

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	5
1.1	Digressione: insiemi numerabili	8
1.2	Tornando agli insiemi di unicità	10
1.3	Giochi di parole	12
1.4	Scopi del corso	13
2	Il linguaggio della teoria degli insiemi	14
2.1	Le regole di inferenza	16
3	I primi assiomi	18
3.1	Assiomi dell'insieme vuoto e di estensionalità	18
3.2	Assioma di separazione	19
3.3	Classi e classi proprie	20
3.4	Assioma del paio e coppia di Kuratowski	21
3.5	Assioma dell'unione e operazioni booleane	24
3.6	Assioma delle parti e prodotto cartesiano	27
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	45
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	65
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	87
8.1	Caratterizzazione dei reali come ordine	90
8.2	La cardinalità del continuo è 2^{\aleph_0}	92
8.3	Operazioni che coinvolgono la cardinalità del continuo	93
8.4	Sottrarre un numerabile dal continuo	94
	Stato del corso	97
9	I buoni ordinamenti	98
9.1	Operazioni aritmetiche fra buoni ordinamenti	103

9.2	Gli ordinali di Von Neumann	108
9.3	L'assioma del rimpiazzamento	115
9.4	Induzione e ricorsione transfinita	119
10	Aritmetica ordinale e forma normale di Cantor	127
10.1	Sottrazione e divisione euclidea	130
10.2	La forma normale di Cantor	132
10.3	Punti fissi e ε -numbers	133
10.4	Operazioni in forma normale di Cantor	135
11	Gli aleph	140
11.1	Teorema di Hartogs	140
11.2	Somme e prodotti di aleph	144
12	L'assioma della scelta	146
12.1	Buon ordinamento \rightarrow AC	149
12.2	AC \rightarrow buon ordinamento (idea)	149
A	Soluzioni di altri esercizi e cardinalità note	150
	Bibliografia	151

Premessa

Queste dispense sono la quasi esatta trascrizione in \LaTeX delle dispense del corso di Elementi di teoria degli insiemi, tenuto dal prof. Marcello Mamino nell'anno accademico 2022-23 presso l'Università di Pisa.

Ringraziamenti

Francesco Sorce, Rubens Martino, Lorenzo Picinelli.

Quest'opera è stata rilasciata con 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

$X \subseteq \mathbb{R}$ è di unicità se (ma non solo se) ogni funzione continua $f : \mathbb{R} \rightarrow \mathbb{R}$ che soddisfi le ipotesi seguenti è necessariamente lineare^a:

- 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^b.

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

^bOvvero f non ha punti angolosi.

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.

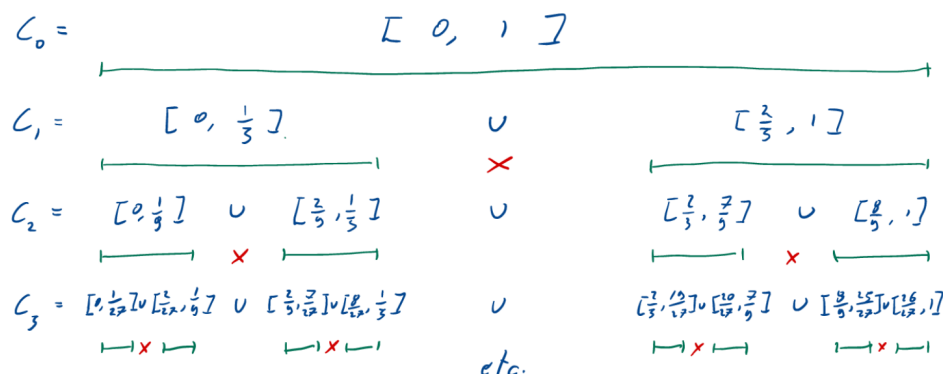
NON Esempio 1.7

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.

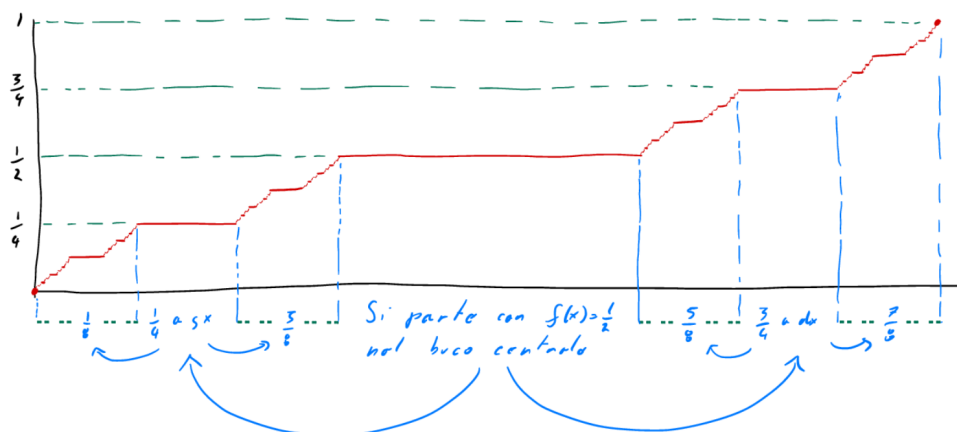
Possiamo costruire l'insieme di Cantor a partire dall'intervallo $C_0 = [0, 1]$ nel seguente modo:



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 , a questo punto definiamo l'insieme di Cantor C come:

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

Esiste una funzione continua (e 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 $x \in C$.

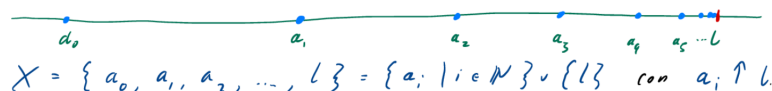


tale funzione si costruisce aggiungendo tratti costanti (prima $\frac{1}{2}$, poi $\frac{1}{4}$, $\frac{3}{4}$ e così via, dividendo l'intervallo $[0, 1]$ sull'asse delle ordinate in parti uguali) alle parti eliminate sull'intervallo $[0, 1]$ sull'asse delle ascisse per costruire l'insieme di Cantor.

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

Esempio buffo 1.10

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

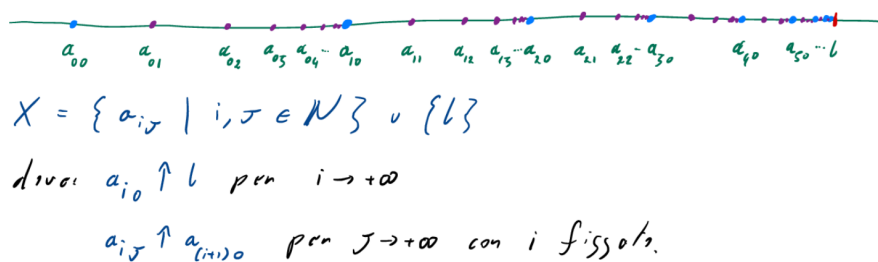


Dimostriamo quindi che X è un insieme di unicità.

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

Esempio più buffo 1.11

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



Dimostriamo che X è di unicità.

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

§1.1 Digressione: insiemi numerabili

Definizione 1.12. Un insieme X è **numerabile** se è il supporto di una successione, $X = \{a_0, a_1, a_2, \dots\} = \{a_i | i \in \mathbb{N}\}$, con $a_i \neq a_j$ per ogni $i \neq j$.¹

Esempio 1.13

Alcuni esempi di insiemi numerabili sono:

- \mathbb{N} , l'insieme dei numeri naturali, infatti, la successione $a_i = i$ realizza la biezione.
- I numeri dispari, con la biezione 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 biezione data da $a_i = (-1)^i \left\lfloor \frac{i}{2} \right\rfloor$.

Esempio meno immediato 1.14

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

Dimostrazione. La funzione $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} : (x, y) \longmapsto 2^x(1 + 2y) - 1$ è biunivoca (perché?), quindi $a_i = f^{-1}(i)$ enumera $\mathbb{N} \times \mathbb{N}$. \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_* 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, $\mathbb{N} \times \mathbb{N} = \{(i, j) | i, j \in \mathbb{N}\}$. Quindi $X \times Y = \{(a_{i_t}, b_{j_t}) | t \in \mathbb{N}\}$. \square

Esempio 1.17

\mathbb{Q} è numerabile.

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

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

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

□

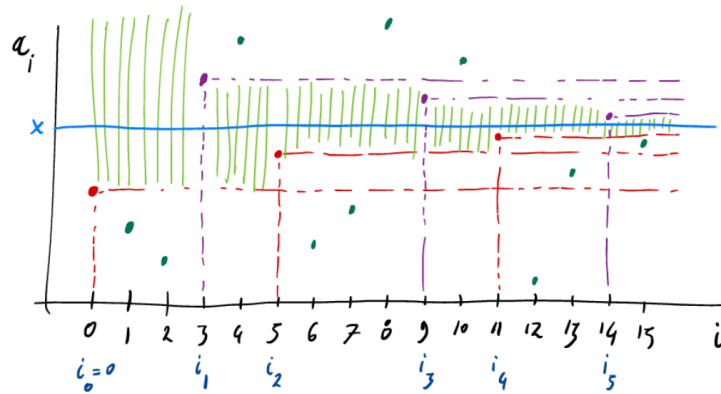
NON Esempio 1.18

\mathbb{R} non è numerabile.

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

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

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.

□

²num. = numeratore, den. = denominatore.

§1.2 Tornando agli insiemi di unicità

Teorema 1.21 (Cantor-Lebesgue)

Se $X \subseteq \mathbb{R}$ è chiuso e numerabile, allora X soddisfa il Fatto 1.5, ed è, quindi, 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 — Se X è chiuso e per X' vale il Fatto 1.5, allora anche per X vale il Fatto 1.5.

Dimostriamo questo fatto.

Dimostrazione. Occorre dimostrare che se f è continua, lineare, ristretta agli intervalli aperti che non intersecano X , e non ha punti angolosi, allora f è lineare ristretta agli intervalli aperti che non intersecano X' . Fatto questo, usando l'ipotesi su X' , f è lineare - abbiamo quindi mostrato che per X vale Fatto 1.5.

Sia $]a, b[\cap X' = \emptyset$, dobbiamo dire che $f|_{]a, b[}$ è lineare. Ci basta dire che per ogni $\varepsilon > 0$, $f|_{[a+\varepsilon, b-\varepsilon]}$ è lineare. Siccome $]a, b[\cap X' = \emptyset$, $]a, b[\cap X = \{\text{punti isolati di } X\}$. Quindi $[a+\varepsilon, b-\varepsilon] \cap X$ è finito - se così non fosse, avrebbe un punto di accumulazione α che non può essere un punto isolato di X (altrimenti si avrebbe un assurdo). Per cui $f|_{[a+\varepsilon, b-\varepsilon]}$ è lineare a tratti, e, siccome non ha punti angolosi, è lineare. \square

Corollario 1.24

Sia $X^{(n)} = X'' \dots^a$. Se $X^{(n)} = \emptyset$ per qualche $n \in \mathbb{N}$, allora per X vale il Fatto 1.5.

^a n volte.


Dimostrazione. Induzione su n . \square

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

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 $a_i \uparrow +\infty$ per $i \rightarrow \infty$.



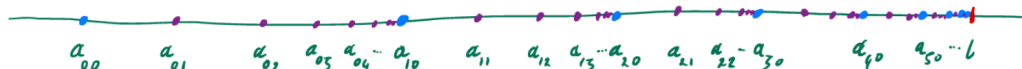
Tutti i punti sono isolati, $X' = \emptyset$.

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

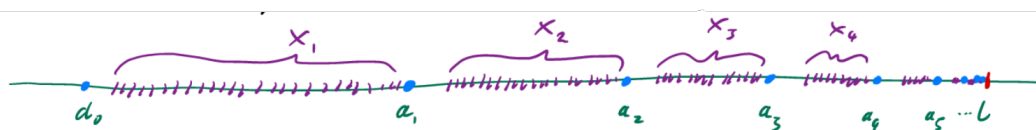


“Successione con punto limite”. Tutti i punti sono isolati salvo l , quindi $X' = \{l\}$ e $X'' = \emptyset$.

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



“Successione di successioni”, $X' = \{a_{1,0}, a_{2,0}, \dots, l\}$, $X'' = \{l\}$ 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.

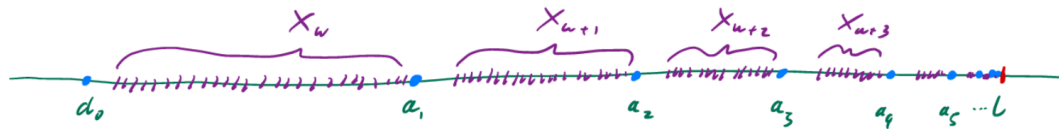
Esercizio 1.26. Perché X_ω è numerabile?

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 $X_{\omega \cdot 2}$?



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 = “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 dicano quali costruzioni sono lecite: quali insiemi esistono. Il ruolo della teoria degli insiemi è, poi, di fondare l’edificio della matematica. L’ambizione, quindi, è che il linguaggio e gli assiomi della teoria degli insiemi, siano in realtà, il linguaggio e gli assiomi della matematica.

