tutti gli elementi uguali e quindi gli insiemi uguali.¹³² \square

Esercizio 11.19. Dimostrare che $\mathcal{P}^{\text{fin.}}(\omega_\alpha) = \aleph_\alpha$.^a

^a**Hint:** Osservare che $|\text{sottoinsiemi finiti di } \omega_\alpha| \leq |\{f : n \rightarrow \omega_\alpha | n \in \omega\}|$ [Typo Mamino], fissare $g : \omega_\alpha \times (\omega_\alpha \sqcup \{\clubsuit\}) \rightarrow \omega_\alpha \sqcup \{\clubsuit\}$ biunivoca e definire $h : \{f : n \rightarrow \omega_\alpha | n \in \omega\} \rightarrow \omega_\alpha$ con $h(\emptyset) = \clubsuit$ e $h(f) = g(f(0), h(x \mapsto f(x+1)))$.

Soluzione. Dal basso naturalmente abbiamo la mappa $\omega_\alpha \hookrightarrow \mathcal{P}^{\text{fin.}}(\omega_\alpha) : x \mapsto \{x\}$, che ci dà $\aleph_\alpha \leq |\mathcal{P}^{\text{fin.}}(\omega_\alpha)|$. Per la diseguaglianza opposta, in primis definiamo la mappa:

$$\mathcal{P}^{\text{fin.}}(\omega_\alpha) \rightarrow \{f \in {}^n\omega_\alpha | n \in \omega\} = \bigcup_{n \in \omega} {}^n\omega_\alpha : A \mapsto f_A$$

dove:

$$f_A : m = |A| \rightarrow \omega_\alpha : x \mapsto \min\{y \in \omega_\alpha | x \in A \wedge y > f_A[x]\}$$

ed osserviamo che poiché le f_A sono strettamente crescenti (in particolare $|A| \in \omega$ ed $A \subseteq \omega_\alpha$ sono bene ordinati, dunque c'è un unico isomorfismo tra loro, ed è quello in cui mappiamo A), allora $f_A = f_B \implies \text{Im}(f_A) = \text{Im}(f_B) \implies A = B$, dunque la mappa è

¹³²Questa stessa idea, leggermente modificata per risolvere il problema nel caso $\mathcal{P}^{\leq n}(\omega_\alpha)$.

iniettiva ed abbiamo la disuguaglianza $|\mathcal{P}^{\text{fin.}}(\omega_\alpha)| \leq |\{f \in {}^n\omega_\alpha \mid n \in \omega\}|$. Osserviamo ora che, fissata una bigezione $g : \omega_\alpha \times (\omega_\alpha \sqcup \{\spadesuit\}) \rightarrow \omega_\alpha \sqcup \{\spadesuit\}$, possiamo definire la mappa:

$$h : \{f \in {}^n\omega_\alpha \mid n \in \omega\} \rightarrow \omega_\alpha \sqcup \{\spadesuit\} : f \mapsto \begin{cases} \spadesuit & \text{se } f = \emptyset \\ g(f(0), h(f(x+1))) & \text{altrimenti} \end{cases}$$

che è naturalmente ben definita (grazie a g) ed iniettiva, infatti, se abbiamo che $h(f) = h(f')$ in arrivo, o $f = f' = \emptyset$ oppure $g(f(0), f(x+1)) = g(f'(0), f'(x+1))$, che, per la bigettività di g , implica $f(0) = f'(0)$ e $h(f(x+1)) = h(f'(x+1))$, che, ripetendo il ragionamento, implica a sua volta $f(1) = f'(1)$, e $h(f(x+2)) = h(f'(x+2))$, e così via, ottenendo $f(i) = f'(i)$, $\forall 0 \leq i \leq n-1$, da cui $f = f'$ ed abbiamo l'iniettività. Abbiamo quindi ottenuto che $|\mathcal{P}^{\text{fin.}}(\omega_\alpha)| \leq |\omega_\alpha \sqcup \{\spadesuit\}| = \aleph_\alpha + 1 = \aleph_\alpha$ ¹³³. \square

Esercizio 11.20. Dimostrare che $\forall \alpha, \beta \in \text{Ord}$ si ha:

$$|\alpha| = |\beta| = \aleph_\gamma \rightarrow |\alpha + \beta| = |\alpha \cdot \beta| = |\alpha^\beta| = \aleph_\gamma$$

dove intendiamo la cardinalità delle tre operazioni ordinali.

Soluzione. Per la monotonia [debole] delle operazioni ordinali nella prima componente si ha $\alpha \leq \alpha + \beta, \alpha \cdot \beta, \alpha^\beta$, da cui si ottiene la disuguaglianza dal basso in tutti e tre i casi, $\aleph_\gamma = |\alpha| \leq |\alpha + \beta|, |\alpha \cdot \beta|, |\alpha^\beta|$. Per il viceversa, vediamo caso per caso:

- $\alpha + \beta = \alpha \sqcup \beta$, per cui $|\alpha + \beta| = |\alpha \sqcup \beta| = |\alpha| + |\beta| = \aleph_\gamma + \aleph_\gamma = \aleph_\gamma$.
- $\alpha \cdot \beta = \alpha \times \beta$, per cui $|\alpha \cdot \beta| = |\alpha \times \beta| = |\alpha| \cdot |\beta| = \aleph_\gamma \cdot \aleph_\gamma = \aleph_\gamma$.
- $\alpha^\beta = \{f \in {}^\alpha\beta : |\text{supp}(f)| < \aleph_0\} \subseteq \mathcal{P}^{\text{fin.}}(\alpha \times \beta)$, per cui $|\alpha^\beta| \leq |\mathcal{P}^{\text{fin.}}(\alpha \times \beta)| = |\mathcal{P}^{\text{fin.}}(\omega_\gamma \times \omega_\gamma)| = |\mathcal{P}^{\text{fin.}}(\omega_\alpha)| = \aleph_\gamma$, dove l'uguaglianza tra la cardinalità delle parti finite è indotta dalla bigezione tra gli insiemi (basta fissare una bigezione e poi definire quella tra gli insiemi mandando ogni elemento delle prime parti finite nella sua immagine tramite la prima bigezione), mentre l'ultima uguaglianza è l'esercizio precedente.

\square

Esercizio 11.21. Se $|X| = \aleph_\alpha$ e $f : X \rightarrow Y$ è una funzione, allora $|f[X]| \leq \aleph_\alpha$.

Soluzione. Possiamo assumere, a meno di bigezione, che $X = \omega_\alpha$ e definire la funzione:

$$g : f[X] \rightarrow X : y \mapsto \min_{<}(f^{-1}(y))$$

che è naturalmente ben definita ed è iniettiva perché stiamo considerando i minimi di una partizione di X , dunque due minimi sono uguali se e solo se consideriamo lo stesso elemento della partizione di X , cioè la stessa controimmagine, da cui si ottiene, applicando f , che in partenza i valori devono essere uguali. \square

Esercizio 11.22. Dimostrare che $\forall \alpha \in \text{Ord}$ $\aleph_{\alpha+1} < 2^{2^{\aleph_\alpha}}$.

Soluzione. Poiché per Cantor si ha $\aleph_\alpha < 2^{\aleph_\alpha}$, essendo per definizione ricorsiva della funzione degli aleph, che $\aleph_{\alpha+1}$ è il più piccolo ordinale iniziale infinito strettamente maggiore di \aleph_α , si ha $\aleph_{\alpha+1} \leq 2^{\aleph_\alpha}$. Infine si osserva che $\aleph_\alpha \leq 2^{\aleph_\alpha} < 2^{2^{\aleph_\alpha}} \rightarrow \aleph_\alpha < 2^{2^{\aleph_\alpha}}$. \square

¹³³L'ultima uguaglianza è vera senza AC e la si può ottenere sfruttando disuguaglianze oppure il fatto che $\omega \hookrightarrow \omega_\alpha$.

§12 L'assioma della scelta

L'assioma della scelta è stato introdotto da **Ernst Zermelo** nel 1904, per dimostrare che ogni insieme è ben 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 fin'ora non permettono, per esempio, né di affermare né di negare la buona 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.

Axiom 12.1 (Axioma della scelta (AC))

Dato un insieme X di insiemi non vuoti, esiste una **funzione di scelta** $f : X \rightarrow \bigcup X$ tale che $\forall a \in X f(a) \in a^a$. In simboli:

$$\forall X(\emptyset \notin X) \rightarrow (\exists f \in {}^X(\bigcup X) \forall a \in X f(a) \in a)^b$$

^aCioè la funzione manda ogni elemento a di X in un suo elemento.

^bLetteralmente le funzioni di scelta “scelgono” un elemento in cui mandare tutto l'insieme, preso a sua volta come elemento.

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 questa o quella proprietà che mi interessano. Formalmente, in questo ragionamento, stiamo dicendo **considero**:

$$X = \{n, +\infty] | n \in \mathbb{N}\}$$

e considero $f : X \rightarrow \bigcup X \subseteq \mathbb{R}$ una funzione di scelta per X . Ora pongo $x_n = f([n, +\infty])$. Si pone quindi una domanda: perché non ci serve alcun assioma per fissare un elemento - come a dire **considero 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 ¹³⁴. 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.

¹³⁴Cioè se fissando x il predicato diventa una proposizione vera, con cui continuare il ragionamento, si dimostra che si può arrivare a ψ anche senza bisogno di fissare x , in questo senso è come se l'azione di “fissare” un elemento fosse un’azione vuota, nel senso che il ragionamento formalmente può essere portato avanti anche senza richiederla, ma noi lo facciamo perché ci è comodo ragionare così, ma si può equivalentemente procedere senza effettivamente farlo.

Tecnicamente, questa legge è vendicata [nel senso di 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 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 ci dice dovrebbero fare. Insomma, questo è l'intoppo: che non sappiamo esprimere il concetto di **fissare infinite variabili** se non tramite l'espeditivo di **fissare una singola funzione di scelta**¹³⁵. Tuttavia, per fare questo dobbiamo asserire l'esistenza di un certo insieme, appunto la funzione di scelta, che, si può dimostrare, non segue dagli assiomi 1-8. Bando alle ciance.

Nota 12.2 (Ogni funzione surgettiva ha inversa destra) — AC equivale all'affermazione che ogni funzione surgettiva ha un inversa destra, ossia:

$$\forall f : X \rightarrow Y \text{ surgettiva } \exists g : Y \rightarrow X \ f \circ g = \text{id}_Y$$

Dimostrazione. Verifichiamo che l'enunciato sopra è un fatto equivalente ad AC.

➡ Consideriamo l'insieme delle controimmagini via f degli elementi di Y :

$$Z \stackrel{\text{def}}{=} \{A \in \mathcal{P}(X) \mid \exists y \in Y \underbrace{\forall x \in X}_{A=f^{-1}(y)} x \in A \leftrightarrow f(x) = y\}$$

Per la surgettività di f gli elementi di Z sono tutti non vuoti, dunque per **AC** esiste $h : Z \rightarrow \bigcup Z = X$ funzione di scelta. Definiamo quindi $g(y) \stackrel{\text{def}}{=} h(f^{-1}(y))$ - più precisamente $g(y) = h(\{x \in X \mid f(x) = y\})$, segue che:

$$f \circ g(y) = f(g(y)) = f(h(\{x \in X \mid f(x) = y\}))$$

ed essendo h una funzione di scelta, si ha che $h(A) \in A$, dunque $h(f^{-1}(y)) \in f^{-1}(y)$, quindi fa un certo elemento nella controimmagine di y , fissato dalla nostra funzione di scelta h , e, indipendentemente da quale sia, torniamo indietro con f , dunque:

$$f(z) = y \quad \text{con } z \in f^{-1}(y)$$

⬅ Verifichiamo ora che da questo fatto derivi l'assioma della scelta. Sia X un insieme di insiemi non vuoti, consideriamo l'insieme $X' = \{(a, A) \in (\bigcup X) \times X \mid a \in A \wedge A \in X\}$. La funzione:

$$f : X' \rightarrow X : (a, A) \mapsto A$$

è banalmente surgettiva, quindi per ipotesi ha un'inversa destra $g : X \hookrightarrow X'$ che manda A in una coppia (a, A) per qualche $a \in A$ ¹³⁶. Ora quindi la funzione:

$$h : X \rightarrow \bigcup X : A \mapsto \text{prima componente di } g(A)$$

è una funzione di scelta per X , perché prendiamo la prima componente di $g(A)$, che sta in A , e questa è determinata da g , cioè $h(A) \in A$.

□

¹³⁵Che fissi in un solo colpo tutti gli infiniti elementi.

¹³⁶Che fissa $a \in A$ senza scriverlo esplicitamente.

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 equivale, nel senso che gli assiomi 1-8, unitamente ad una qualunque delle tre proposizioni, implicano le altre due.

Teorema 12.3 (Teorema del buon ordinamento - o di Zermelo)

Ogni insieme è ben ordinabile, ovvero:

$$\forall S \exists < \in S \times S (S, <) \text{ è un buon ordinamento}$$

Definizione 12.4 (Sottocatena - maggiorante - massimale). Dato $(S, <)$ un ordine parziale abbiamo che:

- una **sottocatena** è un $A \subseteq S$ tale che $(A, <|_A)$, cioè A con la restrizione dell'ordine di S 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 $\neg \exists y \in S x < y$.

Lemma 12.5 (Lemma di Zorn)

Ogni insieme parzialmente ordinato, in cui ogni sottocatena ammette un maggiorante ha elementi massimali.

Teorema 12.6 ($\text{AC} \iff \text{buon ordinamento} \iff \text{Zorn}$)

Le tre affermazioni **assioma della scelta**, **teorema del buon ordinamento** e **lemma di Zorn** sono equivalenti - ossia si implicano vicendevolmente assumendo gli assiomi 1-8.

§12.1 Buon ordinamento \rightarrow AC

Dimostrazione. ($\text{Buon ordinamento} \rightarrow \text{AC}$)

Dato S insieme di insiemi non vuoti, fissiamo, per il **teorema del buon ordinamento**, un buon ordine \prec su $\bigcup S$. Allora la funzione:

$$f : S \rightarrow \bigcup S : x \mapsto \min_{\prec}(x)$$

è una funzione di scelta per S [perché naturalmente $\min_{\prec}(x) \in x$, e il fatto che per Zermelo sappiamo che \prec è un buon ordinamento su S , ma non sappiamo esplicitamente cosa faccia, ci dice che, tale funzione fissa il minimo, ma non sappiamo necessariamente chi sia, perché non conosciamo esplicitamente \prec , da cui la funzione di scelta]. \square

§12.2 AC \rightarrow buon ordinamento (idea)

Dimostreremo questo risultato tramite la catena di deduzioni $\text{AC} \rightarrow \text{Zorn} \rightarrow \text{buon ordinamento}$. Tuttavia conviene studiare l'idea di una dimostrazione diretta.

Dimostrazione. ($\text{AC} \rightarrow$ buon ordinamento (idea))

Fissiamo un insieme X , per AC , esiste una funzione di scelta:

$$f : \mathcal{P}(X) \setminus \{\emptyset\} \rightarrow \bigcup \mathcal{P}(X) = X : A \mapsto f(A) \in A$$

Ora vorremmo mettere in ordine gli elementi di X come segue;

$$F(0) = x_0 = f(X) \quad F(1) = x_1 = f(X \setminus \{x_0\}) \quad F(2) = x_2 = f(X \setminus \{x_0, x_1\}) \quad \dots$$

ogni volta scegliendo un elemento nuovo fra quelli che rimangono ancora da elencare. Chiaramente non è detto che questo procedimento termini in una quantità numerabile di passi, per cui potremmo dover definire $x_\omega = f(X \setminus \{x_0, x_1, x_2, \dots\})$ e, più in generale, possiamo definire per ricorsione transfinita:

$$F(\alpha) = f(X \setminus \{x_\beta \mid \beta < \alpha\}) = f(X \setminus F[\alpha])$$

Questa cosa non può funzionare per tutti gli ordinali, cioè F non è ben definita, perché da un certo punto in poi $F[\alpha] = X$ e non possiamo usare la funzione di scelta sul vuoto, se per assurdo $F[\alpha] \subsetneq X$ per ogni $\alpha \in \text{Ord}$, allora staremmo immagazzinando la classe degli ordinali in un insieme, tramite $\alpha \mapsto F(\alpha) \in X$, che è ancora assurdo (si avrebbe che l'Hartogs $H(X)$ si immerge in X ad un certo punto o anche è violato Burali-Forti).

Per rimediare a questo inconveniente definiamo quindi

$$F(\alpha) = \begin{cases} f(X \setminus F[\alpha]) & \text{se } F[\alpha] \subsetneq X \\ \spadesuit & \text{altrimenti} \end{cases}$$

che ora è una funzione classe $\text{Ord} \rightarrow X \cup \{\spadesuit\}$ ben definita. A questo punto consideriamo $\beta := \min\{\gamma : F(\gamma) = \spadesuit\}$, che è ben definito poiché è un insieme di ordinali, non vuoto in quanto se fosse vuoto ricadremmo in uno dei due assurdi citati sopra, pertanto si ha che $F[\beta] = X$ e $F|_{\beta}$ è una mappa iniettiva in quanto f è iniettiva per definizione, per cui X è in biiezione con l'ordinale β e quindi può essere ben ordinato mediante un ordinamento indotto, per cui abbiamo ottenuto Zermelo. \square

§12.3 Zorn \rightarrow buon ordinamento

Dimostrazione. (Zorn \rightarrow buon ordinamento)

Vogliamo dimostrare che un insieme S è ben ordinabile. Consideriamo:

$$\begin{aligned} T &:= \{f : \alpha \rightarrow S \mid \alpha < H(S) \text{ e } f \text{ iniettiva}\} = \{\text{funzioni iniettive da un ordinale a } S\} \\ &= \{f \in \mathcal{P}(H(S) \times S) \mid f \text{ è una funzione iniettiva e } \text{Dom}(f) \in \text{Ord}\} \end{aligned}$$

¹³⁷Osserviamo che T è parzialmente ordinato dalla relazione d'ordine $f < g \equiv f \subseteq g$. Diamo per buono che $(T, <)$ soddisfa le ipotesi del lemma di Zorn, e quindi esiste $f \in T$ massimale rispetto alla relazione $<$. Abbiamo che f è surgettiva, infatti, se non lo fosse $S \setminus \text{Im}(f) \neq \emptyset$, dunque esiste $y \in S \setminus \text{Im}(f)$ e possiamo definire:

$$f' = f \cup \{(\text{Dom}(f), y)\}$$

dove $\text{Dom}(f)$ è l'ordinale successore al massimo del dominio di f , ed f' è iniettiva perché unione di funzione iniettive su insiemi in arrivo disgiunti, quindi avremmo $f' > f$ e

¹³⁷Deve essere necessariamente che $\alpha < H(S)$, perché se $\alpha \geq H(S)$ si immerge in S , allora una restrizione dell'immersione permetterebbe di immerge anche $H(S)$ in S , che è assurdo, dunque gli ordinali che si possono immerge in S sono soltanto quelli più piccoli del suo Hartogs. Si noti inoltre che T è non vuoto perché c'è sempre la funzione da 0 a S o da 1 ad S , se S è non vuoto.

$f \in T$, che va contro la massimalità di f , quindi è assurdo. Abbiamo quindi che S è in biogezione con $\text{Dom}(f) \in \text{Ord}$, dunque è bene ordinabile, perché possiamo indurre un buon ordinamento su S via f , e quindi abbiamo il teorema del buon ordinamento.

Verifica delle ipotesi del lemma di Zorn

Dobbiamo verificare che data $P \subseteq T$ una sottocatena di T , ha sempre un maggiorante, verifichiamo che $f := \bigcup P$ è il maggiorante in questione. In primis osserviamo che f è una funzione ben definita, infatti, essendo un'unione di funzioni ci basta verificare, per un'osservazione vista in precedenza, che per ogni $g_1, g_2 \in P$ se $x \in \text{Dom}(g_1) \cap \text{Dom}(g_2)$, allora $g_1(x) = g_2(x)$ (in tal modo f è effettivamente una funzione), essendo che $(P, <_{|P})$ è totalmente ordinato, allora vale WLOG $g_1 > g_2$, ovvero $g_2 \subseteq g_1$, dunque le due funzioni coincidono su x , perché una estende l'altra.

Verifichiamo ora che f è iniettiva, se $f(x) = f(y)$, allora esistono, per definizione di unione, $g_1, g_2 \in P$ tali che $g_1(x) = f(x)$ e $g_2(y) = f(y)$, ma, come prima, essendo P totalmente ordinato, vale WLOG $g_1 \supseteq g_2$, per cui $g_1(x) = g_2(y) = g_1(y)$, ed essendo $g_1 \in T$ è iniettiva, dunque si conclude $x = y$. Osserviamo inoltre che, per le proprietà degli ordinali:

$$\text{Dom}(f) = \bigcup \{\text{Dom}(g) | g \in P\} = \sup \{\text{Dom}(g) | g \in P\}$$

dove il sup è un ordinale per quanto visto sugli insiemi di ordinali. A questo punto f è ben definita, ha dominio un ordinale ed è iniettiva, per cui $f \in T$. Ci resta da verificare che f sia un maggiorante per P , ma ciò è banale per come abbiamo costruito f , infatti:

$$\forall g \in P \quad g \subseteq \bigcup P = f \equiv g \leq f$$

□

§12.4 AC → Zorn

Dimostrazione. (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 si traduce nel fatto che ogni elemento di S ammette un maggiorante stretto in S , $\forall x \in S \exists y \in S \ y > x$ (è la negazione della definizione di esistenza di un elemento massimale), ora per ipotesi ogni sottocatena A ammette un maggiorante in S , che può essere a sua volta maggiorato strettamente per quanto appena detto, dunque ogni sottocatena ammette un maggiorante stretto - d'altronde se ci fosse una sottocatena con un maggiorante non stretto, che quindi non può essere maggiorato strettamente da nessun altro elemento di S , allora sarebbe un elemento massimale per quest'ultimo, contraddicendo la nostra ipotesi.

Sia $f : \mathcal{P}(S) \setminus \{\emptyset\} \rightarrow \bigcup \mathcal{P}(S) \setminus \{\emptyset\} = S$ una funzione di scelta per i sottoinsiemi di S . L'idea è ora di costruire per induzione transfinita una funzione classe crescente [quindi iniettiva] $F : \text{Ord} \rightarrow S$ - che chiaramente non può esistere perché altrimenti $F|_{H(S)}$ sarebbe un'immersione di $H(S)$ in S , e dunque avremmo l'assurdo (alternativamente anche perché violeremmo Burali-Forti). Vorremmo costruire F tramite la ricorsione transfinita forte come segue:

$$F(\alpha) = f(\{\text{maggioranti stretti di } F[\alpha]\})$$

perché questa costruzione abbia senso, è necessario che $F|_\alpha$ sia [debolmente] crescente, un questo modo $F[\alpha]$ è una sottocatena di S e, per l'osservazione sopra, l'insieme dei maggioranti stretti non è vuoto, ed ha senso applicare ad esso la funzione di scelta f , e

dunque la F è ben definita, inoltre è strettamente crescente per costruzione.

Per assurdo consideriamo il minimo (possiamo farlo per l'ipotesi assurda e per i soliti motivi sugli insiemi di ordinali) α tale che $F|_\alpha$ non è [debolmente] crescente. Quindi esistono $\gamma < \delta < \alpha$ tali che $F(\gamma) \not\leq F(\delta)$ (S non è detto sia un ordine totale, quindi non possiamo dire che $F(\gamma) > F(\delta)$). Però siccome $\delta < \alpha$, per la minimalità di quest'ultimo, $F|_\delta$ è crescente, per cui $F(\delta)$ è ben definita ed è un maggiorante stretto di $F[\delta]$, quindi, in particolare, $F(\gamma) < F(\delta) \not\leq$.

Questo modo di procedere, però, contiene 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 definita da V a V (in arrivo può essere qualsiasi cosa), come richiesto dal teorema di ricorsione transfinita, perché non è definita se l'immagine di h non ha maggioranti stretti in S . Il ragionamento si aggiusta così: si fissa $\spadesuit \notin S$ e si definisce:

$$F(\alpha) = \begin{cases} f(\{\text{maggioranti stretti di } F[\alpha]\}) & \text{se } F|_\alpha : \alpha \rightarrow S \text{ è crescente} \\ \spadesuit & \text{altrimenti} \end{cases}$$

ora tutti i casi sono coperti ed è lecito applicare il teorema di ricorsione transfinita. Se F non fosse una funzione classe crescente $\text{Ord} \rightarrow S$, ci sarebbe il minimo α tale che $F|_\alpha$ non è $\alpha \rightarrow S$ crescente, e, ragionando come prima si ottiene un assurdo.

Ricapitolando, negando la tesi, abbiamo costruito una funzione classe crescente, dunque iniettiva $\text{Ord} \rightarrow S$, che non può esistere per il teorema di Hartogs. \square

Osservazione 12.7 — Il problema sottile che si presenta sopra è che nell'enunciato del teorema di ricorsione transfinita la G richiesta deve essere ben definita su tutto V , e, prima della correzione (in particolare abbiamo dovuto aggiungere un valore per l'immagine per tutti gli insiemi che non sono ordinali) nel caso sopra, non lo era.

§12.5 Conseguenze immediate di AC

Proposizione 12.8 (Tutti le cardinalità infinite sono aleph)

Ogni insieme è equipotente ad un ordinale iniziale^a. In particolare, ogni cardinalità infinita è un aleph.

^aPer gli insiemi finiti lo sapevamo già, senza bisogno di AC.

Dimostrazione. Per il [teorema del buon ordinamento](#) ogni insieme è bene ordinabile, quindi isomorfo ad un ordinale, e per le proprietà degli ordinali iniziali (cioè sono i rappresentati di tutte le cardinalità [di ordinali](#)), ogni insieme è equipotente ad un ordinale iniziale. La seconda affermazione segue dal fatto che gli ω_α sono tutti e soli gli ordinali iniziali infiniti, per quanto detto, dunque tutte le cardinalità infinite, prima di ordinali ed ora, con AC, di qualunque insieme, sono aleph. \square

Osservazione 12.9 (Tutti gli insiemi sono isomorfi ad un ordinale \implies AC) —

Viceversa, assumere che ogni insieme è equipotente ad un ordinale implica AC.

Dimostrazione. Dal fatto che ogni X è equipotente ad un ordinale deduciamo il teorema del buon ordinamento. Se $|X| = |\alpha|$, con $\alpha \in \text{Ord}$, c'è una bigezione tra X ed α , e tale bigezione induce un buon ordinamento su X . \square

Corollario 12.10 (L'ordine fra le cardinalità è totale)

Tutte le cardinalità sono confrontabili, ovvero:

$$\forall X, Y \quad |X| < |Y| \vee |X| = |Y| \vee |Y| < |X|$$

Dimostrazione. Dalla proposizione sopra sappiamo ora che anche tutte le cardinalità infinite sono ordinali, dunque tutte le cardinalità sono ordinali e queste sappiamo già [senza AC] che sono tutte confrontabili. \square

Osservazione 12.11 (Cardinalità confrontabili \implies AC) — La confrontabilità delle cardinalità implica AC.

Dimostrazione. Dimostriamo che il [teorema del buon ordinamento](#) segue dall'ipotesi che tutte le cardinalità siano confrontabili. Consideriamo il confronto fra $|X|$ e $|H(X)|$. Per la definizione di $H(X)$ non può valere $|H(X)| \leq |X|$, quindi per ipotesi di confrontabilità totale, deve necessariamente valere che $|X| < |H(X)|$, ovvero esiste $f : X \hookrightarrow H(X) \in \text{Ord}$ iniettiva, per cui si ha che $f[X] \subsetneq H(X)$ è un insieme di ordinali, dunque ben ordinato, e ciò induce un buon ordinamento su X . \square

Corollario 12.12 (AC $\implies |X \times X| = |X|$)

Per ogni insieme X infinito, vale che $|X \times X| = |X|$.

Dimostrazione. Per quanto visto, tutte le cardinalità infine sono aleph, dunque $|X| = \aleph_\alpha$, per cui:

$$|X \times X| = \aleph_\alpha \cdot \aleph_\alpha \stackrel{(*)}{=} \aleph_\alpha = |X|$$

dove $(*)$ è il fatto già visto che per ogni $\alpha \in \text{Ord}$ $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$. \square

Nota 12.13 (Teorema di Tarski) — Vale anche che $|X \times X| = |X| \implies \text{AC}$, questo è il teorema di Tarski che vedremo più avanti.

Corollario 12.14 (X infinito $\leftrightarrow \aleph_0 \leq |X|$)

Ogni insieme infinito ha un sottoinsieme numerabile cioè:

$$\forall X \text{ } X \text{ infinito} \leftrightarrow \aleph_0 \leq |X|$$

Dimostrazione. Abbiamo già dimostrato \leftarrow (per l'[osservazione 6.5](#), X non è Dedekind-finito, ma, essendo che finito \implies Dedekind-finito [senza bisogno di AC], la contronominale ci dice che X non è finito, dunque X infinito), mentre la freccia \rightarrow opposta segue dal fatto che, X infinito implica per AC $|X| = \aleph_\alpha$, per quanto visto, ma per la definizione ricorsiva della funzione aleph, $\omega = \omega_0 \leq \omega_\alpha$, $\forall \alpha \in \text{Ord}$, dunque si ha proprio:

$$|X| = \aleph_\alpha = |\omega_\alpha| \geq |\omega| = \aleph_0$$

\square

Ricordiamo che un insieme si dice **Dedekind-finito** (o **finito secondo Dedekind**) se non può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio.

Proposizione 12.15 (Insieme finito \iff Dedekind-finito)

Osserviamo che vale che X finito $\leftrightarrow X$ è Dedekind-finito.

Dimostrazione. Vediamo le due frecce.

\rightarrow Già visto in precedenza, è il [principio dei cassetti](#).

\leftarrow Vediamo la contronominale, se X è infinito, allora per la proposizione precedente $\aleph_0 \leq |X|$, ovvero $\omega \hookrightarrow X$ ¹³⁸, allora possiamo definire la mappa:

$$g : X \rightarrow X : x \mapsto \begin{cases} f \circ s \circ f^{-1}(x) & \text{se } x \in f[\omega] \\ x & \text{altrimenti} \end{cases}$$

tale funzione è iniettiva in quanto in tutti i casi le funzioni sono iniettive (nel primo caso è una composizione di funzioni iniettive), e si osserva

¹³⁸Come accennato nel capitolo sulle cardinalità finite è proprio il fatto che ci serve per concludere l'equivalenza e ci viene dato appunto da AC.

che $f(0) \notin \text{Im}(g)$, infatti in questo caso si avrebbe che $f(s(f^{-1}(x))) = f(x) \implies f(s(y)) = f(0) \implies s(y) = 0$, dunque si ha $|X| = |g[X]|$ e $g[X] \subsetneq X$, per cui X non è Dedekind-finito.

Alternativamente, sempre per dimostrare la contronominalità, per AC abbiamo che X infinito implica $|X| = |\omega_\alpha|$ per qualche $\alpha \in \text{Ord}$, dunque esiste una biogezione f tra X e ω_α e possiamo, in maniera simile a sopra, definire:

$$g : X \rightarrow X : x \mapsto f \circ s \circ f^{-1}(x)$$

come prima tale mappa è iniettiva e $f(0) \notin \text{Im}(g)$, dunque X è in biogezione col sottoinsieme proprio $\text{Im}(g)$, per cui non è Dedekind-finito.

□

Proposizione 12.16 (Surgettività \iff disuguaglianza tra cardinalità)

Vale che:

$$0 < |X| \leq |Y| \iff \exists f : Y \twoheadrightarrow X \text{ surgettiva}$$

Dimostrazione. Vediamo le due implicazioni.

→ Per ipotesi $|X| \leq |Y|$, cioè esiste $g : X \hookrightarrow Y$ iniettiva, fissato $a \in X$ (stiamo usando che X è non vuoto), possiamo definire:

$$f : Y \rightarrow X : y \mapsto \begin{cases} \overset{\text{139}}{g^{-1}(y)} & \text{se } y \in g[X] \\ a & \text{altrimenti} \end{cases}$$

e tale funzione è banalmente surgettiva.

← Viceversa, data $f : Y \twoheadrightarrow X$ surgettiva, abbiamo visto che è un fatto equivalente ad AC dire che esiste un'inversa destra, $h : X \rightarrow Y$, che è iniettiva, per definizione di inversa da $\text{Im}(f) = X$ a Y , e quindi ci dà proprio che $|X| \leq |Y|$.

□

Proposizione 12.17 (Unione di al più \aleph_α insiemi al più \aleph_α)

Se S è un insieme, di cardinalità al più \aleph_α , di insiemi, di cardinalità al più \aleph_α , allora l'unione di S è a sua volta un insieme di cardinalità al più \aleph_α , in simboli:

$$|S| \leq \aleph_\alpha \quad \forall A \in S \quad |A| \leq \aleph_\alpha \rightarrow \left| \bigcup S \right| \leq \aleph_\alpha$$

Dimostrazione. Possiamo assumere $\emptyset \notin S \neq \emptyset$. Cerchiamo una mappa $f : \omega_\alpha \times \omega_\alpha \rightarrow \bigcup S$ surgettiva per avere la disuguaglianza. Per ipotesi possiamo fissare $g : \omega_\alpha \twoheadrightarrow S$ surgettiva, inoltre, detto $H_A = \{h : \omega_\alpha \twoheadrightarrow A \mid h \text{ surgettiva}\}$, sappiamo per ipotesi che per ogni $A \in S$ $H_A \neq \emptyset$, dunque possiamo applicare AC all'insieme $\{H_A\}_{A \in S}$ ed ottenere ι tale che $\iota(H_A) \in H_A$ ¹⁴⁰. A questo punto è facile definire:

$$f : \omega_\alpha \times \omega_\alpha \twoheadrightarrow \bigcup S : (x, y) \mapsto (\iota(H_{g(x)}))(y)$$

¹⁴⁰Anche se fossimo nel caso di \aleph_0 questo passaggio non può essere aggirato, bisogna necessariamente ricorrere ad AC.

¹⁴¹Volendo essere precisissimi, anziché mandare $g(x)$ al pedice di H dovremmo usare due funzioni.

e si osserva che una tale mappa è surgettiva, infatti, preso $z \in \bigcup S$, allora esiste $A \in S$ tale che $z \in A$, dunque per la surgettività di g esiste $x \in \omega_\alpha$ per cui $g(x) = A$; osservando ora che $\iota(H_{g(x)})$ è surgettiva da ω_α ad A si ha che esiste $y \in \omega_\alpha$ tale che $(\iota(H_{g(x)}))(y) = z$, da cui si conclude. \square

Corollario 12.18 (Unione al più numerabile di insiemi al più numerabili)

Un'unione numerabile (o anche al più numerabile) di insiemi numerabili (al più numerabile) è numerabile (al più numerabile).

Osservazione 12.19 (Parti di cardinalità al più n) — Sia $\mathcal{P}^{\leq n}(X) \stackrel{\text{def}}{=} \{A \in \mathcal{P}(X) : |A| \leq n\}$, se X è infinito e $0 < n < \omega$, allora $|\mathcal{P}^{\leq n}(X)| = |X|$.

Dimostrazione. La disegualanza $|X| \leq |\mathcal{P}^{\leq n}(X)|$ si ottiene con la mappa iniettiva che manda ogni elemento nel suo singoletto $X \hookrightarrow \mathcal{P}^{\leq n}(X) : x \mapsto \{x\}$.

Per dimostrare la disegualanza dall'alto possiamo procedere in due modi equivalenti, o definendo la mappa:

$$\mathcal{P}^{\leq n}(X) \supseteq \{A \in \mathcal{P}(X) : 0 < |A| \leq n\} \hookrightarrow {}^n X : A \mapsto \iota(H_A)$$

con $H_A = \{f : n \rightarrow A\}$ (che è non vuoto per A nell'insieme in partenza) e ι funzione di scelta su $\{H_A\}_{0 < |A| \leq n}$, tale mappa è iniettiva perché, presa h nell'immagine per tornare indietro ci basta considerare $\text{Im}(h)$ (oppure si può verificare l'iniettività sfruttando la definizione). Al contrario si può definire:

$${}^n X \twoheadrightarrow \{A \in \mathcal{P}(X) : 0 < |A| \leq n\} \subseteq \mathcal{P}^{\leq n}(X) : f \mapsto \text{Im}(f)$$

che è ben definita perché per AC $|\text{Im}(f)| \leq n$, ed è surgettiva perché per ogni insieme in arrivo esiste per definizione una mappa surgettiva da n a lui [e possiamo fissarla senza AC], dunque in entrambi i casi abbiamo concluso. \square

Esercizio 12.20 ($|\mathcal{P}^n(X)| = |X|$). Se X è infinito e $0 < n < \omega$, allora $|\mathcal{P}^n(X)| = |\{A \in \mathcal{P}(X) : |A| = n\}| = |X|$.

Soluzione. Per la disegualanza dall'alto si può procedere come prima e definire la mappa:

$$\{A \in \mathcal{P}(X) : |A| = n\} \rightarrow {}^n X : A \mapsto \iota(H_A)$$

dove $H_A = \{f \in {}^n X \mid f \text{ bigettiva}\}$ e $\iota : \{H_A\}_{|A|=n} \rightarrow \bigcup_{|A|=n} H_A$ funzione di scelta. Poiché per ipotesi $|A| = n$, si ha $H_A \neq \emptyset$, dunque la mappa è ben definita, inoltre è iniettiva perché presa g in arrivo possiamo tornare indietro considerando $\text{Im}(g)$, pertanto abbiamo che $|\mathcal{P}^n(X)| \leq |{}^n X| = |X|^n = \aleph_\alpha^n = \aleph_\alpha = |X|$.¹⁴²

Per la disegualanza opposta, sia $|X| = \aleph_\alpha = |\omega_\alpha|$, e fissiamo $g : \omega_\alpha \rightarrow X$ bigezione, naturalmente si ha $|\omega_\alpha \setminus n| = |\omega_\alpha|$, per cui possiamo definire:

$$\omega_\alpha \setminus n \rightarrow \{A \in \mathcal{P}(X) : |A| = n\} : x \mapsto g[(n \setminus \{0\}) \cup \{x\}]$$

che è ben definita in quanto $|g[(n \setminus \{0\}) \cup \{x\}]| = |(n \setminus \{0\}) \cup \{x\}| = n$, ed è iniettiva perché g iniettiva e $(n \setminus \{0\}) \cup \{x\} = (n \setminus \{0\}) \cup \{y\} \implies x = y$.¹⁴³ \square

¹⁴² Si poteva anche osservare che $\mathcal{P}^n(X) \subseteq \mathcal{P}^{\leq n}(X)$, e da sopra sappiamo che $|\mathcal{P}^{\leq n}(X)| \leq |X|$.