§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:

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

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):

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

quindi ad esempio:

$$\neg \Phi \equiv \text{“}\Phi \text{ è falsa”}$$

$$\Phi \wedge \psi \equiv \text{“}\Phi \text{ e } \psi \text{ sono entrambe vere”}$$

$$\Phi \vee \psi \equiv \text{“almeno una fra } \Phi \text{ e } \psi \text{ è vera”}$$

- quantificatori** ovvero quello universale “per ogni” e quello esistenziale “esiste”:

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

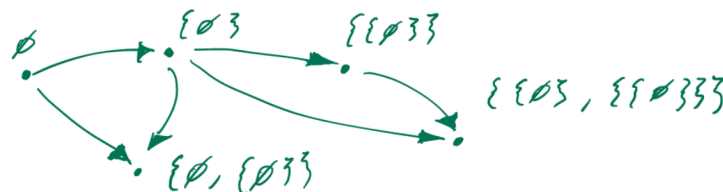
ad esempio:

$$\forall x \Phi \equiv \text{“}\Phi \text{ è vera qualunque sia l'insieme } x\text{”}$$

$$\exists x \Phi \equiv \text{“c'è un insieme } x \text{ che fa sì che } \Phi \text{ sia vera”}$$

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:

$$\begin{aligned} x \neq y &\stackrel{\text{def}}{=} \neg x = y^5 & x \notin y &\stackrel{\text{def}}{=} \neg x \in y & \nexists x \Phi &\stackrel{\text{def}}{=} \neg \exists x \Phi \\ \Phi \rightarrow \psi &\stackrel{\text{def}}{=} \psi \vee \neg \Phi & \Phi \leftrightarrow \psi &\stackrel{\text{def}}{=} (\Phi \rightarrow \psi) \wedge (\psi \rightarrow \Phi) \\ \exists x \in y \Phi &\stackrel{\text{def}}{=} \exists x(x \in y \wedge \Phi) & \forall x \in A \Phi &\stackrel{\text{def}}{=} \forall x(x \in A \rightarrow \Phi) \\ \exists! x \Phi(x) &\stackrel{\text{def}}{=} \exists x(\Phi(x) \wedge \forall y(\Phi(y) \rightarrow y = x)) \\ \exists! x \in A \Phi(x) &\stackrel{\text{def}}{=} \exists! x(x \in A \wedge \Phi(x)) \\ A \subseteq B &\stackrel{\text{def}}{=} \forall x(x \in A \rightarrow x \in B) & A \subsetneq B &\stackrel{\text{def}}{=} (A \subseteq B) \wedge (A \neq B) \\ C = A \cup B &\stackrel{\text{def}}{=} \forall x x \in C \leftrightarrow (x \in A \vee x \in B) \\ C = A \cap B &\stackrel{\text{def}}{=} \forall x x \in C \leftrightarrow (x \in A \wedge x \in B) \end{aligned}$$

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.

⁴Mi riservo in queste dispense di modificare un pochino questa regola, qualora alcune formule risultassero più leggibili con le parentesi.

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, $\neg\Phi \vee \neg\psi \equiv \neg(\Phi \wedge \psi)$. 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 “**tabella di verità**”.

Φ	ψ	$\neg\Phi$	$\neg\psi$	$\neg\Phi \vee \neg\psi$	$\Phi \wedge \psi$	$\neg(\Phi \wedge \psi)$
V	V	F	F	F	V	F
V	F	F	V	V	F	V
F	V	V	F	V	F	V
F	F	V	V	V	F	V

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:

$$\neg\neg\Phi \equiv \Phi \quad \Phi \wedge (\psi \vee \Theta) \equiv (\Phi \wedge \psi) \vee (\Phi \wedge \Theta) \quad \Phi \vee (\psi \wedge \Theta) \equiv (\Phi \vee \psi) \wedge (\Phi \vee \Theta)$$

$$\neg(\Phi \wedge \psi) \equiv \neg\Phi \vee \neg\psi \quad \neg(\Phi \vee \psi) \equiv \neg\Phi \wedge \neg\psi$$

$$\Phi \rightarrow \neg\psi \equiv \psi \rightarrow \neg\Phi \quad \Phi \rightarrow \psi \equiv \neg\psi \rightarrow \neg\Phi$$

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.

$$\begin{aligned}\neg\forall x \Phi &\equiv \exists x \neg\Phi & \neg\forall x \neg\Phi &\equiv \exists x \Phi \\ \neg\exists x \Phi &\equiv \forall x \neg\Phi & \neg\exists x \neg\Phi &\equiv \forall x \Phi\end{aligned}$$

Esercizio 2.5. Convinciti della validità delle equivalenze precedenti.

Esercizio 2.6. Dimostra che:

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

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 $\{x \in A \mid \psi(x)\}$ ^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 $\{x \in A \mid \psi(x)\}$ 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:

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

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.

$$\nexists V \forall x x \in V$$

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

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

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, abbiamo 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:

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

^aNon 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 $\hat{}$ 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:

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

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:

$$\forall y \in c (x \in y) \xrightarrow{\text{ipotesi}} x \in \{a\} \xrightarrow{\text{singoleto}} x = a$$

Determiniamo ora b , studiamo prima il caso in cui $\exists! x (x \in c)$ ¹⁴:

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

ovvero se e solo se i due insiemi che formano $c = (a, b)$ sono il singoletto $\{a\}$ (per **estensionalità**). In questo caso b è determinato, se non fosse così allora $\{a, b\}$ (che corrisponde a b nella coppia ordinata) sarebbe univocamente determinato da:

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

in tal modo abbiamo che:

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

Possiamo quindi ricavare la tesi come segue:

$$\begin{aligned} (a = a' \wedge b = b') &\leftrightarrow (\forall y \in c (a' \in y)) \wedge (b' \in \{a, b\} \wedge b' \neq a) \\ &\leftrightarrow \{a\} = \{a'\} \wedge \{a, b\} = \{a, b'\} \\ &\leftrightarrow (a, b) = (a', b') \end{aligned}$$

(dove nel secondo passaggio abbiamo usato **estensionalità** per giustificare le uguaglianze). \square

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

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

¹³Sostanzialmente stiamo dicendo che preso un elemento x , $x = a$ se e solo se, preso un elemento di $(a, b) = \{\{a\}, \{a, b\}\}$, x appartiene sempre a tale elemento (dovendo appartenere sia ad $\{a\}$ che ad $\{a, b\}$ sarà per forza a).

¹⁴Cioè sto dicendo la coppia è in realtà un insieme fatto da un solo insieme.

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 $x = (a_1, a_2, a_3, \dots, a_{92})$.

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

Assioma 3.28 (Assioma 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** $B_1 = B_2$. □

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

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

^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 **classe**¹⁵ 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 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 [per ipotesi], possiamo prendere $z \in C$. Ora consideriamo (un sottoinsieme di B ottenuto per **separazione** nel modo seguente):

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

¹⁵Quindi, 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).

ovvero il sottoinsieme di z di tutti gli elementi che appartengono a tutti gli elementi di C . Chiaramente (per definizione) $x \in B \rightarrow \forall y \in C(x \in y)$, d'altro canto, $\forall y \in C(x \in y)$ implica, in particolare (un tale x appartiene a tutti gli elementi della classe e quindi anche a z), $x \in z$, quindi in automatico $x \in B$.

Abbiamo così verificato che $x \in B \leftrightarrow \forall y \in C(x \in y)$, ossia $B = \bigcap C$ (moralmente abbiamo costruito l'intersezione di un insieme per separazione su un elemento della classe C (o insieme se lo è), come il sottoinsieme di tutti gli elementi che stanno in tutti gli elementi della classe). L'ultimo ragionamento può essere pensato anche nel seguente modo:

$$\begin{aligned}\forall x x \in B &\leftrightarrow (x \in z \wedge (\forall y \in C(x \in y))) \\ &\stackrel{\text{def.}}{\leftrightarrow} (x \in z) \wedge x \in \bigcap C \\ &\leftrightarrow x \in \bigcap C\end{aligned}$$

dove l'ultima equivalenza è giustificata dal fatto che se x sta in tutti gli elementi degli elementi di C allora x sta in particolare anche in z e quindi il primo termine dell' \wedge può essere rimosso. \square

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

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

Proposizione 3.38 (Caratterizzazione intersezione e differenza di insiemi)

Vale che:

$$\begin{aligned}x \in a \cap b &\leftrightarrow (x \in a \wedge x \in b) \\ x \in a \setminus b &\leftrightarrow (x \in a \wedge x \notin b)\end{aligned}$$

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 :

$$\begin{aligned}\text{commutatività:} & \quad a \cup b = b \cup a \quad \text{e} \quad a \cap b = b \cap a \\ \text{associatività:} & \quad a \cup (b \cup c) = (a \cup b) \cup c \stackrel{\text{def}}{=} a \cup b \cup c \\ & \quad a \cap (b \cap c) = (a \cap b) \cap c \stackrel{\text{def}}{=} a \cap b \cap c \\ \text{distributività:} & \quad a \cup (b \cap c) = (a \cup b) \cap (a \cup c) \\ & \quad a \cap (b \cup c) = (a \cap b) \cup (a \cap c) \\ \text{leggi di De Morgan:} & \quad a \setminus (b \cup c) = (a \setminus b) \cap (a \setminus c) \\ & \quad a \setminus (b \cap c) = (a \setminus b) \cup (a \setminus c)\end{aligned}$$

Dimostrazione. Tutte queste proprietà si 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 $\{\dots\}$ ¹⁶.

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 Assioma 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.

Assioma 3.44 (Assioma delle parti)

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

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

¹⁶Paradossalmente 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.

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 un unico insieme $A \times B$ tale che:

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

^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 dobbiamo 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 $\mathcal{P}(\mathcal{P}(A \cup B))$:^{17 18}

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

pertanto tutte le coppie ordinate di elementi di A e B appartengono a $\mathcal{P}(\mathcal{P}(A \cup B))$ e per separazione possiamo costruire il prodotto cartesiano $A \times B$ come l'insieme di tutte le coppie ordinate. \square

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

¹⁷Poniamo $a, b, \dots \in z \stackrel{\text{def}}{=} a \in z \wedge b \in z \wedge \dots$ e $a, b, \dots \subseteq z \stackrel{\text{def}}{=} a \subseteq z \wedge b \subseteq z \wedge \dots$

¹⁸Tutte 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.

§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:

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

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**: $\forall x, y \in A^{19} \ x \sim y \leftrightarrow y \sim x$.
- (iii) **transitiva**: $\forall x, y, z \in A \ (x \sim y \wedge y \sim z) \rightarrow x \sim z$.

Definizione 3.53. $\leq \subseteq A \times A$ 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. $< \subseteq A \times A$ 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

¹⁹ $\forall x_1, \dots, x_n \stackrel{\text{def}}{=} \forall x_1 \dots \forall x_n$, e lo stesso con \exists e con i quantificatori limitati.

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 di 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.

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 scriveremo $x > y$ 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 disuguaglianze 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 — 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 $f : B \rightarrow C$:

$$f \circ g \stackrel{\text{def}}{=} \{(x, z) \in A \times C \mid z = f(g(x))\}^{20}$$

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

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/bigettive). 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 bigettive 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

²⁰O più formalmente $\exists y(y = g(x) \wedge z = f(y))$.

assurdo, pertanto $x = y$ ²¹. 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 $g : \{0, 1, 2, 3\} \rightarrow \{0, 1, 2\}$, 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

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:

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

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 $B = C$.²²

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 che²³ $f(x) = (\tilde{f} \circ i_\sim)(x), \forall x \in A$ 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

²¹Abbiamo 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

²²Essendo 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 .

²³Per 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.

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

§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 insiemi. Il nostro scopo non è quindi tanto definire, quanto codificare i numeri naturali per mezzo di insiemi opportuni. La scelta della codifica non è obbligata: per esempio potremmo decidere che:

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

Sceglieremo, invece, quest'altra codifica:

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

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

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 successori ²⁴, 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. ²⁵

²⁴Ciò non esclude che ci possano essere altri elementi oltre a \emptyset che non siano successori (questa cosa è sempre falsa in ω).

²⁵Aver 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:

$$\forall x(x \in \omega \leftrightarrow (\forall A \text{ "A è induttivo"} \rightarrow x \in A))^{26}$$

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:

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

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

^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 $x = \{x\} = \{\emptyset\}$ (ossia tutti gli elementi di $s(x)$ devono essere uguali all'unico elemento di $\{\{\emptyset\}\}$). Pertanto avremmo che $x = \{\emptyset\}$, ma $s(x) = s(\{\emptyset\}) = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$, 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 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 $\{\{\emptyset\}\} \notin \omega$.²⁸ \square

²⁶Cioè 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).

²⁷Volendo 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 $\{\emptyset\}$).

²⁸Non 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 ²⁹. In questo senso³⁰, quindi, ω codifica legittimamente i numeri naturali.

Definizione 4.8 (Assiomi di Peano al secondo ordine³¹). Dato un insieme \mathbb{N} , un elemento $0 \in \mathbb{N}$, e una funzione:

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

diciamo che $(\mathbb{N}, 0, \text{succ})$ ³² soddisfa gli assiomi di Peano se:

(a) Il successore è iniettivo:

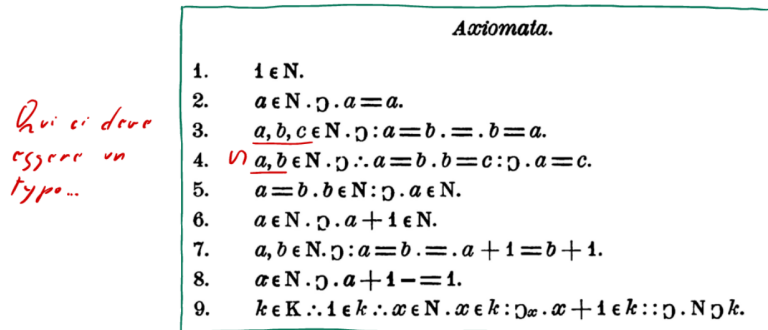
$$\forall n, m \in \mathbb{N} \text{ succ}(m) = \text{succ}(n) \rightarrow m = n$$
³³

(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:

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



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.

²⁹Cioè gli assiomi di Peano diventano enunciati dimostrabili all'interno della ZFC.

³⁰Classicamente 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 .

³¹qualunque cosa questo significhi...

³²La 3-upla ordinata formata dai tre insiemi $\mathbb{N}, 0, \text{succ}$: $((\mathbb{N}, 0), \text{succ}) = \{(\mathbb{N}, 0), \{(\mathbb{N}, 0), \text{succ}\}\} = \{\{\mathbb{N}, \{\mathbb{N}, 0\}\}, \{\{\mathbb{N}, \{\mathbb{N}, 0\}\}, \text{succ}\}\}.$

³³L'altra freccia è banale e sarà data sempre per scontata.

Dimostrazione. Per controllare che succ 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) Dimostriamo che l'insieme $A = \{n \in \omega \mid \Phi(n)\} \subseteq \omega$ è induttivo, da cui $\omega = A$ ³⁴, quindi varrà che $\forall n \in \omega \Phi(n)$.

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

- (2) $n \in A \xrightarrow{\text{def. } A} \Phi(n) \xrightarrow{\text{ipotesi}} \Phi(\text{succ}(n)) = \Phi(s(n)) \xrightarrow{n \in \omega \Rightarrow s(n) \in \omega} s(n) \in A$

- (a) La dimostrazione passa attraverso due lemmi.

Lemma 4.10 (Lemma 1)

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

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

$$\begin{array}{l} \boxed{\Phi(\emptyset)} \quad \bigcup \emptyset = \emptyset \subseteq \emptyset \\ \boxed{\Phi(n) \rightarrow \Phi(s(n))} \quad \bigcup s(n) = \bigcup (n \cup \{n\}) \stackrel{*}{=} \underbrace{\left(\bigcup n \right)}_{\subseteq n} \cup n \stackrel{\text{Hp. indutt.}}{\subseteq} n \cup n = n \subseteq s(n) \end{array}$$

(si noti che il passo base è coerente con le definizioni delle abbreviazioni date), e \star 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

³⁴Stiamo costruendo A come sottoinsieme di ω (che a sua volta sarà contenuto in A , non appena avremo dimostrato che quest'ultimo è induttivo, per definizione).

Lemma 4.11 (Lemma 2)

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

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

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

dove in \star 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:

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

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

§4.2 L'ordine di omega

Convienne, 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)

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

^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 irreflessiva, 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 $b \in s(n) \xrightarrow{\text{Lemma}} s(b) \in s(n) \vee s(b) = s(n)$, abbiamo quindi due casi in base a $s(b)$:

$$s(b) = s(n) \implies a \in s(b) = s(n) \implies a \in s(n)$$

$$s(b) \in s(n) \implies a \in s(b) \in s(n) \implies a \in s(n)$$

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:

$$b = n \implies a \in b = n \xrightarrow{\text{Oss.}} a \in s(n)$$

$$b \in n \implies a \in b \in n \implies a \in n \xrightarrow{\text{Oss.}} a \in s(n)$$

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:

$$s(n) = n \implies n \in n \not\vdash$$

$$s(n) \in n \implies n \in s(n) \in n \implies n \in n \not\vdash$$

($n \in n$ 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 $\forall b \in \omega (\emptyset \in b) \vee (\emptyset = b) \vee (b \in \emptyset)$ ³⁵. 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 $(\emptyset \in m) \vee (\emptyset = m)$. Abbiamo quindi due casi in base all'ipotesi induttiva:

$$\emptyset \in m \implies \emptyset \in s(m)$$

$$\emptyset = m \implies \emptyset \in \{\emptyset\} = s(m)$$

in entrambi i 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:

$$n \in b \xrightarrow{\text{Lemma}} s(n) \in b \vee s(n) = b$$

$$n = b \xrightarrow{\text{Iniett. del succ.}} s(n) = s(b) \implies b \in s(b) = s(n) \implies b \in s(n)$$

$$b \in n \xrightarrow{\text{Oss.}} b \in s(n) \implies b \in a$$

³⁵Ovviamente 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'= \leq , 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.

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

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)

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

^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):

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

($n \not\subseteq n$ 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 corollario³⁶. □

³⁶Mamino 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. Assumiamo vero l’antecedente per ipotesi ovvero assumiamo vera l’implicazione:

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

Dalle tavole di verità quest’espressione può essere vera sia se antecedente e conseguente sono veri sia se l’antecedente è falso. Mostriamo di essere nel primo caso, ovvero dimostriamo per induzione (debole) che [la premessa è vera], ovvero $\forall m \in \omega \psi(m)$ dove:

$$\psi(m) \stackrel{\text{def}}{=} \forall x < m \Phi(x)$$

caso $m = 0$ $\forall x < 0 \Phi(x)$ è vera a vuoto.

caso $m = s(n)$ Per ipotesi induttiva abbiamo $\forall x < n \Phi(x)$. Vogliamo che $x < s(n) \Phi(x)$, dall’osservazione sappiamo che ciò equivale a $x < n \vee x = n$. Si danno quindi due casi:

- Nel caso $x < n$ abbiamo $\Phi(x)$ per ipotesi induttiva.
- Nel caso $x = n$, l’ipotesi induttiva, combinata con l’antecedente ci dà $\Phi(n)$, ossia $\Phi(x)$ (perché abbiamo che $\forall x < n \Phi(x) \rightarrow \Phi(n)$, ma tutta l’espressione è vera per ipotesi e per ipotesi induttiva l’antecedente è vero, quindi anche $\Phi(n)$ lo è). (Per l’arbitrarietà di $x < m$ abbiamo dimostrato $\forall x < m \Phi(x)$)³⁷.

Ora abbiamo dimostrato che $\forall m \in \omega \forall x < m \Phi(x)$, quindi siamo nel secondo caso, e otteniamo che nella premessa $\Phi(n)$ è vera. Ora dato un $n \in \omega$ qualunque, ci basta prendere nell’antecedente $m = n + 1$ e $x = n$ e otteniamo in automatico $\Phi(n)$ (e siamo sicuri sia vera visto che abbiamo per ipotesi un’implicazione con antecedente vero). \square

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.

³⁷Stiamo solo giustificando formalmente il per ogni.

Osservazione 4.22 (Idea [e parte] della dimostrazione) — Si dimostra per induzione forte che, se $n \in A$, allora A ha un minimo. Poi, siccome A non è vuoto, deve esserci qualche $n \in A$, quindi A ha minimo. L'induzione funziona così. Se $n \in A$, si danno due casi. O esiste $x < n$ con $x \in A$, e allora A ha minimo per ipotesi induttiva (che è quello che stiamo per dimostrare), oppure $\forall x < n \ x \notin A$, ma allora n è il minimo di A (e abbiamo concluso).

Dimostrazione. Dimostriamo la contronominale della tesi (nel caso in cui $x \in A$), ovvero dobbiamo dimostrare che se A non ha un minimo elemento, allora A è vuoto.

Assumiamo quindi per ipotesi induttiva che esista un elemento strettamente più piccolo di tutti gli altri, ovvero $\forall n \in A \ \exists x \in A \ x < n$ (stiamo usando il $<$ perché il caso in cui $x = n$ è già contemplato nell'osservazione dicendo che $x \notin A$). Osserviamo che la contronominale della nostra tesi³⁸ è:

$$(\neg \exists x < n \ x \in A) \rightarrow n \notin A$$

ed equivale a:

$$\begin{aligned} & (\neg \exists x (x < n) \wedge (x \in A)) \rightarrow n \notin A \\ & \stackrel{\wedge \text{ commut.}}{\iff} (\neg \exists x \in A \ x < n) \rightarrow n \notin A \\ & \stackrel{\text{contronom.}}{\iff} n \in A \rightarrow (\exists x \in A \ x < n) \end{aligned}$$

ma la cosa appena scritta è equivalente all'ipotesi induttiva, pertanto la contronominale della tesi è vera, e quindi anche la tesi. Abbiamo quindi dimostrato anche il secondo caso dell'induzione forte e ciò conclude la dimostrazione del principio del minimo (perché stiamo supponendo ci sia sempre un elemento, come visto nell'osservazione iniziale). \square

Osservazione 4.23 — Per completare l'equivalenza tra induzione, induzione forte e principio del minimo, andrebbe dimostrato anche che principio del minimo \implies induzione.

Definizione 4.24 (Insieme ben ordinato). Un insieme totalmente ordinato $(S, <)$ si dice **bene ordinato** se ogni sottoinsieme non vuoto ha un minimo.³⁹

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

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 4.25

$(\omega, <)$ 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 4.26. Dimostra che $X = s(s(s(\omega)))$ è bene ordinato dalla relazione $a < b \stackrel{\text{def}}{=} a \in b$.

³⁸Cioè di questo caso della dimostrazione come visto nell'osservazione.

³⁹Cioè se vale il principio del minimo c(ome vale in ω).

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

$$\prec := < \cup (\omega \times \{\omega\}) \cup (s(\omega) \times \{s(\omega)\}) \cup (s(s(\omega)) \times \{s(s(\omega))\})^{40}$$

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 $f : \omega \rightarrow \text{qualcosa}$, 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.

Esempio 4.27 (Operazioni aritmetiche)

Possiamo definire somma e prodotto come:

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

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 4.28 (Potenza e fattoriale)

Possiamo definire ricorsivamente potenze e fattoriali come segue:

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

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

⁴⁰Che formalmente è un sottoinsieme di $s(s(s(\omega))) \times s(s(s(\omega)))$.

Esempio 4.29 (Sommatoria)

Possiamo definire la sommatoria come:

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

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

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

Esempio 4.30 (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 ricoprimenti in funzione di n :

$$F_n = F_{n-1} + F_{n-2}^{41}$$

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 4.31 (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 $A \times B$).

⁴¹Cioè 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 ricoprimenti in funzione di n .

Dimostrazione. Si osserva che:

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

e si conclude per [estensionalità](#) che quanto scritto sopra equivale a dire che gli insiemi f e g sono uguali. \square

Notazione 4.32 (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 4.33 (Ricorsione numerabile - prima forma)

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

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

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

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

^a k sarà il caso base della ricorsione.

Esempio 4.34 (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 $h(0, x) = k = 1$.

Esercizio 4.35. Come potrei costruire F_n usando questo teorema?

Dimostrazione. 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 $\omega \times A$ (f è una funzione da ω ad A) usando la formula Φ . Per dire “ $y = f(x)$ ” diremo equivalentemente “i primi x passaggi della ricorsione, partendo da k , conducono a y ”. Dato $x \in \omega$ diciamo che g è una **x -approssimazione** se la vale la formula seguente:

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

ovvero la funzione $g : \{0, \dots, x\} \rightarrow A$ soddisfa la definizione ricorsiva di f , ristretta, naturalmente, al dominio $\{0, \dots, x\}$ (cioè $s(x)$). Il vantaggio di tagliuzzare f in x -approssimazioni è che così otteniamo un parametro, x , su cui impostare un'induzione.

Lemma 4.36 (Esistenza e unicità delle x -approssimazioni in ω)

$\forall x \in \omega \exists! g$ “ g è una x -approssimazione”.

Dimostrazione. Induzione su x .

caso $x = \emptyset$ Basta osservare che l'unica \emptyset -approssimazione è la funzione $\{(\emptyset, k)\}$. Infatti il dominio è $\{\emptyset\}$ per definizione, e per soddisfare la definizione deve valere necessariamente $g(\emptyset) = k$, quindi l'unica \emptyset -approssimazione possibile è la funzione $g = \{(\emptyset, k)\}$.

caso $x = s(a)$ Per ipotesi induttiva abbiamo che esiste un'unica a -approssimazione g . Poniamo:

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

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

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

□

Stabilito il lemma, introdurremo la formula Φ :

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

Per l'unicità della x -approssimazione $\forall x \in \omega \exists! y \Phi(x, y)$, possiamo quindi definire, per ogni $x \in \omega$ e $y \in A$ la funzione via [separazione](#):

$$f(x) = y \stackrel{\text{def}}{=} \Phi(x, y)^{42}$$

Occorre verificare che f soddisfa le condizioni della ricorsione.

$f(\emptyset) = k$ Immediata, infatti $f(\emptyset) = g(\emptyset)$, ma abbiamo visto nel lemma che l'unica \emptyset -approssimazione possibile in ω è $\{(0, k)\}$ (cioè soddisfa semplicemente il caso base), quindi $f(\emptyset) = g(\emptyset) = k$.