¹⁴³ In alternativa andava bene anche $x \mapsto g[\{x + i\}_{i \in n}]$, infatti la prima mappa è iniettiva in quanto se due insiemi in arrivo sono uguali hanno anche lo stesso minimo e quindi stesso elemento in partenza.

Osservazione 12.21 — Assumendo la tesi dell'ultimo esercizio troviamo anche una dimostrazione alternativa per l'upper bound dell'ultima osservazione, infatti sappiamo che:

$$\mathcal{P}^{\leq n}(X) = \bigcup_{i \leq n} \mathcal{P}^i(X)$$

e, assumendo il risultato precedente, $|\mathcal{P}^i(X)| = |X| = \aleph_\alpha$, dunque abbiamo un'unione finita di insiemi di cardinalità al più \aleph_α , e per la proposizione sopra la cardinalità dell'unione è a sua volta al più \aleph_α , da cui $|\mathcal{P}^{\leq n}(X)| \leq |X|$.

Proposizione 12.22 ($|\mathcal{P}^{\text{fin.}}(X)| = |X|$)

Se X è infinito, allora vale che $|\mathcal{P}^{\text{fin.}}(X)| = |X|$.

Dimostrazione. Sia $|X| = \aleph_\alpha$, sappiamo che:

$$\mathcal{P}^{\text{fin.}}(X) = \bigcup_{n \in \omega} \mathcal{P}^{\leq n}(X)$$

dove per l'osservazione sopra sappiamo che $|\mathcal{P}^{\leq n}(X)| = |X| = \aleph_\alpha$, dunque abbiamo un'unione al più \aleph_0 di insiemi al più \aleph_α , per cui dalla proposizione dimostrata prima, $|\mathcal{P}^{\text{fin.}}(X)| \leq |X| = \aleph_\alpha$. La disegualanza dal basso è banale, basta considerare la mappa $X \hookrightarrow \mathcal{P}^{\text{fin.}}(X) : x \mapsto \{x\}$, e si conclude. \square

Proposizione 12.23 (Principio della discesa infinita generalizzato)

Un ordine totale $(A, <)$ è un buon ordine se e solo se non esiste una successione [strettamente] decrescente $\{a_n\}_{n \in \omega}$ di elementi di A .

Dimostrazione. Vediamo le due implicazioni.

\Rightarrow Vediamo la contronominale, ovvero, se esiste una successione [strettamente] decrescente di elementi di A , allora il sottoinsieme:

$$\{a_n \in A \mid n \in \omega\} \subseteq A$$

non può avere minimo, dunque $(A, <)$ non può essere un buon ordinamento.

\Leftarrow Viceversa, anche in questo caso possiamo dimostrare la contronominale, dunque verifichiamo che un ordine totale, che non sia bene ordinato, ci dà una successione di elementi [strettamente] decrescente. Per ipotesi $\exists S \subseteq A, S \neq \emptyset$, che non ha elemento minimo, fissato $s \in S$ possiamo definire per ricorsione numerabile:

$$x_0 = s \quad x_{n+1} = f(\{y \in A \mid y < x_n\})$$

con $f : \mathcal{P}(A) \setminus \{\emptyset\} \rightarrow A$ funzione di scelta. Tale successione è ben definita in quanto per ipotesi A non ha minimo, dunque la funzione di scelta viene applicata sempre su insiemi non vuoti, inoltre, la successione [di elementi di A] è strettamente decrescente per costruzione.

\square

§12.6 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 la seguente caratterizzazione dei suoi sottoinsiemi chiusi.

Proposizione 12.24 (Caratterizzazione della chiusura di un sottoinsieme di \mathbb{R})

Sia $A \subseteq \mathbb{R}$, allora abbiamo che:

$$x \in \bar{A} \iff \exists(x_i)_{i \in \omega} (\forall i \in \omega x_i \in A) \wedge \left(\lim_{i \rightarrow +\infty} x_i = x \right)$$

dove $x \in \bar{A} \equiv \forall \varepsilon > 0]x - \varepsilon, x + \varepsilon[\cap A \neq \emptyset$.

Dimostrazione. Vediamo le due implicazioni.

← Fissato $\varepsilon > 0$, per definizione di limite:

$$\exists j \in \omega \forall i \geq j |x - x_i| \leq \varepsilon$$

inoltre, per ipotesi $x_i \in A$ per ogni $i \in \omega$, segue $\forall i \geq j x_i \in]x - \varepsilon, x + \varepsilon[\cap A$, che quindi è diversa dal vuoto, pertanto, dall'arbitrarietà di ε , segue che $x \in \bar{A}$.

→ Fissata una funzione di scelta sui sottoinsiemi di A , $f : \mathcal{P}(A) \setminus \{\emptyset\} \rightarrow A$, possiamo definire per ricorsione numerabile forte:

$$x_i = f \left(\left] x - \frac{1}{i+1}, x + \frac{1}{i-1} \right[\cap A \right)$$

che è ben definita in quanto l'insieme su cui applichiamo f non è mai vuoto per ipotesi, inoltre $x_i \rightarrow x$ per il teorema dei carabinieri.

□

§12.7 Basi di spazi vettoriali

Un'altra applicazione è l'esistenza delle basi di spazi vettoriali infinito-dimensionali [e non finitamente generati]. 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 $x_1, \dots, x_n \in F$:

$$x_1 a_1 + \dots + x_n a_n = 0 \iff x_1 = \dots = x_n = 0$$

$B \subseteq V$ linearmente indipendente è una base se, dato qualunque $v \in V$, esistono $b_1, \dots, b_n \in B$ e $x_1, \dots, x_n \in F$ 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 . Né avrebbe senso, in generale, parlare di combinazioni lineari se non finite.

L'osservazione segue è la chiave per applicare il lemma di Zorn.

Osservazione 12.25 (Base \iff sottoinsieme linearmente indipendente massimale) —

B è una base, ovvero un insieme linearmente indipendente di generatori, se e solo se è un sottoinsieme linearmente indipendente di V , massimale rispetto alla relazione d'ordine di inclusione.

Dimostrazione. Vediamo prima che la definizione data di base implica che sia un insieme linearmente indipendente massimale e poi viceversa.

\Rightarrow Se B non fosse massimale rispetto alla relazione di inclusione, allora esisterebbe $B' \supsetneq B$ linearmente indipendente, ovvero $\exists v \in B' \setminus B$, con $v \neq 0$ e linearmente indipendente da tutti gli altri elementi di B' . Essendo B un insieme di generatori si ha $v = b_1x_1 + \dots + b_nx_n$ per opportuni $b_1, \dots, b_n \in B$ e $x_1, \dots, x_n \in F$, con almeno un $x_i \neq 0$ in quanto $v \neq 0$, da cui:

$$b_1x_1 + \dots + b_nx_n + v \cdot (-1) = 0$$

che è una combinazione lineare nulla con coefficienti non tutti nulli, per cui v non è linearmente indipendente rispetto a $b_1, \dots, b_n \in B$ e $x_1, \dots, x_n \in F$ e quindi non può appartenere a $B' \setminus B$, che di conseguenza è vuota e quindi è assurdo supporre che B non sia massimale rispetto alla relazione di inclusione.

\Leftarrow Sia B massimale e linearmente indipendente è sufficiente verificare che genera. Dato $v \in V$, se $v \in B$, chiaramente $v = v \cdot 1$, altrimenti, per la massimalità di B , $B \cup \{v\}$ non è linearmente indipendente, dunque esistono $b_1, \dots, b_n \in B$ e $x_1, \dots, x_n, y \in F$ tali che:

$$x_1b_1 + \dots + x_nb_n + yv = 0$$

ma non accade che tutti i coefficienti della combinazione lineare sono contemporaneamente nulli $x_1 = \dots = x_n = y = 0$. Se y fosse uguale a 0, avremmo $x_1 = \dots = x_n = 0$ per l'indipendenza di B e avremmo trovato un insieme linearmente indipendente più grande, che è assurdo. Quindi $y \neq 0$ e di conseguenza possiamo scrivere $v = \left(-\frac{x_1}{y}\right)b_1 + \dots + \left(-\frac{x_n}{y}\right)b_n \in \text{span}(B)$, dunque B genera.

□

Proposizione 12.26 (Esistenza delle basi in uno spazio vettoriale)

Dato uno spazio vettoriale V e $X \subseteq V$ linearmente indipendente^a, esiste una base B di V tale che $X \subseteq B$.

^aSe $V \neq \emptyset$ c'è sempre almeno un vettore e quindi $X \neq \emptyset$.

Dimostrazione. Applichiamo il lemma di Zorn al sottoinsieme:

$$Y := \{A \in \mathcal{P}(V) \mid A \text{ linearmente indipendente e } A \subseteq X\} \quad ^{144}$$

che è parzialmente ordinato dall'inclusione \subseteq . Una volta verificate le ipotesi di Zorn avremo che c'è almeno un elemento massimale di Y , dunque c'è almeno un sottoinsieme linearmente indipendente massimale rispetto all'inclusione che contiene un fissato

¹⁴⁴Stiamo dimostrando un po' di più dell'esistenza di una base in ogni spazio vettoriale, cioè stiamo anche dimostrando che in ogni spazio vettoriale ogni insieme linearmente indipendente è contenuto in una base, se volessimo solo l'esistenza ci basterebbe applicare Zorn al sottoinsieme degli insieme linearmente indipendenti e basta.

sottoinsieme linearmente indipendente, e che per l'equivalenza precedente è una base di V . Sia $S \subseteq Y$ una sottocatena, verifichiamo che $\bar{A} := \bigcup_{A \in S} A$ è un maggiorante per quest'ultima, naturalmente $X \subseteq \bar{A}$, osserviamo inoltre che:

$$\forall A \in S \quad X \subseteq \bigcup_{A \in S} A = \bar{A}$$

dunque \bar{A} è un maggiorante per S . Ci resta da verificare che \bar{A} è un insieme linearmente indipendente per avere $\bar{A} \in Y$, siano $b_1, \dots, b_n \in \bar{A} = \bigcup_{A \in S} A$, vogliamo vedere che:

$$x_1 b_1 + \dots + x_n b_n = 0 \rightarrow x_1 = \dots = x_n = 0$$

poiché gli x_i appartengono ad un'unione, possiamo considerare $A_i \in S$ tale che $x_i \in A_i$, ora $\{A_i\}_{1 \leq i \leq n} \subseteq S$ è un sottoinsieme finito e totalmente ordinato ha un massimo, sia $A_j \in S$, ed essendo un massimo per la relazione di inclusione si ha proprio che $x_1, \dots, x_n \in X_j$, quest'ultimo è linearmente indipendente e quindi vale l'implicazione scritta sopra, che ci permette di concludere la lineare indipendenza di \bar{A} . \square

Esercizio 12.27 (\mathbb{R} come \mathbb{Q} -spazio vettoriale). Sia B una base di \mathbb{R} preso come \mathbb{Q} -spazio vettoriale^a, determinare $|B|$.

^aTali basi prendono il nome di **basi di Hamel** di \mathbb{R} come \mathbb{Q} -spazio.

Osservazione 12.28 (Combinazioni lineari finite e infinite) — Per AC, come abbiamo appena visto, ogni spazio vettoriale ha necessariamente una base, ciò giustifica l'esistenza di una base di \mathbb{R} come \mathbb{Q} -spazio. Nonostante, come stiamo per dimostrare, tale spazio abbia dimensione infinita, la definizione di span tuttavia rimane limitata a combinazioni lineari finite di elementi di una base, queste prendono il nome di **basi di Hamel** (o basi nel senso algebrico)^a, ciò significa che ogni reale può essere ottenuto come combinazione lineare finita di elementi della base, esattamente come accade ad esempio nello spazio vettoriale dei polinomi.

Per estendere il concetto di combinazioni lineari a somme infinite c'è invece bisogno di avere una topologia sullo spazio che si considera in modo da poter definire i limiti e il concetto annesso di serie per fare appunto queste somme infinite, e questo è il caso delle **basi di Schauder**.

^aNel caso di uno spazio di dimensione finita la nozione di base di Hamel coincide con quella di base in ogni caso.

Soluzione. Sia B una base di \mathbb{R} come \mathbb{Q} -spazio, per definizione $B \subseteq \mathbb{R} \implies |B| \leq 2^{\aleph_0}$. Viceversa, ricordando che stiamo considerando solo combinazioni lineari finite per definizione, abbiamo che lo span della base non è altro che l'unione di tutti i possibili span di sottoinsiemi finiti dei suoi elementi, per cui:

$$2^{\aleph_0} = |\mathbb{R}| = |\text{span}_{\mathbb{Q}}(B)| = \left| \bigcup_{\{x_1, \dots, x_n\} \in \mathcal{P}^{\text{fin.}}(B)} \text{span}_{\mathbb{Q}}(x_1, \dots, x_n) \right|$$

dove $|\text{span}_{\mathbb{Q}}(x_1, \dots, x_n)| = \aleph_0^n = \aleph_0$, infatti, fissati gli n vettori della base, si tratta soltanto di scegliere un coefficiente razionale per ognuno e questo lo possiamo fare in \aleph_0 modi¹⁴⁵. Inoltre, per AC, $|\mathcal{P}^{\text{fin.}}(B)| = |B|$, per B infinito (e B è necessariamente infinito

¹⁴⁵Volendo essere formalissimi stiamo semplicemente dicendo che $\text{span}_{\mathbb{Q}}(x_1, \dots, x_n)$ è in biiezione con \mathbb{Q}^n , fissando una combinazione lineare basta mandare l' i -esimo coefficiente razionale nell' i -esima componente della n -upla.

perché se non lo fosse avremmo con inclusione-esclusione che sopra il RHS è $\leq \aleph_0$, che è assurdo), a questo punto, sempre per AC, abbiamo che $|B| = \aleph_\alpha \geq \aleph_0$, per cui abbiamo un'unione al più \aleph_α di insiemi al più \aleph_0 , che per una proposizione precedente è appunto al più \aleph_α . Abbiamo quindi ottenuto che $2^{\aleph_0} \leq |B|$. \square

Soluzione. (Alternativa)

Dato V spazio vettoriale su un campo K , fissata una sua base B , dall'algebra lineare sappiamo che:

$$|V| = |\{f \in K^B : |\text{supp}(f)| < \aleph_0\}|^{146}$$

e le funzioni a supporto finito si immagazzinano in $\mathcal{P}^{\text{fin}}(B \times K)$, che, per AC, ha cardinalità $|B \times K|$. Nel caso di \mathbb{R} come \mathbb{Q} -spazio si ottiene:

$$2^{\aleph_0} = |\mathbb{R}| \leq |B \times \mathbb{Q}| = |B| \cdot \aleph_0 \implies 2^{\aleph_0} \leq |B|$$

la disegualanza dall'alto si ottiene come prima perché $B \subseteq \mathbb{R}$. \square

Esempio 12.29 (Equazione funzionale di Cauchy)

Esiste una funzione $f : \mathbb{R} \rightarrow \mathbb{R}$ tale che:

$$\forall x, y \in \mathbb{R} \quad f(x + y) = f(x) + f(y)$$

tuttavia f **NON** è della forma $f(x) = k \cdot x$.

Dimostrazione. Sia $B = \{b_1, \dots, b_n\}$ una base di \mathbb{R} come \mathbb{Q} -spazio vettoriale, allora ogni $x \in \mathbb{R}$ si può scrivere in modo unico come $x = b_1 r_1 + \dots + b_n r_n$ con $r_1, \dots, r_n \in \mathbb{Q}$, e la funzione che associa x ad r_1 - la proiezione di x al sottospazio $\text{span}_{\mathbb{Q}}(b_1)$ - cioè:

$$f : \mathbb{R} \rightarrow \mathbb{Q} : x \mapsto r_1$$

è ben definita (vista l'unicità della scrittura in base) ed è una funzione additiva, infatti, dato $y \in \mathbb{R}$, allora $y = b_1 p_1 + \dots + b_n p_n$, per cui $f(y) = p_1$ e:

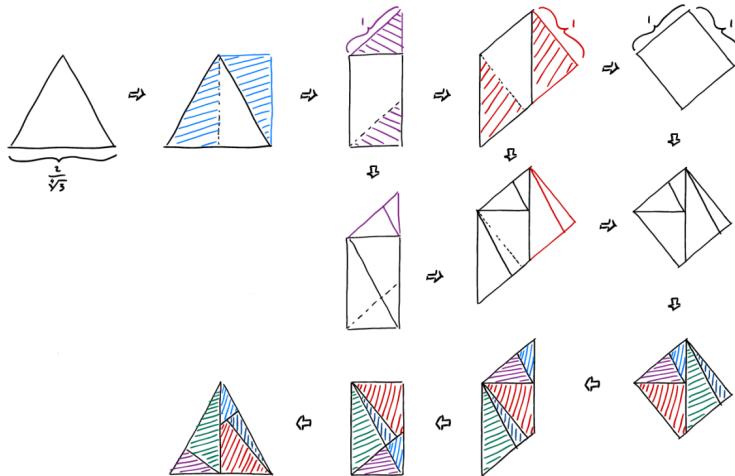
$$\begin{aligned} f(x + y) &= (b_1(r_1 + p_1) + \dots + b_n(r_n + p_n)) \\ &= r_1 + p_1 \\ &= f(x) + f(y) \end{aligned}$$

e data l'arbitrarietà di $x, y \in \mathbb{R}$, allora f è additiva e si vede banalmente che non è lineare - $f(2x) = 2r_1 \neq 2x$ (a meno che $b_1 = 2$, ma allora basta cambiare numero e si conclude comunque) -. \square

¹⁴⁶Una possibile bigezione è ad esempio $f \mapsto \sum_{\substack{1 \leq i \leq |B| \\ f(v_i) \neq 0}} f(v_i) \cdot v_i \in V$, con $v_i \in B$ (è una somma finita visto che richiediamo $f(v_i) \neq 0$, ed f è a supporto finito), infatti è iniettiva per l'unicità della scrittura in base, ed è surgettiva perché ogni vettore si scrive come combinazione lineare finita di vettori della base a coefficienti in K ed è facile identificare tale scrittura con una funzione a supporto finito che associa ogni vettore della base al suo coefficiente (è ciò che si fa quando si passa in coordinate).

§12.8 Invariante di Dehn

È nato 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 [= con la stessa area], è sufficiente spezzarlo in triangoli, poi trasformare i triangoli in rettangoli, poi, passando per un parallelogramma, si trasforma un rettangolo in un altro con uno dei due lati arbitrario. Infine, portando tutti i rettangoli ad avere un lato uguale, unendoli, e trasformando il nuovo rettangolo in un quadrato, di nuovo col trucco del parallelogramma, si ottiene appunto il quadrato desiderato.

Nota 12.30 (L'area secondo Euclide) — 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 $\text{Area}(A) = \text{Area}(B)$ 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 sistematizzazione formale di questi concetti è dovuta a **Hilbert**, e al XIX secolo.

Ebbene, tutti questi anacronismi solo per dire che **in tre dimensioni questa definizione (per il volume in questo caso) non funziona**, ovvero non è detto che due poliedri con lo stesso volume si possano scomporre in parti congruenti (e quindi non possiamo ottenere l'uno dall'altro come nel caso bidimensionale).

Teorema 12.31 (Dehn)

Un cubo ed un tetraedro regolare, sia pure aventi il medesimo volume, non si possono scomporre in un numero finito di poliedri congruenti (cioè non sono equiscomponibili).^a

^aQuesta proposizione e annessa dimostrazione sono un caso particolare della soluzione generale di Dehn al **terzo problema di Hilbert**.

Dimostrazione. Supponiamo di avere una funzione $f : \mathbb{R} \rightarrow \mathbb{R}$ 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 $\ell \cdot f(\alpha)$.

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 quindi vale che $\ell \cdot f(\alpha_1) + \ell \cdot f(\alpha_2) = \ell \cdot f(\alpha_1 + \alpha_2) = \ell \cdot f(\pi) \stackrel{\text{def. di } f}{=} 0$.

Può dividere spigoli vecchi, in **verde**, in due, poniamo di lunghezza ℓ_1 e ℓ_2 , senza alterare l'angolo diedro, per cui $(\ell_1 + \ell_2) \cdot f(\alpha) = \ell_1 \cdot f(\alpha) + \ell_2 \cdot f(\alpha)$. Infine, in **azzurro**, può spezzare l'angolo diedro lasciando inalterata la lunghezza, e si conclude similmente.

Abbiamo concluso quindi che il **valore** è invariante per equiscomposizioni, pertanto **due figure equiscomponibili devono avere necessariamente lo stesso valore**, non ci resta che 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 $\{\pi\}$ (che è una applicazione diretta della proposizione dimostrata in precedenza). 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 completamento 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 $x = \pi q_0$, con $q_0 \in \mathbb{Q}$.

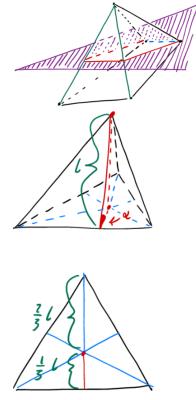
Ora è chiaro che il valore di un cubo è nullo, perché tutti i diedri hanno ampiezza $\frac{\pi}{2}$, quindi i valori dei singoli spigoli sono tutti nulli e così la loro somma (che per definizione è appunto il valore del cubo).

Vediamo ora che il valore di un tetraedro regolare non è mai nullo - anche se il tetraedro avesse lo stesso volume del cubo -, in tal modo, per quanto detto sul valore, cubo e tetraedro non sono equiscomponibili.

Si vede che gli angoli diedri del tetraedro valgono $\alpha = \arccos \frac{1}{3}$, quindi basta dire che questo α non è multiplo razionale di π , in tal modo il valore del tetraedro sarà non nullo. In altri termini, vogliamo verificare che, $n\alpha$, per $n \in \omega$, non è un multiplo intero di π . Questo fatto si può esprimere, altresì, dicendo che $z^n \notin \mathbb{R}$, dove $z = \cos \alpha + i \sin \alpha \in \mathbb{C}$ - $z^n = \cos(n\alpha) + i \sin(n\alpha)$, dunque se $n\alpha$ fosse multiplo di π si avrebbe $\Im(z^n) = 0 \implies z^n \in \mathbb{R}$. Ora, avendo $\alpha = \arccos \frac{1}{3}$, $z = \frac{1}{3}(1 + 2i\sqrt{2})$, e, si vede immediatamente per induzione, che $(1 + 2i\sqrt{2})^n = x_n + y_n i\sqrt{2}$ per qualche $x_n, y_n \in \mathbb{Z}$ (ci basta controllare che $y_n \neq 0$ per ogni n). Inoltre, sempre per induzione, riducendo x_n e y_n modulo 3, otteniamo che:

- per n dispari $x_n \equiv 1 \pmod{3}$ e $y_n \equiv 2 \pmod{3}$.
- per n pari e diverso da 0 invece $x_n \equiv 2 \pmod{3}$ e $y_n \equiv 1 \pmod{3}$.

In nessun caso, in particolare, si ottiene che $y_n \equiv 0 \pmod{3}$, quindi non potrà essere mai che $y_n = 0$, pertanto z^n non sarà mai reale e quindi $n\alpha$ mai multiplo razionale di π . \square



§12.9 Insieme di Vitali

Vediamo ora un'altra applicazione che da luogo ad un risultato negativo: il **controesempio di Vitali**.

Definizione 12.32 (Misura σ -additiva). Una **misura σ -additiva** su $\mathcal{P}(\mathbb{R})$ è una funzione $\mu : \mathcal{P}(\mathbb{R}) \rightarrow \mathbb{R}_{\geq 0} \cup \{+\infty\}$, tale che $\mu(\emptyset) = 0$ e, se $\{A_i\}_{i \in \omega}$ è una successione di elementi **disgiunti** di $\mathcal{P}(\mathbb{R})$ allora:

$$\mu\left(\bigcup_{i \in \omega} A_i\right) = \sum_{i=0}^{+\infty} \mu(A_i)$$

Definizione 12.33 (Misura invariante per traslazioni). Una misura μ si dice **invariante per traslazioni** se $\forall x \in \mathbb{R}$ e $A \in \mathcal{P}(\mathbb{R})$:

$$\mu(A) = \mu(\{y \in \mathbb{R} \mid \underbrace{y - x \in A}_{\stackrel{\text{def}}{=} A+x}\})$$

cioè la misura di un sottoinsieme di \mathbb{R} è invariante se lo trasliamo.

Osservazione 12.34 (Monotonia di una misura) — Si osserva che se $A \subseteq B \subseteq \mathbb{R}$, allora $\mu(A) \leq \mu(B)$.

Dimostrazione. Si vede che $\mu(B) = \mu(A \sqcup (B \setminus A)) \stackrel{\text{additività}}{=} \mu(A) + \mu(B \setminus A) \geq \mu(A)$. \square

Esercizio 12.35. Esibisci una misura σ -additiva ed invariante per traslazioni su $\mathcal{P}(\mathbb{R})$.

Soluzione. La **misura di Lebesgue** è una misura σ -additiva ed invariante per traslazioni su $\mathcal{P}(\mathbb{R})$. \square

Proposizione 12.36 (Controesempio di Vitali)

Non esiste una misura σ -additiva e invariante per traslazioni, $\mu : \mathcal{P}(\mathbb{R}) \rightarrow \mathbb{R}_{\geq 0} \cup \{+\infty\}$, tale che $\mu([0, 1]) = 1$.

Dimostrazione. Supponiamo, per assurdo, che esista una tale misura 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 $[0, 1] = \bigcup_{i \in \omega} A_i$ - stiamo quindi cercando di partizionare $[0, 1]$ con un numero numerabile di insiemi disgiunti e aventi tutti la stessa misura -. Se riusciamo scrivere una tale partizione otteniamo appunto un assurdo, infatti:

- se $\mu(A_i) = \mu(A_j) = 0$ per ogni $i, j \in \omega$, allora $\mu([0, 1]) = \sum_{i \in \omega} \mu(A_i) = \sum_{i \in \omega} 0 = 0 \neq 1 \textcolor{red}{\checkmark}$.
- se $\mu(A_i) = \mu(A_j) = k > 0$ per ogni $i, j \in \omega$, allora $\mu([0, 1]) = \sum_{i \in \omega} \mu(A_i) = \sum_{i \in \omega} k = k \cdot \sum_{i \in \omega} 1 = +\infty \neq 1 \textcolor{red}{\checkmark}$.

Fissiamo $i \mapsto q_i$ un'enumerazione di \mathbb{Q} , e fissiamo **B base di \mathbb{R}** come \mathbb{Q} -spazio vettoriale. Possiamo assumere WLOG che $b_0 = 1 \in B$, infatti, se così non fosse, ci basta prendere $b_0 \in B$ e moltiplicare tutti gli elementi di B per $\frac{1}{b_0}$. Definiamo:

$$R_i := \{x \in \mathbb{R} \mid x = r_0 \cdot 1 + q_i \cdot b_1 + r_2 \cdot b_2 + \dots + r_n \cdot b_n, \text{ con } r_0, r_2, \dots, r_n \in \mathbb{Q}\}$$

cioè l'insieme dei reali che scritti in base B hanno come coefficiente di b_1 l' i -esimo razionale. Definiamo inoltre $A_i := R_i \cap [0, 1[$. Siccome la successione $(q_i)_{i \in \omega}$ enumera i razionali, l'unione degli R_i , al variare di $i \in \omega$, ci dà proprio - tutte le possibili scritture in base B al variare dei coefficienti razionali - $\bigcup_{i \in \omega} R_i = \mathbb{R}$, inoltre gli R_i sono disgiunti per l'unicità della scrittura in base. Abbiamo quindi che la famiglia $\{R_i\}_{i \in \omega}$ è una partizione di \mathbb{R} , e di conseguenza $\{A_i\}_{i \in \omega}$ è una partizione di $[0, 1[$.

Dimostriamo infine che $\mu(A_i) = \mu(A_j)$ per ogni $i, j \in \omega$. Siano $\delta := (q_j - q_i)b_1$ e $k := \lceil \delta \rceil$. Consideriamo l'insieme $A_i + \delta$, osserviamo in primis che si ha:

$$\begin{aligned} x \in R_i &\iff x \in \text{span}(B \setminus \{b_1\}) + q_i b_1 \\ &\iff x + \delta \in \text{span}(B \setminus \{b_1\}) + q_j b_1 \quad (q_j b_1 = \delta + q_i b_1) \\ &\iff x + \delta \in R_j \end{aligned}$$

per cui possiamo scrivere $A_i + \delta$ come:

$$\begin{aligned} A_i + \delta &= (R_i + \delta) \cap [\delta, \delta + 1[\\ &= R_j \cap [\delta, \delta + 1[\quad (R_i + \delta = R_j) \\ &= \underbrace{R_j \cap [\delta, k[}_{=: X_1} \cup \underbrace{R_j \cap [k, \delta + 1[}_{=: X_2} \end{aligned}$$

e naturalmente X_1 ed X_2 sono disgiunti. Similmente per $n \in \omega$:

$$\begin{aligned} x \in R_j &\iff x \in \text{span}(B \setminus \{b_1, 1\}) + \mathbb{Q} + q_j b_1 \\ &\iff x + n \in \text{span}(B \setminus \{b_1, 1\}) + \mathbb{Q} + q_j b_1 \quad (\mathbb{Q} + n = \mathbb{Q}) \\ &\iff x + n \in R_j \end{aligned}$$

(in altre parole stiamo semplicemente assorbendo il termine in \mathbb{Q} nel coefficiente di $b_0 = 1$ nella scrittura in base). Possiamo quindi definire:

$$\begin{aligned} Y_1 &:= X_1 - k + 1 = R_j \cap [\delta - k + 1, 1[\\ Y_2 &:= X_2 - k = R_j \cap [0, \delta - k + 1[\end{aligned}$$

dove abbiamo usato che $R_j = R_j - k + 1$ e $R_j = R_j - k$ per l'osservazione vista prima. 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 assieme segue quindi:

$$\mu(A_j) = \mu(Y_1) + \mu(Y_2) \stackrel{\text{invar. per trasl.}}{=} \mu(X_1) + \mu(X_2) = \mu(A_i + \delta) \stackrel{\text{invar. per trasl.}}{=} \mu(A_i)$$

□

Esercizio 12.37 (Dimostrazione alternativa). Una maniera alternativa di dimostrare la proposizione precedente è come segue:

- considerare la relazione di equivalenza su $[0, 1[$ data da $x \sim y \iff x - y \in \mathbb{Q}$.
- fissare un $V \subseteq [0, 1[$ che contiene un solo per ogni classe di equivalenza - [si usa AC](#).
- dimostrare che $[0, 1[\subseteq S \stackrel{\text{def}}{=} \bigcup_{r \in \mathbb{Q} \cap [-1, 1[} V + r \subseteq [-1, 2[,$ 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 $\mu(S) = +\infty$.^a

^aPer la soluzione si veda [qui](#).

§12.10 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 $x \in \overline{(S \setminus \{x\})}$ - ossia (è nella chiusura di $S \setminus \{x\}$) se esiste una successione $(x_i)_{i \in \omega}$ di punti di $S \setminus \{x\}$ tale che $\lim_{i \rightarrow +\infty} x_i = x$. Diciamo che $S \subseteq \mathbb{R}$ è **perfetto** se S coincide con l'insieme dei suoi punti di accumulazione ($\mathcal{D}(S)$, il **derivato** di S).

Esempio 12.38 (Gli intervalli chiusi sono insiemi perfetti)

Un intervallo chiuso $[a, b]$ è un esempio di insieme perfetto.

Esercizio 12.39. Esibire un insieme perfetto non vuoto avente **parte interna** - ossia $\{x \in S \mid \exists \varepsilon > 0 \ [x - \varepsilon, x + \varepsilon] \subseteq S\} = \emptyset$.

Soluzione. L'insieme di Cantor rispetta le proprietà richieste, infatti il suo complementare è unione di segmenti aperti, quindi è un aperto e dunque l'insieme di Cantor è un sottoinsieme chiuso dell'intervallo $[0, 1]$. Inoltre in un qualsiasi intorno di un punto dell'insieme di Cantor ci sono sia punti dell'insieme sia punti del suo complementare, la prima cosa ci dice che tutti i punti sono aderenti, dunque è perfetto, la seconda ci dice che non ha punti interni, dunque ha parte interna vuota. \square

Proposizione 12.40 (Sottoinsiemi perfetti di $[0, 1]$)

Se $S \subseteq [0, 1]$ è perfetto, allora $|S| = 2^{\aleph_0}$

Per dimostrare questa proposizione, è comoda l'osservazione seguente.

Osservazione 12.41 (Ogni perfetto di $[0, 1]$ contiene due perfetti disgiunti) — Se $S \subseteq [0, 1]$ è perfetto e non vuoto allora esistono S_1 e S_2 sottoinsiemi di S perfetti, non vuoti e disgiunti.

Dimostrazione. Un singoletto non è perfetto, quindi un perfetto ha almeno due punti, $x_1, x_2 \in S$, e supponiamo WLOG $x_1 < x_2$. Ora si danno due casi:

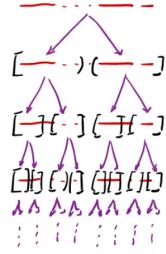
- se $[x_1, x_2] \subseteq S$: consideriamo x_3, x_4 tali che $x_1 < x_2 < x_3 < x_4$ e definiamo $\overline{S_1} = S \cap [0, x_3], S_2 = S \cap [x_4, 1]$, questi ultimi sono naturalmente disgiunti, non vuoti, chiusi e senza punti isolati (se ce ne fosse uno esisterebbe un intorno che lo isola ovvero che non sta nell'intersezione, ed essendo uno dei due intersecandi un intervallo chiuso l'unica possibilità è che l'intorno che isola il punto nell'intersezione non stia nell'intervallo ma stia solo in S , tuttavia in tal modo il punto sarebbe isolato in S che è perfetto \notin).

- se esiste $x_3 \in [x_1, x_2] \setminus S$: definiamo $S_1 = S \cap [0, x_3]$ e $S_2 = S \cap [x_3, 1]$ (in questo caso intersecando con i chiusi otteniamo ancora un chiuso ed x_3 comunque non ci sta dentro, per cui vale lo stesso ragionamento di sopra¹⁴⁷).

□

Veniamo ora alla dimostrazione della proposizione.

L'idea è quella 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 ben 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 delle successioni di cifre binarie a S .



Dimostrazione. Sia P l'insieme dei sottoinsiemi perfetti di $[0, 1]$. Fissiamo $f : P \rightarrow P \times P$ che manda $X \in P$ in una coppia (X_1, X_2) con $X_1 \cup X_2 \subseteq X$ e $X_1 \cap X_2 = \emptyset$, e che è ben definita per l'osservazione precedente.

Assegnamo ad ogni sequenza binaria finita, $\sigma : n \rightarrow \{0, 1\}$, un sottoinsieme perfetto S_σ di S , procedendo per ricorsione finita su n . A questo scopo, data $\sigma : n \rightarrow \{0, 1\}$ e $b \in \{0, 1\}$ indichiamo con $\sigma \frown b$ la sequenza data da $\sigma \cup \{(n, b)\} : n+1 \rightarrow \{0, 1\}$ - cioè la sequenza σ allungata di un passaggio che fa b -. Allora possiamo definire ricorsivamente:

$$S_0 = S \quad S_{\sigma \frown b} = \begin{cases} X & \text{se } b = 0 \\ Y & \text{se } b = 1 \end{cases} \quad \text{dove } (X, Y) = f(S_\sigma)$$

Data una stringa binaria infinita $\tau : \omega \rightarrow \{0, 1\}$, definiamo infine l'intersezione di tutti i perfetti incontrati man mano che si scende nell'albero:

$$S_\tau = \bigcap_{\substack{\sigma = \tau|_n \\ n \in \omega}} S_\sigma$$

Osserviamo che, per ogni successione τ , $S_\tau \neq \emptyset$, infatti, per ogni $n \in \omega$, $S_{\tau|_{s(n)}} \subseteq S_{\tau|_n}$, poiché ad ogni passaggio aggiungiamo alla successione un perfetto contenuto nel precedente, quindi i compatti - siamo in $[0, 1]$ quindi sono tutti limitati - non vuoti $S_{\tau|_n}$ costituiscono una successione decrescente, per cui - è un fatto topologico - la loro intersezione, che è S_τ , è non vuota.

Inoltre se $\tau \neq \rho$ allora $S_\tau \cap S_\rho = \emptyset$ - cioè stringhe diverse corrispondono ad intersezioni diverse -, infatti, detto n il minimo indice per cui $\tau|_{s(n)} \neq \rho|_{s(n)}$ ¹⁴⁸ - senza perdita di generalità assumiamo $\tau_n = 0$ e $\rho_n = 1$ - abbiamo quindi $S_{\tau|_{s(n)}} = A$ e $S_{\rho|_{s(n)}} = B$ con $A \neq B$ e, per minimalità, $(A, B) = f(S_{\tau|_n}) = f(S_{\rho|_n})$, quindi, per la decrescenza, $S_\tau \subseteq A$ 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 12.42. Dimostrare la proposizione con \mathbb{R} al posto di $[0, 1]$.

¹⁴⁷Typo Mamino-

¹⁴⁸Typo Mamino.

Esercizio 12.43. In quali passaggi della dimostrazione precedente abbiamo fatto uso dell'assioma della scelta?

Esercizio 12.44. Dimostrare la proposizione senza fare uso di AC.

Teorema 12.45 (Cantor-Bendixson)

Sia $C \subseteq \mathbb{R}$ chiuso. Allora $C = A \cup P$, con $|A| \leq \aleph_0$ e P perfetto.

Cioè ogni sottoinsieme chiuso di \mathbb{R} è unione di un perfetto e di una quantità al più numerabile di punti isolati.

Dimostrazione. Dato un sottoinsieme chiuso $C \subseteq \mathbb{R}$ indichiamo con X' l'insieme dei suoi punti di accumulazione:

$$X' = \{a \in \mathbb{R} \mid \forall \varepsilon > 0 \ [a - \varepsilon, a + \varepsilon] \cap (X \setminus \{a\}) = \emptyset\}$$

Chiaramente se X è chiuso si ha proprio che i punti di accumulazione sono tutti meno quelli isolati:

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

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 $[s, t]$ aventi estremi razionali che isola $a \in X$, ossia:

$$\exists s, t \in \mathbb{Q} \ s < t \wedge [s, t] \cap X = \{a\}$$

Definiamo ora una successione di sottoinsiemi chiusi a partire da C per ricorsione transfinita come segue:

$$C_\alpha := \begin{cases} C_0 = C \\ C_{\alpha+1} = C'_\alpha \\ C_\lambda = \bigcap_{\gamma < \lambda} C_\gamma \end{cases}$$

cioè partiamo da C e ad ogni passaggio prendiamo il suo derivato - i suoi punti di accumulazione -, al limite prendiamo semplicemente l'intersezione dei precedenti. Per vedere che tutti gli insiemi C_α sono chiusi basta osservare che il derivato di un chiuso è chiuso - di fatto stiamo soltanto togliendo punti isolati - e l'intersezione di chiusi è chiusa. Osserviamo inoltre che $\alpha \leq \beta \rightarrow C_\beta \subseteq C_\alpha$ - la successione è decrescente -. Definiamo quindi:

$$P := \bigcap_{\alpha \in \text{Ord}} C_\alpha = \{a \in \mathbb{R} \mid \forall \alpha \in \text{Ord} \ a \in C_\alpha\}^{149} \quad A := C \setminus P$$

Per verificare la tesi dobbiamo quindi dimostrare che P è perfetto e $|A| \leq \aleph_0$.

P è perfetto

P è chiuso poiché abbiamo osservato che i C_α sono chiusi e l'intersezione di chiusi è chiusa, occorre quindi dimostrare che $\forall a \in P$, a è un punto di accumulazione per P . Procediamo per assurdo e consideriamo $a \in P$ isolato, 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 $x \notin C_\alpha$ - cioè x sta in

¹⁴⁹Non è quindi una vera intersezione, ma un insieme definito per separazione.

un intervallo (bucato) che non sta in P , per cui non appartiene ad almeno un insieme dell'intersezione -, possiamo quindi prendere α_x minimo per cui $x \notin C_{\alpha_x}$. Sia quindi:

$$\beta := \sup_{x \in]a-\varepsilon, a+\varepsilon[\setminus \{a\}} \alpha_x$$

cioè il più piccolo ordinale tale per cui C_β non contiene alcun elemento di $x \in]a-\varepsilon, a+\varepsilon[\setminus \{a\}$. In questo modo l'unico punto dell'intervallo che sta in C_β è a - perché per ipotesi sta in P , quindi in tutti i C_α -, cioè $C_\beta \cap]a-\varepsilon, a+\varepsilon[= \{a\}$, ma allora a è un punto isolato per C_β e quindi per definizione $a \notin C_{s(\beta)}$, che implica $a \notin P$.

A è al più numerabile

Per ogni $x \in A$ possiamo considerare α_x , il minimo ordinale per cui $x \notin C_{\alpha_x}$. Osserviamo che α_x deve essere successore, perché se fosse limite, avremmo $C_{\alpha_x} = \bigcap_{\gamma < \alpha_x} C_\gamma$, e, non stando nell'intersezione, esisterebbe $\gamma < \alpha_x$ per cui $x \notin C_\gamma$ che è contro la minimalità di α_x . Abbiamo quindi che $\alpha_x = s(\beta_x)$, per cui C_{β_x} è l'ultimo elemento della successione che abbiamo costruito che contiene x .

Siccome $x \in C_{\beta_x}$ e $x \notin C_{s(\beta_x)} = C'_{\beta_x}$, ciò vuol dire che x è un punto isolato per C_{β_x} . Per l'osservazione all'inizio possiamo quindi scegliere un intervallo a estremi razionali $]s_x, t_x[$ che isola x in C_{β_x} . A questo punto ci basta definire la funzione:

$$A \rightarrow \mathbb{Q} \times \mathbb{Q} : x \mapsto (s_x, t_x)$$

che è iniettiva. Infatti, siano $x, y \in A$ tali che $]s_x, t_x[=]s_y, t_y[$, supponiamo WLOG che $\beta_x \leq \beta_y$ - cioè $C_{\beta_x} \supseteq C_{\beta_y}$ -, allora:

$$y \in]s_y, t_y[\cap C_{\beta_y} \subseteq]s_x, t_x[\cap C_{\beta_x} = \{x\}$$

dove il contenimento in mezzo vale perché stiamo supponendo gli intervalli uguali e prima abbiamo visto il contenimento dei C_\square , per cui $x = y$ e quindi abbiamo l'iniettività. \square

Corollario 12.46 (Vale l'ipotesi del continuo sui chiusi di \mathbb{R})

Se $C \subseteq \mathbb{R}$ è chiuso allora o $|C| = 2^{\aleph_0}$ o $|C| \leq \aleph_0$.^a

^aCioè tra \aleph_0 e 2^{\aleph_0} non c'è nulla per i chiusi di \mathbb{R} .

Dimostrazione. Usando il teorema di Cantor-Bendixson scriviamo $C = A \cup P$. Se il perfetto è vuoto, $P = \emptyset$, allora $|C| = |A| \leq \aleph_0$. Altrimenti $2^{\aleph_0} = |P| \leq |C| \leq 2^{\aleph_0}$, dove la seconda disegualanza è perché $C \subseteq \mathbb{R}$, mentre la prima uguaglianza deriva dal fatto che abbiamo visto che i perfetti di \mathbb{R} hanno cardinalità 2^{\aleph_0} . \square

L'esempio seguente mostra come l'ipotesi che C sia chiuso non possa essere omessa.

Esempio 12.47

Esiste $S \subseteq \mathbb{R}$ non numerabile che non contiene alcun insieme perfetto non vuoto.

Dimostrazione. Sia $|\mathbb{R}| = 2^{\aleph_0} = \aleph_\alpha$, e sia $f : \mathcal{P}(\mathbb{R}) \setminus \{\emptyset\} \rightarrow \mathbb{R}$ una funzione di scelta per i sottoinsiemi di \mathbb{R} . È evidente che:

$$2^{\aleph_0} = |\{\text{intervalli chiusi}\}| \leq |\{\text{perfetti non vuoti}\}| \leq |\{\text{chiusi di } \mathbb{R}\}| = 2^{\aleph_0}$$

quindi esiste una funzione surgettiva - in realtà bigettiva - data da:

$$\omega_\alpha \rightarrow \{\text{perfetti non vuoti}\} : \beta \mapsto P_\beta$$

Definiamo quindi:

$$g : \omega_\alpha \rightarrow \mathbb{R} \times \mathbb{R} : \beta \mapsto (g_1(\beta), g_2(\beta))$$

dove g_1 e g_2 sono definite per ricorsione transfinita come segue:

$$\begin{aligned} g_1(\beta) &= f(P_\beta \setminus (g_1[\beta] \cup g_2[\beta])) \\ g_2(\beta) &= f(\mathbb{R} \setminus (g_1[\beta] \cup g_2[\beta] \cup \{g_1(\beta)\})) \end{aligned}$$

Per cui g_1 prende un punto in P_β che non sia già stato scelto in precedenza e g_2 prende un punto a caso tra quelli non scelti prima compreso $g_1(\beta)$.

La funzione g è ben definita perché, per ogni $\beta < \omega_\alpha$, si ha $|\beta| < \aleph_\alpha$, quindi $|g_1[\beta]| \leq |\beta| < \aleph_\alpha$ e $|g_2[\beta]| \leq |\beta| < \aleph_\alpha$, d'altro canto - per quanto abbiamo visto in generale sui perfetti - $|P_\beta| = 2^{\aleph_0} = \aleph_\alpha$. Di conseguenza, per differenza di cardinalità, f è sempre applicata ad insiemi non vuoti.

Dimostriamo che $S := g_2[\omega_\alpha]$ soddisfa la tesi. In primis osserviamo che non è numerabile, infatti $g_2 : \omega_\alpha \rightarrow \mathbb{R}$ è iniettiva perché, se WLOG $\gamma < \beta$, $g_2(\gamma) \in g_2[\beta]$ - ovvero il punto $g_2(\gamma)$ è nell'elenco di quelli già scelti quindi in $g_2[\beta]$ - e $g_2(\beta) = f(\mathbb{R} \setminus (\dots g_2[\beta] \dots)) \neq g_2(\gamma)$ - cioè abbiamo scelto su un insieme dove non c'è $g_2(\gamma)$ -. Pertanto si ha $|g_2[\omega_\alpha]| = 2^{\aleph_0}$. Fissiamo ora un perfetto non vuoto P_β . Dobbiamo dimostrare che $P_\beta \not\subseteq g_2[\omega_\alpha]$. Ci basta dire che non c'è un suo punto, quindi ci basta mostrare che $g_1(\beta) \notin g_2[\omega_\alpha]$. Supponiamo per assurdo $g_1(\beta) = g_2(\gamma)$ per qualche $\gamma \in \omega_\alpha$. Se $\gamma < \beta$ allora per le definizioni date:

$$g_1[\beta] \cup g_2[\beta] \not\ni g_1(\beta) = g_2(\gamma) \in g_1[\beta] \cup g_2[\beta] \text{ ↯}$$

Se $\beta \leq \gamma$:

$$g_1[\gamma] \cup g_2[\gamma] \cup \{g_1(\gamma)\} \not\ni g_2(\gamma) = g_1(\beta) \in g_1[\gamma] \cup g_2[\gamma] \cup \{g_1(\gamma)\} \text{ ↯}$$

quindi $g_1(\beta)$ non è immagine di qualche $\gamma \in \omega_\alpha$ per mezzo di g_2 . \square

§12.11 Riepilogo forme equivalenti di AC

Abbiamo visto che diverse proposizioni sono equivalenti all'assioma della scelta. Per esempio, fissati gli altri assiomi, AC e l'affermazione che ogni insieme è bene ordinabile si implicano vicendevolmente. Elenchiamo le principali forme equivalenti dell'assioma della scelta.

Proposizione 12.48 (Forme equivalenti dell'assioma della scelta)

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 inversa destra
- il teorema del buon ordinamento
- il lemma di Zorn
- ogni cardinalità infinita è un aleph
- $\forall X, Y |X| \leq |Y| \vee |Y| \leq |X|$
- $\forall X |X| \leq |\aleph_0| \rightarrow |X \times X| = |X|$.

§12.12 $|X| = |X \times X| \rightarrow \mathbf{AC}$ (Tarski)

Della proposizione precedente ci rimane da dimostrare solo che per ogni insieme infinito $|X \times X| = |X|$ implica scelta.

Teorema 12.49 (Teorema di Tarsk)

Se per ogni X infinito vale che $|X \times X| = |X|$, allora vale AC.

Dimostrazione. Dato un X infinito cerchiamo un buon ordinamento di X . È sufficiente costruire una funzione g che immerge X negli ordinali.

Applicando l'ipotesi a $X \sqcup H(X)$ si ottiene:

$$|X \times H(X)| \leq |(X \sqcup H(X)) \times (X \sqcup H(X))| \stackrel{\text{H.p.}}{=} |X \sqcup H(X)|$$

dove la prima disegualanza è una facile immersione¹⁵⁰. Quindi esiste una funzione iniettiva $f : X \times H(X) \hookrightarrow X \sqcup H(X)$. Per ogni $a \in X$ consideriamo la funzione:

$$f_a : H(X) \rightarrow X \sqcup H(X) : b \mapsto f(a, b)$$

Se l'immagine $f_a[H(X)]$ di f_a fosse contenuta in X (cioè se gli elementi dell'immagine fossero tutte coppie con 0 alla seconda componente), allora avremmo una funzione iniettiva da $H(X)$ ad X , che è assurdo per la definizione di numero di Hartogs. Quindi accade necessariamente che $f_a[H(X)] \cap H(X) \neq \emptyset$. Definiamo:

$$g : X \rightarrow H(X) : a \mapsto \min(f_a[H(X)] \cap H(X))$$

questa funzione è ben definita perché $f_a[H(X)] \cap H(X) \subseteq H(X)$, dunque è un insieme di ordinali, per il quale sappiamo esiste sempre il minimo. Inoltre g è iniettiva perché, se $a \neq b$, allora $g(a) = f(a, \text{qualcosa})$ [per come è definita f], e per l'iniettività di f , $f(a, \text{qualcosa}) \neq f(b, \text{qualcosa}) = g(b)$. Dunque g è l'immersione cercata di X negli ordinali, pertanto X è bene ordinato, dunque segue il teorema del buon ordinamento e quindi l'assioma scelta. \square

¹⁵⁰ Ad esempio la mappa $(x, y) \mapsto ((x, 0), (y, 1))$ è iniettiva.

¹⁵¹ Moralmente $f_a = f(a, \cdot)$.

§13 Aritmetica cardinale

Definizione 13.1 (Cardinali). Diciamo che κ è un **cardinale** se κ è un ordinale iniziale.

Notazione 13.2 (Cardinali successori) — Indichiamo con la notazione:

$$\kappa = \lambda^+ \stackrel{\text{def}}{=} \kappa \text{ è il minimo cardinale} > \lambda$$

ad esempio, $\omega_\alpha^+ = \omega_{\alpha+1}$, ovvero l'ordinale iniziale successivo [che quindi ha cardinalità strettamente più grande].

Possiamo definire le operazioni di prodotto, somma e potenza cardinale (per il [teorema del buon ordinamento](#) le operazioni sulle cardinalità e sugli ordinali iniziali corrispondono), per cui se $\kappa = \omega_\alpha$, $\lambda = \omega_\beta$ e $\mu = \omega_\gamma$ scriviamo:

$$\kappa = \lambda + \mu \quad \kappa = \lambda \cdot \mu \quad \kappa = \lambda^\mu$$

per rispettivamente:

$$\aleph_\alpha = \aleph_\beta + \aleph_\gamma \quad \aleph_\alpha = \aleph_\beta \cdot \aleph_\gamma \quad \aleph_\alpha = \aleph_\beta^{\aleph_\gamma}$$

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 [per [AC](#)], che abbia quella cardinalità, possiamo scrivere:

$$\kappa = |X| \stackrel{\text{def}}{=} \kappa \text{ è un cardinale e } |\kappa| = |X|$$

Cioè stiamo commettendo un piccolo abuso di notazione (o di definizione) e dicendo che la definizione di cardinalità può essere in realtà quella dell'ordinale iniziale a lui associato, in realtà questa cosa non è sbagliata, nel senso che alla fine, tutte le cardinalità degli insiemi (per AC) sono ordinali iniziali, cioè vi è sempre una biiezione tra ordinale iniziale e insieme (se hanno la stessa cardinalità, ma la cardinalità, come detto in precedenza non è qualcosa di per sé, ma è una definizione che considera sempre due insiemi), quello che stiamo facendo con i cardinali non è altro che fissare una notazione per dei “rappresentanti privilegiati” delle cardinalità, che sono appunto gli ordinali iniziali.

Per questi ultimi valgono tutte le proprietà viste sulle cardinalità, che quindi ci danno le operazioni cardinali (che NON sono un'estensione di quelle ordinali, ma altre operazioni definite diversamente e soltanto tra ordinali iniziali, perché entrano in gioco le proprietà viste sulle cardinalità).¹⁵²

¹⁵²Osservare che nel caso degli ordinali [iniziali] finiti le operazioni ordinali coincidono con quelle cardinali ed entrambe coincidono con le operazioni definite per ricorsione numerabile su ω , questo perché gli elementi di ω sono i loro stessi rappresentanti canonici di ordinali e sono tutti ordinali iniziali (per tutte le cardinalità finite).

§13.1 Somme e prodotti infiniti

Definizione 13.3 (Somme e prodotti infiniti). Sia I un insieme e $\{\kappa_i\}_{i \in I}$ una famiglia di cardinali. Definiamo la **somma** e il **prodotto sulla famiglia** indicizzata da I come:¹⁵³

$$\sum_{i \in I} \kappa_i \stackrel{\text{def}}{=} \left| \bigcup_{i \in I} \{\kappa_i \times \{i\} | i \in I\} \right|$$

$$\prod_{i \in I} \kappa_i \stackrel{\text{def}}{=} \left| \left\{ f : I \rightarrow \sup_{i \in I} \kappa_i \mid \forall i \in I \ f(i) \in \kappa_i \right\} \right|$$

(osservare che il sup di una famiglia di cardinali, essendo ordinali iniziali, è dato dall'unione di questi ultimi¹⁵⁴).

Formalmente la famiglia $\{\kappa_i\}_{i \in I}$ è una funzione f con $\text{Dom}(f) = I$ e $\forall i \in I \ f(i)$ è un cardinale, κ_i è un'abbreviazione per f_i .

Osservazione 13.4 (Prodotti cartesiani infiniti) — La definizione sopra generalizza quella di prodotto cartesiano data, a prodotto cartesiano di una famiglia qualunque di insiemi qualunque. Nel caso finito c'è una bigezione tra le due definizioni, infatti, data una f che va da I all'unione $\bigcup_{i \in I} X_i$ [con I finito] di una famiglia di insiemi, tale f per definizione fissa un elemento in ogni insieme, $f(i) \in X_i, \forall i \in I$, a questo punto, possiamo scrivere le immagini di $f(i)$ in una $|I|$ -upla ordinata [secondo l'ordinamento su I], ed ottenere l'elemento del prodotto cartesiano finito voluto.

Viceversa una $|I|$ -upla definisce completamente una mappa da I a $\bigcup_{i \in I} X_i$, infatti basta prendere come $f(i)$ l' i -esima componente della tupla, e tale componente sta in X_i , dunque si ottiene proprio una funzione che rispetta la proprietà richiesta.

Nota 13.5 (Somma di cardinali disgiunti) — Sia $\{X_i\}_{i \in I}$ una famiglia di insiemi a due a due **disgiunti**, e sia $\forall i \in I \ \kappa_i = |X_i|^a$ allora:

$$\sum_{i \in I} \kappa_i = \left| \bigcup_{i \in I} \{X_i | i \in I\} \right|$$

ovvero se gli insiemi a cui sono associati i cardinali sono disgiunti, la somma è semplicemente la cardinalità dell'unione senza bisogno di costruire l'unione disgiunta.^b

^aSe non sono già dati i cardinali c'è bisogno di AC.

^bQuesta proprietà così naturale nel caso finito, richiede AC per essere valida nel caso generale e dare una coerenza alle nostre definizioni, da qui l'importanza di assumere scelta per estendere le operazioni cardinali al caso infinito.

Dimostrazione. (Richiede AC)

Per ogni $i \in I$ scegliamo una bigezione $f_i : \kappa_i \times \{i\} \rightarrow X_i$, con $|\kappa_i \times \{i\}| = |\kappa_i| = |X_i|$ ¹⁵⁵,

¹⁵³La somma non è altro che una naturale estensione della somma tra cardinalità, per la somma di due cardinalità, in altre parole, stiamo rendendo disgiunti tutti gli insiemi e poi li stiamo unendo. Osservare anche che la definizione di prodotto data non usa AC.

¹⁵⁴Inoltre, notare anche come sapessimo già fare prodotti infiniti degli stessi insiemi, considerando le funzioni dall'uno all'altro, ma ciò valeva solo volendo fare un prodotto infinito di uno stesso insieme, per un numero di volte dato dall'insieme di arrivo (e.g. ${}^\omega A = \underbrace{A \times \dots \times A}_{\omega \text{ volte}}$).

¹⁵⁵Per la precisione consideriamo $B = \{B_i\}_{i \in I}$, con $B_i = \{f_i : \kappa_i \times \{i\} \rightarrow X_i | f_i \text{ bigezione}\}$, poiché per ogni $i \in I$ vale l'uguaglianza tra cardinalità scritta sopra, allora nessuno dei B_i è vuoto, ovvero $\emptyset \notin B$, dunque possiamo usare AC e ottenere una funzione $\phi : B \rightarrow \bigcup B : B_i \mapsto \phi(B_i) \in B_i$, che fissa per

allora si ha che:

$$f : \bigcup\{\kappa_i \times \{i\} \mid i \in I\} \rightarrow \bigcup\{X_i \mid i \in I\} : (a, i) \mapsto f_i(a, i)^{156}$$

ossia $f = \bigcup\{f_i \mid i \in I\}$, ed è ben definita perché gli insiemi sono disgiunti inoltre è una bigezione perché unione di bigezioni definite su insiemi disgiunti in arrivo. Abbiamo quindi una bigezione tra l'insieme usato per la definizione di somma di cardinalità e l'unione degli insiemi corrispondenti a tali cardinalità, dunque la cardinalità dell'unione degli insiemi è proprio uguale alla somma delle cardinalità degli insiemi. \square

Nota 13.6 (Disuguaglianza di inclusione-esclusione nel caso generale) — Sia $\{X_i\}_{i \in I}$ una famiglia di insiemi non necessariamente a due a due disgiunti, e sia $\forall i \in I \kappa_i = |X_i|^{156}$ allora in generale vale la disuguaglianza di inclusione-esclusione, ovvero la cardinalità dell'unione della famiglia è minore o uguale alla somma delle cardinalità degli elementi della famiglia:

$$\left| \bigcup\{X_i \mid i \in I\} \right| \leq \sum_{i \in I} \kappa_i$$

Inoltre la definizione di prodotto data è ben posta indipendentemente dagli insiemi di cui si considera la cardinalità:

$$\prod_{i \in I} \kappa_i = \left| \left\{ f : I \rightarrow \bigcup_{i \in I} X_i \mid \forall i \in I f(i) \in X_i \right\} \right|$$

¹⁵⁶Come prima, se non sono già dati i cardinali c'è bisogno di AC.

Dimostrazione. (Richiede AC)

Per la prima disuguaglianza si può fare come nel caso precedente, ovvero $\forall i \in I$ abbiamo $|\kappa_i \times \{i\}| = |X_i|$, per cui (usando AC nel caso generale) possiamo fissare una bigezione f_i , e considerare $f = \bigcup_{i \in I} f_i$, data da:

$$f : \bigcup\{\kappa_i \times \{i\} \mid i \in I\} \rightarrow \bigcup\{X_i \mid i \in I\} : (a, i) \mapsto f_i(a)$$

in questo caso abbiamo che f è unione di bigezioni, ma in arrivo gli insiemi non sono tutti necessariamente disgiunti, quindi ci può essere un elemento che ha più controimmagini, pertanto f è soltanto surgettiva e tale surgettività ci dà:

$$\sum_{i \in I} \kappa_i = \left| \bigcup\{\kappa_i \times \{i\} \mid i \in I\} \right| \geq \left| \bigcup\{X_i \mid i \in I\} \right|$$

Per la seconda osservazione possiamo ancora una volta fissare per ogni $i \in I$ le bigezioni $g_i : \kappa_i \rightarrow X_i$ (con AC) e mandare ogni funzione del primo insieme in una funzione che valutata in ogni i restituisce il valore di $f(i)$ trasportato in X_i mediante la bigezione fissata per quell' i :

$$\begin{aligned} g : \left\{ f : I \rightarrow \sup_{i \in I} \kappa_i \mid \forall i \in I f(i) \in \kappa_i \right\} &\rightarrow \left\{ f : I \rightarrow \bigcup_{i \in I} X_i \mid \forall i \in I f(i) \in X_i \right\} \\ f &\mapsto g(f)(i) = g_i(f(i)) \end{aligned}$$

ogni insieme B_i una sua bigezione. Osservare che usiamo AC per l'arbitrarietà di $|I|$, se fosse finito non avremmo bisogno di AC per fissare le bigezioni (per questo questa proprietà non ha bisogno di AC nel caso finito), ma nel caso infinito non possiamo fare altrimenti.

¹⁵⁶Typo Mamino.

tale mappa è bigettiva, perché se due mappe in arrivo coincidono su tutti gli $i \in I$, essendo le g_i bigezioni, si ha che le mappe in partenza sono uguali, inoltre presa una mappa h nell'insieme in arrivo, si può ottenere la sua controimmagine costruendo una funzione fatta da $g_i^{-1}(h(i))$, per ogni $i \in I$. \square

Osservazione 13.7 (Prodotto infinito di potenze) — Vale la proprietà del prodotto di potenze^a anche nel caso di prodotti arbitrari:

$$\kappa^{\sum_{i \in I} \lambda_i} = \prod_{i \in I} \kappa^{\lambda_i}$$

$$\overline{^a a^{n+m} = a^n a^m}.$$

Dimostrazione. Un elemento dell'insieme al LHS è una funzione $f : \sum_{i \in I} \lambda_i = \bigcup \{\lambda_i \times \{i\} \mid i \in I\} \rightarrow \kappa$, tale funzione può essere identificata in una funzione:

$$\prod_{i \in I} \kappa^{\lambda_i} \ni \tilde{f} : I \rightarrow \bigcup \{\kappa^{\lambda_i} \mid i \in I\} : i \mapsto \tilde{f}_i \in \kappa^{\lambda_i}$$

ovvero mandiamo f in una funzione che associa ad ogni $i \in I$ la funzione $\tilde{f}_i := f(\cdot, i) \in \kappa^{\lambda_i}$. È abbastanza immediato verificare che è iniettiva, infatti se due funzioni in arrivo coincidono praticamente le funzioni in partenza coincidono su tutte le coppie di elementi in $\bigcup \{\lambda_i \times \{i\} \mid i \in I\}$, si verifica inoltre che è anche surgettiva. \square

Esercizio 13.8 (Proprietà delle operazioni cardinali). Valgono le proprietà ragionevoli per le operazioni tra cardinali, ad esempio:

- se $\forall i \in I \ \kappa_i \leq \lambda_i$: (**compatibilità con l'ordinamento - versione infinita**)

$$\sum_{i \in I} \kappa_i \leq \sum_{i \in I} \lambda_i \quad \prod_{i \in I} \kappa_i \leq \prod_{i \in I} \lambda_i$$

- $\forall i \in I \ \kappa_i \leq \sum_{i \in I} \kappa_i$ (**corollario di quella sopra**)
- Se $I = I_1 \sqcup I_2$: (**associatività infinita**)

$$\sum_{i \in I} \kappa_i = \left(\sum_{i \in I_1} \kappa_i \right) + \left(\sum_{i \in I_2} \kappa_i \right) \quad \prod_{i \in I} \kappa_i = \left(\prod_{i \in I_1} \kappa_i \right) \cdot \left(\prod_{i \in I_2} \kappa_i \right)$$

- (**compatibilità tra le definizioni di operazioni cardinali**):

$$\sum_{i \in \kappa} \lambda = \kappa \cdot \lambda \quad \prod_{i \in \kappa} \lambda = \lambda^\kappa$$

- (**prodotto di potenze**):

$$\left(\prod_{i \in I} \kappa_i \right)^\lambda = \prod_{i \in I} \kappa_i^\lambda$$

Proposizione 13.9 (Somma infinita di cardinali)

Supponiamo che $\{\kappa_i\}$, per $i \in I$ sia una famiglia di cardinali diversi da 0, allora:

$$\sum_{i \in I} \kappa_i = |I| \cdot \sup_{i \in I} \kappa_i = \max \left(|I|, \sup_{i \in I} \kappa_i \right)$$

Dimostrazione. La seconda uguaglianza deriva dal fatto che le cardinalità sono tutte aleph, per cui vale la proprietà vista per il prodotto tra aleph. Per la prima dimostriamo le due disuguaglianze come segue [e concludiamo con Cantor-Bernstein].

\leq Deriva facilmente dalle proprietà viste sopra:

$$\sum_{i \in I} \kappa_i \leq \sum_{i \in I} \sup_{i \in I} \kappa_i = |I| \cdot \sup_{i \in I} \kappa_i$$

dove appunto, la prima disuguaglianza è esattamente la compatibilità della somma con l'ordinamento dei cardinali, mentre la seconda uguaglianza è la compatibilità tra le definizioni delle operazioni.

\geq Siccome $|I| \cdot \sup_{i \in I} \kappa_i$ è il massimo fra $|I|$ e $\sup_{i \in I} \kappa_i$ [lo abbiamo già visto all'inizio], basta verificare che la somma al LHS è maggiore di entrambi separatamente. $\sum_{i \in I} \kappa_i \geq \sum_{i \in I} 1 = |I|$, dove la prima disuguaglianza è la compatibilità prodotto-ordinamento [applicata a cardinali > 0 per ipotesi] e la seconda quella delle operazioni. L'altra disuguaglianza segue osservando che:

$$\forall j \in I \quad \sum_{i \in I} \kappa_i \geq \kappa_j$$

cioè tutta la famiglia è più piccola della somma, quindi deve esserlo anche il sup di tale famiglia.

□

§13.2 Teorema di König**Proposizione 13.10 (Teorema di König)**

Se $\forall i \in I \kappa_i < \lambda_i$ allora:

$$\sum_{i \in I} \kappa_i < \prod_{i \in I} \lambda_i$$

Dimostrazione. Dimostriamo che non può valere il \geq . Siano:

$$A := \bigcup \{\kappa_i \times \{i\} \mid i \in I\} \quad B := \left\{ f : I \rightarrow \sup_{i \in I} \lambda_i \mid \forall i \in I f(i) \in \lambda_i \right\}$$

gli insiemi le cui cardinalità definiscono rispettivamente il prodotto della famiglia $\{\lambda_i\}_{i \in I}$ e la somma della famiglia $\{\kappa_i\}_{i \in I}$. Data una qualunque funzione $f : A \rightarrow B$ ¹⁵⁷ dobbiamo dimostrare che non può essere surgettiva (ovvero $\neg |B| \geq |A|$, cioè non è vero che la

¹⁵⁷Tipo di Mamino.

somma è maggiore o uguale al prodotto). Consideriamo la famiglia di funzioni tra i cardinali κ_i e λ_i definita via f da:

$$f_i : \kappa_i \rightarrow \lambda_i : \alpha \mapsto \underbrace{(f(\alpha, i))(i)}_{\in B} \in \lambda_i$$

siccome per ipotesi $\kappa_i < \lambda_i$ le funzioni f_i non possono essere surgettive per ogni $i \in I$, e ciò si traduce nel fatto che, per ogni $i \in I$, $\lambda_i \setminus \text{Im}(f_i) \neq \emptyset$.

Per quanto detto $\emptyset \notin \{\lambda_i \setminus \text{Im}(f_i)\}_{i \in I}$, dunque possiamo usare AC per fissare un elemento in ciascun insieme $\lambda_i \setminus \text{Im}(f_i)$, in particolare possiamo scrivere una funzione che associa l'indice i in I al corrispettivo elemento fissato in $\lambda_i \setminus \text{Im}(f_i)$ come segue:

$$g : I \rightarrow \sup_{i \in I} \lambda_i : i \mapsto g(i) \in \lambda_i \setminus \text{Im}(f_i)$$

osserviamo che $g \in B$ in quanto $g(i) \in \lambda_i$ per ogni $i \in I$, inoltre vale che $g \notin \text{Im}(f)$. Se, per assurdo, $g \in \text{Im}(f)$, allora [ricordando che f è definita sulle coppie di A] abbiamo $g = f(\alpha, i)$, per qualche $(\alpha, i) \in A$, da cui [per estensionalità per funzioni]:

$$g(i) = f(\alpha, i)(i) \stackrel{\text{def. } f_i}{=} f_i(\alpha) \in \text{Im}(f_i) \not\ni$$

che è assurdo in quanto $g(i) \in \lambda_i \setminus \text{Im}(f_i)$ per definizione. Abbiamo quindi verificato che c'è sempre un elemento di B , $g \notin \text{Im}(f)$, che rende falsa la surgettività di una qualunque funzione. Poiché per AC le cardinalità sono totalmente ordinate, deve quindi valere necessariamente che all'inizio si ha $|A| < |B|$. \square

Esempio 13.11 (Disuguaglianza di Cantor)

Osserviamo che applicando il teorema di König sui cardinali 1 e 2, sommati su una famiglia κ , si ottiene:

$$\kappa = \sum_{i \in \kappa} 1 < \prod_{i \in \kappa} 2 = 2^\kappa$$

(dove le uguaglianze laterali sono la compatibilità delle definizioni delle operazioni), ovvero proprio il [teorema di Cantor](#) dimostrato in precedenza, che ora diventa un caso particolare del teorema di König.

Esempio 13.12 ($2^{\aleph_0} \neq \aleph_\omega$)

Osserviamo che vale:

$$\aleph_\omega = \max \left(\aleph_0, \sup_{i \in \omega} \aleph_i \right) = \sum_{i \in \omega} \aleph_i < \prod_{i \in \omega} \aleph_{i+1} \leq \prod_{i \in \omega} \aleph_\omega = \aleph_\omega^{\aleph_0}$$

dove abbiamo usato che $\aleph_i < \aleph_{i+1}$ per la definizione ricorsiva della funzione degli aleph. Questa cosa ci permette di osservare che, se valesse $2^{\aleph_0} = \aleph_\omega$, allora:

$$2^{\aleph_0} = \aleph_\omega < \aleph_\omega^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0} \not<$$

Esercizio 13.13 (Facile). Se $2^{\aleph_0} = \aleph_{41}$, allora $\aleph_{41}^{\aleph_0} = \aleph_{41}$.

Soluzione. Basta sfruttare che il prodotto di numerabili è numerabile, infatti:

$$\aleph_{41}^{\aleph_0} \stackrel{\text{H.P.}}{=} (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0} \stackrel{\text{H.P.}}{=} \aleph_{41}$$

□

Esercizio 13.14 (Difficile). Se $2^{\aleph_0} = \aleph_{41}$, allora $\aleph_{42}^{\aleph_0} = \aleph_{42}$.

Soluzione. La soluzione più breve usa la formula di Hausdorff, che vederemo alla fine del capitolo (sarebbe $(\kappa^+)^{\lambda} = \kappa^{\lambda} \cdot \kappa^+$), per la quale:

$$\aleph_{42}^{\aleph_0} \stackrel{\text{Hausdorff}}{=} \aleph_{41}^{\aleph_0} \cdot \aleph_{42} \stackrel{\text{H.P.}}{=} (2^{\aleph_0})^{\aleph_0} \cdot \aleph_{42} = 2^{\aleph_0} \cdot \aleph_{42} \stackrel{\text{H.P.}}{=} \aleph_{41} \cdot \aleph_{42} = \aleph_{42}$$

□

Esercizio 13.15 (Pure peggio). Se $2^{\aleph_0} = \aleph_1^a$, allora $\aleph_{n+1}^{\aleph_0} = \aleph_{n+1}$, per $n \in \omega$.

^aChe è l'**ipotesi del continuo (CH)**.

Soluzione. Si procede per induzione numerabile e usando la formula di Hausdorff.

caso 0 In questo caso $\aleph_1^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0} = \aleph_1$.

caso successore Assumiamo $\aleph_{n+1}^{\aleph_0} = \aleph_{n+1}$ e dimostriamo che $\aleph_{n+2}^{\aleph_0} = \aleph_{n+2}$. Utilizzando la formula di Hausdorff:

$$\aleph_{n+2}^{\aleph_0} = \aleph_{n+1}^{\aleph_0} \cdot \aleph_{n+2} \stackrel{\text{H.P. indutt.}}{=} \aleph_{n+1} \cdot \aleph_{n+2} = \aleph_{n+2}$$

□

§13.3 Cofinalità

Definizione 13.16 (Cofinalità - v.1). Dato un cardinale infinito κ , la **cofinalità** di κ , $\text{cof}(\kappa)$, è il minimo cardinale μ per cui esiste una famiglia $\{\lambda_i\}_{i \in \mu}$ di cardinali tali che:

$$\forall i \in \mu \quad \lambda_i < \kappa \quad \text{e} \quad \kappa = \sum_{i \in \mu} \lambda_i$$

In altri termini, $\text{cof}(\kappa)$ è il **minimo numero di parti** $< \kappa$ [ovvero proprio μ] in cui può essere diviso un insieme di cardinalità κ .

Esempio 13.17 (Cofinalità v.1 di alcuni cardinali noti)

Vediamone alcuni esempi pratici di cofinalità v.1, tenendo conto che cerchiamo sempre il minimo numero di “pezzi” in cui dividere un cardinale, in modo tale che i “pezzi” abbiano cardinalità strettamente minore:

- $\text{cof}(\aleph_0) = \aleph_0$, qualsiasi cosa più piccola sarebbe un cardinale finito, e dividere \aleph_0 in un numero finito di parti dà ancora parti di cardinalità \aleph_0 , mentre usando \aleph_0 abbiamo tutti “pezzettini” finiti, la cui unione finita è finita, ma l’unione di \aleph_0 cardinali finiti dà proprio \aleph_0 per le proprietà viste:

$$\aleph_0 = \sum_{i < \aleph_0} 1 \leq \sum_{i < \aleph_0} n_i \leq \sum_{i < \aleph_0} \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0$$

- $\text{cof}(\aleph_\omega) = \aleph_0$ in quanto:

$$\sum_{\alpha < \aleph_0} \aleph_\alpha = \aleph_\omega$$

e se usassimo $|I| < \aleph_0$ (ovvero un cardinale finito), accadrebbe che:

$$\sum_{\alpha \in I} \aleph_\alpha = \max \left(|I|, \sup_{\alpha \in I} \aleph_\alpha \right) = \aleph_{\max(I)} < \aleph_\omega$$

- $\text{cof}(\aleph_{42}) = \aleph_{42}$ in quanto:

$$\aleph_{42} = \sum_{i \in I} \kappa_i \leq \sum_{i \in I} \aleph_{41} = \max(|I|, \aleph_{41}) \implies |I| = \aleph_{42}$$

dove la prima uguaglianza è il fatto che stiamo supponendo di poter scrivere \aleph_{42} come somma, la seconda diseguaglianza deriva dal fatto che stiamo supponendo (per avere la definizione di cofinalità v.1) che i cardinali che sommiamo siano strettamente più piccoli di \aleph_{42} , e, nel caso peggiore (perché gli \aleph_{41} sono i pezzi di grandezza massima che possiamo prendere), troviamo calcolando la somma, che l'unica possibilità è che $|I| = \aleph_{42}$.