$f(s(n)) = h(n, f(n))$ Per costruzione $f(s(n)) = g(s(n))$ per una (l'unica) $s(n)$ -approssimazione g . D'altro canto $g(s(n)) = h(n, g(n))$ (per definizione di $s(n)$ -approssimazione). Ora $g_{|s(n)}$ è una n -approssimazione, quindi $g_{|s(n)}(n) = g(n) \stackrel{\text{def}}{=} f(n)$. Mettendo tutto insieme:

$$f(s(n)) \stackrel{\text{def}}{=} g(s(n)) \stackrel{\text{def}}{=} g h(n, g(n)) \stackrel{\text{def}}{=} \stackrel{+}{\text{oss.}} h(n, f(n))$$

Ciò dimostra che una f ottenuta per separazione come abbiamo visto esiste e 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:

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

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

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.

⁴²Formalmente $f = \{(x, y) \in \omega \times A \mid \Phi(x, y)\} = \{(x, y) \in \omega \times A \mid \exists! g \in {}^{s(x)}A \text{ "} g \text{ è una } x\text{-approssimazione" } \wedge g(x) = y\}$, in altre parole, dato $x \in \omega$ affido alla sua (unica) x -approssimazione il compito di trovare un'immagine, e quindi definisco f attraverso g (che dipende dalla x in input).

⁴³E usando l'estensionalità per funzioni su h .

Esempio 4.37 (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:

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

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 4.38 (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:

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

^aCioè è una bigezione tra insiemi, che rispetta lo 0 e la funzione successore che abbiamo definito.

Fa comodo isolare la seguente osservazione.

Osservazione 4.39 (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

Dimostriamo ora il teorema.

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 il principio di induzione (poiché soddisfa gli assiomi di Peano). Dimostriamo quindi per induzione in $(\mathbb{N}, 0, \text{succ})$ che $\forall y \in \mathbb{N} \ \exists x \in \omega \ f(x) = y$.

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

caso $y = \text{succ}(n)$ 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 Consideriamo, per assurdo, il minimo $x \in \omega$ tale che, per qualche $y \in \omega$ con $y \neq x$, $f(x) = f(y)$. Osserviamo che, per la minimalità di x , $x < y$, quindi, in particolare $y \neq \emptyset$, e per l'osservazione possiamo scrivere $y = s(y')$. Procediamo quindi per induzione su x nel trovare un assurdo per ogni $x \in \omega$.

caso $x = \emptyset$ In questo caso si deve avere che:

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

che equivale a dire che 0 è successore di qualche numero contraddicendo l'osservazione (che vale anche per $(\mathbb{N}, 0, \text{succ})$, in quanto soddisfa gli assiomi di Peano per ipotesi).

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

$$\text{succ}(f(x')) = f(s(x')) = f(x) = f(y) = f(s(y')) = \text{succ}(f(y'))$$

e, per l'assioma (a) (iniettività del successore) in $(\mathbb{N}, 0, \text{succ})$, segue che $f(x') = f(y')$. Allora, per la minimalità di x , siccome $x' < x$, dobbiamo avere $x' = y'$ (avevamo posto per ipotesi x come minimo per cui c'è un elemento distinto y che ha la stessa immagine, quindi qualsiasi cosa abbia la stessa immagine e sia più piccola di x deve essere unica). Ma da questo seguirebbe $x = s(x') = s(y') = y$, contro l'ipotesi \nmid

□

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 dipende solo dal termine precedente della sequenza, F_{n-1} , ma anche da F_{n-2} . Ce la si potrebbe cavare con un trucco, per esempio definendo la funzione $n \mapsto (F_n, F_{n+1})$ da ω a $\omega \times \omega$. È comodo, però, disporre di una versione più versatile del teorema di ricorsione numerabile.

Teorema 4.40 (Ricorsione numerabile - seconda forma)

Dato un insieme A , denotiamo con A^* l'insieme delle funzioni $g \subseteq \omega \times A$ con $\text{Dom}(g) \in \omega^a$. Sia $h : A^* \rightarrow A$, allora esiste un'unica funzione $f : \omega \rightarrow A$ tale che:

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

^aCioè è un numero di ω .

^bIn altre parole, $f(n)$, può dipendere in maniera arbitraria dai valori assunti da f sui numeri minori di n . Cioè h è una funzione che manda funzioni che hanno come dominio un $n \in \omega$ in A , in particolare $h(f|_n)$ è una funzione di funzioni con dominio in ω .

Esempio 4.41 (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 $f|_n \in A^*$.

Dimostrazione. L'idea è di definire, mediante la prima forma del [teorema di ricorsione](#), la successione della troncata di f . Ossia la funzione $f' : n \mapsto f|_n$ (che manda f nella sua restrizione al dominio $\{0, \dots, n-1\}$) - un modo alternativo, sarebbe ripetere la dimostrazione della prima forma -. Procediamo nel primo modo e costruiamo per ricorsione - prima forma - la funzione $f' : \omega \rightarrow A^*$ tale che:

$$f'(\emptyset) = \emptyset \quad f'(s(n)) = f'(n) \cup \{(n, h(f'(n)))\}^{44}$$

Ora poniamo $f(n) := f'(s(n))(n)$ ($f' \in A^*$, quindi è una funzione com dominio in ω , quindi $f : \omega \rightarrow A$ è ben definita) e verifichiamo per induzione che effettivamente f' sia la successione della troncata di f , cioè $\forall n \in \omega \ f|_n = f'(n)$.

caso $n = 0$ Si vede subito che $f|_0 = f'(\emptyset)(n) = \emptyset$ (per come l'abbiamo costruita).

caso $n = s(m)$ In questo caso abbiamo:

$$\begin{aligned} f|_{s(m)} &= f|_m \cup \{(m, f(m))\} \\ &= f'(m) \cup \{(m, f'(s(m))(m))\} \\ &= f'(m) \cup \{(m, h(f'(m)))\} = f'(s(m)) \end{aligned}$$

dove la prima uguaglianza segue per definizione di funzione (successione in questo caso specifico), la seconda per com'è definita f in funzione di f' e l'ultima per la definizione ricorsiva di f' . Infine, quindi, $f(n) \stackrel{\text{def.}}{=} f'(s(n))(n) = h(f'(n)) = h(f|_n)$ (dove l'ultima uguaglianza segue per quanto abbiamo dimostrato). \square

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 4.42. Dimostra commutatività, associatività, etc. di $+$ e \cdot .

⁴⁴Esiste ed è unica per il primo teorema di ricorsione

§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 :

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

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

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

ossia $\exists f \in {}^A B$ “ f è iniettiva” (la definizione ci dice proprio che esiste un sottoinsieme di B che è in bigezione con A , e per definizione di iniettività, si ha proprio che $A \hookrightarrow B$)⁴⁵.

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 $\clubsuit[A, B]$ (nel senso che per ora è solo un'abbreviazione per dire bigezione, 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 bigezione 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

⁴⁵Tale 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 bigettive⁴⁶, 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:

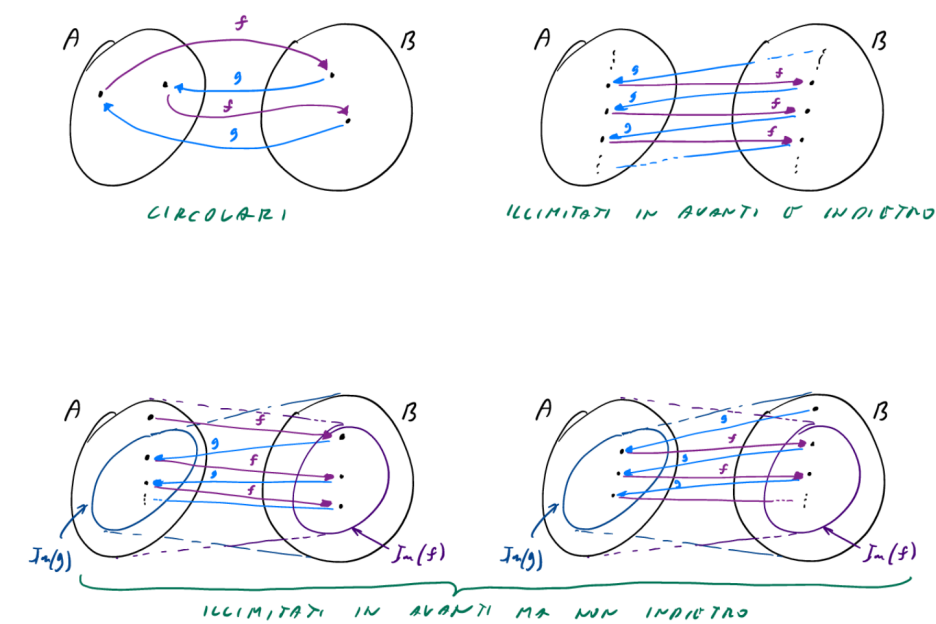
$$a \xrightarrow{f} f(a) \xrightarrow{g} g(f(a)) \xrightarrow{f} f(g(f(a))) \xrightarrow{g} \dots$$

Siccome f e g sono iniettive, questo percorso ha altresì un'unica estensione all'indietro (abbiamo visto che se le funzioni sono iniettive, allora ammettono un'inversa iniettiva dalle rispettive immagini (che è anche surgettiva), dunque possiamo sempre tornare indietro in modo unico, estendendo quindi il nostro percorso anche nell'altra direzione):

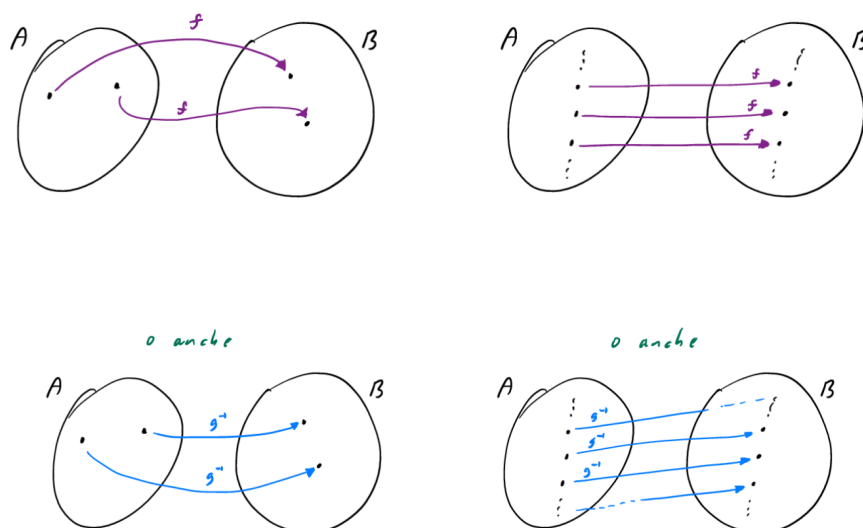
$$f^{-1}(g^{-1}(a)) \xrightarrow{f} g^{-1}(a) \xrightarrow{g} a \xrightarrow{f} f(a) \xrightarrow{g} g(f(a)) \xrightarrow{f} f(g(f(a))) \xrightarrow{g} \dots$$

a patto che $a \in \text{Im}(g)$ (perché l'inversa g^{-1} va da $\text{Im}(g)$ a B), $g^{-1}(a) \in \text{Im}(f)$, etc. Quando, e se, non possiamo più applicare la funzione inversa, il percorso (all'indietro) si interrompe. Con questa catena di composizioni ci sono quindi tre tipi di percorsi possibili:

⁴⁶È una semplice verifica.

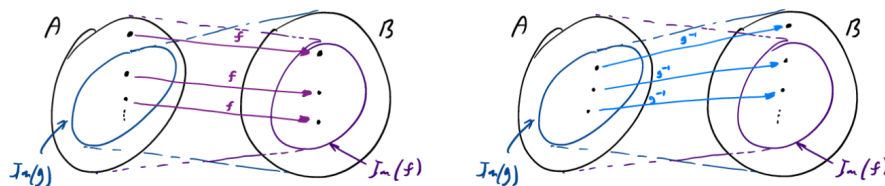


Per gli elementi che si trovano su un percorso circolare, o su un percorso illimitato avanti e indietro, f fornisce una bigezione, come la fornirebbe anche g^{-1} - la scelta è arbitraria a patto di usare la medesima funzione per l'intero percorso - nel modo seguente⁴⁷:



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

⁴⁷Informalmente, 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 [la bigezione h], $h(x) = f(x)$ 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:

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

(ovvero la successione dei B_i è definita con la prima forma della ricorsione, mentre quella degli A_i dipende semplicemente da quest'ultima, ma non direttamente per ricorsione). 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, 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 si ha $h(x) = f(x)$, in tal modo prendiamo tutti gli elementi di tutti i cicli possibili che si formano nei due insiemi usando i percorsi descritti sopra.

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 $x \in A_j \not\subseteq$

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:

$$|A| < |B| \stackrel{\text{def}}{=} |A| \leq |B| \wedge |A| \neq |B| \quad 48$$

§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 disuguaglianza $|A| \leq |\mathcal{P}(A)|$ è facile: basta considerare la funzione iniettiva:

$$A \longrightarrow \mathcal{P}(A) : x \longmapsto \{x\}$$

(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:

$$B = \{x \in A \mid x \notin f(x)\} \quad 49$$

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

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

□

§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.