Definizione 13.18 (Cofinalità - v.2). Dato un insieme ordinato $(S, <)^{158}$, diciamo che $A \subseteq S$ è **cofinale** in S se $\forall x \in S \exists y \in A \ x \leq y$ - ossia A non ha maggioranti stretti in S . La **cofinalità** di $(S, <)$ è la minima cardinalità di un sottoinsieme cofinale di S .

¹⁵⁸Questa definizione di cofinalità, al contrario della precedente è valida su qualsiasi insieme [parzialmente] ordinato, mentre la precedente solo per i cardinali.

Esempio 13.19 (Cofinalità v.2 di alcuni cardinali noti)

Vediamone alcune secondo questa nuova definizione:

- $\text{cof}(\omega) = \aleph_0$, ω è banalmente cofinale in se stesso, inoltre, qualsiasi altro sottoinsieme è finito, dunque ha un maggiorante stretto in ω , pertanto ω è un^a sottoinsieme cofinale di ω , da cui considerando la cardinalità si ha \aleph_0 .
- $\text{cof}(\mathbb{R}, <) = \aleph_0$, infatti ω è cofinale in \mathbb{R} , basta prendere per ogni $x \in \mathbb{R}$ la parte intera superiore, $x \leq \lceil x \rceil \in \omega$, inoltre, per quanto visto con AC \aleph_0 è la più piccola cardinalità infinita (stiamo escludendo con lo stesso ragionamento di sopra che vi siano insiemi cofinali finiti in \mathbb{R}), quindi per la definizione v.2, la minima cardinalità cercata è proprio \aleph_0 .
- $\text{cof}([0, 1], <_{|\mathbb{R}}) = 1$, perché $\{1\}$ è un sottoinsieme cofinale di $[0, 1]$ (non ha maggioranti stretti nel nostro intervallo), e la cofinalità non può essere 0 perché nell'intervallo ha maggioranti stretti.
- $\text{cof}(\omega + 1) = 1$, infatti, il sottoinsieme $\{\omega\} \subset \omega + 1$ non ha maggioranti stretti, per cui è cofinale ed in particolare $|\{\omega\}| = 1$, dunque, non essendo il vuoto (o 0) cofinale in $\omega + 1$, segue necessariamente che $\{\omega\}$ è il più piccolo sottoinsieme cofinale.
- $\text{cof}(\omega_\omega) = \aleph_0$ perché $\{\omega_0, \omega_1, \omega_2, \dots\} = \{\omega_\alpha | \alpha < \omega\}$ è un insieme cofinale in $\omega_\omega = \sup_{i \in \omega} \omega_\alpha$ [banalmente perché abbiamo preso tutti gli ω_α prima di ω_ω , quindi non ci può essere fuori qualcosa di strettamente più grande], inoltre, la cardinalità di questo insieme è ovviamente \aleph_0 , ed è il più piccolo insieme cofinale, infatti, per qualsiasi sottoinsieme finito di ω_ω , è sufficiente prendere il successivo dell' ω_α più grande.
- $\text{cof}(\omega_{42}) = \aleph_{42}$ per la proposizione che segue.

^aVa bene qualsiasi altro sottoinsieme infinito di ω , tanto sono tutti \aleph_0 .

Proposizione 13.20 (Equivalenza delle definizioni di cofinalità)

Dato κ cardinale **infinito**^a, allora vale che $\text{cof}^{(v.1)}(\kappa) = \text{cof}^{(v.2)}(\kappa)$.

^aNel caso κ cardinale finito, non coincidono, ed anzi, la definizione v.1 dà sempre 2, mentre la v.2 dà sempre 1, perché ogni cardinale finito ha sempre un massimo.

Dimostrazione. Siano $\lambda_1 := \text{cof}^{(v.1)}(\kappa)$ e $\lambda_2 := \text{cof}^{(v.2)}(\kappa)$, verifichiamo quindi le due disuguaglianze per avere la tesi.

$\lambda_1 \leq \lambda_2$ Sia A un sottoinsieme cofinale in κ , mostriamo che $\lambda_1 \leq |A|$, cioè che λ_1 è più piccolo di tutte le cardinalità dei sottoinsiemi cofinali di κ in questo modo sarà proprio minore o uguale del minimo, ovvero λ_2 . Osserviamo che (questo vale per tutti gli ordinali limite), essendo κ un ordinale iniziale, dunque limite, $\forall \alpha \in \kappa \exists \beta \in A \ s(\alpha) \leq \beta$ (per cofinalità di A) e quindi $\alpha < \alpha + 1 \leq \beta$, dove $\alpha + 1 \in \kappa$ perché limite. Dunque ogni elemento di κ appartiene

a qualche elemento di A , per cui vale $\kappa = \bigcup A$ ¹⁵⁹. Da ciò segue che:

$$\kappa \leq \sum_{\beta \in A} |\beta| \leq \sum_{\beta \in A} \kappa = |A| \cdot \kappa = \kappa$$

per cui il termine in mezzo è uguale a κ , ed essendo che $\forall \beta \in A \ \beta \in \kappa \rightarrow |\beta| < \kappa$ (poiché κ iniziale), quella ottenuta sopra è proprio una scrittura di κ come somma di termini strettamente più piccoli, per cui si ha $\lambda_1 \leq |A|$.

$\lambda_2 \leq \lambda_1$ Se $\lambda_1 = \kappa$ non c'è niente da dimostrare, perché κ stesso è cofinale in sé, e quindi il minimo nella definizione v.2 comprende già κ per cui la disuguaglianza è automaticamente verificata. Assumiamo quindi che $\lambda_1 < \kappa$, ci basta trovare un insieme cofinale in κ di cardinalità λ_1 , in questo modo sta nel minimo dell'altra definizione e otteniamo la disuguaglianza voluta. Per ipotesi esiste $\{\kappa_i\}_{i \in I}$ con $|I| = \lambda_1$, tale che per la definizione di cofinalità v.1:

$$\kappa = \sum_{i \in I} \kappa_i = \max \left(|I|, \sup_{i \in I} \kappa_i \right) = \max \left(\lambda_1, \sup_{i \in I} \kappa_i \right) \stackrel{\lambda_1 \leq \kappa}{=} \sup_{i \in I} \kappa_i$$

Osserviamo ora che $A := \{\kappa_i \mid i \in I\}$ è cofinale in κ e da questo segue la tesi in quanto $\lambda_2 \stackrel{\text{def. cof(v.2)}}{\leq} |A| \stackrel{i \rightarrow \kappa_i}{\leq} |I| = \lambda_1$. Dato $x \in \kappa$, se x non fosse maggiorato da qualche elemento di A , avremmo che x è un maggiorante di A stesso, per cui:

$$\sup_{i \in I} \kappa_i \leq x < \kappa \nabla$$

dove l'assurdo deriva dal fatto che sopra avevamo ottenuto che $\kappa = \sup_{i \in I} \kappa_i$. Alternativamente si può anche osservare che $x \in \kappa = \sup_{i \in I} \kappa_i = \bigcup_{i \in I} \kappa_i (= \bigcup A)$, ovvero $x \in \kappa_i$, per qualche $i \in I$, per cui $x < \kappa_i$, e dunque A è cofinale in κ .

□

Proposizione 13.21 (Transitività della cofinalità)

Sia $(S, <_S)$ totalmente ordinato e $T \subseteq S$ cofinale in S , allora:

$$\text{cof}(S, <_S) = \text{cof}(T, <_T)$$

con $<_T = <_S \cap (T \times T)$.

Dimostrazione. Per dimostrare la proposizione dimostriamo due cose, in primis che se $A \subseteq T$ è cofinale in T , allora è cofinale anche in S , dunque i sottoinsiemi cofinali di T sono contenuti in quelli di S , per cui, per definizione v.2, si ha $\text{cof}(S, <_S) \leq \text{cof}(T, <_T)$.

- Dato $A \subseteq T$ cofinale in T , verifichiamo che è cofinale anche in S . Sia $x \in S$, dobbiamo trovare un $y \in A$ tale che $x \leq y$. Siccome T è cofinale in S per ipotesi, esiste $t \in T$ tale per cui $x \leq t$, e, siccome A è cofinale in T , esiste $y \in A$ per il quale $t \leq y$, da cui $x \leq y$.

¹⁵⁹Per essere precisi questo è un solo contenimento, l'altro segue dal fatto che $A \subseteq \kappa$ e κ è un insieme transitivo, quindi $\bigcup A \subseteq \kappa$.

¹⁶⁰Se il max fosse λ_1 , avremmo $\kappa = \lambda_1$, che è contro il fatto supposto poco sopra, ovvero $\lambda_1 < \kappa$, pertanto il max deve essere necessariamente il sup.

La seconda cosa che dimostriamo è che se $B \subseteq S$ è cofinale in $(S, <_S)$, allora esiste un sottoinsieme $B' \subseteq T$, con $|B'| \leq |B|$, cofinale in T , in tal modo per la definizione v.2, si ha $\text{cof}(T, <_T) \leq \text{cof}(S, <_S)$, e si conclude la tesi.

- Dato $B \subseteq S$ cofinale, siccome T è cofinale in S , possiamo usare la cofinalità di quest'ultimo rispetto a B , e quindi per ogni $b \in B \subseteq S$ possiamo fissare (in generale con AC) un $y_b \in T$ con $b \leq y_b$. Sia $B' := \{y_b \in T : b \in B\} \subseteq T$. Naturalmente la mappa $b \mapsto y_b$ è una funzione surgettiva da B a B' , per cui abbiamo $|B'| \leq |B|$. Infine, non ci resta che osservare che B' è cofinale in T , preso dunque $x \in T$, poiché B è cofinale in S esiste $b \in B$ $b \geq x$, possiamo quindi considerare l' $y_b \in B'$ associato e ottenere $y_b \geq b \geq x$, che ci garantisce la cofinalità.

□

Proposizione 13.22 (I cardinali infiniti sono sempre cofinali in se stessi)

Sia κ un cardinale infinito, allora vale che $\text{cof}(\kappa) \leq \kappa$.^a

^aUsando la definizione v.2, questo fatto è vero per un qualsiasi ordinale parziale.

Dimostrazione. Infatti, κ si può scrivere come:

$$\kappa = \sum_{i \in \kappa} 1$$

che rispetta la definizione v.1 di cofinalità. Pertanto κ è tra le cardinalità di cui si prende il minimo nella definizione, e, essendo un elemento del minimo segue anche che necessariamente il minimo sarà più piccolo, da cui $\text{cof}(\kappa) \leq \kappa$.

Ragionamento analogo se si usa la definizione v.2 di cofinalità, infatti ogni insieme è cofinale in se stesso, per cui κ è tra gli insiemi di cui si considera il minimo della cardinalità per avere la cofinalità secondo questa definizione. □

Osservazione 13.23 (La cofinalità è sempre un cardinale regolare) — Sia $(S, <)$ totalmente ordinato, allora:

$$\text{cof}(\text{cof}(S, <)) = \text{cof}(S, <)$$

in particolare, per ogni cardinale infinito κ , si ha $\text{cof}(\text{cof}(\kappa)) = \text{cof}(\kappa)$.

Dimostrazione. Sia $\kappa = \text{cof}(S, <)$ e $A \subseteq S$ cofinale, quindi $|A| = \kappa$, sappiamo che vale in generale $\text{cof}(\kappa) \leq \kappa$. Supponiamo per assurdo che $\text{cof}(\kappa) < \kappa$, per definizione di cofinalità esistono $\{\kappa_i\}_{i \in I}$, $\forall i \in I \kappa_i < \kappa$ e $\text{cof}(\kappa) = |I| < \kappa$, tali che:

$$\kappa = \sum_{i \in I} \kappa_i = |I| \cdot \sup_{i \in I} \kappa_i = \sup_{i \in I} \kappa_i$$

dunque che possiamo fissare una famiglia $\{A_i\}_{i \in I}$ di sottoinsiemi di A disgiunti tali che $\forall i \in I |A_i| = \kappa_i$ e $\bigcup\{A_i | i \in I\} = A$ (è l'osservazione vista all'inizio per cui data una famiglia arbitraria di insiemi disgiunti, la cardinalità della loro unione è proprio la somma dei cardinali associati).

Osserviamo ora che ogni $i \in I$, A_i non è cofinale in S siccome $|A_i| = \kappa_i < \kappa = \text{cof}(S, <)$, quindi possiamo scegliere per tutti gli A_i un maggiorante stretto $y_i \in S$. Sia $B := \{y_i \in$

$S|i \in I\} \subseteq A^{161}$, vale che $|B| \stackrel{i \rightarrow y_i}{\leq} |I| \stackrel{\text{Hp. assurda}}{<} \kappa$.

D'altro canto B è cofinale in S , infatti, preso $x \in S$, per la cofinalità di A , $\exists a \in A$ tale che $x \leq a$, ora a è necessariamente in uno degli A_i , quindi si ha $x \leq a \leq y_i \in B$. Ma allora B è cofinale in $(S, <)$ e ciò è assurdo perché $\text{cof}(S, <) = \kappa$ e vale la disuguaglianza scritta sopra. \square

Vediamo ora alcune applicazioni della cofinalità.

Corollario 13.24 (di König - o disuguaglianze di cofinalità)

Per κ cardinale infinito, e λ cardinale ≥ 2 vale:

$$\kappa < \kappa^{\text{cof}(\kappa)} \quad \kappa < \text{cof}(\lambda^\kappa)$$

Dimostrazione. Cominciamo dalla prima disuguaglianza. Per definizione di $\text{cof}(\kappa)$ esiste una famiglia $\{\kappa_i\}_{i \in \text{cof}(\kappa)}$, con $\kappa_i < \kappa$ per ogni $i \in \text{cof}(\kappa)$, dunque usando König si ha:

$$\kappa = \sum_{i \in \text{cof}(\kappa)} \kappa_i \color{red}{<} \prod_{i \in \text{cof}(\kappa)} \kappa = \kappa^{\text{cof}(\kappa)}$$

Per la seconda disuguaglianza ragioniamo per assurdo e assumiamo che $\kappa \geq \text{cof}(\lambda^\kappa)$. A questo punto possiamo applicare la disuguaglianza precedente a λ^κ ed ottenere:

$$\lambda^\kappa \color{red}{<} (\lambda^\kappa)^{\text{cof}(\lambda^\kappa)} \stackrel{\text{Hp. assurda}}{\leq} (\lambda^\kappa)^\kappa = \lambda^{\kappa \cdot \kappa} = \lambda^\kappa \not\leq$$

\square

Definizione 13.25 (Funzione \beth). La funzione \beth^{162} è definita sui cardinali infiniti da:

$$\beth(\kappa) = \kappa^{\text{cof}(\kappa)}$$

Corollario 13.26 (Disuguaglianze di cofinalità via \beth)

Con la funzione \beth , dato κ cardinale infinito, abbiamo le disuguaglianze di cofinalità:

$$\kappa < \beth(\kappa) \quad \text{cof}(\kappa) < \text{cof}(\beth(\kappa))$$

Dimostrazione. La prima disuguaglianza è una riscrittura di quella sopra, infatti $\kappa < \kappa^{\text{cof}(\kappa)} = \beth(\kappa)$. La seconda disuguaglianza è un corollario della seconda disuguaglianza sopra che si ottiene prendendo $\lambda = \kappa$ ed usando $\text{cof}(\kappa)$ al posto di κ . \square

Definizione 13.27 (Proprietà dei cardinali). Dato un cardinale κ , diciamo che è:

- **regolare** se $\text{cof}(\kappa) = \kappa$
- **singolare** se $\text{cof}(\kappa) < \kappa$
- **successore** se $\kappa = \aleph_{\alpha+1}$ per qualche $\alpha \in \text{Ord}$
- **limite** se $\kappa = \aleph_\lambda$ per λ ordinale limite

¹⁶¹Tipo di Mamino.

¹⁶²“Gimel”, pronunciata “ghimel”.

- **limite forte** se $\aleph_0 < \kappa$ e $\forall \alpha \in \text{Ord} \quad \aleph_\alpha < \kappa \rightarrow 2^{\aleph_\alpha} < \kappa$
- **debolmente inaccessible** se è regolare e limite
- **(fortemente) inaccessible** se è regolare e limite forte.

Proposizione 13.28 (Limite forte \implies limite)

Un cardinale limite forte è anche limite.

Dimostrazione. Se per assurdo fosse successore, $\kappa = \aleph_{\alpha+1}$, poiché $\aleph_\alpha < \aleph_{\alpha+1}$ avremmo per ipotesi di limite forte che $2^{\aleph_\alpha} < \aleph_{\alpha+1}$, ma questo è assurdo in quanto $\aleph_{\alpha+1} \leq 2^{\aleph_\alpha}$ poiché è per definizione il più piccolo cardinale strettamente maggiore di \aleph_α . \square

Proposizione 13.29 (Successore \implies regolare)

I cardinali successori sono regolari.

Dimostrazione. Sia $\kappa = \aleph_{\alpha+1}$, da sopra sappiamo che vale sempre $\text{cof}(\kappa) \leq \kappa$, supponiamo per assurdo che κ non sia regolare, cioè $\text{cof}(\kappa) < \kappa$. Usando la definizione di cofinalità si ottiene:

$$\aleph_{\alpha+1} = \kappa = \sum_{i \in \text{cof}(\kappa)} \kappa_i \leq \sum_{i \in \text{cof}(\kappa)} \aleph_\alpha = \text{cof}(\kappa) \cdot \aleph_\alpha \leq \aleph_\alpha < \aleph_{\alpha+1} \not\vdash$$

dove nella penultima diseguaglianza abbiamo usato che $\text{cof}(\kappa) < \kappa = \aleph_{\alpha+1} \implies \text{cof}(\kappa) \leq \aleph_\alpha$, poiché \aleph_α è il più grande cardinale strettamente più piccolo di $\aleph_{\alpha+1}$. \square

Corollario 13.30 (\beth di cardinali regolari)

Se κ è **successore**, allora $\beth(\kappa) = 2^\kappa$.

Dimostrazione. È ovvio che $\beth(\kappa) = \kappa^{\text{cof}(\kappa)}$ è regolare $\stackrel{\kappa \text{ regolare}}{=} \kappa^\kappa = 2^\kappa$, dove l'ultima diseguaglianza come al solito vale perché:

$$2^\kappa \stackrel{2 \leq \kappa}{\leq} \kappa^\kappa \stackrel{\kappa \leq 2^\kappa}{\leq} (2^\kappa)^\kappa = 2^\kappa$$

\square

Proposizione 13.31 (Cofinalità dei cardinali limiti)

Se λ è un cardinale limite, allora $\text{cof}(\aleph_\lambda) = \text{cof}(\lambda)$.

Dimostrazione. Osserviamo che $\{\aleph_\alpha : \alpha < \lambda\}$ è un sottoinsieme cofinale in \aleph_λ , infatti, dato $y \in \aleph_\lambda = \bigcup_{\alpha < \lambda} \aleph_\alpha$, si ha $y \in \aleph_\alpha$, per qualche $\alpha < \lambda$, dunque è sempre maggiorato da un elemento dell'insieme. Inoltre, essendo la mappa $\alpha \mapsto \aleph_\alpha$ strettamente crescente e surgettiva si ha $\{\aleph_\alpha : \alpha < \lambda\} \sim \lambda$ ¹⁶³, dunque la cofinalità di questo insieme è proprio uguale a $\text{cof}(\lambda)$, e si conclude ricordando che abbiamo visto che la cofinalità è transitiva per i sottoinsiemi cofinali, dunque $\text{cof}(\aleph_\lambda) = \text{cof}(\lambda)$. \square

¹⁶³Stiamo implicitamente usando che la cofinalità di insiemi totalmente ordinati isomorfi sia la stessa, questa proprietà è un'immediata conseguenza del fatto di star usando una mappa strettamente crescente tra gli insiemi, da cui si ottiene che se le cofinalità non fossero uguali si avrebbe un assurdo.

Nota 13.32 (Esistenza di cardinali inaccessibili nella ZFC) — In generale, un cardinale **limite** potrebbe essere **singolare o regolare**. Tuttavia, benché sia facile esibire cardinali limiti singolari (abbiamo visto ad esempio \aleph_ω), gli assiomi della ZFC non implicano l'esistenza [all'interno della teoria] di un cardinale limite e regolare - che abbiamo detto si chiama appunto **debolmente inaccessibile**. Insomma, non si può dimostrare che tutti i cardinali limiti sono singolari - e non c'è una buona ragione per assumere che lo siano (quindi non aggiungiamo un altro assioma) - ma sarebbe comunque coerente con gli assiomi della teoria degli insiemi che tutti i cardinali limiti fossero singolari (quindi potremmo aggiungere questo assioma senza perdere la coerenza).

Osservazione 13.33 (Cardinali limiti ed inaccessibili) — L'idea dietro ai cardinali debolmente limiti è che non possano essere “raggiunti” a partire da un altro cardinale ripetendo l'operazione di successore cardinale (proprio come accade per gli ordinali limite con l'operazione di successore ordinale).

I cardinali che sono limiti forti, oltre alla proprietà precedente, per definizione, non sono ottenibili ripetendo l'operazione di prendere le parti^a, infatti vale appunto che se λ è limite forte, preso $\kappa < \lambda$ si ha $2^\kappa < \lambda$, dunque prendere le parti di cardinali più piccoli non ci fa arrivare mai a κ .

I cardinali limiti e limiti forti possono essere ancora costruiti per unione (come ad esempio capita per i \beth_λ , con λ limite), quindi avere un cardinale limite forte non è ancora sufficiente per avere qualcosa di inaccessibile, la nozione vera di inaccessibilità può essere definita solo tramite la cofinalità. Infatti, per un cardinale κ limite [forte] richiedere che sia regolare ci dice che tale cardinale **non** può essere espresso come somma (unione) di cardinali meno di κ cardinali minori di κ .

^aUn esempio può essere \beth_ω , che è un cardinale limite forte [singolare], che, da definizione (si veda negli esercizi in fondo), non è ottenibile prendendo le parti di un qualche \beth_α , per $\alpha < \omega$.

§13.4 Formula di Hausdorff

Proposizione 13.34 (Formula di Hausdorff)

Siano κ e λ cardinali infiniti, allora:

$$(\kappa^+)^{\lambda} = \kappa^{\lambda} \cdot \kappa^+$$

Dimostrazione. Dimostriamo le due disuguaglianze tra LHS e RHS.

\geq Siccome $\kappa^{\lambda} \cdot \kappa^+ = \max(\kappa^{\lambda}, \kappa^+)$, è ovvio che $(\kappa^+)^{\lambda}$ è maggiore o uguale di entrambi i termini per debole monotonia dell'esponenziale. Alternativamente, sempre sfruttando la debole monotonia dell'esponenziale si ha:

$$\kappa^{\lambda} \cdot \kappa^+ \leq (\kappa^+)^{\lambda} \cdot \kappa^+ = (\kappa^+)^{\lambda+1} \stackrel{\lambda \text{ infinito}}{=} (\kappa^+)^{\lambda}$$

\leq Distinguiamo due casi:

- se $\kappa < \lambda$: in questo caso si ha, per definizione, che $\kappa^+ \leq \lambda$, da cui:

$$(\kappa^+)^{\lambda} \leq \lambda^{\lambda} = 2^{\lambda} \stackrel{\kappa < \lambda}{=} \kappa^{\lambda} \leq \kappa^{\lambda} \cdot \kappa^+$$

- se $\kappa \geq \lambda$: essendo κ^+ successore, è regolare, dunque $\text{cof}(\kappa^+) = \kappa^+$, si osserva dunque che data $f \in (\kappa^+)^{\lambda}$ si ha:

$$|\text{Im}(f)| \leq \lambda \leq \kappa < \kappa^+ \implies \text{Im}(f) \text{ non cofinale in } \kappa^+$$

ovvero esiste un ordinale $\alpha \in \kappa^+$ tale che [è un maggiorante di tutta l'immagine] $\text{Im}(f) \subseteq \alpha$, per cui segue che $f \in \alpha^{\lambda}$. Quanto visto implica che $(\kappa^+)^{\lambda} \subseteq \bigcup_{\alpha < \kappa^+} \alpha^{\lambda}$, ed essendo che per ogni $\alpha \in \kappa^+$ è ovvio che $\alpha^{\lambda} \subseteq (\kappa^+)^{\lambda}$, si ha anche che $\bigcup_{\alpha < \kappa^+} \alpha^{\lambda} \subseteq (\kappa^+)^{\lambda}$.

A questo punto possiamo stimare la cardinalità di $(\kappa^+)^{\lambda}$ facendo uso della disuguaglianza di inclusione-esclusione come segue:

$$(\kappa^+)^{\lambda} = \left| \bigcup_{\alpha < \kappa^+} \alpha^{\lambda} \right| \leq \sum_{\alpha < \kappa^+} |\alpha^{\lambda}| = \sum_{\alpha < \kappa^+} |\alpha|^{\lambda} \leq \sum_{\alpha < \kappa^+} \kappa^{\lambda} = \kappa^{\lambda} \cdot \kappa^+$$

□

Osservazione 13.35 (Alternativa per la seconda disuguaglianza) — Nella dimostrazione precedente, per dimostrare che $(\kappa^+)^{\lambda} \leq \kappa^{\lambda} \cdot \kappa^+$, nel caso in cui $\kappa < \lambda$, si poteva procedere alternativamente, sfruttando il fatto che $\kappa < 2^{\kappa} \rightarrow \kappa^+ \leq 2^{\kappa}$:

$$(\kappa^+)^{\lambda} \leq (2^{\kappa})^{\lambda} = (\kappa^{\lambda})^{\lambda} = \kappa^{\lambda} \leq \kappa^{\lambda} \cdot \kappa^+$$

Osservazione 13.36 (Disuguaglianza somma-prodotto) — Data una famiglia infinita di cardinali $\{\kappa_i\}_{i \in I}$ vale una disuguaglianza somma-prodotto^a:

$$\sum_{i \in I} \kappa_i \leq \prod_{i \in I} \kappa_i$$

^aKönig normalmente ha come condizione iniziale una disuguaglianza stretta che ne implica un'altra stretta, e quest'ultima a sua volta ne implica una larga, tuttavia, questo ragionamento non funziona se la disuguaglianza iniziale è larga perché non potremmo applicare König.

Dimostrazione. Ci basta trovare una funzione iniettiva:

$$F : \bigcup_{i \in I} \kappa_i \times \{i\} \rightarrow \prod_{i \in I} \kappa_i = \left\{ f : I \rightarrow \sup_{i \in I} \kappa_i \mid \forall i \in I \ f(i) \in \kappa_i \right\}$$

Osserviamo che essendo il prodotto fatto da cardinali infiniti, dunque aleph, vale che $\prod_{i \in I} \kappa_i = \prod_{i \in I} (\kappa_i + 1)$ ¹⁶⁴, con quest'ultimo che è dato dall'insieme:

$$\left\{ f : I \rightarrow \sup_{i \in I} (\kappa_i + 1) \mid \forall i \in I \ f(i) \in \kappa_i \cup \{\spadesuit\} \right\}$$

A questo punto la mappa più naturale possibile associa ogni coppia (a_i, i) (con $a_i \in \kappa_i$) ad una funzione nell'insieme di arrivo che su i fa a_i e fa \spadesuit altrove:

$$F : \bigcup_{i \in I} \kappa_i \hookrightarrow \prod_{i \in I} (\kappa_i + 1) : (a_i, i) \mapsto \underbrace{f(x)}_{\in^I(\sup_{i \in I} (\kappa_i + 1))} = \begin{cases} a_i & \text{se } x = i \\ \spadesuit & \text{se } x \neq i \end{cases}$$

ed è iniettiva appunto perché la coppia (a_i, i) può essere pensata mappata nella $|I|$ -upla (o funzione) $(\spadesuit, \dots, \underbrace{a_i, \dots, \spadesuit}_{i}, \dots)$, dunque è facile vedere che due funzioni uguali ci danno che le coppie in partenza sono esattamente uguali. \square

Esercizio 13.37 ($\aleph_\omega^{\aleph_0}$). Dimostrare che $\aleph_\omega^{\aleph_0} = \prod_{n \in \omega} \aleph_n$.

Soluzione. Vediamo le due disuguaglianze.

\geq Facile stima che deriva dalla monotonia del prodotto cardinale:

$$\prod_{n \in \omega} \aleph_n \leq \prod_{n \in \omega} \aleph_\omega = \aleph_\omega^{\aleph_0}$$

\leq Consideriamo $\Lambda = \bigsqcup \{\Lambda_k \mid k \in \omega\} \subseteq \omega$, con $\Lambda_k = \{p_k^{n+1} \mid n \in \omega\}$ (abbiamo escluso 1 da tutti gli insiemi per renderli [insiemi numerabili] disgiunti), dove p_k è il k -esimo primo (ricordiamo che sono enumerabili da ω).

¹⁶⁴Stiamo aggiungendo a tutti i cardinali $\{\spadesuit\}$ e fare il conto così non cambia, perché abbiamo visto che il prodotto è ben definito (cioè anche usando un insieme che non sia il cardinale stesso, purché abbia la stessa cardinalità, ciò che esce dal prodotto è in biogezione col risultato del prodotto fatto con i cardinali).

A questo punto abbiamo:

$$\begin{aligned}
 \prod_{n \in \omega} \aleph_n &\geq \prod_{n \in \Lambda} \aleph_n & (\Lambda \subseteq \omega) \\
 &= \prod_{n \in \Lambda_1 \sqcup \dots \sqcup \Lambda_k \sqcup \dots} \aleph_n \\
 &= \left(\prod_{n \in \Lambda_1} \aleph_n \right) \cdot \dots \cdot \left(\prod_{n \in \Lambda_k} \aleph_n \right) \cdot \dots \quad (\text{associatività infinita}) \\
 &= \prod_{k \in \omega} \prod_{n \in \Lambda_k} \aleph_n \\
 &\geq \prod_{k \in \omega} \left(\sum_{n \in \Lambda_k} \aleph_n \right) & (\text{disuguaglianza somma-prodotto}) \\
 &= \prod_{k \in \omega} \left(|\aleph_0| \cdot \sup_{n \in \omega} \aleph_n \right) \\
 &= \prod_{k \in \omega} \aleph_\omega = \aleph_\omega^{\aleph_0}
 \end{aligned}$$

□

Osservazione 13.38 (Alternativa per la seconda disuguaglianza precedente) — Osserviamo che al posto di usare l'associatività infinita su un'unione disgiunta infinita di insiemi, nella seconda disuguaglianza precedente, avremmo anche potuto fissare una biiezione $f : \omega \times \omega \rightarrow \omega$ e riscrivere la produttoria come segue [cambiando di fatto solo il nome dell'insieme su cui la facciamo]:

$$\prod_{n \in \omega} \aleph_n = \prod_{(a,b) \in \omega \times \omega} \aleph_{f(a,b)} = \prod_{a \in \omega} \prod_{b \in \omega} \aleph_{f(a,b)}$$

(dove l'ultima uguaglianza è semplicemente una riscrittura dell'insieme), osserviamo ora che il prodotto è maggiore di tutti gli elementi di $\{\aleph_{f(a,b)} | b \in \omega\}$ dunque è maggiore o uguale del sup di tale insieme (per definizione):

$$\prod_{b \in \omega} \aleph_{f(a,b)} \geq \sup \{\aleph_{f(a,b)} | b \in \omega\} = \aleph_\omega$$

dove l'uguaglianza deriva dal fatto che l'insieme su cui stiamo facendo il sup coincide con $\{\aleph_n | n \in \omega\}$. Dunque possiamo stimare $\prod_{b \in \omega} \aleph_{f(a,b)} \geq \aleph_\omega$ e ottenere:

$$\prod_{n \in \omega} \aleph_n \geq \prod_{a \in \omega} \aleph_\omega = \aleph_\omega^{\aleph_0}$$

Esercizio 13.39 ($\aleph_n^{\aleph_1} = \aleph_0^{\aleph_1} \cdot \aleph_n$). Dimostrare che per ogni $n \in \omega$ vale $\aleph_n^{\aleph_1} = \aleph_0^{\aleph_1} \cdot \aleph_n$.^a

^aOsservare che con la stessa identica dimostrazione vale di più: $\aleph_n^{\aleph_\alpha} = \aleph_0^{\aleph_\alpha} \cdot \aleph_n$, per $\alpha \in \text{Ord}$.

Soluzione. Procediamo per induzione numerabile.

caso $n = 0$ In questo caso si ha che $\aleph_0^{\aleph_1} = \aleph_0^{\aleph_1} \cdot \aleph_0$, infatti per monotonia dell'esponenziale $\aleph_0 \leq \aleph_0^{\aleph_1}$, dunque nel prodotto tra cardinali \aleph_0 viene assorbito.

caso $n + 1$ Supponiamo per ipotesi induttiva che $\aleph_n^{\aleph_1} = \aleph_0^{\aleph_1} \cdot \aleph_n$ e osserviamo che:

$$\aleph_{n+1}^{\aleph_0} \stackrel{\text{Hausdorff}}{=} \aleph_n^{\aleph_0} \cdot \aleph_{n+1} \stackrel{\text{Hp. induttiva}}{=} \aleph_0^{\aleph_1} \cdot \aleph_n \cdot \aleph_{n+1} = \aleph_0^{\aleph_1} \cdot \aleph_{n+1}$$

□

Esercizio 13.40 ($\aleph_\omega^{\aleph_1}$). Dimostrare che $\aleph_\omega^{\aleph_1} = \beth(\aleph_1) \cdot \beth(\aleph_\omega)$. [a](#)

^aHint: Studiare $(\prod_{n \in \omega} \aleph_n)^{\aleph_1}$.

Soluzione. Osserviamo innanzitutto che $\beth(\aleph_1) = \aleph_1^{\text{cof}(\aleph_1)} = \aleph_1^{\aleph_1}$ (abbiamo appena visto che i cardinali successori sono regolari) e $\beth(\aleph_\omega) = \aleph_\omega^{\text{cof}(\aleph_\omega)} = \aleph_\omega^{\text{cof}(\omega, <)}$ quindi il RHS è $\aleph_1^{\aleph_1} \cdot \aleph_\omega^{\aleph_0}$. Si tratta quindi di dimostrare come al solito due diseguaglianze.

\geq È una facile stima sfruttando la monotonia dell'esponenziale e le proprietà delle potenze:

$$\aleph_1^{\aleph_1} \cdot \aleph_\omega^{\aleph_0} \leq \aleph_1^{\aleph_1} \cdot \aleph_\omega^{\aleph_1} = (\aleph_1 \cdot \aleph_\omega)^{\aleph_1} = \aleph_\omega^{\aleph_1}$$

\leq Per questa diseguagliaza sono necessari i due esercizi precedenti, infatti:

$$\begin{aligned} \aleph_\omega^{\aleph_1} &= \left(\sum_{n \in \omega} \aleph_n \right)^{\aleph_1} \\ &\leq \left(\prod_{n \in \omega} \aleph_n \right)^{\aleph_1} && \text{(diseguagliaza somma-prodotto)} \\ &= \prod_{n \in \omega} \aleph_n^{\aleph_1} \\ &= \prod_{n \in \omega} \aleph_0^{\aleph_1} \cdot \aleph_n && (\aleph_n^{\aleph_1} = \aleph_0^{\aleph_1} \cdot \aleph_n) \\ &= \aleph_0^{\aleph_1} \cdot \prod_{n \in \omega} \aleph_n \\ &= \aleph_0^{\aleph_1} \cdot \aleph_\omega^{\aleph_0} \leq \aleph_1^{\aleph_1} \cdot \aleph_\omega^{\aleph_0} \end{aligned}$$

□

Fatto 13.41 (Esponenziazione di cardinali)

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 $\beth(\kappa)$.

Definizione 13.42 (Quasi esponenziazione di un cardinale limite). Sia κ un cardinale **limite**. Definiamo:

$$2^{<\kappa} \stackrel{\text{def}}{=} \sup\{2^\lambda \mid \lambda \text{ cardinale} < \kappa\}$$

Lema 13.43 (2 alla cardinale limite)

Dato κ cardinale limite vale:

$$2^\kappa = (2^{<\kappa})^{\text{cof}(\kappa)}$$

Dimostrazione. Per definizione di cofinalità sia $\{\kappa_i\}_{i \in \lambda}$, tale che $\kappa_i < \kappa$ per ogni $i \in \text{cof}(\kappa)$, per cui $\kappa = \sum_{i \in \text{cof}(\kappa)} \kappa_i$. Allora vale la segue catena di disuguaglianze:

$$2^\kappa = 2^{\sum_{i \in \text{cof}(\kappa)} \kappa_i} = \prod_{i \in \text{cof}(\kappa)} 2^{<\kappa} = (2^{<\kappa})^{\text{cof}(\kappa)} \leq (2^\kappa)^{\text{cof}(\kappa)} = 2^\kappa$$

dove: la prima uguaglianza è la definizione di cofinalità, la seconda la proprietà del prodotto infinito di potenze (visto in un'osservazione ad inizio capitolo), la terza è una delle proprietà dei prodotti infiniti, e la quarta è la monotonia debole dell'esponenziale, in quanto $2^{<\kappa} = \sup\{2^\lambda \mid \lambda \text{ cardinale e } \lambda < \kappa\} \leq 2^\kappa$. \square

Definizione 13.44 (Funzione del continuo definitivamente costante sotto un cardinale). Sia κ un cardinale, diciamo che la funzione del continuo $\lambda \mapsto 2^\lambda$ è **definitivamente costante sotto κ** se esiste un cardinale $\mu < \kappa$ tale che [la funzione del continuo è costante da lì in poi fino a κ escluso] $\forall \nu \text{ cardinale } \mu \leq \nu < \kappa \rightarrow 2^\nu = 2^\mu$.