⁴⁸Dove ricordiamo che $|A| \neq |B| \stackrel{\text{def}}{=} \neg(|A| = |B|)$.

⁴⁹ $f(x) \in \mathcal{P}(A)$, 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).

Proposizione 5.11 (Buona definizione delle operazioni)

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

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

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

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

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 $|\mathcal{P}(A)| = |{}^A \{0, 1\}| = |{}^A 2|$ 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 $(|A|^{|D|})^{|C|} = |A|^{|C| \cdot |B|}$. 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:

$$\tilde{f}(c, b) = \underbrace{(f(c))}_{\in {}^B A} \underbrace{(b)}_{\in B} \quad {}^{51}$$

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:

$$\bar{g}(c) : B \longrightarrow A : b \longmapsto g(c, b) \quad {}^{52}$$

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

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

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

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

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

⁵¹Cioè 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 $b \in B$.

⁵²Ovvero 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 $\exists n \in \omega \mid |A| = |n|$. 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:

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

§6.1 Principio dei cassetti

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

Proposizione 6.3 (Principio dei cassetti - ossia - $\text{finito} \rightarrow \text{Dedekind-finito}$)

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 $|B| \neq |A|$.

Supponiamo per assurdo che $|B| = |A|$. Osserviamo che, senza perdita di generalità, possiamo assumere $A = n \in \omega$ ⁵³. Per ipotesi, infatti esiste $f : A \rightarrow n$ bigettiva, per un opportuno $n \in \omega$. Quindi $f[B] \subsetneq n$ (volendo perché la restrizione di f a B è ancora iniettiva ma non surgettiva⁵⁴, quindi non può avere in arrivo tutto n). D'altro canto, per l'iniettività di f , $|f[B]| = |B| \stackrel{\text{Hp. assurda}}{=} |A| = n$. Ci basta quindi dimostrare per induzione su n , che:

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

(cioè che ogni sottoinsieme di un numero naturale con la stessa cardinalità è il numero stesso) in questo modo avremmo $f[B] = f[A] = n$ (prima avevamo un sottoinsieme di A non di n), che è assurdo in quanto abbiamo detto che $f[B] \subsetneq n$.

caso $n = \emptyset$ Necessariamente $B = \emptyset$, quindi $B = n$ come richiesto dalla tesi.

caso $n = s(m)$ L'ipotesi induttiva è $\forall C \subseteq m \mid |C| = |m| \rightarrow C = m$, vogliamo dimostrare che $\forall B \subseteq s(m) \mid |B| = |s(m)| \rightarrow B = s(m)$.

Sia $f : s(m) \rightarrow B$ bigettiva (come ipotesi antecedente). Si danno due casi. Se $f(m) = m$ (ricordiamo che l'insieme d'arrivo è un sottoinsieme di $s(m)$), allora sia $C := \text{Im}(f|_m)$, e, per l'iniettività di f , si ha $|C| = |m|$, quindi, per l'ipotesi induttiva (essendo $C \subseteq m$), vale $C = m$. Ma in questo modo $B = \text{Im}(f) = C \cup \underbrace{\{f(m)\}}_{=m} = m \cup \{m\} = s(m) = n$.

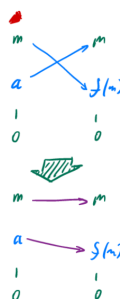
⁵³Quello che faremo è proprio portare $B \subsetneq A$ in $f[B] \subsetneq f[A] = n$ e qui trovare l'assurdo, che è come assumere sempre che $A = n$, perché possiamo sempre spostare il problema in ω con una bigezione.

⁵⁴È conseguenza del fatto che B sia un sottoinsieme proprio e che f è bigettiva.



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

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



in altre parole stiamo “aggiustando” la bigezione f in modo che venga di nuovo una bigezione f' , tale che $f'(m) = m$ e si ricade nel caso precedente (e lo possiamo sempre fare, come osservato).

□

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 bigezione:

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

Dimostrazione. Se $|m| = |A| = |n|$, possiamo assumere, senza perdita di generalità $m \leq n$, ossia $m \subseteq n$, quindi, usando il [principio dei cassetti](#) $m = n$, abbiamo quindi l'unicità. □

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.

Dimostrazione. Basta considerare la funzione iniettiva:

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

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 biezione con un suo sottoinsieme proprio, per cui non può essere Dedekind-finito.



□

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 (nel senso che la h del teorema di ricorsione essendo un insieme deve avere tutti gli elementi già fissati, cosa che non può avvenire in questo caso) uno degli a . A patto di averne una, ne andrebbe bene una qualunque.

Purtroppo però, a partire dalla mera ipotesi che A è infinito, non abbiamo modo di procurarci nessuna funzione del genere. Potremmo cavarcela se avessimo qualche struttura su A , sulla quale far leva - per esempio per dire "prendo il minimo fra gli $a \notin \text{Im}(f|_n)$ ", 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 immergono tutti i numeri naturali.

Proposizione 6.6 (Tutti i naturali si immergono in un 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, $f = \emptyset$.

caso $n = m + 1$ Per ipotesi induttiva esiste $f : m \rightarrow A$ iniettiva. Siccome A è infinito (e m è finito), esiste $a \in A \setminus \text{Im}(f)$ (e non ci serve fissarlo poiché non stiamo usando il teorema di ricorsione). La funzione $f' = f \cup \{(n, a)\}$, che si ottiene estendendo f col mandare n in a , è iniettiva $n \hookrightarrow A$.

□

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 $|A| < |B| \leq |A| \nlessdot$ (poiché $|A| = |n|$ per definizione di finito e per la proposizione precedente tutti gli n si immergono in un insieme infinito si ha $A \rightarrow n \hookrightarrow B$, dove la prima funzione è bigettiva e la seconda iniettiva, e per le proprietà di composizione delle funzioni iniettive, la composizione di queste ultime due ci dà $A \hookrightarrow B$, da cui $A \hookrightarrow A$, ma essendo finito è anche Dedekind-finito, quindi questo è assurdo). □

Esercizio 6.8. Dimostrare che:

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

^aFondamentalmente ogni sottoinsieme di ω (che non è detto sia un elemento di ω) è in biezione con un elemento di ω .

Soluzione. Verifichiamo le due cose separatamente:

- Se $|A| < |n|$, allora esiste una funzione $f : A \hookrightarrow n$ iniettiva ma non surgettiva, in particolare si ottiene che $f[A] \subsetneq n$, con $|A| = |f[A]|$, osservando che n è finito e usando il corollario sopra, si ottiene che $f[A]$ è finito, in particolare $|A| = |f[A]| = m$, per $m \in \omega$. Infine, abbiamo che $|m| = |A| < |n|$, ci resta da osservare che:

$$\forall m, n \in \omega \quad |m| < |n| \iff m < n$$

La freccia \leftarrow è banale, perché, per un noto corollario $m < n \iff m \subsetneq n$, che implica $|m| < |n|$ (basta usare id_m).⁵⁵

Viceversa, posto $|m| < |n|$, se per assurdo fosse $m \geq n$, allora per definizione di \leq tra cardinalità $|n| \leq |m|$, da cui $|m| < |n| \leq |m| \implies |m| < |m|$, che è assurdo perché viola il principio dei cassetti.

- Diamo per buono che in generale $|f[A]| \leq |A|$. Ora $|A|$ è finito, dunque, per il corollario sopra, il suo sottoinsieme $g[f[A]]$ è finito (con g la mappa iniettiva da $f[A]$ ad A), pertanto [poiché g iniettiva] $|f[A]| = |g[f[A]]| = m$, per $m \in \omega$, e quindi abbiamo che $f[A]$ è finito.

Ci resta da verificare l'assunzione iniziale, possiamo farlo con la seguente funzione:

$$g : f[A] \longrightarrow A : x \longmapsto \min_{<_n} \{h[f^{-1}(x)]\}$$

⁵⁵Per concludere si può osservare, alternativamente, che n finito implica Dedekind-finito, dunque non può essere in biezione con un suo sottoinsieme in proprio m (di fatto stiamo nascondendo sotto al tappeto la definizione di $<$ tra cardinalità), dunque la disuguaglianza [ottenuta da $m \subseteq n$] deve essere stretta.

dove $<_n$ è l'ordine usuale di ω ristretto ad n e h è la bigezione che esiste per ipotesi da A ad n . Vediamo che g è iniettiva:

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

con $a \in f^{-1}(x)$ e $b \in f^{-1}(y)$ (in altre parole abbiamo dato un nome ai minimi). Ora, essendo h bigettiva 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 disuguaglianza iniziale. □

§6.2 Operazioni fra le cardinalità finite

Proposizione 6.9 (Le operazioni tra cardinalità finite possono essere definite in funzione delle operazioni su ω)

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 $(m \times \{0\}) \cup \{(0, 1)\}$ ⁵⁶ 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 .

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

$$\boxed{\text{caso } n = 0} \quad |m| + |0| = |(m \times \{0\}) \cup \emptyset| = |m| = |m + 0|.$$

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

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

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

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

⁵⁶Typo del prof. Mamino sui suoi appunti in quanto $1 = \{0\}$.

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

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

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

caso $n = 0$ $|m|^{|0|} = |{}^0m| = |\{f : 0 \rightarrow m\}| = |\{\emptyset\}| = |1| = |m^0|$ (l'unica funzione possibile dal vuoto a m è $f = \emptyset$ ⁵⁷).

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

$$\begin{aligned}
 |m|^{|s(a)|} &\stackrel{\text{oss. iniziale}}{=} |m|^{|a|+|1|} \\
 &\stackrel{\text{ propr. operaz. card. }}{=} |m|^{|a|} \cdot \underbrace{|m|^{|1|}}_{=|m|} \\
 &\stackrel{\text{Hp. indutt}}{=} |m^a| \cdot |m| \\
 &\stackrel{\text{ propr. del } \cdot \text{ card. }}{=} |m^a \cdot m| \\
 &\stackrel{\text{def. potenza}}{=} |m^{s(a)}|
 \end{aligned}$$

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

□

Nota 6.10 — Questa proposizione ci fornisce una dimostrazione delle proprietà aritmetiche elementari delle operazioni su ω [sfruttando le proprietà delle operazione 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 $m \leq n$, esista un unico $n - m \in \omega$ tale che $m + (n - m) = n$. In due modi diversi.

Soluzione.

□

⁵⁷E quindi ${}^0m = \{f : \emptyset \rightarrow m\} = \{\emptyset\} = 1$, o in alternativa si può pensare che $f \subseteq \emptyset \times m = \emptyset \implies f \in \mathcal{P}(\emptyset) = \{\emptyset\}$ e quindi $f = \emptyset \implies {}^0m = \{f\} = \{\emptyset\} = 1$.

§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 bigezione con ω .

Proposizione 7.3

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 [non è altro che una formulazione equivalente della proposizione sopra].

Potremmo dimostrare la proposizione direttamente, ma ci conviene, invece, passare attraverso alcune considerazioni che saranno utili in seguito.

In generale, per costruire una bigezione 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 bigezione, e spesso, per costruire bigezioni, costruiamo isomorfismi di ordini.

Definizione 7.5 (Isomorfismo). Due insiemi (parzialmente⁵⁸) ordinati $(A, <_A)$ e $(B, <_B)$ sono **isomorfi**, in simboli $(A, <_A) \sim (B, <_B)$ se esiste una bigezione $f : A \rightarrow B$ tale che:

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

(cioè se esiste una bigezione che rispetta le relazioni d'ordine).

Osservazione 7.6 (Funzioni strettamente crescenti) — Due insiemi TOTALMENTE ordinati $(A, <_A)$ e $(B, <_B)$ sono isomorfi se e solo se esiste una funzione $f : A \rightarrow B$ surgettiva e **strettamente crescente** - cioè tale che:

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

(non è altro che la definizione in cui supponiamo gli insiemi totalmente ordinati e diamo un nome alla funzione che realizza l'isomorfismo in questo caso).

⁵⁸Dove 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 l'ordinamento [buono^a] indotto da ω (cioè l'ordine che abbiamo definito su ω ristretto a n).

^aPer restrizione.

Dimostrazione. Procediamo per induzione su n .

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

caso $n = s(m)$ Se $m = 0$, allora $A = \{a\}$ e $(A, <_A) \sim (1, <)$, cioè la tesi è banalmente vera. Assumiamo quindi $m > 0$. Dimostriamo intanto che $(A, <_A)$ ha un massimo elemento. Fissiamo una bigezione $f : s(m) \rightarrow A$ (esiste per ipotesi). Allora $|f[m]| = m$, quindi $f[m]$ con l'ordinamento indotto da $<_A$ è isomorfo a $(m, <)$ per ipotesi induttiva e, in particolare, ha massimo M . Ora per la totalità di $<_A$, o $M < f(m)$ oppure $f(m) < M$. Si verifica immediata che, nel primo caso, $f(m)$ è il massimo di A , e nel secondo M è il massimo di A . Stabilito che A ha un massimo N , osserviamo che, detto $A' := A \setminus \{N\}$, siccome $|A'| = m$, usando nuovamente l'ipotesi induttiva abbiamo un isomorfismo $f : A' \rightarrow m$ fra A' , con l'ordinamento indotto da $<_A$ e $(m, <)$. Si verifica facilmente che l'isomorfismo cercato è:

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

□

Osservazione 7.9 (Ogni ordine finito totale 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 [come vedremo a breve nella caratterizzazione di ω].

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

Proposizione 7.10 (Proprietà di $(\omega, <)$)

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, l'ordinamento totale su A (eredita la totalità da quello di ω) definito da:

$$x \prec y \stackrel{\text{def}}{=} y < x$$

è buono [perché ogni insieme finito è isomorfo al buon ordine della sua cardinalità], quindi, in particolare, c'è il minimo di A (sottoinsieme improprio di se stesso) secondo l'ordinamento \prec . Questo è il massimo di A (secondo l'ordinamento $<$). \square

Proposizione 7.11 (Caratterizzazione di ω come ordine)

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 crescita col successore \implies stretta crescita)

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

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

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

^aTypo di Mamino nelle dispense.

Dimostrazione. Considero, per assurdo, $m < n$ tali che $f(m) \not\prec f(n)$, con n minimo [tale per cui accade ciò]. Siccome $0 \leq m < n$, esiste n' tale che $n = s(n')$. Ora, da un'osservazione precedente, essendo $m < s(n')$, si ha $m = n' \vee m < n'$. Nel primo caso, dall'ipotesi segue:

$$f(m) \prec f(s(m)) = f(s(n')) = f(n)$$

contraddicendo $f(m) \not\prec f(n)$. Nel secondo caso, per la minimalità di n (quindi ciò che è più piccolo di n ha immagine sopra m), deve accadere per forza $f(m) \prec f(n')$, ma $f(n') \prec f(s(n')) = f(n)$ per ipotesi, quindi abbiamo di nuovo una contraddizione, pertanto deve essere necessariamente $f(m) \prec f(n)$. \square

Possiamo ora dimostrare la proposizione.

Dimostrazione. Costruiamo per ricorsione un isomorfismo f da $(\omega, <)$ a $(A, <)$:

$$f(0) = \min_{<} A \quad f(s(n)) = \min_{<}\{a \in A \mid f(n) < a\}^{59}$$

dove $\min_{<}$ denota il minimo secondo la relazione d'ordine (buona) $<$ di A . Occorre dimostrare intanto che f è ben definita. $f(0)$ è ben definita, perché $A \neq \emptyset$, e quindi vale il principio del minimo (che abbiamo per ipotesi). Per dire che $f(s(n))$ è ben definita, occorre dire che la funzione $h : A \rightarrow A$, $h(x) = \min_{<}\{a \in A \mid x < a\}$ è ben definita (sarebbe la funzione che definisce la ricorsione - prima forma -), ossia che $\{a \in A \mid x < a\}$ è non vuoto, e quindi di nuovo esiste il minimo usando che per ipotesi A è ben ordinato. Ma questo [cioè il fatto che quell'insieme sia non vuoto] avviene, qualsiasi sia $x \in A$, perché altrimenti A sarebbe limitato [superiormente] da x (e non illimitato superiormente come abbiamo supposto nelle ipotesi).

Per come è costruita, e per il lemma, f è [strettamente] crescente (cioè l'abbiamo costruita in modo che sia una funzione da ω in A crescente rispetto al successore, per cui vale il lemma sopra, dunque è sempre crescente), quindi iniettiva. Di conseguenza, ci basta dimostrare la surgettività.

Prendiamo $y \in A$ e cerchiamo $x \in \omega$ tale che $y = f(x)$. Se, per ogni $x \in \omega$, avessi $f(x) < y$, allora $f[\omega]$ sarebbe [non vuoto e] superiormente limitato da y , tuttavia non avrebbe massimo perché ogni $f(x)$ è $<$ di $f(s(x))$, il che è assurdo [qui stiamo usando che violerebbe 3.]. Quindi c'è il **minimo** $x \in \omega$ tale che $y \leq f(x)$. Dimostriamo che, per tale x , $f(x) \leq y$, da cui l'uguaglianza (e quindi la surgettività).

$x = 0$ in tal caso $f(x)$ è il minimo di A , quindi $f(x) \leq y \in A$.

$x = s(x')$ in questo caso $f(x') < y$ per la minimalità di x (avendo preso x come il minimo in ω tale che $f(x) \leq y$, tutto ciò che sta sotto non può rispettare l'ultima condizione), ma allora, $y \in \{a \in A \mid f(x') < a\}$, quindi $f(x) = f(s(x')) = \min_{<}\{a \in A \mid f(x') < a\} \leq y$ (dove l'ultima disuguaglianza deriva dal fatto che y appartiene all'insieme di cui stiamo facendo il minimo, mentre la seconda uguaglianza è la definizione di f).

□

Tornando alla proposizione iniziale.

Proposizione 7.13 (Caratterizzazione insiemi al più numerabili)

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.

Sia $B \subseteq \omega$ infinito, dimostriamo che B , con l'ordinamento indotto dall'ordine naturale di ω soddisfa le ipotesi della proposizione precedente. 1 e 3⁶⁰ valgono in quanto ogni sottoinsieme di B è in particolare, sottoinsieme di ω (dunque abbiamo buon ordinamento ed esistenza del massimo). Per ottenere 2 dobbiamo dire che B non ha un massimo elemento (cioè è illimitato). Se, infatti, ci fosse un $M \in B$ tale che $\forall b \in B \ b \leq M$, allora avremmo che $B \subseteq s(M)$, B sarebbe dunque finito [perché sottoinsieme di un insieme finito], contro l'ipotesi. Pertanto $(B, <|_B) \sim (\omega, <) \implies |B| = \aleph_0$, dunque se un

⁵⁹Cioè la funzione manda il successore nel più piccolo termine in $(A, <)$ che sta "sopra" a $f(n)$ (in pratica la stiamo costruendo apposta affinché sia strettamente crescente).

⁶⁰Typo di Mamino.

sottoinsieme di ω è infinito, allora è necessariamente numerabile.

Il caso di un sottoinsieme non infinito coincide col caso di un elemento di ω (che sappiamo essere un sottoinsieme per le proprietà di ω), che è dunque banalmente in bigezione con se stesso (via identità) e quindi finito per definizione. \square

Esercizio 7.14. 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:

$$h(b) = \min_{<} (g[\underbrace{\{a \in A \mid f(a) = b\}}_{= "f^{-1}(b)"}])^{61}$$

l'insieme tra graffe è non vuoto per surgettività di f , dunque il minimo è ben definito. Inoltre, se $h(b) = h(b')$, allora i minimi [che chiamiamo] $g(a)$ 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 $f(a) = f(a')$ (ovviamente sono lo stesso elemento), 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 $|B| = |B'|$ (come al solito per definizione di disuguaglianza tra cardinalità), quindi basta dimostrare le disuguaglianze asserite con B' al posto di B ⁶². Ora, giocando sul fatto che $B' \subseteq C$ (abbiamo fatto apposta lo scambio tra B e B' per poter usare i contenimenti), si vede che queste disuguaglianze rappresentano, in realtà, relazioni di contenimento fra RHS e LHS. Per esempio:

$$\begin{aligned} B' \subseteq C &\xrightarrow{\text{ovvio}} (A \times \{0\}) \cup (B' \times \{1\}) \subseteq (A \times \{0\}) \cup (C \times \{1\}) = A \sqcup B' \subseteq A \sqcup C \\ &\xrightarrow{\text{id}_A \times \text{id}_{B'}} |(A \times \{0\}) \cup (B' \times \{1\})| \leq |(A \times \{0\}) \cup (C \times \{1\})| \\ &\xLeftrightarrow{\text{def.}} |A| + |B'| \leq |A| + |C| \end{aligned}$$

Le altre si ottengono allo stesso modo. \square

⁶¹Si noti che, essendo f non necessariamente iniettiva, f^{-1} denota la controimmagine, non la funzione inversa, da cui la scelta delle parentesi quadre quando si applica g , per evidenziare che stiamo facendo l'immagine di un'insieme.

⁶²Oppure 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.

Osservazione 7.16 (Disuguaglianza di inclusione-esclusione) — $|A \cup B| \leq |A| + |B|$.

Dimostrazione. Basta osservare che la seguente funzione è iniettiva:

$$f : A \cup B \longrightarrow (A \times \{0\}) \cup (B \times \{1\}) : x \longmapsto \begin{cases} (x, 0) & \text{se } x \in A \\ (x, 1) & \text{altrimenti} \end{cases}^{63}$$

□

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)

$\aleph_0 + \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0^n = \aleph_0$, 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 disuguaglianze:

$$\aleph_0 \stackrel{\text{op. card.}}{=} \aleph_0 + 0 \stackrel{\text{oss. sopra}}{\leq} \aleph_0 + \aleph_0 \stackrel{\text{op. card.}}{=} \aleph_0 \cdot 2 \stackrel{\text{oss. sopra}}{\leq} \aleph_0 \cdot \aleph_0 \stackrel{\text{ipotesi}}{=} \aleph_0$$

Da cui per il [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 $\aleph_0^{n+1} = \aleph_0^n \cdot \aleph_0 \stackrel{\text{Hp. indutt.}}{=} \aleph_0 \cdot \aleph_0 = \aleph_0$. □

Per concludere la dimostrazione precedente, resta da dimostrare il lemma seguente.

§7.2 Prodotto di numerabili è numerabile

Lemma 7.18 ($\aleph_0 \cdot \aleph_0 = \aleph_0$)

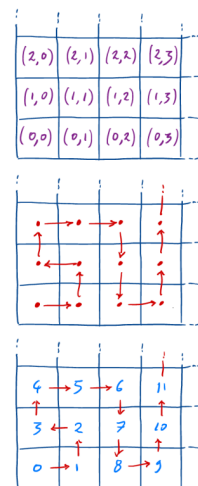
$\aleph_0 \cdot \aleph_0 = \aleph_0$, ossia esiste una biezione fra $\omega \times \omega$ e ω .

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, possibilmente, da convincere il lettore che vi debba essere un metodo. Infine numeriamo le maglie secondo l'ordine in cui sono visitate dal percorso. Avremo così numerato tutte le coppie di numeri naturali del disegno.

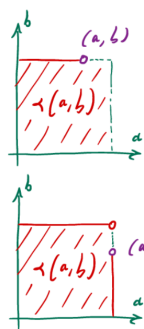
Altrimenti, è possibile esibire delle biezioni esplicite, per esempio:

$$f(x, y) = 2^x \cdot (2y + 1) - 1 \quad g(x, y) = \frac{(x + y)^2 + 3x + y}{2}$$

È possibile scrivere i due numeri della coppia in base 10 a cifre alternate, tipo: $(64, 4096) \mapsto 400906644$.



Dimostrazione. Consideriamo l'ordinamento su $\omega \times \omega$ definito come segue:



$$(a, b) \prec (a', b') \stackrel{\text{def}}{=} \max(a, b) < \max(a', b') \\ \vee (\max(a, b) = \max(a', b') \wedge a < a') \\ \vee (\max(a, b) = \max(a', b') \wedge a = a' \wedge b < b')$$

(dove per \max sulla coppia si intende il \max tra a e 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' (cioè se hanno una delle due componenti con lo stesso modulo massimo, si passa a confrontare il valore delle prime componenti); se queste coincidono, allora si confrontano b e b' .⁶⁴

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

Formalmente, iniziamo col verificare che \prec sia effettivamente un ordine stretto e totale. La proprietà irreflessiva è immediata (perché in tutti gli OR nella definizione stiamo usando l'ordinamento stretto di ω , dunque $\neg(a, b) \prec (a, b)$). Per verificare la proprietà transitiva, prendiamo $(a, b) \prec (a', b') \prec (a'', b'')$ (vorremo vedere che questo implica $(a, b) \prec (a'', b'')$). 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 avremmo concluso), altrimenti $\max(a, b) = \max(a', b') = \max(a'', b'')$, segue dalla definizione che $a \leq a' \leq a''$. Nuovamente, se una disuguaglianza è stretta abbiamo concluso, altrimenti $a = a' = a''$, quindi, affinché la scrittura iniziale sia ancora vera deve essere necessariamente che $b < b' < b''$, da cui $b < b''$, e quindi anche in questo caso vale $(a, b) \prec (a'', b'')$. Per dire che l'ordine è totale osserviamo che se (a, b) e (a', b') non sono né \prec né \succ allora dobbiamo avere $\max(a, b) = \max(a', b')$, $a = a'$, $b = b'$, ovvero $(a, b) = (a', b')$, dunque l'ordine stretto è anche totale.

Ora vogliamo dire che $(\omega \times \omega, \prec) \sim (\omega, <)$ (in questo modo, avendo un'isomorfismo di ordini, avremmo in particolare una bigezione tra ω e $\omega \times \omega$, dunque il prodotto di cardinalità numerabili è numerabile). 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 $(\omega \times \omega)_{(a,b)} \subseteq s(\max(a, b)) \times s(\max(a, b))$ (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 $A \neq \emptyset$, considero $a \in A$. Se $(\omega \times \omega)_a \cap A = \emptyset$ (stiamo considerando il segmento iniziale rispetto a un generico elemento $a \in \omega \times \omega$), allora a è il minimo di A (sta in a e non c'è nulla più piccolo nell'insieme perché l'intersezione col segmento iniziale di a (= cose strettamente più piccole in $(\omega \times \omega, \prec)$) è vuota). Altrimenti $A' = (\omega \times \omega)_{(a,a)} \cap A$ è non vuoto e finito [perché sto intersecando con un insieme finito], quindi ha minimo m (perché $\prec|_A$ è un ordine totale).