Proposizione 13.45 (Esponenziazione cardinale di 2)

La funzione del continuo $\kappa \mapsto 2^\kappa$ è determinata da \beth come segue:

$$2^\kappa = \begin{cases} \beth(\kappa) & \text{se } \kappa \text{ è successore} \\ 2^{<\kappa} \cdot \beth(\kappa) & \text{se } \lambda \mapsto 2^\lambda \text{ è definitivamente costante sotto } \kappa \\ \beth(2^{<\kappa}) & \text{se } \lambda \mapsto 2^\lambda \text{ non è definitivamente costante sotto } \kappa \end{cases}$$

Dimostrazione. Abbiamo già visto il caso successore in precedenza. Supponiamo quindi che κ sia un cardinale limite e vediamo prima i casi in cui la funzione del continuo è definitivamente costante e κ .

- Caso $\lambda \mapsto 2^\lambda$ è definitivamente costante sotto κ e κ regolare.

Osserviamo che vale:

$$2^{<\kappa} \cdot \beth(\kappa) \stackrel{\kappa \text{ regolare}}{=} 2^{<\kappa} \cdot \kappa^\kappa = 2^{<\kappa} \cdot 2^\kappa = 2^\kappa$$

dove nell'ultima uguaglianza abbiamo usato che 2^κ è un maggiorante dell'insieme $\{2^\lambda \mid \lambda < \kappa \text{ e } \lambda \text{ cardinale}\}$, dunque è maggiore o uguale del sup, ovvero $2^{<\kappa}$.

- Caso $\lambda \mapsto 2^\lambda$ è definitivamente costante sotto κ e κ singolare.

In questo caso l'ipotesi che la funzione del continuo sia definitivamente costante sotto κ ci dice che $\exists \mu < \kappa$ tale che per ogni cardinale $\mu \leq \nu < \kappa$, si ha $2^\mu = 2^\nu$, in particolare ciò significa che $2^\mu = 2^{<\kappa}$ (soddisfa esattamente la definizione di sup dell'insieme), e ciò ci dà:

$$2^\kappa \stackrel{\text{lemma}}{=} (2^{<\kappa})^{\text{cof}(\kappa)} = \overbrace{2^\mu \cdot \text{cof}(\kappa)}^{\mu \leq <\kappa} = 2^\mu = 2^{<\kappa}$$

Per concludere osserviamo che in questo caso $\beth(\kappa) = 2^{<\kappa}$:

$$\beth(\kappa) = \kappa^{\text{cof}(\kappa)} \stackrel{\text{cof}(\kappa) < \kappa}{\leq} \kappa^\kappa = 2^\kappa \stackrel{\text{sopra}}{=} 2^{<\kappa}$$

Vediamo ora il caso in cui la funzione del continuo non è definitivamente costante sotto κ .

- Caso $\lambda \mapsto 2^\lambda$ non definitivamente costante sotto κ .

Basta dimostrare che $\text{cof}(2^{<\kappa}) = \text{cof}(\kappa)$, e da questo segue immediatamente che:

$$2^\kappa = (2^{<\kappa})^{\text{cof}(\kappa)} = (2^{<\kappa})^{\text{cof}(2^{<\kappa})} = \beth(2^{<\kappa})$$

dunque non dobbiamo far altro che dimostrare l'assunto.

$\boxed{\text{cof}(2^{<\kappa}) \leq \text{cof}(\kappa)}$ Sia $A \subseteq \kappa$ cofinale in κ e consideriamo $B := \{2^\alpha | \alpha \in A\} \subseteq 2^{<\kappa}$, naturalmente

si ha $|B| \stackrel{\alpha \rightarrow 2^\alpha}{\leq} |A|$, se verifichiamo che B è cofinale in $2^{<\kappa}$, avremmo la disuguaglianza per la definizione v.2 di cofinalità.

Sia $x < 2^{<\kappa}$, allora, per definizione di sup, esiste $\gamma < \kappa$ tale che $x < 2^\gamma$, siccome A è cofinale in κ , allora esiste $\beta \in A$ tale che $\beta \geq \gamma > x$, dunque per monotonia si ottiene $x < 2^\gamma \leq 2^\beta \in B$.

$\boxed{\text{cof}(\kappa) \leq \text{cof}(2^{<\kappa})}$ Per definizione $\alpha < 2^{<\kappa}$ significa che esiste un cardinale $\beta < \kappa$, tale che $\alpha < 2^\beta$,

indichiamo con β_α il minimo cardinale per cui ciò accade. Sia ora $A \subseteq 2^{<\kappa}$ un sottoinsieme cofinale, definiamo $B := \{\beta_\alpha : \alpha \in A\}$, naturalmente la mappa $\alpha \mapsto \beta_\alpha$ ci dà la disuguaglianza $|B| \leq |A|$, se dimostriamo quindi che B è cofinale in κ abbiamo concluso.

Sia $x < \kappa$, si ha $2^x \leq 2^\kappa$, non può valere che $2^x = 2^\kappa$, altrimenti la funzione del continuo sarebbe definitivamente costante sotto κ (contro l'ipotesi), per cui esiste $y < \kappa$ tale che $2^x < 2^y < 2^\kappa$. Quanto detto ci assicura che $2^x < 2^\kappa$, a questo punto, per la cofinalità di A , si ha $2^x \leq \alpha \in A$, da cui $2^x \leq \alpha < 2^{\beta_\alpha}$. Osserviamo infine che $x \leq \beta_\alpha$, infatti, se fosse $x > \beta_\alpha$, allora $2^x \geq 2^{\beta_\alpha}$, che è assurdo.

□

§14 La gerarchia di Von Neumann e l'assioma di buona fondazione

Insiemi come questi sono (forse?) mostri indesiderabili:

$$\left\{ \left\{ \left\{ \dots \right\} \right\} \right\} \quad x = \{x\} \quad y = \{y\} \quad z = \{y\}$$

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 l'esistenza di insiemi del genere.

Startegia: costruiamo un universo insiemistico V_* , che è una classe propria, al cui interno gli assiomi sono veri, e che, tuttavia, non contiene quella robaccia.

Definizione 14.1 (Gerarchia di Von Neumann). Costruiamo per ricorsione transfinita la **gerarchia di Von Neumann** come segue:

$$\begin{aligned} V_0 &= \emptyset \\ V_{s(\alpha)} &= \mathcal{P}(V_\alpha) \\ V_\lambda &= \bigcup\{V_\alpha \mid \alpha < \lambda\} \text{ per } \lambda \text{ limite} \end{aligned}$$

La classe V_* è l'unione degli insiemi V_α , formalmente:

$$x \in V_* \stackrel{\text{def}}{=} \exists \alpha \in \text{Ord } x \in V_\alpha$$

(dove V_* è una classe perché l'abbiamo definita come la formula al RHS).

Lemma 14.2 (V_α è transitivo)

$\forall \alpha \in \text{Ord } V_\alpha$ è un insieme transitivo.

Dimostrazione. Procediamo per induzione transfinita.

caso V_0 Immediato perché \emptyset è un insieme transitivo a vuoto.

caso successore Supponiamo che V_α sia un insieme transitivo e dimostriamo che anche $V_{s(\alpha)}$ lo è. Dato $x \in V_{s(\alpha)}$ vogliamo arrivare a dire che $x \subseteq V_{s(\alpha)}$ (o equivalentemente che $\forall y \in x \ y \in V_{s(\alpha)}$). Per farlo ci basta osservare che:

$$x \in V_{s(\alpha)} = \mathcal{P}(V_\alpha) \implies x \subseteq V_\alpha$$

ora, poiché V_α è transitivo per ipotesi induttiva, tutti gli elementi di x sono a loro volta sottoinsiemi di V_α [cioè essendo elementi di un sottoinsieme sono in primis elementi di V_α , poi per la transitività di quest'ultimo sappiamo che tutti gli elementi sono sottoinsiemi]¹⁶⁵, ovvero $\forall y \in x \ y \subseteq V_\alpha \implies \forall y \in x \ y \in \mathcal{P}(V_\alpha) = V_{s(\alpha)}$, pertanto è verificata la definizione di transitività in $V_{s(\alpha)}$.

¹⁶⁵Attenzione al fatto che transitivo non dice che i sottoinsiemi sono necessariamente elementi, quindi x non è detto sia un elemento di V_α , ma è un sottoinsieme di V_α e questo ci basta.

caso limite Assumiamo per ipotesi induttiva che V_α sia transitivo per ogni $\alpha < \lambda$. Per definizione:

$$x \in V_\lambda \implies x \in V_\alpha$$

per qualche $\alpha < \lambda$, ma allora per ipotesi induttiva $x \subseteq V_\alpha \subseteq V_\lambda$ [la seconda uguaglianza è la definizione nel caso limite].

□

Corollario 14.3 (V_* è una classe transitiva)

V_* è una **classe transitiva**, ossia $\forall x \in V_* x \subseteq V_*$.

Dimostrazione. Se $x \in V_*$, allora per definizione $x \in V_\alpha$ per qualche $\alpha \in \text{Ord}$, quindi per la proposizione sopra $x \subseteq V_\alpha$, ovvero x è un insieme di cose che soddisfano il predicato che definisce V_* , quindi $x \subseteq V_*$. □

Lemma 14.4 (“Ordinamento” di V_*)

$$\forall \alpha, \beta \in \text{Ord} \quad \alpha < \beta \rightarrow V_\alpha \subseteq V_\beta.$$

Dimostrazione. Procediamo per induzione transfinita su β .

caso $\beta = 0$ Vero a vuoto.

caso successore Dobbiamo dimostrare che $\forall \alpha < s(\beta) V_\alpha \subseteq V_{s(\beta)}$, e abbiamo per ipotesi induttiva $\forall \alpha < \beta V_\alpha \subseteq V_\beta$. Siccome $\alpha < s(\beta) \leftrightarrow \alpha \leq \beta$, si danno due casi, e $\alpha = \beta$ è banalmente vero, dunque abbiamo $\alpha < \beta$, quindi per ipotesi induttiva $V_\alpha \subseteq V_\beta$. Per la definizione ricorsiva si ha $V_\alpha \subseteq V_\beta \implies V_\alpha \in \mathcal{P}(V_\beta) = V_{s(\beta)}$, ma, per la transitività di quest’ultimo, si ottiene che $V_\alpha \subseteq V_{s(\beta)}$.

caso limite Abbiamo per ipotesi che $\forall \alpha < \beta < \lambda V_\alpha \subseteq V_\beta$, e vogliamo dimostrare che $\forall \alpha < \lambda V_\alpha \subseteq V_\lambda$. Questo segue facilmente dall’ipotesi e dalla definizione, infatti, $V_\lambda = \bigcup\{V_\gamma | \gamma < \lambda\}$, ciò significa che $V_\beta \subseteq V_\lambda$ per ogni $\beta < \lambda$, unendo ciò all’ipotesi si ottiene la tesi, $\forall \alpha < \beta < \lambda V_\alpha \stackrel{\text{Hp. indutt.}}{\subseteq} V_\beta \stackrel{\text{def. } V_\lambda}{\subseteq} V_\lambda \implies \forall \alpha < \lambda V_\alpha \subseteq V_\lambda$. ¹⁶⁶

□

Lemma 14.5 (Ogni ordinale è contenuto nella sua immagine in V_*)

$$\forall \alpha \in \text{Ord} \quad \alpha \subseteq V_\alpha.$$

Dimostrazione. Come al solito per induzione transfinita.

caso 0 $0 \subseteq V_0 = \emptyset$, vera [perché scrivendo estesamente la formula insiemistica si ha una premessa falsa].

¹⁶⁶In realtà si poteva concludere anche senza usare l’ipotesi induttiva, in quanto $\alpha < \lambda \implies V_\alpha \subseteq \bigcup V_\gamma | \gamma < \lambda = V_\lambda \implies V_\alpha \subseteq V_\lambda$.

caso successore Supponiamo che $\alpha \subseteq V_\alpha$ e dimostriamo che $s(\alpha) \subseteq V_{s(\alpha)}$. Osserviamo che dall'ipotesi si ha:

$$\alpha \subseteq V_\alpha \implies \alpha \in \mathcal{P}(V_\alpha) = V_{s(\alpha)} \xrightarrow{\text{transitività}} \alpha \subseteq V_{s(\alpha)}$$

inoltre $\alpha \in V_{s(\alpha)}$ implica che $\{\alpha\} \subseteq V_{s(\alpha)}$ (se c'è come elemento, allora il suo singoletto è un suo sottoinsieme). Si conclude dunque: $s(\alpha) = \underbrace{\alpha}_{\subseteq V_{s(\alpha)}} \cup \underbrace{\{\alpha\}}_{\subseteq V_{s(\alpha)}} \subseteq V_{s(\alpha)}$.

caso limite Per ipotesi induttiva abbiamo che $\alpha < \lambda \rightarrow \alpha \subseteq V_\alpha$, ma allora $\bigcup\{\alpha | \alpha < \lambda\} \subseteq \bigcup\{V_\alpha | \alpha < \lambda\}$ [perché abbiamo per ipotesi che ogni elemento dell'insieme al LHS è contenuto in un elemento dell'insieme al RHS, quindi, prendere l'unione genera un insieme che contiene necessariamente almeno tutti gli elementi dell'altro insieme], da cui:

$$\lambda = \bigcup\{\alpha | \alpha < \lambda\} \subseteq \bigcup\{V_\alpha | \alpha < \lambda\} = V_\lambda$$

□

§14.1 Formule relativizzate ad una classe

Definizione 14.6 (Relativizzazione a V_*). Data una formula insiemistica, la possiamo **relativizzare a V_*** rimpiazzando i quantificatori [non limitati] $\exists \square$ e $\forall \square$ rispettivamente con $\exists \square \in V_*$ e $\forall \square \in V_*$.

Esempio 14.7 (Relativizzazione di una formula a V_*)

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 ricondurla al linguaggio della teoria degli insiemi puro, ovvero dobbiamo rimuovere gradualmente tutte le abbreviazioni:^a

$$\begin{aligned} &\exists x \forall y \in x \exists z \in y z \cap x = \emptyset \\ &\exists x \forall y (y \in x \rightarrow \exists z (z \in y \wedge \neg \exists t (t \in z \cap x))) \\ &\exists x \forall y (y \in x \rightarrow \exists z (z \in y \wedge \neg \exists t (t \in z \wedge t \in x))) \end{aligned}$$

A questo punto rimpiazziamo meccanicamente tutti i quantificatori con quantificatori limitati a V_* :

$$\begin{aligned} &\exists x \forall y (y \in x \rightarrow \exists z (z \in y \wedge \neg \exists t (t \in z \wedge t \in x))) \\ &\exists x \in V_* \forall y \in V_* (y \in x \rightarrow \exists z \in V_* (z \in y \wedge \neg \exists t \in V_* (t \in z \wedge t \in x))) \end{aligned}$$

Questa nuova formula, φ relativizzata a V_* , come è scritta qui sopra, non è espressa nel linguaggio della teoria degli insiemi puro, per via dei quantificatori limitati $\exists \square \in V_*$ e $\forall \square \in V_*$, tuttavia, se volessimo, potremmo semplicemente rimpiazzare questi quantificatori con le rispettive definizioni e ottenere così una formula insiemistica pura relativizzata a V_* .

^aTipo di Mamino alla fine della terza riga, mette $t \in y$ anziché $t \in x$.

Teorema 14.8 (Gli assiomi 1-9 relativizzati sono veri in V_*)

Valgono gli assiomi 1-9 della teoria degli insiemi relativizzati a V_* .

Dimostrazione. Verifichiamo che valgono uno per uno gli assiomi 1-9 relativizzati in V_* , sfruttandone la definizione.

- (1) **Vuoto:** $\exists x \in V_* \forall y \in V_* y \notin x$

Basta prendere come $x = \emptyset \in V_1 = \mathcal{P}(V_0) = \mathcal{P}(\emptyset) = \{\emptyset\}$, dunque $\emptyset \in V_*$, e tale insieme rispetta la proprietà richiesta perché la rispettava in V .

- (2) **Estensionalità:** $\forall a, b \in V_*(a = b \leftrightarrow \forall x \in V_*(x \in a \leftrightarrow x \in b))$

Fissati $a, b \in V_*$ osserviamo che, per transitività, i loro elementi sono anch'essi elementi di V_* , quindi $x \in a$ o $x \in b$ implicano $x \in V_*$, per cui si ha:

$$\forall x(x \in a \leftrightarrow x \in b) \leftrightarrow \forall x(x \in V_* \wedge (x \in a \leftrightarrow x \in b) \vee x \notin V_* \wedge (x \in a \leftrightarrow x \in b))$$

ora il secondo elemento dell'OR è sempre falso per quanto detto prima, dunque possiamo escluderlo dall'equivalenza, e ciò ci lascia $\forall x \in V_*(x \in a \leftrightarrow x \in b)$. Dunque, per estensionalità, abbiamo l'equivalenza con $a = b$.

- (3) **Separazione:** $\forall A \in V_* \exists B \in V_* \forall x \in V_* x \in B \leftrightarrow (x \in A \wedge \varphi(x))$

Sia $A \in V_*$, ovvero $A \in V_\alpha$, per qualche α , allora per separazione esiste l'insieme $B := \{x \in A | x \in V_* \wedge \varphi(x)\}$. Siccome $B \subseteq A \in V_\alpha$, e $A \subseteq V_\alpha$ per transitività, si ha $B \subseteq V_\alpha \implies B \in V_{\alpha+1}$, per cui per definizione $B \in V_*$.

- (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, WLOG possiamo assumere $\alpha \leq \beta$, allora $\alpha, \beta \in V_\beta$, da cui necessariamente il paio, che esiste per l'assioma non relativizzato, è nelle parti di V_β , $\{a, b\} \in \mathcal{P}(V_\beta) = V_{\beta+1}$, in questo modo, per definizione si ottiene che $\{a, b\} \in V_*$.

- (5) **Unione:** $\forall A \in V_* \exists B \in V_* \forall x \in V_* x \in B \leftrightarrow \exists y \in A x \in y$

Sia $A \in V_\alpha$, per qualche ordinale α , per transitività, $A \subseteq V_\alpha$, ciò significa che $\bigcup A$, che esiste per unione non relativizzata, ed è l'insieme degli elementi degli elementi di $A \subseteq V_\alpha$, è a sua volta contenuto in V_α (perché gli elementi degli elementi di A per transitività sono a loro volta elementi di V_α), dunque $\bigcup A \subseteq V_\alpha$ ¹⁶⁷ $\implies \bigcup A \in \mathcal{P}(V_\alpha) = V_{\alpha+1}$, e quindi come prima, per definizione si conclude che $\bigcup A \in V_*$.

- (6) **Parti:** $\forall A \in V_* \exists B \in V_* \forall x \in V_* x \in B \leftrightarrow x \subseteq B$

Sia $A \in V_\alpha$, quindi per transitività $A \subseteq V_\alpha$, allora vale che $\mathcal{P}(A) \subseteq \mathcal{P}(V_\alpha) = V_{\alpha+1}$, dove le parti esistono per l'assioma non relativizzato, quindi $\mathcal{P}(A) \in \mathcal{P}(V_{\alpha+1}) = V_{\alpha+2}$, per cui $\mathcal{P}(A) \in V_*$.

- (7) **Infinito:** $\exists X \in V_* \emptyset \in X \wedge \forall y \in V_* y \in X \rightarrow y \cup \{y\} \in X$

Ci basta prendere $X = \omega \in V_{\omega+1}$, infatti sappiamo che $\omega \subseteq V_\omega$, per quanto visto prima, quindi $\omega \in V_{\omega+1}$, da cui $\omega \in V_*$, e naturalmente ω esiste per il corrispondente assioma non relativizzato.

- (8) **Rimpiazzamento:** $F : V_* \rightarrow V_*$ funzione classe e $X \in V_* \rightarrow F[X] \in V_*$

Se $X \in V_\alpha$, per transitività, $a \in X \rightarrow a \in V_\alpha$, quindi $F(a)$ è ben definito (perché $a \in V_*$) ed ha senso considerare $F[X]$, inoltre $F(a) \in V_*$ (perché F va da V_* a V_*).

¹⁶⁷Osserviamo che in generale $A \subseteq B \implies \bigcup A \subseteq B \iff B$ è transitivo (infatti in questo caso gli elementi di A sono sottoinsiemi a loro volta di B , per cui la loro unione è contenuta in B).

Sia α_a il minimo ordinale per cui $F(a) \in V_{\alpha_a}$ e sia $\beta := \sup\{\alpha_a | a \in X\}$ ¹⁶⁸. Allora $F(a) \in V_\beta, \forall a \in X$, per cui $F[X] \subseteq V_\beta \implies F[X] \in V_{\beta+1}$, dunque per definizione $F[X] \in V_*$.

(9) **Scelta:** $\forall X \in V_* (\forall y \in X y \neq \emptyset) \rightarrow \exists f \in V_*$ funzione di scelta su X

Sia f una funzione di scelta su $X \in V_\alpha$, che esiste per AC, sappiamo che $f \in {}^X \cup X$, cioè $f \in \mathcal{P}(X \times \bigcup X)$. Ricordando che $X \times \bigcup X \subseteq \mathcal{P}(\mathcal{P}(X \cup \bigcup X))$ e che $X \subseteq V_\alpha$ (che vale per transitività) implica $\bigcup X \subseteq V_\alpha$, abbiamo:

$$X \cup \bigcup X \subseteq V_\alpha \implies f \in \mathcal{P}\left(\mathcal{P}\left(\mathcal{P}\left(X \cup \bigcup X\right)\right)\right) \subseteq \mathcal{P}(\mathcal{P}(\mathcal{P}(V_\alpha))) = V_{\alpha+3}$$

e quindi si conclude che $f \in V_*$, per definizione di quest'ultima.

□

Osservazione 14.9 (Ogni $x \in V_*$ è contenuto un insieme dato da un ordinale successore)

— Dato $x \in V_*$ esiste il minimo α tale che $x \in V_\alpha$ (la classe degli ordinali è ben ordinata), e questo è necessariamente un ordinale successore, perché se $x \in V_\lambda = \bigcup\{V_\alpha | \alpha < \lambda\}$, allora [per definizione di unione] $x \in V_\alpha$ per qualche $\alpha < \lambda$, e quindi sarà in un ordinale successore. Possiamo quindi dare la definizione seguente.

Definizione 14.10 (Rango in V_*). Dato $x \in V_*$, detto **α il minimo** ordinale [successore per l'osservazione] per cui $x \in V_\alpha$, il **rango** di x , $\text{rank}(x)$, è definito da $\alpha = \text{rank}(x) + 1$ ¹⁷⁰. Ossia:

$$x \in V_\alpha \leftrightarrow \text{rank}(x) < \alpha$$

e tale definizione è ben posta per l'osservazione precedente.

Lemma 14.11 (Disegualanza tra ranghi)

Se $x \in y \in V_*$, allora $\text{rank}(x) < \text{rank}(y)$.

Dimostrazione. Per definizione di rango $y \in V_{s(\text{rank}(y))} = \mathcal{P}(V_{\text{rank}(y)})$, quindi $y \subseteq V_{\text{rank}(y)}$, di conseguenza, l'ipotesi $x \in y$ ci dice che $x \in V_{\text{rank}(y)}$, per cui si ha che $\text{rank}(x) < \text{rank}(y)$. □

Definizione 14.12 (Classi ben fondate). Diciamo che una classe C è **ben fondata** se per ogni insieme S di elementi di C , S contiene un x **minimale per appartenenza** (**ε-minimale**)¹⁷¹, ossia tale che $x \cap S = \emptyset$.

Proposizione 14.13 (Caratterizzazione classi ben fondate)

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:

$$\forall i \in \omega x_{i+1} \in x_i$$

¹⁶⁸Per essere più precisi stiamo considerando $\sup\{\text{rank}(a) + 1 | a \in X\}$, e quindi il sup esiste perché $\{\text{rank}(a) + 1 | a \in X\}$ è effettivamente un insieme di ordinali, per rimpiazzamento (è l'immagine della funzione classe $G(a) = \text{rank}(a) + 1$).

¹⁶⁹Cioè se $\emptyset \notin X$.

¹⁷⁰Cioè il rango di un elemento è il predecessore del minimo ordinale per cui $x \in V_\alpha$.

¹⁷¹“epsilon-minimale”.

Ossia non esiste una catena infinita discendente per appartenenza:

$$x_0 \ni x_1 \ni x_2 \ni \dots$$

Dimostrazione. Se $\{x_i\}_{i \in \omega}$ è una catena infinita discendente, allora $\{x_i | i \in \omega\}$ non ha un elemento ϵ -minimale, perché per l'appartenenza infinita discendente qualsiasi elemento dell'insieme ha intersezione non vuota con quest'ultimo.¹⁷²

D'altro canto, se S non ha un elemento ϵ -minimale, fissata una funzione di scelta f su S , possiamo definire una catena discendente per ricorsione numerabile. Fissiamo $\bar{x} \in S$ e definiamo:

$$x_0 = \bar{x} \quad x_{n+1} = f(\{y \in S | y \in x_n\}) = f(S \cap x_n)$$

dove l'insieme a cui è applicata f è non vuoto, altrimenti x_n sarebbe ϵ -minimale, che è contro l'ipotesi.¹⁷³ \square

Per questa caratterizzazione una classe **transitiva**¹⁷⁴ ben fondata non può quindi contenere mostri. Infatti, i mostri del primo tipo generano catene infinite discendenti per appartenenza, ed abbiamo visto che avere una classe ben fondata è equivalente al fatto che tali catene non esistano. I mostri del secondo e terzo tipo, si riconduco, sfruttando la transitività a mostri del primi tipo, e pertanto in una classe ben fondata non esistono, come segue: dato ad esempio $x = \{x\}$, si ha che $x \in x$, ma $x = \{x\}$, cioè $\{x\} \in x \implies x \in \underbrace{\{x\}}_{=x} \in x$, e continuando in questo modo abbiamo la catena infinita discendente per appartenenza:

$$x \ni x \ni x \ni x \ni \dots$$

Dati invece $y = \{z\}$ e $z = \{y\}$ si ha che $z \in y$, ma per definizione di z , $y \in z$, e ripetendo questo all'infinito si ottiene:

$$y \ni z \ni y \ni z \ni \dots$$

[o anche una catena che parte da z], e quindi non esistono.

Proposizione 14.14 (V_* è ben fondata)

La classe (transitiva) V_* è ben fondata.

Dimostrazione. Dato un insieme S di elementi di V_* , consideriamo $x \in S$ di rango minimo (cioè stiamo considerando un elemento di S di rango $\text{min}(\text{rank}[S])$). Osserviamo che x è un elemento ϵ -minimale per S . Infatti, se $x \cap S \neq \emptyset$, cioè se esistesse $y \in x \cap S = \{z \in S | z \in x\}$, allora, per il lemma sul rango, essendo $y \in x$ si avrebbe $\text{rank}(y) < \text{rank}(x)$, ma in tal caso avremmo un elemento di S con rango minore di x , e ciò è assurdo perché contro la minimalità di $\text{rank}(x)$. Di conseguenza $x \cap S = \emptyset$. \square

¹⁷²Questa è la contronominale di \implies , che quindi è fatta.

¹⁷³Questa è la contronominale della \iff .

¹⁷⁴Typo o forse no di Mamino, in ogni caso il discorso successivo non richiede la transitività, in particolare, affinché una classe non abbia mostri basta solo che sia ben fondata.

Teorema 14.15 (Gli assiomi 1-9 non implicano che V non sia ben fondato)

Se gli assiomi della teoria degli insiemi sono coerenti^a, essi non dimostrano l'esistenza di una catena infinita discendente per appartenenza.^b

^aIn caso contrario dimostrerebbero qualsiasi cosa.

^bMa non la escludono neanche, per questo abbiamo bisogno di aggiungere alla teoria un assioma apposta che ce lo assicuri.

Dimostrazione. Supponiamo di poter dimostrare che tale catena esiste. Allora, siccome gli assiomi valgono anche relativizzati a V_* , potremmo riportare l'intera dimostrazione ad una versione relativizzata, e ottenere così una catena infinita discendente per appartenenza in V_* , ma ciò è assurdo perché abbiamo dimostrato che V_* è una classe ben fondata. Pertanto gli assiomi 1-9 non ci permettono di dimostrare che un tale oggetto esiste nella nostra teoria. \square

§14.2 Assioma di buona fondazione

A questo punto 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.¹⁷⁵

Assioma 14.16 (Assioma di buona fondazione)

La classe di tutti gli insiemi è ben fondata.

$$\forall S \neq \emptyset \exists x \in S x \cap S = \emptyset^a$$

^aCioè ogni insieme ha un elemento ϵ -minimale.

¹⁷⁵In realtà assumendo buona fondazioneabbiamo già risolto il problema della presenza di mostri senza necessità di dimostrare che $V = V_*$, tuttavia lo facciamo comunque perché ciò ci dà ulteriori informazioni su V . In particolare avremo dimostrato che la classe di tutti gli insiemi coincide proprio con la gerarchia di Von Neumann, e cioè, oltre alla transitività ed a tutte le informazioni che conosciamo su V_* , ci dice anche che pensare alla classe di tutti gli insiemi organizzata come nella gerarchia è corretto (non è detto tuttavia che sia l'unico modo di pensare a V).

§14.3 Principio di ϵ -induzione

Per dimostrare che $V = V_*$ usando la buona fondazione, è comodo fare leva sul **principio di ϵ -induzione** (epsilon-induzione).

Teorema 14.17 (Principio di ϵ -induzione)

Se una classe C soddisfa:

$$\forall S(\forall x \in S x \in X) \rightarrow S \in C$$

Allora $C = V$, ossia $\forall S S \in C$.^a

^aStiamo dicendo che, se supponiamo che tutti gli elementi di tutti gli insiemi soddisfano il predicato che definisce C , e questa cosa ci dice che allora anche S stesso soddisfa tale predicato (da qui la nomenclatura con la ϵ , cioè dal fatto che il soddisfare una certa proprietà **passi dagli elementi a tutto l'insieme**), abbiamo che C è proprio la classe di tutti gli insiemi V .

La dimostrazione di questo enunciato richiede **buona fondazione**. Prima, però, enunciamo una proposizione che non la richiede.

Proposizione 14.18 (Esistenza della chiusura transitiva)

Dato un insieme X esiste più piccolo insieme transitivo $\text{tc}(X)$ tale che $X \subseteq \text{tc}(X)$, e prende il nome di **chiusura transitiva**.

Dimostrazione. Costruiamo la successione $(X_n)_{n \in \omega}$ in questo modo:

$$X_0 = X \quad X_{n+1} = \bigcup X_n$$

Si verifica immediatamente che per definizione:

$$\text{tc}(X) = \bigcup \{X_n \mid n \in \omega\}$$

perché contiene $X = X_0 \in (X_n)_{n \in \omega}$ e tutti i suoi elementi sono anche sottoinsiemi per costruzione. \square

Dimostriamo ora il principio di ϵ -induzione.

Dimostrazione. Procediamo per assurdo e supponiamo che si abbia $S \notin C$. Sia:

$$S' := \{x \in \text{tc}(\{S\}) \mid x \notin C\}^{176}$$

Per assurdo abbiamo detto che $S \notin C$, e questo, per la definizione di chiusura transitiva, ci assicura che $S \in S'$, che quindi è non vuoto. Per **buona fondazione** esiste $x \in S'$ tale che $\forall y \in x y \notin S'$ [cioè tale che $x \cap S' = \emptyset$]. Abbiamo quindi per costruzione che $x \in S' \iff x \notin C \wedge x \in \text{tc}(\{S\})$, ma la seconda cosa equivale a $x \subseteq \text{tc}(\{S\})$, cioè $\forall y \in x y \in \text{tc}(\{S\})$. Avendo preso x ϵ -minimale con buona fondazione, dovendo essere l'intersezione vuota, vogliamo che tutti gli elementi di x non stiano in S' , e visto che abbiamo appena verificato che stanno nella chiusura transitiva, l'unica possibilità è che soddisfino C , cioè $\forall y \in x y \in C$. Ma, per ipotesi induttiva, questa cosa implica che $x \in C$, ma avevamo che $x \in S'$, quindi $x \notin C$, abbiamo ottenuto quindi un assurdo. \square

¹⁷⁶Stiamo mettendo $\{S\}$ anziché S , in modo che $S \in \text{tc}(\{S\})$, cosa che nel primo caso non sarebbe avvenuta.

Proposizione 14.19 ($V = V_*$)

$$\forall x \exists \alpha \in \text{Ord} \ x \in V_\alpha.$$

Dimostrazione. Per ϵ -induzione, ci basta dire che, fissato un insieme S , se [ipotesi induttiva] $\forall x \in S \ x \in V_*$, allora [passo induttivo] $S \in V_*$. Consideriamo:

$$\alpha := \sup\{\text{rank}(x) + 1 \mid x \in S\}$$

cioè l'ordinale che corrisponde all'insieme più grande, che contiene tutti gli elementi. Per ogni $x \in S$ abbiamo quindi che $x \in V_{\text{rank}(x)+1} \subseteq V_\alpha$ (cioè ognuno è contenuto nel suo, e sono tutti contenuti da V_α), questa cosa [è una mezza freccia di extensionalità], e dice che $S \subseteq V_\alpha$, quindi $S \in \mathcal{P}(V_\alpha) = V_{\alpha+1} \implies S \in V_*$. Quindi per ϵ -induzione $V = V_*$. \square

Corollario 14.20 (V è transitivo e tutti i suoi insiemi sono costruibili in ZFC)

Non esistono catene infinite discendenti per appartenenza.

Dimostrazione. Avendo dimostrato che $V = V_*$, sappiamo che V è una classe transitiva e ben fondata, quindi non possono esistere al suo interno dei mostri. La buona fondatezza in realtà l'avevamo già gratis assumendo **buona fondazione**, e di conseguenza i mostri non vi erano già, il motivo principale per cui abbiamo dimostrato l'uguaglianza è dire che V è anche transitivo e che la classe di tutti gli insiemi costruibili con gli assiomi 1-9, ossia V_* , coincide proprio con la classe di tutti gli insiemi [esistenti] V (per l'assioma 10). \square

I mostri sono stati sconfitti.

Fine della storia.



Esercizi

Esercizio 14.21 ($|V_{\omega+\alpha}| = \beth_\alpha$). Definiamo $\beth_0^{\text{a}} = \aleph_0$, $\beth_{\alpha+1} = 2^{\beth_\alpha}$, $\beth_\lambda = \sup\{\beth_\alpha | \alpha < \lambda\}$, con λ limite (questi cardinali definiti ricorsivamente si chiamano **beth numbers**). Dimostrare che $\forall \alpha \in \text{Ord} |V_{\omega+\alpha}| = \beth_\alpha$.

^a “beth”.

Lemma 14.22 ($\alpha \leq \beth_\alpha$)

$\forall \alpha \in \text{Ord} \alpha \leq \beth_\alpha^{\text{a}}$

^aIn realtà si può vedere come banale conseguenza del fatto che $\beth_\alpha : \text{Ord} \rightarrow \text{Ord}$ è una funzione classe strettamente crescente tra classi bene ordinate.

Dimostrazione. Per induzione transfinita.

caso 0 $0 \leq \beth_0 = \aleph_0$ è banalmente vero.

caso $s(\alpha)$ Supponiamo $\alpha < \beth_\alpha$ e osserviamo che questo significa $\alpha \leq s(\alpha) \leq \beth_\alpha$ (stiamo usando che $s(\alpha)$ è il più piccolo ordinale maggiore o uguale a α). Da ciò si conclude osservando che per Cantor $\beth_\alpha < 2^{\beth_\alpha} = \beth_{s(\alpha)}$, e mettendo assieme le disuguaglianze $s(\alpha) \leq \beth_{s(\alpha)}$.

caso limite Per ipotesi induttiva abbiamo che $\alpha \leq \beth_\alpha$, per ogni $\alpha < \lambda$, essendo $x \mapsto \beth_x$ una funzione continua per costruzione, tale disuguaglianza passa quindi al sup, per cui si ottiene:

$$\lambda = \sup_{\alpha < \lambda} \alpha \leq \sup_{\alpha < \lambda} \beth_\alpha = \beth_\lambda$$

□

Soluzione. Procediamo per induzione transfinita.

caso 0 $|V_{\omega+0}| = |V_\omega|$, per una proposizione dimostrata sulla gerarchia, sappiamo che $\omega \subseteq V_\omega \implies \aleph_0 \leq |V_\omega|$, d'altra parte:

$$V_\omega = \bigcup_{\alpha \in \omega} V_\alpha \stackrel{\text{inclusione-esclusione}}{\implies} |V_\omega| \leq \sum_{\alpha \in \omega} |V_\alpha| = \max(|\omega|, |V_\alpha|)$$

ma, $|V_\alpha| < \aleph_0$ ¹⁷⁷, quindi abbiamo ottenuto $|V_\omega| \leq \aleph_0$.

caso $s(\alpha)$ Supponiamo $|V_{\omega+\alpha}| = \beth_\alpha$ e osserviamo che $|V_{\omega+s(\alpha)}| = |\mathcal{P}(V_{\omega+\alpha})| = 2^{|V_{\omega+\alpha}|}$, ora usando l'ipotesi induttiva si ottiene:

$$|V_{\omega+s(\alpha)}| = 2^{|V_{\omega+\alpha}|} \stackrel{\text{H.p. indutt.}}{=} 2^{\beth_\alpha} = \beth_{\alpha+1}$$

caso limite Per ipotesi induttiva abbiamo che $|V_{\omega+\alpha}| = \beth_\alpha$, per $\alpha < \lambda$, ci basta osservare che per definizione $V_{\omega+\alpha} \subseteq V_{\omega+\lambda}, \forall \alpha < \lambda$, dunque $|V_{\omega+\alpha}| \leq |V_{\omega+\lambda}|$, ovvero $|V_{\omega+\lambda}|$ è un maggiorante di $\{|V_{\omega+\alpha}| : \alpha < \lambda\}$, per cui:

$$\beth_\lambda = \sup_{\alpha < \lambda} \beth_\alpha \stackrel{\text{H.p. indutt.}}{=} \sup_{\alpha < \lambda} |V_{\omega+\alpha}| \leq |V_{\omega+\lambda}|$$

¹⁷⁷Andrebbe dimostrato che, nel caso di ordinali finiti, si ha $|V_n| = 2^{V_n - 1} \wedge |V_0| = 0$ (è una facile verifica per induzione numerabile), e ciò ci permette di dire $|V_n| \in \omega, \forall n \in \omega$.

mentre, per la disuguaglianza dall'alto, dato che $V_{\omega+\lambda} = \bigcup_{\alpha<\lambda} V_\alpha$, abbiamo:

$$|V_{\omega+\lambda}| \leq \sum_{\alpha<\lambda} |V_{\omega+\alpha}| = \max \left(|\lambda|, \sup_{\alpha<\lambda} |V_{\omega+\alpha}| \right) \stackrel{\text{Hp. indutt.}}{=} \max(|\lambda|, \beth_\lambda) \stackrel{\text{lemma}}{=} \beth_\lambda$$

in tal modo concludiamo anche il caso successore.