Questo deve essere anche il minimo di A , perché se $x \in A \setminus A'$, con $(A \setminus A') \cap (\omega \times \omega)_a =$

⁶⁴Come si vede nella figura a lato, nel primo caso, avendo b modulo massimo, ci sono anche punti più a destra, che in quest'ordinamento sono più piccoli (perché hanno un valore più piccolo come massima componente).

- \emptyset , allora $m \prec a \preceq x$ (dove la seconda disuguaglianza segue esattamente per il caso dell'intersezione vuota, mentre la prima disuguaglianza perché $m, a \in (\omega \times \omega)_a \cap A$, e quindi $m \prec_A a$ per come è definito).
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 $A \subseteq (\omega \times \omega)_{(a+1, b+1)}$ è finito (per quanto osservato sopra), quindi ammette massimo perché \prec è totale (abbiamo un numero finito di elementi da confrontare).

□

§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 3.73](#) - 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:

$$(a, b) \sim_{\mathbb{Z}} (a', b') \stackrel{\text{def}}{=} a + b' = b + a' \text{ }^{65}$$

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:

$$(n, d) \sim_{\mathbb{Q}} (n', d') \stackrel{\text{def}}{=} n \cdot d' = n' \cdot d \text{ }^{66}$$

Esercizio 7.23. Dimostrare che $\sim_{\mathbb{Q}}$ è una relazione di equivalenza.

⁶⁵Morale: " $(a, b) = a - b$ ".

⁶⁶Morale: " $(n, d) = \frac{n}{d}$ ".

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:

$$\forall a, b \in \mathbb{Q} \ a < b \rightarrow \exists c \in \mathbb{Q} \ a < c < b^a$$

^aTypo di Mamino.

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 risolviamo⁶⁷.

Corollario 7.27 (Definizione di al più numerabile al contrario)

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

^aFormalmente da questo momento in poi, avere una funzione surgettiva da un insieme al più numerabile (e nulla di più per ora) ad un altro, ci permette di dire che la cardinalità del primo è \geq cardinalità del secondo (cosa che fin'ora non potevamo dire).

Dimostrazione. La freccia \Leftarrow deriva dall'esercizio citato prima con $A = \omega$ (l'insieme al più numerabile) e $B = A$ (l'insieme a cui arriva la mappa surgettiva)⁶⁸.

Per l'inverso, supponiamo A al più numerabile e mostriamo che c'è sempre una mappa surgettiva tra ω ed A . Abbiamo dimostrato che se un insieme è al più numerabile, o è finito o è numerabile, se $|A| = \aleph_0$ allora c'è f bigettiva (e quindi in particolare surgettiva), se $|A| < \aleph_0$ allora c'è [per definizione] $g : n \rightarrow A$ bigettiva per qualche $n \in \omega \setminus \{0\}$, da questa definiamo:

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

come mappa surgettiva da ω in A (cioè estendiamo la funzione che già c'è con n a tutti i naturali maggiori o uguali ponendola come $g(0)$). \square

⁶⁷La soluzione riportata è quella di Mamino.

⁶⁸Quelli al LHS sono quelli nell'enunciato dell'esercizio, quelli al RHS sono quelli presi dalle ipotesi del corollario.

Notazione 7.28 (Successione) — Con **successione** (numerabile) intendiamo semplicemente una funzione con dominio ω , per cui:

$$\alpha = \{\alpha_i\}_{i \in \omega} \stackrel{\text{def}}{=} \alpha : \omega \longrightarrow \dots : i \longmapsto \alpha_i^a$$

una **enumerazione**^b di A è una successione $\alpha = \{\alpha_i\}_{i \in \omega}$ tale che $A = \text{Im}(\alpha)$ (come nella notazione sopra α è la successione che associa ai naturali gli elementi dell'insieme, ed è surgettiva, affinché $\text{Im}(\alpha) = A$), ossia, informalmente, $A = \{\alpha_i | i \in \omega\}$.

^aStiamo abbreviando la successione elencando direttamente i suoi elementi indicizzati.

^bMoralmente: una successione surgettiva.

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 $\omega \times \omega : (a, b) \mapsto a - b$ 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 numerabile⁶⁹ dunque $|\mathbb{Z}| \leq \aleph_0$.

D'altro canto, la funzione $\omega \rightarrow \mathbb{Z} : n \mapsto [(n, 0)]_{\mathbb{Z}}$ è iniettiva, infatti $[(n, 0)]_{\mathbb{Z}} = [(m, 0)]_{\mathbb{Z}} \iff (n, 0) \sim (m, 0) \iff n = m$ (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 quoziente $\mathbb{Z} \times (\omega \setminus \{0\}) \rightarrow \mathbb{Q} : (n, d) \mapsto \frac{n}{d}$ (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 $\frac{n}{1} = \frac{m}{1} \iff n \cdot 1 = m \cdot 1 \iff m = n$, 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. D'altro canto è ragionevole: se esiste una enumerazione $\{a_i\}_{i \in \omega}$ di A ($= A$ è al più numerabile), e, per ogni $i \in \omega$, esista una enumerazione $\alpha_i = \{a_{i,j}\}_{j \in \omega}$ ($=$ per ogni elemento $a_i \in A$ esiste una enumerazione, dunque ogni elemento ($=$ insieme) è a sua volta al più numerabile) di a_i , allora possiamo mandare surgettivamente [cioè enumerare] $\omega \times \omega$ in $\bigcup A$: $(i, j) \mapsto \alpha_{i,j}$ (in questo modo abbiamo un'enumerazione degli elementi degli elementi, e quindi l'unione di A è al più numerabile), e, siccome $\omega \times \omega$ è al più numerabile, lo è anche A (per il solito **corollario**).

L'**errore** è credere di poter fissare una α_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

⁶⁹ $|\omega \times \omega| = \aleph_0 \cdot \aleph_0 = \aleph_0$.

$i \mapsto \alpha_i$ (cioè la funzione che sceglie in quale enumerazione mandare ogni $i \in \omega$). 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 $A = \{a_i \in A \mid i \in \omega\}$ e sia $\{\alpha_i\}_{i \in \omega}$ una **successione di funzioni**^a tali che, per ogni $i \in \omega$, $\alpha_i : \omega \rightarrow a_i$ è una enumerazione di a_i ^b. Allora $|\bigcup A| \leq \aleph_0$.

^aCome prima stiamo supponendo di averle già, altrimenti ci vuole scelta per procurarci la famiglia numerabile di enumerazioni, con tale assioma la parte in rosso di questo enunciato può essere rimossa.

^bCioè è una famiglia di enumerazioni degli elementi dell' i -esimo elemento (ciò ci dice anche che gli elementi di A sono a loro volta AL PIÙ numerabili).

Dimostrazione. Basta osservare che la funzione:

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

è surgettiva e vale quindi il solito **corollario**. □

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 $A = \{a_i \mid i \in \omega\}$ (cioè sto enumerando gli elementi di A):

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

(cioè gli elementi degli elementi di tutti gli elementi a_i sono la stessa cosa che prendere gli elementi degli dell'unione di A , cioè l'immagine dell'enumerazione data per come è definito).

Definizione 7.33 (Parti finite). Definiamo le **parti finite** di un insieme A come:

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

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. Per induzione, il caso $A = \emptyset$ è immediato. Assumiamo $A \neq \emptyset$, sia:

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

siccome $\mathcal{P}^{\text{fin.}}(A) = \bigcup_{n \in \omega} \mathcal{P}^{\leq n}(A)$ ⁷⁰, basta esibire una successione di enumerazione α_n di $\mathcal{P}^{\leq n}(A)$ (cioè una mappa surgettiva da ω a $\mathcal{P}^{\leq n}(A)$, in modo da poter usare il **corollario** ed ottenere che $\mathcal{P}^{\leq n}(A)$ è al più numerabile, da cui, per la proposizione precedente

⁷⁰Ricordiamo che $\bigcup_{n \in \omega} \mathcal{P}^{\leq n}(A) = \bigcup \{\mathcal{P}^{\leq n}(A) \mid n \in \omega\}$, dunque stiamo facendo l'unione di un insieme numerabile.

l'unione è al più numerabile). Fissiamo $f : \omega \rightarrow \omega \times A : x \mapsto (f_1(x), f_2(x))$ surgettiva, che esiste perché A è al più numerabile [quindi anche $\omega \times A$ lo è] (per il [corollario](#) l'avere una funzione surgettiva da ω ad un altro insieme è un fatto equivalente al fatto che il secondo insieme sia al più numerabile).

Costruiamo una enumerazione⁷¹ $\{\alpha_n\}_{n \in \omega}$ di $\mathcal{P}^{\leq n}(A)$, cioè, data la famiglia numerabile $\{\mathcal{P}^{\leq n}(A)\}_{n \in \omega}$, costruiamo una successione $\{\alpha_n\}_{n \in \omega}$ di successioni surgettive della prima famiglia (in modo da enumerare tutti gli elementi degli elementi e poter dire che la famiglia numerabile all'inizio è fatta da elementi al più numerabili, in questo modo siamo nelle ipotesi del lemma dell'unione visto prima).

Costruire una famiglia numerabile di enumerazioni è equivalente al costruire una successione di successioni surgettive, e, come ogni successione, la si può costruire per ricorsione numerabile - prima forma -:

Per $n = 0$ poniamo $\mathcal{P}^0(A) = \{\emptyset\}$, dunque α_0 è la costante [funzione vuota] \emptyset (cioè la successione α_0 che enumera $\mathcal{P}^0(A) = \{\emptyset\}$, è la funzione vuota).

Per $n = s(m)$ in questo caso dobbiamo definire un'enumerazione per $\mathcal{P}^{\leq s(m)}$, dando per nota un'enumerazione α_m per $\mathcal{P}^{\leq m}(A)$, e ciò lo possiamo fare definendo $\alpha_{s(m)}$ ricorsivamente come segue:

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

Stiamo di fatto partendo dal vuoto e aggiungendo in ogni passaggio un elemento di A dato da f_2 (viceversa stiamo “tornando indietro ricorsivamente” tramite f_1 , che rimanda indietro $x-1 \in \omega$).

Vogliamo ora dimostrare per induzione che, per ogni $n \in \omega$, $\alpha_n : \omega \rightarrow \mathcal{P}^{\leq n}(A)$ è surgettiva⁷², cioè che la nostra successione di successioni, è in particolare una successione di enumerazioni:

caso $n = 0$ la successione vuota α_0 è banalmente surgettiva.

caso $n = s(m)$ per ipotesi induttiva la successione $\alpha_m : \omega \rightarrow \mathcal{P}^{\leq m}(A)$ è surgettiva. Dato $Y \in \mathcal{P}^{\leq s(m)}(A)$ si danno due casi. Se $Y = \emptyset$, allora $Y = \alpha_{s(m)}(0) = \emptyset$. Oppure esiste almeno un elemento $y \in Y$.

In questo caso $|Y \setminus \{y\}| \leq m$, quindi vale l'ipotesi induttiva e $Y \setminus \{y\} = \alpha_m(t)$ per qualche $t \in \omega$ (cioè α_m è surgettiva, quindi Y è immagine di qualche $t \in \omega$). Per la surgettività di f , la funzione surgettiva da ω a $\omega \times A$, la coppia (t, y) è uguale a $f(x)$ per qualche $x \in \omega$, cioè $f(x) = (f_1(x), f_2(x)) = (t, y)$. Quindi si ha proprio che $x+1$ dà Y :

$$\begin{aligned} \alpha_{s(m)}(x+1) &\stackrel{\text{def.}}{=} \alpha_m(f_1(x)) \cup \{f_2(x)\} \\ f(x) &\stackrel{(t,y)}{=} \alpha_m(t) \cup \{y\} \\ \text{Hp. indutt.} &\stackrel{=}{=} (Y \setminus \{y\}) \cup \{y\} = Y \end{aligned}$$

(di fatto, fatto il caso $Y = \emptyset$, facciamo in modo di poter sempre tornare indietro a α_0 , da $\alpha_{s(m)}$ e aggiungere ricorsivamente tutti gli elementi a Y a partire dal vuoto). \square

⁷¹In questo caso è una successione di enumerazioni, cioè una successione di funzioni surgettive.

⁷²In questo modo abbiamo enumerato gli elementi degli elementi, e in realtà abbiamo anche già enumerati gli elementi $\mathcal{P}^{\leq i}(A)$, perché lo abbiamo detto all'inizio (formalmente è proprio per costruzione delle parti finite che i $\mathcal{P}^{\leq i}(A)$ sono numerabili).