□

Osservazione 14.23 — Si noti che con un ragionamento analogo a quello fatto per il caso limite è possibile dimostrare che:

$$|V_\lambda| = \left| \bigcup_{\alpha<\lambda} V_\alpha \right| = \sup_{\alpha<\lambda} |V_\alpha|$$

e analogamente (sfruttando il lemma di sopra):

$$|V_{\omega+\lambda}| = \left| \bigcup_{\alpha<\lambda} V_{\omega+\alpha} \right| = \sup_{\alpha<\lambda} |V_{\omega+\alpha}|$$

Esercizio 14.24 (Caratterizzazione del rango). Dimostrare che vale la seguente identità: $\text{rank}(x) = \sup\{\text{rank}(y) + 1 \mid y \in x\}$.

Soluzione. Abbiamo visto che $y \in x \implies \text{rank}(y) < \text{rank}(x)$, ed essendo ordinali vale $\text{rank}(y) + 1 \leq \text{rank}(x)$, per ogni $y \in x$, dunque $\text{rank}(x)$ è un maggiorante dell'insieme $\{\text{rank}(y) + 1 \mid y \in x\}$. Ci rimane da verificare che sia effettivamente il più piccolo maggiorante. Supponiamo che esista un ordinale α che sia maggiorante dell'insieme e allo stesso tempo $\alpha < \text{rank}(x)$, da questo segue che $\forall y \in x \ y \in V_\alpha$, per cui $x \subseteq V_\alpha \implies x \in V_{\alpha+1}$, pertanto, da definizione, $\text{rank}(x) \leq \alpha$, che è assurdo. □

Esercizio 14.25 (V_ω). Dimostrare che V_ω soddisfa tutti gli assiomi eccetto l'assioma dell'infinito.

Soluzione. Verifichiamo che valgono uno per uno gli assiomi 1-9¹⁷⁸ relativizzati in V_ω , eccetto l'assioma 7, ovvero l'assioma dell'infinito, ricordando che:

$$V_\omega = \bigcup_{\alpha<\omega} V_\alpha$$

(1) **Vuoto:** $\exists x \in V_\omega \ \forall y \in V_\omega \ y \notin x$

Basta prendere come $x = \emptyset \in V_1 = \mathcal{P}(V_0) = \mathcal{P}(\emptyset) = \{\emptyset\}$, tale insieme rispetta la proprietà richiesta e, poiché $\emptyset \in V_1 \in V_\omega$, per transitività [basta quella di V_ω stesso, ma la abbiamo comunque su tutto V_*] $\emptyset \in V_\omega$.

(2) **Estensionalità:** $\forall a, b \in V_\omega (a = b \leftrightarrow \forall x \in V_\omega (x \in a \leftrightarrow x \in b))$

Fissati $a, b \in V_\omega$ osserviamo che, per transitività, i loro elementi sono anch'essi elementi di V_ω , quindi $x \in a$ o $x \in b$ implicano $x \in V_\omega$, per cui si ha:

$$\forall x (x \in a \leftrightarrow x \in b) \leftrightarrow \forall x (x \in V_\omega \wedge (x \in a \leftrightarrow x \in b) \vee x \notin V_\omega \wedge (x \in a \leftrightarrow x \in b))$$

¹⁷⁸Avendo dimostrato che V_* è ben fondata, in automatico lo è anche V_ω , altrimenti si violerebbe il fatto che V_* è ben fondata, pertanto non è necessario verificare che questo assioma valga in V_ω .

ora il secondo elemento dell'OR è sempre falso per quanto detto prima, dunque possiamo escluderlo dall'equivalenza, e ciò ci lascia $\forall x \in V_\omega (x \in a \leftrightarrow x \in b)$. Dunque, per estensionalità, abbiamo l'equivalenza con $a = b$.

- (3) **Separazione:** $\forall A \in V_\omega \exists B \in V_\omega \forall x \in V_\omega x \in B \leftrightarrow (x \in A \wedge \varphi(x))$

Per separazione esiste l'insieme $B := \{x \in A | x \in V_\omega \wedge \varphi(x)\}$. Per ipotesi $A \in V_\omega$, ovvero $A \in V_\alpha$, per qualche α ordinale, pertanto, si ha $B \subseteq A \in V_\alpha$, e per transitività $B \subseteq V_\alpha$, dunque $B \in V_{\alpha+1}$, con $\alpha + 1 < \omega$ perché ω è limite, quindi otteniamo che $B \in V_\omega$.

- (4) **Paio:** $\forall a, b \in V_\omega \exists B \in V_\omega \forall x \in V_\omega x \in B \leftrightarrow (x = a \vee x = b)$

Dati $a, b \in V_\omega$, abbiamo che $a \in V_\alpha$ e $b \in V_\beta$, e, WLOG, possiamo assumere $\alpha \leq \beta$, allora $a, b \in V_\beta$, da cui necessariamente il paio, che esiste per l'assioma non relativizzato, è nelle parti di V_β , $\{a, b\} \in \mathcal{P}(V_\beta) = V_{\beta+1}$, dove naturalmente $\beta + 1 < \omega$, e in questo modo, per transitività, si ottiene che $\{a, b\} \in V_\omega$.

- (5) **Unione:** $\forall A \in V_\omega \exists B \in V_\omega \forall x \in V_\omega x \in B \leftrightarrow \exists y \in A x \in y$

Sia $A \in V_\alpha$, per qualche ordinale $\alpha < \omega$, per transitività, $A \subseteq V_\alpha$, ciò significa che $\bigcup A$, che esiste per unione non relativizzata, ed è l'insieme degli elementi degli elementi di $A \subseteq V_\alpha$, è a sua volta contenuto in V_α (perché gli elementi degli elementi di A per transitività sono a loro volta elementi di V_α), dunque $\bigcup A \subseteq V_\alpha$ ¹⁷⁹ $\implies \bigcup A \in \mathcal{P}(V_\alpha) = V_{\alpha+1}$, e quindi come prima, per transitività si conclude che $\bigcup A \in V_\omega$.

- (6) **Parti:** $\forall A \in V_\omega \exists B \in V_\omega \forall x \in V_\omega x \in B \leftrightarrow x \subseteq B$

Sia $A \in V_\alpha$, quindi per transitività $A \subseteq V_\alpha$, allora si ha $\mathcal{P}(A) \subseteq \mathcal{P}(V_\alpha) = V_{\alpha+1}$, dove le parti esistono per l'assioma non relativizzato, quindi $\mathcal{P}(A) \in \mathcal{P}(V_{s(\alpha)}) = V_{\alpha+2}$, per cui $\mathcal{P}(A) \in V_\omega$.

- (7) **Rimpiazzamento:** $F : V_\omega \rightarrow V_\omega$ funzione classe e $X \in V_\omega \rightarrow F[X] \in V_\omega$

Sia $X \in V_\alpha$, per transitività, $\forall x \in X \rightarrow x \in V_\alpha$, cioè $X \subseteq V_\alpha$, dunque è ben definita $F[X]$ in quanto possiamo fare $F(a)$ per ogni $a \in X$, perché, come detto, $a \in V_\alpha \in V_\omega$. A questo punto, definiamo $\alpha_a := \min\{\gamma \in \omega | F(a) \in V_\gamma\}$ e $\beta := \sup\{\alpha_a\}_{a \in X}$, e osserviamo che l'insieme su cui stiamo prendendo il sup è finito, in quanto $|F[X]| \leq |X| \leq |V_\alpha| = 2^{|V_{\alpha-1}|}$ ¹⁸⁰ (e qui stiamo usando che $\alpha \in \omega$), dunque ha proprio un massimo $\beta \in \omega$, per cui $F(a) \in V_\beta$, $\forall a \in X$, ovvero $F[x] \subseteq V_\beta \implies F[X] \in V_{\beta+1}$, e per transitività $F[X] \in V_\omega$.

- (8) **Scelta:** $\forall X \in V_\omega (\forall y \in X y \neq \emptyset)^{181} \rightarrow \exists f \in V_\omega$ funzione di scelta su X

Sia f una funzione di scelta su $X \in V_\alpha$, che esiste per AC, sappiamo che $f \in {}^X \bigcup X$, cioè $f \in \mathcal{P}(X \times \bigcup X)$. Ricordando che $X \times \bigcup X \subseteq \mathcal{P}(\mathcal{P}(X \cup \bigcup X))$ e che $X \subseteq V_\alpha$ (che vale per transitività) implica $\bigcup X \subseteq V_\alpha$, abbiamo:

$$X \cup \bigcup X \subseteq V_\alpha \implies f \in \mathcal{P}\left(\mathcal{P}\left(X \cup \bigcup X\right)\right) \subseteq \mathcal{P}(\mathcal{P}(\mathcal{P}(V_\alpha))) = V_{\alpha+3}$$

naturalmente $\alpha + 3 < \omega$, quindi $V_{\alpha+3} \in V_\omega$, e per transitività si ha che $f \in V_\omega$.

Infine, non ci resta che verificare che V_ω non soddisfa l'assioma dell'infinito, in primis osserviamo che $\omega \notin V_\omega$, in quanto $\text{rank}(\omega) = \omega$, inoltre se esistesse un insieme induttivo

¹⁷⁹ Osserviamo che in generale $A \subseteq B \implies \bigcup A \subseteq B \iff B$ è transitivo.

¹⁸⁰ Osserviamo sempre che ciò esclude il caso banale, e che andrebbe dimostrato che $|V_n| = 2^{|V_{n-1}|} \wedge |V_0| = 0$ (è una facilissima induzione numerabile) per poter assicurare la finitezza di ciò che stiamo facendo.

¹⁸¹ Cioè se $\emptyset \notin X$.

$X \in V_\omega$, poiché avevamo definito ω come l'intersezione della classe di tutti gli insiemi induttivi, avremmo che $\omega \subseteq X$, e siccome $X \in V_\omega \implies X \in V_\alpha$, per $\alpha < \omega$, si ha che $\omega \in V_{\alpha+1} \in V_\omega \implies \omega \in V_\omega$. \square

Osservazione 14.26 (Esistenza di insiemi infiniti) — L'esercizio appena risolto ha come conseguenza che l'esistenza di un insieme induttivo è indipendente dagli assiomi della ZFC ad eccezione dell'assioma dell'infinito, e ciò ci dà appunto una giustificazione all'introduzione di tale assioma. In particolare senza questo insieme non possiamo costruire ω e quindi nessun altro insieme infinito (potremmo costruire solo insiemi ereditariamente finiti usando gli altri assiomi), pertanto si capisce ancora meglio perché l'assioma dell'infinito ci garantisce la possibilità di definire insiemi infiniti.

Esercizio 14.27 ($V_{\omega+\omega}$). Dimostrare che $V_{\omega+\omega}$ soddisfa tutti gli assiomi eccetto l'assioma del rimpiazzamento.

Soluzione. Verifichiamo che valgono uno per uno gli assiomi 1-9¹⁸² relativizzati in $V_{\omega+\omega}$, eccetto l'assioma 8, ovvero l'assioma del rimpiazzamento, ricordando che:

$$V_{\omega+\omega} = \bigcup_{\alpha<\omega} V_{\omega+\alpha}$$

(1) **Vuoto:** $\exists x \in V_{\omega+\omega} \forall y \in V_{\omega+\omega} y \notin x$

Basta prendere come $x = \emptyset \in V_1 = \mathcal{P}(V_0) = \mathcal{P}(\emptyset) = \{\emptyset\}$, tale insieme rispetta la proprietà richiesta e, poiché $\emptyset \in V_1 \in V_{\omega+\omega}$, per transitività [basta quella di $V_{\omega+\omega}$ stesso, ma la abbiamo comunque su tutto V_*] $\emptyset \in V_{\omega+\omega}$.

(2) **Estensionalità:** $\forall a, b \in V_{\omega+\omega} (a = b \leftrightarrow \forall x \in V_{\omega+\omega} (x \in a \leftrightarrow x \in b))$

Fissati $a, b \in V_{\omega+\omega}$ osserviamo che, per transitività, i loro elementi sono anch'essi elementi di $V_{\omega+\omega}$, quindi $x \in a$ o $x \in b$ implicano $x \in V_{\omega+\omega}$, per cui si ha:

$$\forall x (x \in a \leftrightarrow x \in b) \leftrightarrow \forall x (x \in V_{\omega+\omega} \wedge (x \in a \leftrightarrow x \in b) \vee x \notin V_{\omega+\omega} \wedge (x \in a \leftrightarrow x \in b))$$

ora il secondo elemento dell'OR è sempre falso per quanto detto prima, dunque possiamo escluderlo dall'equivalenza, e ciò ci lascia $\forall x \in V_{\omega+\omega} (x \in a \leftrightarrow x \in b)$. Dunque, per estensionalità, abbiamo l'equivalenza con $a = b$.

(3) **Separazione:** $\forall A \in V_{\omega+\omega} \exists B \in V_{\omega+\omega} \forall x \in V_{\omega+\omega} x \in B \leftrightarrow (x \in A \wedge \varphi(x))$

Per separazione esiste l'insieme $B := \{x \in A | x \in V_{\omega+\omega} \wedge \varphi(x)\}$. Per ipotesi $A \in V_{\omega+\omega}$, ovvero $A \in V_\alpha$, per qualche α ordinale, pertanto, si ha $B \subseteq A \in V_\alpha$, e per transitività $B \subseteq V_\alpha$, dunque $B \in V_{\alpha+1}$, con $\alpha + 1 < \omega + \omega$ perché $\omega + \omega$ è limite, quindi otteniamo che $B \in V_{\omega+\omega}$.

(4) **Paio:** $\forall a, b \in V_{\omega+\omega} \exists B \in V_{\omega+\omega} \forall x \in V_{\omega+\omega} x \in B \leftrightarrow (x = a \vee x = b)$

Dati $a, b \in V_{\omega+\omega}$, abbiamo che $a \in V_\alpha$ e $b \in V_\beta$, e, WLOG, possiamo assumere $\alpha \leq \beta$, allora $a, b \in V_\beta$, da cui necessariamente il paio, che esiste per l'assioma non relativizzato, è nelle parti di V_β , $\{a, b\} \in \mathcal{P}(V_\beta) = V_{\beta+1}$, dove naturalmente $\beta + 1 < \omega + \omega$, e in questo modo, per transitività, si ottiene che $\{a, b\} \in V_{\omega+\omega}$.

¹⁸²Esattamente come per V_ω non è necessario dimostrare che valga buona fondazione.

(5) **Unione:** $\forall A \in V_{\omega+\omega} \exists B \in V_{\omega+\omega} \forall x \in V_{\omega+\omega} x \in B \leftrightarrow \exists y \in A x \in y$

Sia $A \in V_\alpha$, per qualche ordinale $\alpha < \omega + \omega$, per transitività, $A \subseteq V_\alpha$, ciò significa che $\bigcup A$, che esiste per unione non relativizzata, ed è l'insieme degli elementi degli elementi di $A \subseteq V_\alpha$, è a sua volta contenuto in V_α (perché gli elementi degli elementi di A per transitività sono a loro volta elementi di V_α), dunque $\bigcup A \subseteq V_\alpha$ ¹⁸³ $\implies \bigcup A \in \mathcal{P}(V_\alpha) = V_{\alpha+1}$, e quindi come prima, per transitività si conclude che $\bigcup A \in V_{\omega+\omega}$.

(6) **Parti:** $\forall A \in V_{\omega+\omega} \exists B \in V_{\omega+\omega} \forall x \in V_{\omega+\omega} x \in B \leftrightarrow x \subseteq B$

Sia $A \in V_\alpha$, quindi per transitività $A \subseteq V_\alpha$, allora si ha $\mathcal{P}(A) \subseteq \mathcal{P}(V_\alpha) = V_{\alpha+1}$, dove le parti esistono per l'assioma non relativizzato, quindi $\mathcal{P}(A) \in \mathcal{P}(V_{s(\alpha)}) = V_{\alpha+2}$, per cui $\mathcal{P}(A) \in V_{\omega+\omega}$.

(7) **Infinito:** $\exists X \in V_{\omega+\omega} \emptyset \in X \wedge \forall x \in X \rightarrow x \cup \{x\} \in X$

Basta prendere $X = \omega \in V_{\omega+1}$, con $V_{\omega+1} \in V_{\omega+\omega}$, e per transitività $X \in V_{\omega+\omega}$.

(8) **Scelta:** $\forall X \in V_{\omega+\omega} (\forall y \in X y \neq \emptyset)^{184} \rightarrow \exists f \in V_{\omega+\omega} \text{ funzione di scelta su } X$

Sia f una funzione di scelta su $X \in V_\alpha$, che esiste per AC, sappiamo che $f \in {}^X \bigcup X$, cioè $f \in \mathcal{P}(X \times \bigcup X)$. Ricordando che $X \times \bigcup X \subseteq \mathcal{P}(\mathcal{P}(X \cup \bigcup X))$ e che $X \subseteq V_\alpha$ (che vale per transitività) implica $\bigcup X \subseteq V_\alpha$, abbiamo:

$$X \cup \bigcup X \subseteq V_\alpha \implies f \in \mathcal{P}(\mathcal{P}(\mathcal{P}(X \cup \bigcup X))) \subseteq \mathcal{P}(\mathcal{P}(\mathcal{P}(V_\alpha))) = V_{\alpha+3}$$

naturalmente $\alpha + 3 < \omega + \omega$, quindi $V_{\alpha+3} \in V_{\omega+\omega}$, e per transitività si ha che $f \in V_{\omega+\omega}$.

Infine, dobbiamo dimostrare che non vale l'assioma del rimpiazzamento, osserviamo in primis che l'argomento utilizzato per dimostrare la validità di questo assioma per V_ω qui fallisce in quanto β non è necessariamente finito, ed in particolare potrebbe accadere che $\beta = \omega + \omega$, il che implicherebbe $F[X] \in V_{\omega+\omega+1}$, e ciò fa fallire la dimostrazione in questo caso. Supponiamo per assurdo che $V_{\omega+\omega}$ soddisfi l'assioma del rimpiazzamento, allora esiste l'insieme $\omega + \omega \in V_{\omega+\omega}$, per la dimostrazione vista che ogni classe di isomorfismo ha associato un ordinale (ed in particolare ci basta prendere l'ordinale associato all'insieme di vuoto e ω in un numero finito di singoletti che abbiamo visto in un esercizio nella sezione sugli ordinali), ma ciò è assurdo in quanto, per la proprietà del rango di un ordinale, si ha $\text{rank}(\omega + \omega) = \omega + \omega \implies \omega + \omega \notin V_{\omega+\omega}$. \square

Esercizio 14.28 (Rimpiazzamento $\implies \exists \omega + \omega$). Dimostrare che l'esistenza dell'ordinale $\omega + \omega$ non segue dagli assiomi della teoria degli insiemi, escluso l'assioma del rimpiazzamento, a patto che questi non si contraddicono.

Soluzione. Se per assurdo l'esistenza di $\omega + \omega$ seguisse dagli assiomi della ZFC tranne rimpiazzamento, assumendo che sono coerenti (e quindi non si contraddicono, altrimenti potremmo dimostrare qualsiasi cosa), allora un tale ordinale esisterebbe anche in $V_{\omega+\omega}$, visto che abbiamo dimostrato che in tale insieme valgono tutti gli assiomi tranne appunto rimpiazzamento. Tuttavia, sappiamo che $\text{rank}(\omega + \omega) = \omega + \omega$, quindi $\omega + \omega \notin V_{\omega+\omega}$, pertanto ciò è assurdo. Abbiamo quindi dimostrato che l'esistenza dell'ordinale $\omega + \omega$ è indipendente dagli assiomi della ZFC, escluso il rimpiazzamento. \square

¹⁸³Osserviamo che in generale $A \subseteq B \implies \bigcup A \subseteq B \iff B$ è transitivo.

¹⁸⁴Cioè se $\emptyset \notin X$.

Esercizio 14.29 (V_κ - κ fortemente inaccessibile). Dimostrare che, se κ è [fortemente] inaccessibile, allora tutti gli assiomi della teoria degli insiemi valgono in V_κ .

Soluzione. Ricordiamo innanzitutto che κ fortemente inaccessibile significa che κ è un ordinale iniziale (quindi limite) regolare, $\text{cof}(\kappa) = \kappa$, ed è limite forte, cioè $\aleph_0 < \kappa$ e $\forall \alpha \aleph_\alpha < \kappa \rightarrow 2^{\aleph_\alpha} < \kappa$. Ciò significa che $\omega < \kappa \rightarrow V_\omega \in V_\kappa$.¹⁸⁵

(1) **Vuoto:** $\exists x \in V_\kappa \forall y \in V_\kappa y \notin x$

Basta prendere come $x = \emptyset \in V_1 = \mathcal{P}(V_0) = \mathcal{P}(\emptyset) = \{\emptyset\}$, tale insieme rispetta la proprietà richiesta e, poiché $\emptyset \in V_1 \in V_\kappa$, per transitività [basta quella di V_κ stesso, ma la abbiamo comunque su tutto V_*] $\emptyset \in V_\kappa$.

(2) **Estensionalità:** $\forall a, b \in V_\kappa (a = b \leftrightarrow \forall x \in V_\kappa (x \in a \leftrightarrow x \in b))$

Fissati $a, b \in V_\kappa$ osserviamo che, per transitività, i loro elementi sono anch'essi elementi di V_κ , quindi $x \in a$ o $x \in b$ implicano $x \in V_\kappa$, per cui si ha:

$$\forall x(x \in a \leftrightarrow x \in b) \leftrightarrow \forall x(x \in V_\kappa \wedge (x \in a \leftrightarrow x \in b) \vee x \notin V_\kappa \wedge (x \in a \leftrightarrow x \in b))$$

ora il secondo elemento dell'OR è sempre falso per quanto detto prima, dunque possiamo escluderlo dall'equivalenza, e ciò ci lascia $\forall x \in V_\kappa (x \in a \leftrightarrow x \in b)$. Dunque, per estensionalità, abbiamo l'equivalenza con $a = b$.

(3) **Separazione:** $\forall A \in V_\kappa \exists B \in V_\kappa \forall x \in V_\kappa x \in B \leftrightarrow (x \in A \wedge \varphi(x))$

Per separazione esiste l'insieme $B := \{x \in A | x \in V_\kappa \wedge \varphi(x)\}$. Per ipotesi $A \in V_\kappa$, ovvero $A \in V_\alpha$, per qualche α ordinale, pertanto, si ha $B \subseteq A \in V_\alpha$, e per transitività $B \subseteq V_\alpha$, dunque $B \in V_{\alpha+1}$, con $\alpha + 1 < \kappa$ perché κ è limite, quindi otteniamo che $B \in V_\kappa$.

(4) **Paio:** $\forall a, b \in V_\kappa \exists B \in V_\kappa \forall x \in V_\kappa x \in B \leftrightarrow (x = a \vee x = b)$

Dati $a, b \in V_\kappa$, abbiamo che $a \in V_\alpha$ e $b \in V_\beta$, e, WLOG, possiamo assumere $\alpha \leq \beta$, allora $a, b \in V_\beta$, da cui necessariamente il paio, che esiste per l'assioma non relativizzato, è nelle parti di V_β , $\{a, b\} \in \mathcal{P}(V_\beta) = V_{\beta+1}$, dove naturalmente $\beta + 1 < \kappa$, e in questo modo, per transitività, si ottiene che $\{a, b\} \in V_\kappa$.

(5) **Unione:** $\forall A \in V_\kappa \exists B \in V_\kappa \forall x \in V_\kappa x \in B \leftrightarrow \exists y \in A x \in y$

Sia $A \in V_\alpha$, per qualche ordinale $\alpha < \kappa$, per transitività, $A \subseteq V_\alpha$, ciò significa che $\bigcup A$, che esiste per unione non relativizzata, ed è l'insieme degli elementi degli elementi di $A \subseteq V_\alpha$, è a sua volta contenuto in V_α (perché gli elementi degli elementi di A per transitività sono a loro volta elementi di V_α), dunque $\bigcup A \subseteq V_\alpha$ ¹⁸⁶ $\implies \bigcup A \in \mathcal{P}(V_\alpha) = V_{\alpha+1}$, e quindi come prima, per transitività si conclude che $\bigcup A \in V_\kappa$.

(6) **Parti:** $\forall A \in V_\kappa \exists B \in V_\kappa \forall x \in V_\kappa x \in B \leftrightarrow x \subseteq B$

Sia $A \in V_\alpha$, quindi per transitività $A \subseteq V_\alpha$, allora si ha $\mathcal{P}(A) \subseteq \mathcal{P}(V_\alpha) = V_{\alpha+1}$, dove le parti esistono per l'assioma non relativizzato, quindi $\mathcal{P}(A) \in \mathcal{P}(V_{s(\alpha)}) = V_{\alpha+2}$, per cui $\mathcal{P}(A) \in V_\kappa$.

(7) **Infinito:** $\exists X \in V_\kappa \emptyset \in X \wedge \forall x \in X \rightarrow x \cup \{x\} \in X$

Basta prendere $X = \omega \in V_{\omega+1}$, con $V_{\omega+1} \in V_\kappa$, e per transitività $X \in V_\kappa$.

¹⁸⁵Come al solito V_* è ben fondata, dunque non è necessario verificare buona fondazione in V_κ , in quanto è già dato.

¹⁸⁶Osserviamo che in generale $A \subseteq B \implies \bigcup A \subseteq B \iff B$ è transitivo.

(8) **Scelta:** $\forall X \in V_\kappa (\forall y \in X y \neq \emptyset)^{187} \rightarrow \exists f \in V_\kappa$ funzione di scelta su X

Sia f una funzione di scelta su $X \in V_\alpha$, che esiste per AC, sappiamo che $f \in {}^X \cup X$, cioè $f \in \mathcal{P}(X \times \bigcup X)$. Ricordando che $X \times \bigcup X \subseteq \mathcal{P}(\mathcal{P}(X \cup \bigcup X))$ e che $X \subseteq V_\alpha$ (che vale per transitività) implica $\bigcup X \subseteq V_\alpha$, abbiamo:

$$X \cup \bigcup X \subseteq V_\alpha \implies f \in \mathcal{P}\left(\mathcal{P}\left(\mathcal{P}(X \cup \bigcup X)\right)\right) \subseteq \mathcal{P}(\mathcal{P}(\mathcal{P}(V_\alpha))) = V_{\alpha+3}$$

naturalmente $\alpha + 3 < \kappa$, quindi $V_{\alpha+3} \in V_\kappa$, e per transitività si ha che $f \in V_\kappa$.

(9) **Rimpiazzamento:** $F : V_\kappa \rightarrow V_\kappa$ funzione classe e $X \in V_\kappa \rightarrow F[X] \in V_\kappa$

Sia $X \in V_\alpha$, con $\alpha < \kappa$, per transitività, $\forall x \in X \rightarrow x \in V_\alpha$, cioè $X \subseteq V_\alpha$, dunque è ben definita $F[X]$ in quanto possiamo fare $F(a)$ per ogni $a \in X$, perché, come detto, $a \in V_\alpha \in V_\kappa$, inoltre $F(a) \in V_\kappa$ per definizione di F . A questo punto, definiamo $\alpha_a := \min\{\gamma \in \kappa | F(a) \in V_\gamma\}^{188}$ e $\beta := \sup\{\alpha_a\}_{a \in X}$, essendo $F : V_\kappa \rightarrow V_\kappa$ abbiamo che $\beta \leq \kappa$, se escludiamo che $\beta = \kappa$, allora $\beta < \kappa$, per cui, essendo κ limite, $\beta + 1 < \kappa$ ed a questo punto abbiamo $F[X] \subseteq V_\beta \implies F[X] \in V_{\beta+1} \in V_\kappa$ e si conclude per transitività.

Ci rimane quindi da escludere che $\beta = \kappa$. Per ipotesi sappiamo che $\beta = \kappa = \text{cof}(\kappa)$, osserviamo che $\{\alpha_a | a \in X\}$ è un sottoinsieme cofinale di β praticamente perché β è l'estremo superiore di questo insieme (dunque la definizione di sottoinsieme cofinale è verificata immediatamente), inoltre si ha $|\{\alpha_a | a \in X\}| \leq |X|$ (ci basta considerare la mappa $x \mapsto \alpha_x$ che è surgettiva¹⁸⁹), a questo punto, se verifichiamo che $|X| < \kappa$ abbiamo un assurdo:

$$\kappa = \text{cof}(\kappa) = \text{cof}(\beta) \leq |X| < \kappa \not\models$$

Per dimostrare l'ultima cosa ci basta dimostrare per induzione transfinita che $|V_\alpha| < \kappa, \forall \alpha < \kappa$, da cui si ha $X \subseteq V_\alpha \implies |X| \leq |V_\alpha| < \kappa, \alpha < \kappa$.

caso 0 È ovvio che $0 = |V_0| < \kappa$, in quanto $\kappa > \aleph_0$ poiché limite forte.

caso successore Supponiamo $|V_\alpha| < \kappa$, a questo punto $|V_{\alpha+1}| = 2^{|V_\alpha|} < \kappa$, dove l'ultima disegualanza vale perché κ è limite forte.

caso limite Abbiamo per ipotesi $|V_\alpha| < \kappa$, per $\alpha < \lambda < \kappa$, dunque:

$$|V_\lambda| = \left| \bigcup_{\alpha < \lambda} V_\alpha \right| \leq \sum_{\alpha < \lambda} |V_\alpha| = |\lambda| \cdot \sup_{\alpha < \lambda} |V_\alpha| \leq \kappa$$

ora, essendo che $|\lambda| < \kappa$ e per ipotesi induttiva $|V_\alpha| < \kappa$, con $\alpha < \kappa$, se la somma facesse κ , avremmo trovato una stima dall'alto per la cofinalità, data da $|\lambda| < \kappa$, ma $\text{cof}(\kappa) = \kappa$, dunque ciò è assurdo, e la somma è $< \kappa$.

□

Osservazione 14.30 (Alternativa per il rimpiazzamento in V_κ) — Il punto chiave della dimostrazione della validità dell'assioma del rimpiazzamento in V_κ è l'assurdo ottenuto violando il fatto che κ sia regolare, questa cosa può essere fatta anche ragionando sulla prima definizione data di cofinalità, così da escludere che $\beta = \kappa$. Per verificare che $\beta < \kappa$ è sufficiente verificare che $|\beta| < \kappa$, essendo κ un ordinale

¹⁸⁷Cioè se $\emptyset \notin X$.

¹⁸⁸Per la precisione, per definizione di F e V_κ , si ha $F(a) \in V_\kappa \rightarrow F(a) \in V_\gamma, \gamma \in \kappa$. Dunque gli α_a sono tutti strettamente minori di κ , il problema è che potrebbe non esserlo il loro sup.

¹⁸⁹Per la precisione $X \rightarrowtail s[\text{rank}[X]] : x \rightarrow \alpha_x$, dove l'insieme d'arrivo è un insieme per rimpiazzamento non relativizzato.

iniziale, e, essendo $\beta = \bigcup_{a \in X} \alpha_a$ si ha:

$$|\beta| \leq \sum_{a \in X} |\alpha_a| = |X| \cdot \sup_{a \in X} |\alpha_a|$$

a questo punto, come nella dimostrazione sopra, sappiamo che $|X| < \kappa$, per cui, se la somma sopra fosse uguale a κ , allora il sup sarebbe uguale a κ , ma $|\alpha_a| < \kappa, \forall a \in X$, in quanto $a \in X$, per cui avremmo ottenuto una stima dall'alto per la cofinalità (v.1) di κ (cioè avremmo ottenuto che κ si può scrivere come somma di cose più piccole un numero di volte $< \kappa$) che è assurda in quanto $\kappa = \text{cof}(\kappa) \leq |X| < \kappa$. Segue quindi che la somma è minore strettamente di κ , dunque $|\beta| < \kappa$.^a

^aIdea proposta da Rubens Alessio Martino.

Esercizio 14.31 (ZFC $\not\Rightarrow$ esiste un cardinale fortemente inaccessibile). Dimostrare che, se la teoria degli insiemi è coerente, allora non dimostra l'esistenza di un cardinale [fortemente] inaccessibile.

Soluzione. Se per assurdo l'esistenza di un cardinale fortemente inaccessibile κ seguisse dagli assiomi della ZFC, assumendo che sono coerenti (e quindi non si contraddicono, altrimenti potremmo dimostrare qualsiasi cosa), allora, per quanto dimostrato nell'esercizio precedente, l'esistenza di κ seguirebbe anche in V_κ , avendo dimostrato che anche qui valgono tutti gli assiomi. Tuttavia ciò è assurdo in quanto $\text{rank}(\kappa) = \kappa$ (κ è un cardinale, dunque un ordinale iniziale, quindi vale anche per lui la proprietà del rango degli ordinali), quindi $\kappa \notin V_\kappa$, pertanto l'esistenza di un cardinale fortemente inaccessibile è indipendente dagli assiomi della ZFC. \square

Osservazione 14.32 (V_κ - κ debolmente inaccessibile) — Si potrebbe essere tentati di dimostrare che anche nel caso di V_κ , con κ cardinale debolmente inaccessibile siano verificati tutti gli assiomi della ZFC, ed in effetti lo sono tutti ad eccezione del rimpiazzamento. In particolare, non solo la dimostrazione fatta nel caso di κ fortemente inaccessibile non funziona (poiché avevamo usato l'ipotesi di limite forte), ma si verifica addirittura che rimpiazzamento non può proprio valere in V_κ , con κ debolmente inaccessibile.

Dimostrazione. Sia V_κ , con κ cardinale debolmente inaccessibile, essendo che κ non è limite forte, esiste almeno un cardinale $\lambda < \kappa$, tale che $2^\lambda \geq \kappa$. A questo punto ci basta considerare l'Hartogs $H(2^\lambda) > 2^\lambda$, se valesse il rimpiazzamento si avrebbe che $H(2^\lambda) \in V_\kappa$, ma, d'altra parte, si ha:

$$\kappa \leq 2^\lambda < H(2^\lambda) \in V_\kappa \implies \kappa \in H(2^\lambda) \in V_\kappa \implies \kappa \in V_\kappa \not\subseteq$$

\square

Osservazione 14.33 (Esistenza di un cardinale debolmente inaccessibile in ZFC) — L'esistenza di cardinali debolmente inaccessibili, analogamente a quella dei fortemente inaccessibili, è indipendente dalla ZFC, ma non possiamo dimostrarlo usando solo la gerarchia di Von Neumann come fatto nel caso dei fortemente inaccessibili per il motivo appena visto.

§A Appendice

§A.1 Cardinalità note

In questa sezione risolviamo gli esercizi lasciati nel foglio di esercizi [5], proposto a metà del corso dal prof. Mamino (le note aggiunte sono quelle del prof. stesso alle soluzioni da lui proposte [6]).

Esercizio A.1 (Cardinalità di base). Determinare le seguenti cardinalità.

- $|\text{numeri irrazionali}| = |\mathbb{R} \setminus \mathbb{Q}|$

Soluzione. (Senza AC)

Poiché \mathbb{R} è continuo e \mathbb{Q} numerabile, per il lemma, la differenza rimane continua e quindi $|\mathbb{R} \setminus \mathbb{Q}| = 2^{\aleph_0}$. \square

Nota A.2 (Sulla sottrazione di cardinalità) — In sostanza $2^{\aleph_0} - \aleph_0 = 2^{\aleph_0}$, ma scrivere questa sottrazione sarebbe SBAGLIATO, perché, in generale, la differenza di cardinalità non è definita. Sarebbe anche SBAGLIATO PENSARE che stiamo usando il fatto che $2^{\aleph_0} + \aleph_0 = 2^{\aleph_0}$, infatti, da questa uguaglianza, **non** si deduce che se $|X| + \aleph_0 = 2^{\aleph_0}$ allora $|X| = 2^{\aleph_0}$. In realtà stiamo usando un lemma visto a lezione (dimostrato senza AC):

$$|A| = 2^{\aleph_0} \wedge B \subseteq A \wedge |B| \leq \aleph_0 \rightarrow |A \setminus B| = 2^{\aleph_0}$$

e la soluzione cita esattamente le ipotesi del lemma.

- $|\text{reali trascendenti}| = |\mathbb{R} \setminus \mathbb{A}_{\mathbb{R}}|$

Soluzione. (Senza AC)

Abbiamo già dimostrato che $|\mathbb{A}_{\mathbb{R}}| = \aleph_0$, quindi per il lemma, si ha $|\mathbb{R} \setminus \mathbb{A}_{\mathbb{R}}| = 2^{\aleph_0}$. \square

- $|\text{sottoinsiemi infiniti di } \omega| = |\mathcal{P}(\omega) \setminus \mathcal{P}^{\text{fin.}}(\omega)|$

Soluzione. (Senza AC)

Abbiamo dimostrato che $|\mathcal{P}^{\text{fin.}}(\omega)| = \aleph_0$ e dal lemma si ottiene $|\mathcal{P}(\omega) \setminus \mathcal{P}^{\text{fin.}}(\omega)| = 2^{\aleph_0}$. \square

- $|\text{sottoinsiemi finiti di } \mathbb{R}| = |\mathcal{P}^{\text{fin.}}(\mathbb{R})|^{190}$

Idea: Va da sé che i sottoinsiemi finiti di \mathbb{R} sono almeno tanti quanti i reali stessi. D'altro canto, se avessimo l'assioma della scelta, potremmo dimostrare, che, fatto per altro intuitivo, l'immagine di una funzione ha cardinalità al più pari al dominio: $|f[X]| \leq |X|$.¹⁹¹ Siccome ogni insieme finito di reali è immagine di una successione di reali, considerando la funzione f che manda una successione nella sua immagine avremmo $|\text{sottoinsiemi finite dei reali}| \leq |\text{successioni di reali}| = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0}$. Per aggirare il lemma vietato $|f[X]| \leq |X|$, possiamo lavorare al contrario, cercando una funzione iniettiva che manda i sottoinsiemi finiti di \mathbb{R} nella successioni.

¹⁹⁰È banale con AC, poiché lo abbiamo dimostrato in generale, che $|\mathcal{P}^{\text{fin.}}(\mathbb{R})| = |\mathbb{R}| = 2^{\aleph_0}$.

¹⁹¹In realtà abbiamo dimostrato per esercizio che questa cosa è vera anche senza AC nel caso in cui l'insieme sia finito, ma la dimostrazione si adatta subito al caso al più numerabile (assieme anche al fatto che le diseguaglianze di surgettività, sempre nel caso di insiemi al più numerabili, sono valide anche senza AC).

Soluzione. È facile vedere la funzione $\mathbb{R} \hookrightarrow \mathcal{P}^{\text{fin.}}(\mathbb{R}) : x \mapsto \{x\}$ è iniettiva e ci dà la disuguaglianza dal basso $2^{\aleph_0} \leq |\mathcal{P}^{\text{fin.}}(\mathbb{R})|$. Viceversa, dato $A \in \mathcal{P}^{\text{fin.}}(\mathbb{R})$, per definizione esiste $n \in \omega$ tale che $n = |A|$, quindi possiamo definire la funzione $\mathcal{P}^{\text{fin.}}(\mathbb{R}) \rightarrow {}^\omega(\mathbb{R} \cup \{\spadesuit\}) : A \mapsto a_i$, dove:

$$a_i = \begin{cases} \min_{\mathbb{R}|A}(A \setminus \text{Im}(a_{|i})) & \text{se } i < n \\ \spadesuit & \text{se } i \geq n \end{cases}$$

in tal modo si ha che $\text{Im}(a_{|i}) \cap \mathbb{R} = A$. Quindi segue facilmente che questa mappa è iniettiva (due successioni con la stessa immagine, per la proprietà appena menzionata, danno lo stesso insieme usato in partenza) e ci dà la disuguaglianza dall'alto $|\mathcal{P}^{\text{fin.}}(\mathbb{R})| \leq |\mathbb{R} \cup \{\spadesuit\}| \leq 2^{\aleph_0}$ (dove l'ultima uguaglianza è inclusione-esclusione). ¹⁹² \square

Soluzione. (Soluzione alternativa buffa (idea)) La funzione $g : \mathcal{P}^{\text{fin.}}(\mathbb{R}) \rightarrow {}^\omega\mathbb{R} : X \mapsto g(X)$ definita da:

$$g(X) : n \mapsto \sum_{x \in X} e^{n \cdot x}$$

è iniettiva. \square

- $|\text{sottoinsiemi infiniti di } \mathbb{R}| = |\mathcal{P}(\mathbb{R}) \setminus \mathcal{P}^{\text{fin.}}(\mathbb{R})| = |\mathcal{P}^{\text{inf.}}(\mathbb{R})|$

Soluzione. (Senza AC)

Ovviamente $\mathcal{P}^{\text{inf.}}(\mathbb{R}) := \mathcal{P}(\mathbb{R}) \setminus \mathcal{P}^{\text{fin.}}(\mathbb{R}) \subseteq \mathcal{P}(\mathbb{R}) \implies |\mathcal{P}^{\text{inf.}}(\mathbb{R})| \leq 2^{2^{\aleph_0}}$. Viceversa (per la caratterizzazione di $(\mathbb{R}, <)$ come ordine) abbiamo che $|]0, 1[| = |\mathbb{R}|$, quindi abbiamo almeno una bigezione g tra i due insiemi, da questa possiamo definire:

$$\mathcal{P}(\mathbb{R}) \rightarrow \mathcal{P}^{\text{inf.}}(\mathbb{R}) : X \mapsto g[X] \cup]1, 2[$$

essendo g una mappa bigettiva preserva la cardinalità degli insiemi, e unendo $(1, 2)$ alla fine otteniamo necessariamente insiemi tutti infiniti [il problema si poneva solo per insiemi finiti in partenza], per cui la mappa è ben definita. Inoltre la funzione è anche iniettiva in quanto due insiemi in arrivo, $g[X] \cup]1, 2[$ e $g[Y] \cup]1, 2[$, sono uguali se e solo se $g[X] = g[Y]$, ma g è una bigezione, quindi questa cosa equivale a $X = Y$. Abbiamo così ottenuto che $2^{2^{\aleph_0}} \leq |\mathcal{P}^{\text{inf.}}(\mathbb{R})|$. Un'alternativa per quest'ultima disuguaglianza, osservando che $|\mathcal{P}(]0, 1[)| = 2^{2^{\aleph_0}}$ può essere:

$$\mathcal{P}(]0, 1[) \rightarrow \mathcal{P}^{\text{inf.}}(\mathbb{R}) : X \mapsto \begin{cases} X & \text{se } X \text{ è infinito} \\ \mathbb{R} \setminus X & \text{se } X \text{ è finito} \end{cases}$$

che è iniettiva perché dati $X, Y \in \mathcal{P}(]0, 1[)$ in partenza, se sono entrambi infiniti o finiti è banale che se sono uguali vanno in cose uguali, mentre se sono uno finito e l'altro infinito, in arrivo l'infinito è contenuto in $]0, 1[$ mentre il finito diventa un sottoinsieme di \mathbb{R} che comprende anche punti al di fuori di $]0, 1[$ (in tal modo sono distinti e l'iniettività è preservata). \square

Soluzione. (Soluzione alternativa, senza AC)

La stima dall'alto è sempre la stessa, mentre dal basso, osservando che $|\mathbb{R} \cup \{\spadesuit\}| = |\mathbb{R}|$, possiamo definire la mappa:

$$f : \mathcal{P}(\mathbb{R}) \rightarrow \mathcal{P}^{\text{inf.}}(\mathbb{R} \cup \{\spadesuit\}) : A \mapsto \begin{cases} A & \text{se } A \text{ è infinito} \\ (\mathbb{R} \setminus A) \cup \{\spadesuit\} & \text{se } A \text{ è finito} \end{cases}$$

¹⁹²Osservare che questa identica dimostrazione funziona per tutte le parti finite di un insieme in cui abbiamo un modo per scegliere un elemento da un suo sottoinsieme, mentre fallisce su ω [nonostante qui il modo di scegliere lo abbiamo] in quanto qualsiasi insieme di successioni su un insieme infinito ha almeno sempre cardinalità $\aleph_0^{\aleph_0} = 2^{\aleph_0}$.

tale mappa è iniettiva, infatti preso $B \in \text{Im}(f)$ possiamo definire (la funzione inversa che quindi ci assicura che quella iniziale è una bigezione tra $\mathcal{P}(\mathbb{R})$ e l'immagine di f in B , in tal modo f è iniettiva quando in arrivo consideriamo tutto l'insieme):

$$B \mapsto \begin{cases} B & \text{se } \{\spadesuit\} \notin B \\ \mathbb{R} \setminus (B \setminus \{\spadesuit\}) & \text{se } \{\spadesuit\} \in B \end{cases}$$

da cui si ha $|\mathcal{P}^{\text{inf.}}(\mathbb{R})| = |\mathcal{P}^{\text{inf.}}(\mathbb{R} \cup \{\spadesuit\})| \geq |\mathcal{P}(\mathbb{R})| = 2^{2^{\aleph_0}}$. ¹⁹³ \square

- $|\text{successioni di naturali}| = |{}^\omega\omega|$

Soluzione. (Senza AC)

Per definizione di esponenziazione di cardinalità: $|{}^\omega\omega| = |\omega|^{\omega} = \aleph_0^{\aleph_0}$, e come abbiamo visto tante volte, essendo l'esponenziale di cardinalità debolmente crescente in entrambe le componenti, si ha:

$$2 \leq \aleph_0 \leq 2^{\aleph_0} \implies 2^{\aleph_0} \leq \aleph_0^{\aleph_0} \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} \implies \aleph_0^{\aleph_0} = 2^{\aleph_0}$$

\square

- $|\text{successioni crescenti di naturali}| = |\{f \in {}^\omega\omega \mid f \text{ crescente}\}|$

Soluzione. (Senza AC)

Iniziamo osservando in primis che:

$$\{f \in {}^\omega\omega \mid f \text{ strett. crescente}\} \subseteq \{f \in {}^\omega\omega \mid f \text{ debolm. crescente}\} \subseteq {}^\omega\omega$$

da cui si ottiene la stima dall'alto con 2^{\aleph_0} per entrambe le cardinalità. Viceversa, possiamo considerare la funzione:

$$f : {}^\omega\omega \rightarrow \{f \in {}^\omega\omega \mid f \text{ strett. crescente}\} : (a_i)_{i \in \omega} \mapsto \left(i + \sum_{n=0}^i a_n \right)_{i \in \omega}$$

ovvero la funzione che associa ogni successione alla successione delle sue somme parziali traslata in ogni termine di $\frac{i(i+1)}{2}$. La mappa f è ben definita, perché grazie alla traslazione la successione in arrivo è in particolare strettamente crescente (in particolare la differenza di due termini successivi è proprio $a_{i+1} + 1 > 0$), ed inoltre è iniettiva, in quanto $f((a_i)_{i \in \omega})(i+1) - f((a_i)_{i \in \omega})(i) - 1 = a_{i+1}$, dunque se in arrivo abbiamo due successioni uguali, ricaviamo che i termini iniziali sono uguali e [dalla relazione appena vista che] le successioni in partenza sono a loro volta necessariamente uguali.

Abbiamo così ottenuto che:

$$2^{\aleph_0} \leq |\{f \in {}^\omega\omega \mid f \text{ strett. crescente}\}| \leq |\{f \in {}^\omega\omega \mid f \text{ debolm. crescente}\}| \leq 2^{\aleph_0}$$

(dove l'ultima disegualanza è il contenimento iniziale), che ci permettono di concludere la cardinalità in entrambi i casi. \square

¹⁹³Un'ultima osservazione degna di nota, senza AC sappiamo che $|X \cup \{\spadesuit\}| \geq |X|$ (infatti basta immergere X in $X \cup \{\spadesuit\}$), ma la disegualanza dal basso NON è sufficiente per concludere nella nostra soluzione senza AC. Per l'uguaglianza ci serve anche la disegualanza dall'alto, per inclusione-esclusione sappiamo che $|X \cup \{\spadesuit\}| \leq |X| + 1$, ma non possiamo dire che [per X infinito] $|X| = |X| + 1$ senza AC. Fondamentalmente abbiamo bisogno di costruire una bigezione tra i due, ma questa cosa la si fa considerando il fatto che (per AC) $\omega \hookrightarrow X$ [per ogni insieme infinito]. Tuttavia, possiamo concludere lo stesso in questo caso senza AC, perché abbiamo visto nella costruzione di \mathbb{R} che $\omega \hookrightarrow \mathbb{R}$ senza bisogno di scelta.

Soluzione. (Soluzione alternativa buffa (idea))

Basta trovare una funzione $g : \mathbb{R}_{>0} = \{x \in \mathbb{R} | x > 0\} \rightarrow \{\text{succ. strett. crescenti}\}$. Poniamo $(g(x))_i = \lfloor i \cdot x \rfloor$, tale successione è naturalmente strettamente crescente, ed è la successione che approssima ogni reale come limite di razionali, infatti si ha $kx - 1 < \lfloor kx \rfloor \leq kx$, da cui segue che $\lim_{k \rightarrow +\infty} \frac{\lfloor kx \rfloor}{k} = x$, $\forall x \in \mathbb{R}$. Abbiamo quindi che $(\lfloor i \cdot x \rfloor)_{i \in \omega}$ determina univocamente x , pertanto g è iniettiva. \square

- $|\text{successioni di reali}| = |\omega\mathbb{R}|$

Soluzione. (Senza AC)

Per definizione di esponenziale di cardinalità $|\omega\mathbb{R}| = |\mathbb{R}|^{|\omega|} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$. \square

- $|\text{successioni crescenti di reali}| = |\{f \in \omega\mathbb{R} | f \text{ crescente}\}|$

Soluzione. (Senza AC)

Iniziamo osservando in primis che:

$$\{f \in \omega\mathbb{R} | f \text{ strett. crescente}\} \subseteq \{f \in \omega\mathbb{R} | f \text{ debolm. crescente}\} \subseteq \omega\mathbb{R}$$

e quindi abbiamo una disuguaglianza dall'alto per entrambi gli insiemi. D'altra parte, si ha che $\mathbb{R} \rightarrow \omega\mathbb{R} : r \mapsto f_r$, con $f_r(x) = r$, $\forall r \in \mathbb{R}$ è ben definita (perché le funzioni costanti sono debolmente crescenti) ed è iniettiva, quindi concludiamo che $|\{f \in \omega\mathbb{R} | f \text{ debolm. crescente}\}| = 2^{\aleph_0}$. Questa cosa naturalmente non ci dà nessuna nuova stima per le strettamente crescenti, tuttavia anche in questo caso è facile costruirle esplicitamente come segue:

$$\mathbb{R} \times \omega \rightarrow \{f \in \omega\mathbb{R} | f \text{ strett. crescente}\} : (x, n) \mapsto (a_i)_{i \in \omega}$$

dove (a_i) è definita per ricorsione numerabile da:

$$\begin{cases} a_0 = x \\ a_{i+1} = a_i + n \end{cases}$$

e naturalmente la mappa è iniettiva (l'uguaglianza di due successioni in arrivo ci assicura l'uguaglianza dei termini iniziali, e quindi della prima componente in partenza, mentre l'uguaglianza di tutti gli altri ci dà l'uguaglianza degli incrementi). A questo punto, avendo visto (senza AC¹⁹⁴) che $|\mathbb{R} \times \omega| = 2^{\aleph_0} \cdot \aleph_0 = 2^{\aleph_0}$, abbiamo la disuguaglianza dal basso, e possiamo concludere che $|\{f \in \omega\mathbb{R} | f \text{ strett. crescente}\}| = 2^{\aleph_0}$. \square

Nota A.3 (Variante per la disuguaglianza dal basso) — Per la cardinalità precedente avremmo anche potuto utilizzare la funzione:

$$f : \mathbb{R} \rightarrow \{\text{succ. strett. crescente}\} : x \mapsto (i \cdot e^x)_{i \in \omega}^a$$

che manda ogni reale x nella successione $0, e^x, 2e^x, 3e^x, \dots$, che è iniettiva per l'iniettività della funzione esponenziale (la verifica dell'iniettività avviene in \mathbb{R} quindi si possono usare tutte le proprietà usuali di quest'ultimo).

¹⁹⁴L'idea di usare "rette" con coefficiente angolare > 0 tornerà anche dopo per funzioni strettamente crescenti da \mathbb{N} in \mathbb{R} e da \mathbb{R} in \mathbb{R} allo stesso identico modo.

¹⁹⁴Bastano Cantor e le disuguaglianze tra cardinalità.

- $|\text{successioni definitivamente costanti di naturali}| = |\{f \in {}^\omega\omega \mid \exists n_0 \in \omega \ \forall n \geq n_0 \ f(n) = \text{cost.}\}|$

Idea: La disegualanza dal basso con \aleph_0 è immediata. La disegualanza opposta deve basarsi sul fatto che $|\text{sequenze finite di naturali}| = \aleph_0$, perché, tutto sommato, una successione definitivamente costante è una sequenza finita il cui ultimo elemento si ripete incessantemente. Attenzione però che la stessa successione, es. $1, 2, 3, 3, 3, \dots$ può essere rappresentata in più di un modo, es. $(1, 2, 3, 3), (1, 2, 3, 3, 3)$.

Soluzione. (Con AC)

Sia X l'insieme delle successioni da ω in ω definitivamente costanti, naturalmente tutte le successioni costanti sono nell'insieme ed abbiammo quindi $\aleph_0 \leq |X|$.

Per la disegualanza opposta esibiamo $f : X \rightarrow \bigcup\{\omega^i \mid i \in \omega \setminus \{0\}\} \subseteq \mathcal{P}^{\text{fin.}}(\omega \times \omega)$ ¹⁹⁵ iniettive. A questo scopo, per $a \in X$ (una fissata funzione definitivamente costante), sia $I(a)$ il minimo $i \in \omega$ tale che $\forall j > i \ a_j = a_i$ (cioè il primo termine costante della successione), che esiste perché a è definitivamente costante (quindi prendiamo il minimo su un insieme non vuoto etc.).

Sia $f(a) = a_{|1+I(a)}$ (cioè tronchiamo la successione a al primo termine $I(a)$ (incluso) in cui è costante¹⁹⁶), ossia rimappiamo la successione usando in arrivo un sottoinsieme finito in arrivo (e quindi troncandola ad un numero finito di termini):

$$f(a) : 1 + I(a) \rightarrow \omega : i \mapsto a_i$$

Per verificare l'iniettività osserviamo che $I(a) = \max(\text{Dom}(f(a)))$ (per come l'abbiamo costruita), quindi $f(a)$ determina $I(a)$, inoltre se $i \leq I(a)$, $a_i = (f(a))_i$, altrimenti, $a_i = a_{I(a)} = (f(a))_{I(a)}$ (cioè il termine indicizzato da $I(a)$ in arrivo). Per cui a è determinata da $f(a)$. \square

Soluzione. (Soluzioni alternative, con AC)

Detto $S := \{\text{successioni definitivamente costanti di naturali}\}$, osserviamo che $\omega \rightarrow S : m \mapsto f_m$, con $f_m(n) = m$, $\forall m \in \omega$, è iniettiva e dà la prima disegualanza, ovvero $\aleph_0 \leq |S|$. Viceversa, la funzione:

$$\omega \times \omega \times \omega^{<\omega} \rightarrow S : (n_0, k, (\alpha_i)) \mapsto a_i = \begin{cases} \alpha_i & \text{se } i < n_0 \\ k & \text{se } i \geq n_0 \end{cases}$$

è surgettiva, in quanto, per ogni successione definitivamente costante, per definizione, $\exists n_0 \in \omega \ \forall n \geq n_0 \ a_n = k$, inoltre i valori assunti in precedenza sono in numero finito (precisamente n_0 , quindi abbiammo la n_0 -upla in ω^{n_0} che salva i primi termini).

Se usassimo AC, avremmo già finito, tuttavia non lo stiamo usando, ma possiamo comunque provare a salvare questa soluzione in due modi. Il primo è osservare che le disegualanze di cardinalità con le funzioni surgettive valgono anche senza AC per gli insiemi al più numerabili (per l'[esercizio visto](#)), il problema è in questo caso dimostrare che $\omega^{<\omega}$ è numerabile, infatti abbiamo:

$$\omega^{<\omega} = \bigcup_{n \in \omega} \omega^n$$

¹⁹⁵Sono tutte le funzioni da un numero finito ad ω , e quindi possono essere pensate come parti finite (unione di tutti i $\mathcal{P}^n(\omega^2)$) di ω^2 (e si identificano con le funzioni a supporto finito da ω in ω). Inoltre per dire che le parti finite di un insieme numerabile sono numerabili abbiammo comunque usato scelta nella teoria, per cui questa soluzione non può farne a meno.

¹⁹⁶Notare che abbiammo preso $a_{|m+1}$ quindi tutti i valori della successione da a_0 ad a_m escludendo l'ultimo perché è lo stesso insieme a cui ci siamo ristretti.

e per dimostrare che la cardinalità di questa cosa è ancora \aleph_0 (o almeno la disuguaglianza dall'alto), abbiamo inevitabilmente bisogno di AC. L'ultima possibilità che ci rimane è definire allora funziona al contrario, cioè:

$$S \hookrightarrow \omega \times \omega \times \omega^{<\omega} : a_i \mapsto (n_0, k, (\alpha_i))$$

che è ben definita e iniettiva come la precedente. A questo punto la disuguaglianza la abbiamo, cioè $|S| \leq |\omega \times \omega \times \omega^{<\omega}| = \aleph_0 \cdot \aleph_0 \cdot |\omega^{<\omega}|$, ma di nuovo incappiamo nel problema di determinare la cardinalità di $\omega^{<\omega}$ senza usare AC. Morale della favola: tutte e tre le soluzioni che abbiamo trovato funzionano perfettamente assumendo AC. \square

- $|\text{successioni periodiche di naturali}| = |\{f \in {}^\omega\omega \mid f \text{ periodica}\}|$

Soluzione. (Con AC)

Sia X l'insieme delle successioni periodiche di naturali. Le successioni costanti sono periodiche e danno la disuguaglianza dal basso con \aleph_0 . Per la disuguaglianza dall'alto esibiamo una funzione iniettiva da X alle parti finite di $\omega \times \omega$ (che contengono le sequenze finite ordinate $\bigcup \{\omega^i \mid i \in \omega\}$ ¹⁹⁷). Detto $T(a)$ il minimo periodo della successione a , sia $f(a) = a_{|T(a)}$ (cioè i termini da a_0 a $a_{T(a)-1}$ (incluso), ciò fino all'ultimo che non si può ottenere come ripetizione).

Per verificare l'iniettività osserviamo che $f(a)$ determina $T(a) = 1 + \max(\text{Dom}(f(a)))$ - tecnicamente è uguale a $\text{Dom}(f(a))$. Ora $a_i = (f(a))_j$, dove $j < T(a)$ è l'unico naturale congruo ad i modulo $T(a)$, cioè per assegnare l' i -esimo valore ad (a_i) vediamo a quale valore i è congruo modulo $T(a)$ e fissiamo un rappresentante $< T(a)$, sia j , a questo punto $a_i = (f(a))_j$ (cioè prendiamo l'elemento giusto nella stringa ordinata che determina il periodo¹⁹⁸). Ciò determina completamente (a) , dandoci l'iniettività e quindi la disuguaglianza dall'alto. \square

- $|\text{funzioni da } \mathbb{R} \text{ in } \mathbb{R}| = |{}^\mathbb{R}\mathbb{R}|$

Soluzione. (Senza AC)

Per la definizione di esponenziazione di cardinalità $|{}^\mathbb{R}\mathbb{R}| = |\mathbb{R}|^{|\mathbb{R}|} = (2^{\aleph_0})^{2^{\aleph_0}} = 2^{\aleph_0 \cdot 2^{\aleph_0}} = 2^{2^{\aleph_0}}$. Osservare che, oltre alla definizione, e alla proprietà associativa delle potenze, abbiamo usato soltanto che $\aleph_0 \cdot 2^{\aleph_0} = 2^{\aleph_0}$, che è immediato con AC, ma che abbiamo dimostrato anche senza. \square

- $|\text{funzioni da } \mathbb{R} \text{ in } \mathbb{R} \text{ continue}| = |\text{C}^0(\mathbb{R})|$

Idea: una funzione continua è determinata dai valori che assume sui razionali, quindi è come se ci bastasse definirla su \mathbb{Q} , ovvero come sottoinsieme di ${}^\mathbb{Q}\mathbb{R}$.

Soluzione. (Senza AC)

Consideriamo la mappa $\mathbb{R} \hookrightarrow \text{C}^0(\mathbb{R}) : r \mapsto f_r$, tale che $f_r : x \mapsto x$, ossia la funzione che mappa ogni reale nella sua funzione costante [che è continua], tale funziona è banalmente iniettiva e ci dice che $2^{\aleph_0} \leq |\text{C}^0(\mathbb{R})|$.

Per la disuguaglianza opposta, consideriamo $|_{\mathbb{Q}} : \text{C}^0(\mathbb{R}) \rightarrow {}^\mathbb{Q}\mathbb{R} : f \mapsto f|_{\mathbb{Q}}$ e osserviamo che $|{}^\mathbb{Q}\mathbb{R}| = |\mathbb{R}|^{|\mathbb{Q}|} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0}$. Verifichiamo che la mappa $|_{\mathbb{Q}}$ è iniettiva, date $f|_{\mathbb{Q}}, g|_{\mathbb{Q}} \in {}^\mathbb{Q}\mathbb{R}$ si ha [per l'estensionalità di funzioni che]:

$$f|_{\mathbb{Q}} = g|_{\mathbb{Q}} \implies f|_{\mathbb{Q}}(x) = g|_{\mathbb{Q}}(x) \quad \forall x \in \mathbb{Q}$$

¹⁹⁷Qui stiamo usando AC.

¹⁹⁸Notare come questo procedimento non richieda nemmeno salvare il periodo nella funzione iniziale, ci basta solo la stringa finita dei primi $T(a)$ termini per ricostruire l'intera successione.

Ora, $\forall x \in \mathbb{R}$ esiste [una successione di razionali che lo approssima] $\{x_n\}_{n \in \omega} \subseteq \mathbb{Q}$ tale che $x_n \rightarrow x^{199}$, dunque:

$$\begin{aligned} f(x) = g(x) &\iff f\left(\lim_{n \rightarrow +\infty} x_n\right) = g\left(\lim_{n \rightarrow +\infty} x_n\right) \quad \forall x \in \mathbb{R} \\ &\iff \lim_{n \rightarrow +\infty} f(x_n) = \lim_{n \rightarrow +\infty} g(x_n) \end{aligned}$$

dove abbiamo usato il fatto che f e g continue, implica che commutano con i limiti. A questo punto, visto che le due funzioni sono uguali sulla restrizione a \mathbb{Q} , e che $\{x_n\}_{n \in \omega} \subseteq \mathbb{Q}$, i due limiti coincidono e rendono vero il primo termine, ossia $f(x) = g(x)$, $\forall x \in \mathbb{R}$, e per estensionalità per funzioni, si conclude che $f = g$, quindi $|_{\mathbb{Q}}$ è iniettiva e ci dà la disuguaglianza $|C^0(\mathbb{R})| \leq 2^{\aleph_0}$, con cui si conclude. \square

Osservazione A.4 — Per concludere l'iniettività di $|_{\mathbb{Q}}$ si poteva anche osservare che, se $f \neq g$, WLOG si può assumere che esista x_0 tale per cui $f(x_0) > g(x_0)$ e per permanenza del segno esiste $\varepsilon > 0$ tale che $f(x) > g(x)$ per ogni $x \in]x_0 - \varepsilon, x_0 + \varepsilon[$. Per la densità di \mathbb{Q} in \mathbb{R} esiste necessariamente un razionale in questo intervallo, per cui accade $f(q) > g(q)$ e quindi $f|_{\mathbb{Q}} \neq g|_{\mathbb{Q}}$.

- $|\text{funzioni da } \mathbb{R} \text{ in } \mathbb{R} \text{ crescenti}| = |\{f \in {}^{\mathbb{R}}\mathbb{R} \mid f \text{ crescente}\}|$

Idea: Una funzione crescente supera ogni barriera in un punto ben determinato, e questi punti quasi determinano la funzione. Quasi perché c'è più di un modo di superare un razionale nei punti di discontinuità. Converrà quindi codificare una funzione crescente con la funzione che manda ogni razionale nel punto di superamento corredata dall'informazione necessaria per disambiguare la discontinuità.

Idea più dettagliata: Sia f crescente $\mathbb{R} \rightarrow \mathbb{R}$. Per definizione, il reale $f(x)$ è l'insieme dei razionali: $r < f(x)$. Quindi f è determinata dall'insieme delle coppie $(r, x) \in \mathbb{Q} \times \mathbb{R}$ tali che $r < f(x)$. Se ora fissiamo r , siccome f è crescente, l'insieme dei $-x$ tali che $r < f(x)$ è un segmento iniziale di \mathbb{R} . Quindi f è determinata dalla funzione $\mathbb{Q} \rightarrow \{\text{segm. iniz. di } \mathbb{R}\}$ che manda r in $\{-x \in \mathbb{R} \mid r < f(x)\}$. Siccome i segmenti iniziali di \mathbb{R} sono: $\mathbb{R}, \emptyset,]-\infty, x[$ e $]-\infty, x]$, ce ne sono $1 + 1 + 2^{\aleph_0} + 2^{\aleph_0} = 2^{\aleph_0}$. Abbiamo quindi al più $(2^{\aleph_0})^{\aleph_0}$ funzioni crescenti.

Soluzione. (Senza AC)

Osserviamo intanto che la cardinalità cercata è maggiore o uguale di 2^{\aleph_0} perché per ogni $k \in \mathbb{R}$ la funzione $f_k(x) = x \cdot e^k$ è strettamente crescente. Dobbiamo dimostrare la disuguaglianza opposta. Abbiamo bisogno di osservare che i segmenti iniziali di \mathbb{R} sono: \emptyset, \mathbb{R} e gli insiemi della forma $] -\infty, x[$ o $] -\infty, x]$ per $x \in \mathbb{R}$ [naturalmente tutti soddisfano la definizione di segmento iniziale, quindi c'è bisogno di dimostrare soltanto che tutti i possibili segmenti iniziali di \mathbb{R} sono tra quelli di questa forma]. Consideriamo infatti un segmento iniziale $I \neq \emptyset$ di \mathbb{R} . O I è superiormente limitato o no. Se non è superiormente limitato (moralmente non è una semiretta, ma una retta oppure verifica la definizione di illimitato a vuoto) allora $I = \mathbb{R}$ (si possono verificare facilmente le due inclusioni) oppure $I = \emptyset$. Se è superiormente limitato, I è o $] -\infty, \sup I[$ o $] -\infty, \sup I[$. Segue quindi che $|\{\text{segmenti iniziali di } \mathbb{R}\}| = 1 + 1 + 2^{\aleph_0} + 2^{\aleph_0}$. Ci basta quindi trovare

¹⁹⁹Deriva dalla densità di \mathbb{Q} in \mathbb{R} e lo si può verificare in tanti modi, per esempio mostrando una successione esplicita di razionali, ad esempio $x_n := \frac{\lfloor nx \rfloor}{n} \in \mathbb{Q}$.

una funzione iniettiva dalle funzioni [debolmente] crescenti alle funzioni da \mathbb{Q} a tali segmenti iniziali di \mathbb{R} :

$$F : \{f \in \mathbb{R}^{\mathbb{R}} \text{ crescenti}\} \rightarrow \mathbb{Q} \{\text{segmenti iniziali di } \mathbb{R}\}$$

possiamo definirla come segue:

$$F(f) : \mathbb{Q} \rightarrow \{\text{segmenti iniziali di } \mathbb{R}\} : q \mapsto \{x \in \mathbb{R} | q < f(-x)\}$$

Verifichiamo che F è ben definita ed iniettiva:

- ◊ Buona definizione: Vogliamo vedere che $(F(f))(q)$ è un segmento iniziale. Sia $x \in (F(f))(q)$ e sia $y < x$, vogliamo mostrare che $y \in (F(f))(q)$, osserviamo che $y < x \implies -y > -x$ (per le proprietà di \mathbb{R}), da cui $f(-y) > f(-x) > q \implies f(-y) > q$ (poiché f crescente), ovvero $y \in (F(f))(q)$.
- ◊ Iniettività: Consideriamo $f, g \in \mathbb{R}^{\mathbb{R}}$ crescenti distinte, ossia esiste almeno un $x \in \mathbb{R}$ tale che (WLOG) $f(x) < g(x)$, vogliamo dimostrare che $F(f) \neq F(g)$. Per la densità di \mathbb{Q} esiste un razionale tale che $f(x) < q < g(x)$, per cui possiamo valutare $(F(g))(q)$ e $(F(f))(q)$, e osservare che [considerando l' x iniziale] $-x \in (F(g))(q)$, cioè $q < g(x)$ e allo stesso tempo $-x \notin (F(f))(q)$ poiché abbiamo dalla disuguaglianza sopra che $f(x) < q$, ovvero $F(f)$ e $F(g)$ sono distinte su $q \in \mathbb{Q}$, quindi abbiamo l'injectività.

□

Definizione A.5 (Partizione). Diciamo che A è una **partizione** di B se:

$$\bigcup A = B \quad \emptyset \notin A \quad \forall x, y \in A \quad x \cap y = \emptyset$$

- $|\text{partizioni di } \omega|$

Soluzione. (Senza AC)

Osserviamo che la mappa $\mathcal{P}(\omega \setminus \{0, 1\}) \setminus \{\emptyset\} \hookrightarrow \{\text{partizioni di } \omega\} : A \mapsto \{A \cup \{0\}, (\omega \setminus A) \cup \{1\}\}$ è iniettiva per estensionalità [basta addirittura solo il paio] (o anche osservare che, detto $z(x)$ l'unico elemento dei due della partizione che contiene lo 0, si ha proprio che $z(\{A \cup \{0\}, \omega \setminus A \cup \{1\}\}) \cap (\omega \setminus \{0\}) = A$, da cui segue ancora più banalmente l'iniettività), dunque abbiamo la disegualanza $2^{\aleph_0} \leq |\{\text{partizioni di } \omega\}|$.

Per il viceversa, osserviamo che data una partizione $A = \{A_i\}_{i \in I}$ di ω , per la definizione che ne abbiamo dato, si ha $\forall n \in \omega \exists i \in I \ n \in A_i$, per cui possiamo definire la mappa $\{\text{partizioni di } \omega\} \rightarrow {}^\omega \mathcal{P}(\omega) : A \mapsto f_A$, con $f_A : \omega \rightarrow \mathcal{P}(\omega) : n \mapsto A_i$. Tale funzione è ben definita perché A è una partizione di ω , inoltre è iniettiva, perché, osservando che $\text{Im}(f_A) = A$ [perché banalmente otteniamo tutti gli insiemi disgiunti che formano la partizione originale, quindi l'insieme di tali insiemi, cioè l'immagine di f_A è proprio la partizione stessa], si ottiene che $f_A = f_B \implies \text{Im}(f_A) = \text{Im}(f_B) \iff A = B$, quindi abbiamo ottenuto anche che $|\{\text{partizioni di } \omega\}| \leq 2^{\aleph_0}$. \square

Osservazione A.6 (Disegualanza dall'alto alternativa) — Un'alternativa alla seconda disegualanza della soluzione precedente è data dalla funzione:

$$\{\text{partizioni di } \omega\} \hookrightarrow {}^\omega \omega : A \mapsto g_A$$

con $g_A : \omega \rightarrow \omega : n \mapsto \min(A_i)$, dove A_i è l'elemento della partizione che per definizione contiene n . Tale funzione è naturalmente iniettiva, infatti, stiamo facendo la stessa cosa fatta nella soluzione, con la differenza che, anziché mandare l'elemento nell'insieme lo mandiamo nel suo minimo, ed essendo tutti gli insiemi della partizione disgiunti, tale minimo non può essere assunto da nessun altro elemento della partizione.

Nota A.7 (Quando il complementare fa fallire le partizioni distinte) — Potrebbe venire la tentazione di definire $f(A) = \{A, \omega \setminus A\}$, però questa funzione non è iniettiva, per esempio, il sottoinsieme dei numeri pari e il sottoinsieme dei numeri dispari vanno nella stessa partizione.

- $|\text{partizioni finite di } \omega|$

Soluzione. (Senza AC)

Per la disegualanza dal basso, va bene la stessa mappa usata sopra, cioè $\mathcal{P}(\omega \setminus \{0, 1\}) \setminus \{\emptyset\} \hookrightarrow \{\text{partizioni di } \omega\} : A \mapsto \{A \cup \{0\}, (\omega \setminus A) \cup \{1\}\}$, che è iniettiva, produce delle partizioni fatte da due elementi, e quindi ci dice che $2^{\aleph_0} \leq |\{\text{partizioni finite di } \omega\}|$ (naturalmente numerabile - finito = numerabile, per un fatto visto in precedenza, quindi abbiamo $|\omega| = |\omega \setminus \{0, 1\}|$).

Per il viceversa basta osservare che $\{\text{partizioni finite di } \omega\} \subseteq \{\text{partizioni di } \omega\}$, che abbiamo contato sopra, dunque otteniamo che $|\{\text{partizioni finite di } \omega\}| \leq 2^{\aleph_0}$. \square

- |partizioni di ω in parti finite|

Soluzione. (Senza AC)

Osserviamo che $\mathcal{P}(\omega) \setminus \{\emptyset\} \rightarrow \{\text{partizioni di } \omega \text{ in parti finite}\} : A \mapsto \{2i, 2i+1\}_{i \in A} \cup \{2i\}_{i \notin A} \cup \{2i+1\}_{i \notin A}$ dà la disuguaglianza dal basso, infatti, tale funzione è ben definita in quanto:

$$\{2i, 2i+1\}_{i \in A} \cup \{2i\}_{i \notin A} \cup \{2i+1\}_{i \notin A} = ^{200} \{i\}_{i \in \omega} \cup \{2i\}_{i \in \omega} = \omega$$

e vale che $\{2i\}_{i \notin A} \cap \{2i+1\}_{i \notin A} = \emptyset$ (altrimenti esisterebbero numeri pari e dispari contemporaneamente) e $\{2i, 2i+1\}_{i \in A} \cap \{2i\}_{i \notin A} = \{2i, 2i+1\}_{i \in A} \cap \{2i+1\}_{i \notin A} = \emptyset$, in quanto se una delle due intersezioni non fosse vuota potremmo scrivere $2i = 2j \implies i = j$ per $i \in A$ e $j \notin A$, oppure $2i+1 = 2j+1 \implies i = j$ per $i \in A$ e $j \notin A$, che è assurdo. Inoltre tale mappa è iniettiva, infatti, prese due partizioni nell'immagine:

$$P_A = \{2i, 2i+1\}_{i \in A} \cup \{2i\}_{i \notin A} \cup \{2i+1\}_{i \notin A} \quad P_B = \{2i, 2i+1\}_{i \in B} \cup \{2i\}_{i \notin B} \cup \{2i+1\}_{i \notin B}$$

per estensionalità (essendo insiemi di insiemi), $P_A = P_B$ se e solo se tutti i singoletti e gli insiemi con due elementi sono uguali, e l'ultima cosa significa che $\{2i, 2i+1\}_{i \in A} = \{2i, 2i+1\}_{i \in B}$, ma questa cosa è possibile [di nuovo per estensionalità] se e solo se $A = B$. Abbiamo quindi ottenuto che $2^{\aleph_0} \leq |\{\text{partizioni di } \omega \text{ in parti finite}\}|$. L'altra disuguaglianza si ottiene osservando che $\{\text{partizioni di } \omega \text{ in parti finite}\} \subseteq \{\text{partizioni di } \omega\}$. \square

Soluzione. (Soluzione alternativa, senza AC)

Per la disuguaglianza dall'alto possiamo fare come prima, mentre dal basso possiamo codificare una partizione in parti finite usando stringhe di 0 e 1 per ottenere coppie di insiemi che ci danno tutte le classi di resto modulo 3 man mano. Utilizziamo 2 insiemi associati ad una cifra della stringa, perché usandone uno solo si perde l'iniettività (avremmo che la prima cifra della stringa da sempre lo stesso insieme di tre elementi). Inoltre, possiamo fissare man mano un elemento ad esempio nell'insieme da due elementi tenere sempre $3i+1$, e far variare il primo elemento del secondo insieme e il secondo elemento del secondo insieme per poter distinguere le partizioni ottenute da 0 e 1 (in quella posizione rispettivamente). Dunque definiamo:

$$f : \omega^2 \rightarrow \{\text{partizioni di } \omega \text{ in parti finite}\} : (a_i)_{i \in \omega} \mapsto \{\{3i+2a_i\}, \{3i+1, 3i+2-2a_i\}\}_{i \in \omega}$$

quindi ad esempio:

$$(0, 1, 1, 0, \dots) \mapsto \underbrace{\{\{0\}, \{1, 2\}\}}_{a_0=0}, \underbrace{\{\{5\}, \{4, 3\}\}}_{a_1=1}, \underbrace{\{\{8\}, \{7, 6\}\}}_{a_2=1}, \underbrace{\{\{9\}, \{10, 11\}\}}_{a_3=0}, \dots$$

Infine f è iniettiva, perché due partizioni sono uguali se e solo se tutti gli insiemi sono uguali e usando la formula possiamo determinare per ogni coppia di insiemi se a_i è 1 o 0 in posizione i .²⁰¹ Da ciò si conclude che abbiamo almeno $|\omega^2| = 2^{\aleph_0}$ partizioni di ω in sottoinsiemi finiti. \square

- |partizioni di ω in parti infinite|

Idea: È facile risolvere questo esercizio con una costruzione ad hoc, ma si può anche ragionare così. C'è una corrispondenza biunivoca fra ω e $\omega \times \omega$, quindi anche fra le rispettive partizioni in parti infinite. D'altro canto, tutte le partizioni di ω si mappano iniettivamente nelle partizioni in parti infinite di $\omega \times \omega$ moltiplicando ciascuna delle parti per ω (così abbiamo contato tutte le partizioni in parti infinite di $\omega \times \omega$).

²⁰⁰Si verifica facilmente usando estensionalità.

²⁰¹Notare infine che per costruzione scambiare 0 e 1 nella stringa non fa altro che scambiare l'elemento del singoletto col "secondo" elemento del secondo insieme.

Soluzione. Dagli esercizi precedenti abbiamo immediatamente la disuguaglianza dall'alto, data da 2^{\aleph_0} . Osserviamo preliminarmente che una bigezione $f : A \rightarrow B$ ne induce una tra le parti definita in questo modo:

$$\bar{f} : \mathcal{P}(A) \rightarrow \mathcal{P}(B) : X \mapsto f[X]^{202}$$

che preserva naturalmente le cardinalità $|\bar{f}(X)| = |X|$. Sia $\text{Part}^{\geq\aleph_0}(\square)$ l'insieme delle parti infinite di \square , si verifica facilmente che:

$$\bar{\bar{f}}_{|\text{Part}^{\geq\aleph_0}(A)} : \text{Part}^{\geq\aleph_0}(A) \rightarrow \text{Part}^{\geq\aleph_0}(B)^{203}$$

è una bigezione, di conseguenza $|\text{Part}^{\geq\aleph_0}(A)| = |\text{Part}^{\geq\aleph_0}(B)|$. Ci basta quindi contare le partizioni in insiemi infiniti di $\omega \times \omega$, in particolare ci basta una stima dal basso (visto che per le partizioni in insiemi infiniti su ω abbiamo già la stima dall'alto).

Possiamo quindi usare la mappa di cui abbiamo parlato sopra:

$$g : \{\text{partizioni di } \omega\} \rightarrow \text{Part}^{\geq\aleph_0}(\omega \times \omega) : P \mapsto \{A \times \omega \mid A \in P\}$$

ed è iniettiva, poiché presa Q in arrivo è sufficiente mandarla nell'insieme fatto da $\{\pi[X] \mid X \in Q\}$, con $\pi : \omega \times \omega \rightarrow \omega$ proiezione alla prima componente. \square

- $|\text{sottoinsiemi chiusi di } \mathbb{R}|$

Soluzione. (Senza AC)

I singoletti di \mathbb{R} soddisfano la definizione di insieme chiuso, quindi la mappa $\mathbb{R} \rightarrow \{\text{chiusi di } \mathbb{R}\} : x \mapsto \{x\}$ è iniettiva e ci dà la disuguaglianza $2^{\aleph_0} \leq |\{\text{chiusi di } \mathbb{R}\}|$.

Per il viceversa dimostriamo che la seguente mappa è iniettiva:

$$f : \{\text{chiusi di } \mathbb{R}\} \rightarrow \mathcal{P}(\mathbb{Q} \times \mathbb{Q}) : A \mapsto \{(a, b) \in \mathbb{Q} \times \mathbb{Q} \mid a < b \wedge [a, b] \cap A = \emptyset\}$$

(ovvero mappiamo il chiuso nell'insieme degli estremi razionali di tutti gli intervalli aperti disgiunti da A). Basta osservare che, per definizione di insieme chiuso, $x \notin A$ se e solo esistono $y, z \in \mathbb{R}$ tali che $y < x < z$, e l'intorno $]x, z[$ di x non interseca A^{204} . In questo caso, per la densità di \mathbb{Q} , possiamo trovare $a, b \in \mathbb{Q}$, $y < a < x < b < z$. Di conseguenza:

$$A = \mathbb{R} \setminus \bigcup \{[a, b] \mid (a, b) \in f(A)\}^{205}$$

Questo prova l'iniettività di f , per cui:

$$|\{\text{chiusi di } \mathbb{R}\}| \leq |\mathcal{P}(\mathbb{Q} \times \mathbb{Q})| = 2^{\aleph_0}$$

\square

Soluzione. (Soluzione alternativa, senza AC)

I chiusi sono in bigezione con gli aperti, per mezzo del complementare, inoltre la disuguaglianza dal basso si fa esattamente con i complementari dei singoletti.

²⁰²È un'idea che verrà usata anche dopo per contare i sottoinsiemi di \mathbb{R} isomorfi a $(\mathbb{Q}, <)$.

²⁰³Ciò la funzione che applica due volte \bar{f} prima sugli insiemi che contengono gli elementi della partizione e poi su questi ultimi (la stiamo prendendo già ristretta).

²⁰⁴Typo Mamino.

²⁰⁵Stiamo trovando il chiuso come complementare dell'aperto e osservando che l'aperto complementare è univocamente determinato dagli intervalli a estremi razionali che non intersecano A , e che quindi sono contenuti interamente nel complementare (quest'idea è la versione complementare di quella nella soluzione alternativa).

Per il viceversa osserviamo che ogni aperto di \mathbb{R} si può scrivere come unione al più numerabile di intervalli con estremi razionali, infatti, dato $x \in A \subseteq \mathbb{R}$ (aperto), si ha che $\exists \varepsilon > 0$ $]x - \varepsilon, x + \varepsilon[\subseteq A$ e, per la densità di \mathbb{Q} , esistono $a, b \in \mathbb{Q}$ tali che $x - \varepsilon < a < x < b < x + \varepsilon$. A questo punto $\forall x \in A$ esistono $a, b \in \mathbb{Q} \cap A$ tali che $x \in]a, b[$, in particolare ciò significa che $A \subseteq \bigcup_{\substack{a, b \in \mathbb{Q} \cap A \\ a < b}} I_{(a,b)}$ (con $I_{(a,b)} =]a, b[$), inoltre essendo tutti gli intervalli aperti contenuti in A vale anche il contenimento opposto, dunque abbiamo:²⁰⁶

$$A = \bigcup_{\substack{a, b \in \mathbb{Q} \cap A \\ a < b}} I_{(a,b)}$$

Abbiamo quindi scoperto che un aperto di \mathbb{R} è univocamente determinato dai razionali che contiene, dunque possiamo definire la mappa:

$$\{\text{aperti di } \mathbb{R}\} \rightarrow \mathcal{P}(\mathbb{Q}) : A \mapsto A \cap \mathbb{Q}$$

che è banalmente iniettiva (ed anzi è addirittura una biiezione) perché preso B in arrivo otteniamo che $A = \bigcup_{\substack{a, b \in B \\ a < b}} I_{(a,b)}$, dunque abbiamo la disegualanza dall'alto con 2^{\aleph_0} . \square

²⁰⁶Osserviamo che prendere l'unione degli intervalli su tutti i razionali nell'aperto è anche eccessivo, in realtà potremmo addirittura partizionare ogni aperto in un'unione al più numerabile di intervalli disgiunti, tuttavia si complicherebbe definire una mappa iniettiva come stiamo per fare.

Esercizio A.8. Delle seguenti, a quali è possibile rispondere, assumendo che, senza scelta, non si può dire se valga o no $|\text{sottoinsiemi numerabili di } \mathbb{R}| = 2^{\aleph_0}$?

- |sottoinsiemi di \mathbb{R} isomorfi a $(\omega, <)$ con l'ordinamento indotto|

Soluzione. (Non necessita di AC²⁰⁷)

Questa è una conseguenza di un esercizio precedente, ovvero il fatto che la cardinalità delle successioni crescenti da ω in \mathbb{R} sia 2^{\aleph_0} . Per trovare la cardinalità richiesta è sufficiente osservare che la funzione:

$$I_n : \{\text{succ. cresc. di reali}\} \rightarrow \{\text{sottoins. di } \mathbb{R} \sim (\omega, <)\} : (a_i)_{i \in \omega} \mapsto \{a_i \mid i \in \omega\}$$

è bigettiva. Tale mappa è ben definita in quanto l'immagine di una successione crescente è un insieme isomorfo a $(\omega, <)$, inoltre è surgettiva in quanto per ogni elemento in arrivo esiste per definizione una mappa strettamente crescente da ω ad \mathbb{R} di cui è l'immagine (si ha proprio che $(\text{Im}(a_n), <_{\mathbb{R}}) \sim (\omega, <)$).

Dire che è iniettiva significa dire che dato $\text{Im}(a_n)$, un sottoinsieme di \mathbb{R} isomorfo a $(\omega, <)$, (a_n) è l'unico isomorfismo di ordini fra $(\omega, <)$ e $\text{Im}(a_n)$. Sia (b_m) un secondo isomorfismo tra $\text{Im}(a_n)$ e $(\omega, <)$, ne segue che $f = b_m^{-1} \circ a_n$ è un isomorfismo tra $(\omega, <)$ e se stesso diverso dall'identità, ma ciò è assurdo per quanto visto. Infatti f è crescente ed essendo $(\omega, <)$ un buon ordinamento si deve avere $f(n) \geq n$ (vale la dimostrazione già vista, oppure la si può fare per induzione osservando che il passo induttivo è: $f(n+1) > f(n) \geq n \implies f(n+1) \geq n+1$), ma parimenti $f^{-1}(n) \geq n$, quindi si ha necessariamente che $f(n) = n$. \square

- |sottoinsiemi di \mathbb{R} isomorfi a \mathbb{Q} con l'ordinamento indotto|

Soluzione. (Non si può rispondere senza AC)

Ci basta argomentare che se sapessimo rispondere a questa domanda, allora sapremmo altresì la cardinalità dell'insieme dei sottoinsiemi numerabili di \mathbb{R} (come conseguenza). Usando scelta, e quindi dando per buono che i sottoinsiemi numerabili di \mathbb{R} sono 2^{\aleph_0} , ci basta trovare una stima dal basso, tale stima è data da:

$$f : \{\text{sottoinsiemi numerabili di } \mathbb{R}\} = \mathcal{P}^{\aleph_0}(\mathbb{R}) \rightarrow \{\text{sottoinsiemi } \sim \mathbb{Q}\}$$

infatti, trovata una f iniettiva avremmo concluso. Per costruire f , ricordiamo che abbiamo dimostrato che $|\mathbb{R} \setminus \mathbb{Q}| = 2^{\aleph_0} = |\mathbb{R}|$ e consideriamo $g : \mathbb{R} \rightarrow \mathbb{R} \setminus \mathbb{Q}$ una bigezione. Osservato questo l'idea è chiara: vogliamo prendere un sottoinsieme numerabile di \mathbb{R} , mandarlo in un sottoinsieme [numerabile] di \mathbb{R} disgiunto da \mathbb{Q} via g e vogliamo unirlo a \mathbb{Q} per avere nuovo insieme isomorfo a \mathbb{Q} . Possiamo quindi definire: $f : \mathcal{P}^{\aleph_0}(\mathbb{R}) \rightarrow \{\text{sottoinsiemi } \sim \mathbb{Q}\} : X \mapsto g[X] \cup \mathbb{Q}$.

* f è ben definita: cioè in arrivo abbiamo sempre ordini isomorfi a \mathbb{Q} . Per verificare ciò è sufficiente verificare le ipotesi del teorema di isomorfismo di Cantor. $g[X] \cup \mathbb{Q}$ è numerabile in quanto unione (finita) di numerabili, inoltre $g[X] \cup \mathbb{Q}$ contiene \mathbb{Q} , quindi è denso in \mathbb{R} e di conseguenza in se stesso, infine è illimitato, perché se lo fosse vorrebbe dire che \mathbb{Q} è limitato, ma ciò è assurdo.

²⁰⁷In ogni caso AC ci darebbe solo la disuguaglianza dall'alto gratuitamente, ma nella soluzione che stiamo per vedere possiamo costruire direttamente una bigezione. Un'idea per avere poi una disuguaglianza dal basso è osservare che i singoletti $\{x\}$ per $x \in \mathbb{R}$ sono bene ordinati, dunque tutte le somme di buoni ordini $\{x\} + \omega$ sono buoni ordini contenuti in \mathbb{R} e dunque ne abbiamo proprio 2^{\aleph_0} .

* f è iniettiva: essendo $g[X] \cap \mathbb{Q} = \emptyset$ (per costruzione), si ha $g[X] \cup \mathbb{Q} = g[Y] \cup \mathbb{Q} \implies g[X] = g[Y]$ $\xrightarrow{g \text{ biogeze}} X = Y$.

e quindi abbiamo ottenuto anche $|\{\text{sottoinsiemi di } \mathbb{R} \sim \mathbb{Q}\}| \leq 2^{\aleph_0}$. \square

- |sottoinsiemi di \mathbb{R} ben ordinati dall'ordinamento indotto|

Idea: Se S è bene ordinato e $x \in S$, allora o x è il massimo di S o esiste il minimo $y \in S$ $y > x$. Comunque sia, possiamo trovare un razionale $q \in \mathbb{Q}$ tale che x è il massimo di S prima di q . Possiamo quindi sperare di usare questi razionali come codici degli elementi di S .

Soluzione. (Senza AC²⁰⁸)

I singoletti di \mathbb{R} sono bene ordinati con l'ordinamento indotto, quindi ne abbiamo almeno 2^{\aleph_0} (andavano bene anche i sottoinsiemi bene ordinati isomorfi ad $(\omega, <)$ visti sopra). Ci basta quindi mostrare che la seguente funzione è iniettiva:

$$f : \{\text{sottoins. bene ordinati di } \mathbb{R}\} \rightarrow \mathbb{Q}(\mathbb{R} \cup \{\spadesuit\}) : S \mapsto f(S)$$

con:

$$f(S) : \mathbb{Q} \rightarrow \mathbb{R} \cup \{\spadesuit\} : r \mapsto \begin{cases} \max\{x \in S | x < r\} & \text{se esiste} \\ \spadesuit & \text{altrimenti} \end{cases}$$

ossia la mappa che associa ogni sottoinsieme bene ordinato di \mathbb{R} alla funzione da \mathbb{Q} in $\mathbb{R} \cup \{\spadesuit\}$. Chiaramente $|\mathbb{R} \cup \{\spadesuit\}| = 2^{\aleph_0} + 1 = 2^{\aleph_0}$, da cui l'asserto.

Va da sé che $\text{Im}(f(S)) \setminus \{\spadesuit\} \subseteq S$, ci basta quindi dimostrare l'inclusione opposta, ossia che, dato $S \subseteq \mathbb{R}$ bene ordinato da $<_{\mathbb{R}}$, per ogni $x \in S$ esiste un $r \in \mathbb{Q}$ tale che $(f(S))(r) = x$. Ci sono due casi:

- se $x = \max(S)$, allora basta un qualunque $r > x$
- se x non è il massimo di S , sia $y := \min\{z \in S | z > x\}$, che esiste perché S è bene ordinato. Per densità c'è $r \in \mathbb{Q}$ con $x < r < y$ e chiaramente $x = (f(S))(r)$.

\square

²⁰⁸In realtà con AC si fa la stessa cosa, ma si evita di definire una mappa come quella sotto, poiché in ogni intervallo tra elementi ordinati di S possiamo semplicemente scegliere un elemento e concludere allo stesso modo (usando le parti di \mathbb{Q}).

§A.2 Forma normale di ω_α

Proposizione A.9 ($\omega_\alpha = \omega^{\omega_\alpha}$)

Dato ω_α , l'immagine di α mediante la funzione degli aleph, la sua forma normale di Cantor è data da:

$$\omega_\alpha = \omega^{\omega_\alpha}$$

Dimostrazione. Ci basta dimostrare le due diseguaglianze.

\leq Osserviamo che la mappa $x \mapsto \omega^x$ è strettamente crescente tra ordinali (se la pensiamo come funzione da Ord a Ord), ci basta osservare che per le funzioni classe strettamente crescenti, da una classe a se stessa, vale la medesima proprietà che abbiamo visto per funzioni strettamente crescenti da un buon ordine a se stesso, ovvero l'immagine sta sopra la diagonale ($F(n) \geq n$).

Questa cosa continua a funzionare con la stessa dimostrazione (in particolare ci serve semplicemente dire che ogni sottoinsieme di ordinali ha minimo), infatti se per assurdo ci fosse un $m \in \text{Ord}$ per cui $F(m) < m$, allora l'insieme di ordinali per cui ciò è vero è non vuoto ed ha minimo k [come abbiamo dimostrato per gli insiemi di ordinali], per il quale si ha $F(k) < k$ e $F(F(k)) < F(k)$, cioè $F(k)$ appartiene all'insieme degli ordinali che non rispettano la proprietà ed è più piccolo di k , che è contro la minimalità di k , quindi assurdo.

A questo punto quanto dimostrato vale anche per l'esponenziazione di ω ad un ordinale in quanto la funzione è strettamente crescente, da cui si ha $\omega_\alpha \leq \omega^{\omega_\alpha}$.

\geq Vogliamo dimostrare che $\omega^{\omega_\alpha} \leq \omega_\alpha$, per definizione (essendo un ordinale limite):

$$\omega^{\omega_\alpha} = \{\omega^\beta \mid \beta < \omega_\alpha\} = \sup\{\omega^\beta \mid |\beta| < \aleph_\alpha\}$$

dove la seconda uguaglianza deriva dal fatto che è equivalente considerare un ordinale che sta in ω_α o che ha cardinalità \aleph_α , in quanto ω_α è l'ordinale più piccolo della sua cardinalità, quindi qualsiasi ordinale più grande ha necessariamente cardinalità maggiore e viceversa.

Basta quindi dimostrare che $|\beta| < \aleph_\alpha \rightarrow |\omega^\beta| < \aleph_\alpha$ (da cui $\sup\{\omega^\beta \mid \beta < \omega_\alpha\} \leq \omega_\alpha$, perché stiamo di fatto dimostrando che ω_α è un maggiorante di $\{\omega^\beta \mid \beta < \omega_\alpha\}$, dunque essendo il sup il minimo dei maggioranti si ha la diseguaglianza). Sappiamo che ω^β è isomorfo [come buon ordinamento] a $S_\beta : \{f : \beta \rightarrow \omega \mid |\text{supp}(f)| < \aleph_0\}$ con un opportuno ordinamento. Ad ogni $f \in S_\beta$ associamo $f_{|\text{supp}(f)} \in \mathcal{P}^{\text{fin.}}(\beta \times \omega)$, tale corrispondenza è naturalmente iniettiva e ci dà:

$$|\omega^\beta| \leq |\mathcal{P}^{\text{fin.}}(\beta \times \omega)| \stackrel{\text{AC}}{=} |\beta| \cdot \aleph_0 \stackrel{\text{H.p.}}{<} \aleph_\alpha$$

□

§A.3 Sottoinsiemi infiniti di cardinalità fissata

Proposizione A.10 (Numero di sottoinsiemi infiniti di cardinalità fissata)

Dato un insieme X infinito, con $|X| = \kappa$, dato $\nu \leq \kappa$, cardinale infinito, allora:

$$|\mathcal{P}^\nu(X)| = |\{Y \in \mathcal{P}(X) : |Y| = \nu\}| = \kappa^\nu$$

Dimostrazione. Per la disegualanza dall'alto è facile osservare che $\mathcal{P}^\nu(X) \subseteq \mathcal{P}^{\leq\nu}(X)$ e la mappa:

$$\kappa^\nu \rightarrow \mathcal{P}^{\leq\nu}(X) : f \mapsto \text{Im}(f)$$

è surgettiva, infatti, dato $Z \in \mathcal{P}^{\leq\nu}(X)$, si ha $|Z| \leq \nu$, dunque esiste $g : \nu \rightarrow Z$ surgettiva, che può essere naturalmente considerata come funzione da ν a κ con l'immagine voluta.²⁰⁹ Abbiamo quindi che $|\mathcal{P}^\nu(X)| \leq |\mathcal{P}^{\leq\nu}(X)| \leq \kappa^\nu$. Per il viceversa ci basta osservare che $f \in \kappa^\nu$ è un sottoinsieme di $\nu \times \kappa$ di cardinalità ν , per cui $\kappa^\nu \subseteq \mathcal{P}^\nu(\nu \times \kappa)$, ma essendo che $\kappa \cdot \nu = \kappa = |X|$, allora $|\mathcal{P}^\nu(X)| = |\mathcal{P}^\nu(\nu \times \kappa)|$ - dove la bigezione è indotta da una bigezione tra $\nu \times \kappa$ e X -. Abbiamo quindi: $\kappa^\nu \leq |\mathcal{P}^\nu(\nu \times \kappa)| \leq |\mathcal{P}^\nu(X)|$. \square

§A.4 Sottrazione cardinale

Proposizione A.11 (Sottrarre cardinali)

Sia $A \subseteq X$ e $|X| \geq \aleph_0$ (cioè almeno infinito per AC^a), se $|A| < |X|$ allora abbiamo che vale: $|X \setminus A| = |X|$.

^aQuesta proposizione e la dimostrazione annessa dipendono pesantemente da AC.

Dimostrazione. Per AC $|X| = \aleph_\alpha$ e $|A| = |\aleph_\beta|$, con $\alpha > \beta$ ordinali (per la monotonia della funzione degli aleph). Abbiamo che:

$$X = (A \sqcup X) \setminus A$$

cioè $|X| = |A| + |X \setminus A| \iff \aleph_\alpha = \aleph_\beta + \aleph_\gamma$, con $\aleph_\beta + \aleph_\gamma = \aleph_{\max(\beta, \gamma)}$. A questo punto se $\gamma < \alpha \implies \max(\beta, \gamma) < \alpha$ e per monotonia della funzione degli aleph $\aleph_{\max(\beta, \gamma)} < \aleph_\alpha$, che è assurdo. Se $\gamma > \alpha \implies \max(\beta, \gamma) = \gamma$ (perché $\beta < \alpha$) e si otterrebbe, di nuovo per monotonia, $\aleph_\alpha < \aleph_\gamma$ che è ancora assurdo. L'unica possibilità che rimane²¹⁰ quindi è che $\gamma = \alpha \implies \aleph_\gamma = \aleph_\alpha \iff |X \setminus A| = |X|$. \square

²⁰⁹Osservare che avremmo anche potuto fare la mappa iniettiva al contrario fissando bigezioni con AC.

²¹⁰Notare che questo è vero anche senza AC perché gli ordinali sono totalmente ordinati per quanto abbiamo detto sulla relazione d'ordine tra buoni ordinamenti (naturalmente stiamo facendo pesante uso di AC, quindi in ogni caso varrebbe).

§A.5 Rango ordinale

Il seguente risultato amplia quanto già visto nel capitolo dedicato a buona fondazione, ovvero che $\alpha \subseteq V_\alpha$, dandoci un risultato più generale.

Proposizione A.12 (Rango di un ordinale)

Dato $\alpha \in \text{Ord}$ vale che $\text{rank}(\alpha) = \alpha$.

Dimostrazione. Procediamo per induzione transfinita.

caso 0 È ovvio che $\emptyset \notin V_0$ e $\emptyset \in V_1$, dunque $\text{rank}(0) = 0$.

caso successore Supponiamo che $\text{rank}(\alpha) = \alpha$ e dimostriamo che $\text{rank}(\alpha + 1) = \alpha + 1$. Per ipotesi $\alpha \in V_{\alpha+1}$, cioè il minimo elemento della gerarchia che ha come elemento α è $V_\alpha + 1$, ciò implica in automatico che $V_{\alpha+1}$ è anche il minimo insieme ad avere $\{\alpha\}$ come sottoinsieme, altrimenti α apparterrebbe a qualche V_β con $\beta < \alpha$ e non può accadere. Osserviamo inoltre che, per transitività, $\alpha \in V_{\alpha+1} \implies \alpha \subseteq V_{\alpha+1}$, per cui abbiamo:

$$\alpha + 1 = \underbrace{\alpha}_{\subseteq V_{\alpha+1}} \cup \underbrace{\{\alpha\}}_{\subseteq V_{\alpha+1}} \subseteq V_{\alpha+1} \implies \alpha + 1 \in V_{\alpha+2}$$

da cui $\text{rank}(\alpha + 1) \leq \alpha + 1$. D'altra parte $\alpha \in \alpha + 1$ per costruzione, quindi $\alpha = \text{rank}(\alpha) < \text{rank}(\alpha + 1)$, ovvero $\alpha + 1 \leq \text{rank}(\alpha + 1)$ e ciò ci fa concludere. Alternativamente si poteva notare che se fosse minore o uguale ad α , $\{\alpha\}$ non potrebbe essere un sottoinsieme di $\alpha + 1$ (che è assurdo), in quanto, come visto sopra, per avere $\{\alpha\}$ come sottoinsieme abbiamo bisogno almeno di essere in $V_{\alpha+1}$, dunque $\alpha + 1 \leq \text{rank}(\alpha + 1)$, e si conclude di nuovo.

caso limite Supponiamo che $\forall \alpha < \lambda \text{ rank}(\alpha) = \alpha$ e dimostriamo che $\text{rank}(\lambda) = \lambda$. Osserviamo che, sapendo che $y \in x \implies \text{rank}(y) < \text{rank}(x)$, si ha:

$$\forall \alpha < \lambda \alpha = \text{rank}(\alpha) < \text{rank}(\lambda)$$

cioè $\text{rank}(\lambda)$ è un maggiorante di $\{\alpha | \alpha < \lambda\}$, quindi è maggiore o uguale dell'estremo superiore di questo insieme, $\lambda \leq \text{rank}(\lambda)$. D'altra parte, sappiamo che $\lambda \subseteq V_\lambda \implies \lambda \in V_\lambda$, per cui $\text{rank}(\lambda) = \lambda$.

□

Osservazione A.13 (Alternativa per il caso limite) — Da un esercizio alla fine del capitolo su buona fondazione sappiamo che $\text{rank}(x) = \sup\{\text{rank}(y) + 1 | y \in x\}$, e possiamo sfruttare questa caratterizzazione per fare il caso limite della dimostrazione precedente in maniera alternativa:

$$\begin{aligned} \text{rank}(\lambda) &= \sup\{\text{rank}(\alpha) + 1 | \alpha < \lambda\} && (\text{Hp. induttiva}) \\ &= \sup\{\alpha + 1 | \alpha < \lambda\} = \lambda \end{aligned}$$

Volendo questa caratterizzazione la si poteva usare anche per fare il caso successore in maniera alternativa.

§A.6 Teorema di Cantor-Lebesgue

Richiamiamo brevemente tre fatti visti nel prologo.

Fatto A.14 (Criterio per gli insiemi di unicità)

Dato $X \subseteq \mathbb{R}$ se (ma non solo se) ogni funzione continua $f : \mathbb{R} \rightarrow \mathbb{R}$ che soddisfi:

- per ogni intervallo aperto $]a, b[$ con $]a, b[\cap X = \emptyset$, $f|_{]a, b[}$ è lineare.
- per ogni $x \in \mathbb{R}$, se f ha derivate destre e sinistre in x , allora queste coincidono^a.

è lineare^b, allora X è di unicità.

^aOvvero f non ha punti angolosi.

^b $f(x) = \alpha x + \beta$.

Ricordiamo che con (\star) indichiamo la proprietà in viola.

Osservazione A.15 (Derivato di un chiuso soddisfa $(\star) \implies$ chiuso soddisfa (\star)) —

Se X è chiuso e X' soddisfa (\star) - per cui X' è di unicità per il criterio -, allora anche X è di unicità.

Corollario A.16 (Derivato n -esimo soddisfa $(\star) \implies$ insieme soddisfa (\star))

Detto $X^{(n)}$ il derivato n -esimo di X , se per $X^{(n)}$ vale (\star) , per qualche $n \in \mathbb{N}$, allora anche per X vale (\star) , quindi per il Fatto 1.5 è di unicità.^a

^aIl caso con $X^{(n)} = \emptyset$ scritto da Mamino nelle note è un caso particolare di questo.

Questi, uniti a quanto visto nella sezione sul teorema di Cantor-Bendixson, ci permettono finitamente di dimostrare il seguente risultato.

Teorema A.17 (Teorema di Cantor-Lebesgue)

Se $X \subseteq \mathbb{R}$ è chiuso e numerabile, allora X soddisfa (\star) , e quindi è di unicità.

Dimostrazione. Per il teorema di Cantor-Bendixson possiamo scrivere $C = P \cup A$, con P perfetto e A al più numerabile, ed essendo per ipotesi C numerabile ed i perfetti non vuoti di \mathbb{R} continui, si deve avere che $P = \emptyset$ e $C = A$. Dove P è il **derivato di Cantor-Bendixson**, che era definito come:

$$P = \bigcap_{\alpha \in \text{Ord}} X_\alpha = \{x \in \mathbb{R} \mid \forall \alpha \in \text{Ord } x \in X_\alpha\} \quad \text{con } X_\alpha = \begin{cases} X_0 = X \\ X_{\alpha+1} = X'_\alpha \\ X_\lambda = \bigcap_{\gamma < \lambda} X_\gamma \quad \lambda \text{ limite} \end{cases}$$

Ora essendo X chiuso la successione così definita è decrescente - perché $X' = X \setminus \{\text{punti isolati di } X\}$ - e naturalmente per il principio della discesa infinita generalizzato si deve stabilizzare, essendo $P = \emptyset$, la successione si stabilizza necessariamente nel vuoto, ovvero $\exists \beta \in \text{Ord } \forall \delta \geq \beta X_\delta = \emptyset$. Abbiamo quindi che $X_\beta = \emptyset$ per $\beta \in \text{Ord}$, per cui X_β soddisfa (\star) , non ci resta che generalizzare il corollario sopra per ottenere la tesi.

Vogliamo dimostrare che se X_α soddisfa (\star) per qualche $\alpha \in \text{Ord}$, allora anche X (chiuso)

soddisfa (\star) , ed è quindi di unicità per il fatto sopra. Procediamo per induzione transfinita assumendo il risultato dell'osservazione, che abbiamo già dimostrato nel prologo.

caso 0 Se $X^{(0)} = X$ soddisfa (\star) allora abbiamo finito.

caso successore Supponiamo che se X_α soddisfa (\star) allora X soddisfa (\star) e dimostriamo che se $X_{\alpha+1}$ soddisfa (\star) , allora X soddisfa (\star) . Detto $Y = X_\alpha$, allora $Y' = X_{\alpha+1}$, per cui, per l'osservazione $Y = X_\alpha$ soddisfa (\star) , quindi per ipotesi induttiva anche X soddisfa (\star) e abbiamo concluso.

caso limite Supponiamo che $\forall \gamma < \lambda X_\gamma$ se X_γ soddisfa (\star) , allora X soddisfa (\star) , e dimostriamo che se X_λ soddisfa (\star) allora anche X soddisfa (\star) .

Ci basta verificare che uno degli X_γ , per $\gamma < \lambda$, rispetta (\star) per poter applicare l'ipotesi induttiva ed ottenere quanto voluto. Data $f \in C^0(\mathbb{R})$, senza punti angolosi e lineare quando ristretta ad intervalli aperti che non intersecano X_γ , verifichiamo che è lineare. Poiché $X_\lambda \subseteq X_\gamma$, e per X_λ vale (\star) , f rispetta la condizione di essere lineare sugli intervalli aperti che non intersecano $X_\gamma \supseteq X_\lambda$, quindi la rispetta in automatico su X_λ , e poiché rispetta banalmente anche le altre due condizioni per X_λ allora è lineare - perché per ipotesi appunto la proprietà (\star) vale per X_λ e questo ci dà la linearità globale di f -, e quindi anche X_γ rispetta (\star) .

□

§A.7 ϵ -ricorsione

Teorema A.18 (Principio di ϵ -ricorsione)

Data una funzione classe $G : V \rightarrow V$ esiste ed è unica la funzione classe $F : V \rightarrow V$ tale che:

$$\forall x F(x) = G(F|_x)$$

L'idea è imitare la dimostrazione del teorema di ricorsione transfinita v.1 usando l' ϵ -induzione al posto dell'induzione transfinita.

INCOMPLETA. Definiamo una funzione delle troncate della funzione F che vogliamo definire, per mezzo di delle approssimazioni finite come segue:

$$y = H(x) \stackrel{\text{def}}{=} \begin{cases} \exists f \text{ funzione} \\ \text{Dom}(f) = \text{tc}(x) \\ \forall z \in x f(z) = G(f(z)) \end{cases} \wedge y = f$$

Per avere che $H : V \rightarrow V$ è ben definita come funzione classe, vogliamo dimostrare:

$$\forall x \exists ! f \quad f \text{ è una } x\text{-approssimazione}$$

procediamo per ϵ -induzione come segue. Dato x , supponiamo per ipotesi induttiva che per ogni $y \in x$ esistano e siano uniche le y -approssimazioni, f_y , e dimostriamo che esiste ed è unica una x -approssimazione. Consideriamo:

$$f := \bigcup_{y \in x} f_y$$

e osserviamo che:

- ◊ f è una funzione: dobbiamo dire che prese f_{y_1}, f_{y_2} due funzioni dell'unione, queste due coincidono sull'intersezione, preso infatti $z \in \text{tc}(y_1) \cap \text{tc}(y_2)$
- ◊ $\text{Dom}(f) = \text{tc}(x)$: si osserva che:

$$\text{Dom}(f) = \bigcup_{y \in x} \text{Dom}(f_y) = \bigcup_{y \in x} \text{tc}(y) = \text{tc}(x)$$

dove l'ultima uguaglianza è una facile verifica.

- ◊ $\forall z \in x f(z) = G(f|_z)$: se $z \in x$, allora $z \in \text{tc}(y)$ per qualche $y \in X$, per cui $f(z) = f_y(z) \stackrel{\text{Hp. indutt.}}{=} G(f|_z) = G(f|_z)$, dove l'ultima uguaglianza vale perché f è un'estensione di f_y per definizione - che è lo stesso motivo per cui vale la prima -.

Resta infine da verificare l'unicità di f come unica x -approssimazione, date f' e f'' entrambe x -approssimazioni osserviamo che:

$$\forall z \in x f'(z) = G(f'|_z) = G(f''|_z) = f''(z)$$

A questo punto possiamo definire $F : V \rightarrow V$ come segue:

$$y = F(x) \stackrel{\text{def}}{=} f = H(\text{tc}(x)) \wedge y = f(x)$$

quindi si ha $F(x) = f(x) = G(f_x)$, per cui non ci resta che verificare che $f_{|x} = F_{|x}$, ovvero $\forall z \in x F(z) = f(z)$. Per ipotesi si ha che $z \in \text{tc}(y)$ per qualche $y \in x$, per cui $F(z) = f'(z)$, con $f' = H(y)$, quindi $f'(z) = f(z)$ poiché le funzioni date da $H(\cdot)$ coincidono sull'intersezione dei loro domini per l'unicità vista prima.

Non ci rimane altro che verificare l'unicità di F , per farlo procediamo ancora per ϵ -induzione, date F_1 ed F_2 che soddisfano la tesi, per ipotesi induttiva abbiamo che $F_{1|x} = F_{2|x}$, per cui:

$$F_1(x) = G(F_{1|x}) \stackrel{\text{Hyp. indutt.}}{=} G(F_{2|x}) = F_2(x)$$

pertanto vale il passo induttivo, e quindi l'induzione ci garantisce che $\forall x F_1(x) = F_2(x)$, ovvero F è unica come funzione classe. \square

Riferimenti bibliografici

- [1] Marcello Mamino, *Elementi di teoria degli insiemi*, Università di Pisa, Pisa, 2022-23.
- [2] Karel Hrbacek, Thomas Jech, *Introduction to Set Theory, Revised and Expanded*, CRC Press, Boca Raton, Florida, 3rd edition, 1999.
- [3] Mauro Di Nasso, *Elementi di teoria degli insiemi, Dispensa 4*, Università di Pisa, Pisa, 2019-20.
- [4] Marcello Mamino, *Elementi di teoria degli insiemi*, Università di Pisa, Pisa, 2020-21.
- [5] Marcello Mamino, *Elementi di teoria degli insiemi - esercizi sulle cardinalità*, Università di Pisa, Pisa, 2022-23.
- [6] Marcello Mamino, *Elementi di teoria degli insiemi - soluzioni esercizi sulle cardinalità*, Università di Pisa, Pisa, 2020-21.