Applicazione Dimostriamo che l'insieme dei numeri reali algebrici \mathbb{A}_R ⁷³ è numerabile. Per questa applicazione, assumiamo le proprietà elementari di \mathbb{R} . L'insieme \mathbb{A}_R è definito come l'insieme degli $x \in \mathbb{R}$ che sono zeri di qualche polinomio a coefficienti razionali:

$$\mathbb{A}_R \stackrel{\text{def}}{=} \{x \in \mathbb{R} \mid \exists p(x) \in \mathbb{Q}[x] \setminus \{0\} p(x) = 0\}$$

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}_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:

$$p(x) = a_0 + a_1x + a_2x^2 + \dots + a_dx^d$$

con l'insieme dei suoi monomi:

$$p(x) = \{a_0, a_1x, a_2x^2, \dots, a_dx^d\}$$

e ciascun monomio con la coppia (grado, coefficiente):

$$p(x) = \{(0, a_0), (1, a_1), \dots, (d, a_d)\}$$
⁷⁴

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:

$$\mathbb{Q}[x] \subseteq \mathcal{P}^{\text{fin.}}(\omega \times \mathbb{Q})$$
⁷⁵

per cui, essendo che $|\omega \times \mathbb{Q}| = \aleph_0 \implies |\mathcal{P}^{\text{fin.}}(\omega \times \mathbb{Q})| = \aleph_0$, e che $\mathbb{Q}[x]$ si immerge in quest'ultimo insieme (ad esempio con $\text{id}_{\mathbb{Q}[x]}$), 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 disuguaglianza di cardinalità e quindi [come al solito per [Cantor-Bernstein](#)] $|\mathbb{Q}[x]| = \aleph_0$. Venendo ad \mathbb{A}_R abbiamo una facile surgezione:

$$f : (\mathbb{Q}[x] \setminus \{0\}) \times \omega \longrightarrow \mathbb{A}_R : \\ (p, i) \longmapsto \text{"la } i\text{-esima radice di } p \text{ se questa esiste, altrimenti } 0"$$

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

$$\text{"}\alpha \text{ è la } i\text{-esima radice di } p\text{"} \equiv p(\alpha) = 0 \wedge |\{x \in \mathbb{R} \mid x \leq \alpha \wedge p(x) = 0\}| = i$$
⁷⁶

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

Per separazione esiste, quindi, f , e, di conseguenza $|\mathbb{A}_R| \leq \aleph_0$. La disuguaglianza opposta è immediata perché $\mathbb{Q} \subseteq \mathbb{A}_R$ (è facile scrivere un polinomio in $\mathbb{Q}[x]$ che abbia come radice un qualsiasi $q \in \mathbb{Q}$ fissato).

⁷³Sarebbe $\overline{\mathbb{Q}} \cap \mathbb{R}$.

⁷⁴Può essere pensata come funzione da d in \mathbb{Q} .

⁷⁵Cioè, abbiamo visto che un polinomio può essere pensato come una funzione da un qualche elemento di ω (= anche sottoinsieme) a \mathbb{Q} , in particolare ogni elemento di ω né è un sottoinsieme finito, quindi tutti i polinomi a coefficienti in \mathbb{Q} saranno funzioni da un sottoinsieme (in particolare funzioni) finito di ω a \mathbb{Q} , e ricordando, come visto in un esercizio che l'immagine di un insieme finito è finita, abbiamo che i polinomi, viste come funzioni di questo tipo, sono sottoinsiemi finiti di $\omega \times \mathbb{Q}$, pertanto l'insieme dei polinomi $\mathbb{Q}[x]$ è contenuto nelle parti finite di $\omega \times \mathbb{Q}$.

⁷⁶Nell'ordine di \mathbb{R} che prima non avevamo.

Esercizio 7.35. Dato un insieme X , una funzione $f : X^2 \rightarrow X$, e un sottoinsieme $A \subseteq X$ al più numerabile, dimostra che esiste un $\bar{A} \subseteq X$ al più numerabile tale che $f[\bar{A} \times \bar{A}] \subseteq \bar{A}$. Concludi che un gruppo finitamente generato è al più numerabile.

Soluzione.

□

§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 $B \subseteq A$. B è **denso in** $(A, <)$ se:

$$\forall x, y \in A \ x < y \rightarrow \exists z \in B \ x < z < y$$

(cioè tra due elementi di A c'è sempre un elemento di B). $(A, <)$ è **denso**, cioè è denso in se stesso, se:

$$\forall x, y \in A \ x < y \rightarrow \exists z \in A \ x < z < y$$

(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 disuguaglianze 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 $\nexists z \in \omega \ 0 < z < 1$.

Teorema 7.39 (Teorema di isomorfismo di Cantor)

Sia $(A, <)$ un insieme totalmente ordinato tale che:

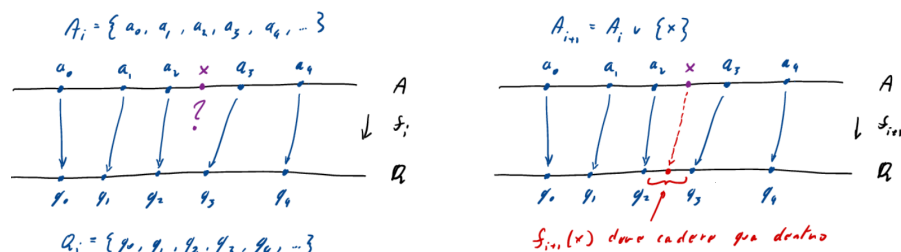
1. $|A| = \aleph_0$
2. $(A, <)$ è denso
3. $(A, <)$ non ha **estremi**, ossia non ha né massimo né minimo elemento

allora $(A, <) \sim (\mathbb{Q}, <)$.^a

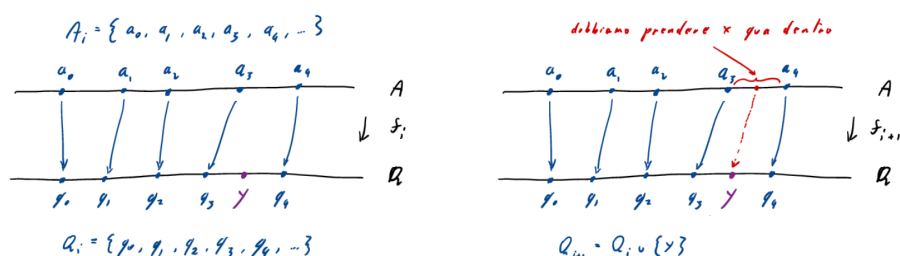
^aQuesta è una condizione sufficiente, quella necessaria consisterebbe nel verificare che $(\mathbb{Q}, <)$ soddisfa le tre proprietà, ma sono ovvie per osservazioni precedenti.

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 elemento 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 segue osservazione.

Osservazione 7.40 (L'unione di un insieme di funzioni 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 :^a

$$\bigcup F : \bigcup \{\text{Dom}(f) | f \in F\} \rightarrow B$$

^aMoralmente se prendiamo l'unione delle funzioni sull'unione dei domini, se tutti i pezzi che "incolliamo" coincidono sugli intervalli dove sono definiti comunemente, allora non c'è alcun problema di buona definizione di una funzione.

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:

$$y_1 = f_1(x) = f_2(x) = y_2$$

□

Siamo ora pronti per dimostrare formalmente il teorema.

Dimostrazione. Per l'ipotesi 1. possiamo fissare un'enumerazione di A e \mathbb{Q} rispettivamente:

$$A = \{a_i | i \in \omega\} \quad \mathbb{Q} = \{q_i | i \in \omega\}$$

Intendiamo costruire una successione di funzioni $\{f_i\}_{i \in \omega}$ tali che, per ogni $i \in \omega$:

1. $f_i : A_i \rightarrow Q_i$ con $|A_i| = |Q_i| < \aleph_0$ ⁷⁷
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. $\forall j < i \ a_j \in A_i \wedge q_j \in Q_i$, ossia $A_i = \{a_0, \dots, a_{i-1}\} \subseteq \text{Dom}(f_i)$ e $Q_i = \{q_0, \dots, q_{i-1}\} \subseteq \text{Im}(f_i)$, $\forall i \in \omega$.

Verifichiamo, per cominciare, che dalle proprietà appena elencate segue che $f \stackrel{\text{def}}{=} \bigcup_{i \in \omega} f_i$ è un isomorfismo di ordini fra A e \mathbb{Q} .

Da 3. segue, con una facile induzione, che $\forall i, j \in \omega \ i \leq j \rightarrow f_i \subseteq f_j$ (stiamo semplicemente estendendo il fatto che la successiva estenda la precedente a due arbitrarie nell'ordine giusto). Quindi [visto che sono tutte estensioni] siamo nelle ipotesi dell'osservazione precedente e f è una funzione.

4. invece implica che [l'unione numerabile dei domini dà proprio] $\text{Dom}(f) = A$ e $\text{Im}(f) = \mathbb{Q}$ (avendo usato a_i e q_i per enumerare A e \mathbb{Q} , questa cosa implica in automatico f surgettiva). Ci resta quindi da verificare che, dati $x, y \in A$ la mappa è crescente [e quindi in automatico anche iniettiva]:

$$x < y \leftrightarrow f(x) < f(y)$$

Fissati $x, y \in A$, siccome $\{a_i\}_{i \in \omega}$ enumera [aka è surgettiva] A , esistono $m, n \in \omega$ tali che $x = a_m$ e $y = a_n$. Preso $t \in \omega$, con $m, n < t$ [possiamo perché ω è illimitato], per la 4., $a_m, a_n \in \text{Dom}(f_t)$ e, siccome f_t è un isomorfismo di ordini per la 2. [ora possiamo usarla perché ha nel suo dominio sia a_m che a_n e quindi ha senso usare la proprietà di isomorfismo], abbiamo:

$$x \stackrel{\text{enum.}}{=} a_m < a_n \stackrel{\text{enum.}}{=} y \leftrightarrow f(x) \stackrel{\text{def.}}{=} f_t(a_m) < f_t(a_n) \stackrel{\text{def.}}{=} f(y)$$

abbiamo quindi che f è ben definita [è una bigezione] ed è l'isomorfismo di ordini tra $(\mathbb{Q}, <)$ e $(A, <)$ cercato. Non ci resta altro da fare che definire per ricorsione numerabile la successione di funzioni $\{f_i\}_{i \in \omega}$ (in particolare stiamo definendo via ricorsione numerabile una mappa $\omega \rightarrow {}^\omega A$). Intanto poniamo $f_0 = \emptyset$.

Per costruire $f_{s(i)}$ definiamo prima un passo intermedio $f_{i+0.5}$ (notazione puramente indicativa). Se $a_i \in \text{Dom}(f_i)$ [a_i è preso in A_{i+1} perché stiamo estendendo, dunque dobbiamo aggiungere il nuovo elemento nell'insieme di partenza], allora $f_{i+0.5} = f_i$ [cioè è già definita ed è f_i]. Altrimenti [ovvero se $a_i \notin \text{Dom}(f_i)$] sia:

$$\bar{j} := \min\{j \in \omega | f_i \cup \{(a_i, q_j)\} \text{ è un isomorfismo}\}$$

⁷⁷Ricordiamo che $A_i = \{a_0, \dots, a_{i-1}\} \subseteq A$ e $Q_i = \{q_0, \dots, q_{i-1}\} \subseteq \mathbb{Q}$.

poniamo $f_{i+0.5} = f_i \cup \{(a_i, q_{\bar{j}})\}$. Ora possiamo definire $f_{s(i)}$.

Se $q_i \in \text{Im}(f_{i+0.5})$ ⁷⁸ [q_i preso in Q_{i+1} , stiamo estendendo l'insieme d'arrivo (e estendendo a sua volta f_i in modo che rimanga un isomorfismo)] allora $f_{s(i)} = f_{i+0.5}$ [in analogia con prima, l'isomorfismo estende il precedente se l'elemento cade dentro $\text{Im}(f_i)$]. Altrimenti, sia:

$$\bar{i} := \min\{\iota \in \omega \mid f_{i+0.5} \cup \{(a_\iota, q_i)\} \text{ è un isomorfismo}\}$$

poniamo $f_{s(i)} = f_{i+0.5} \cup \{(a_{\bar{i}}, q_i)\}$. Le proprietà 1., ..., 4. seguono in maniera immediata per induzione, a patto che la costruzione sia ben posta, ossia i minimi esistano.

Ad essere precisi, occorre quindi dimostrare, per induzione su i , la proposizione:

$$\forall i \in \omega \text{ "la costruzione di } f_i \text{ è ben posta e valgono 1., ..., 4."}$$

Per verificare che la costruzione della successione delle f_i sia ben posta, vediamo che esiste il minimo nel primo passaggio:

$$\bar{j} = \min\{j \in \omega \mid f_i \cup \{(a_i, q_j)\} \text{ è un isomorfismo}\}$$

ossia che l'insieme di cui si prende il minimo non è vuoto, il secondo caso [per vedere che il minimo esiste] sarà analogo.

Per ipotesi induttiva A_i è finito. Se $A_i = \emptyset$ non c'è niente da dimostrare, altrimenti, detto $n = |A_i|$, e sfruttando il fatto che un ordine totale finito è isomorfismo ad un numero naturale [lo si può ordinare totalmente]:

$$A_i = \{\alpha_0, \dots, \alpha_{n-1}\} \quad \text{con } \alpha_0 < \dots < \alpha_{n-1}$$

Ora, l'ipotesi [nella costruzione] è che $a_i \notin A_i$, quindi [sta fuori o in uno dei "buchi" nel dominio, ovvero] o $a_i < \alpha_0$, o $\alpha_k < a_i < \alpha_{k+1}$ per qualche k , o $\alpha_{n-1} < a_i$. Nel primo e terzo caso, rispettivamente, siccome \mathbb{Q} non ha estremi, c'è un $q_j < f_i(\alpha_0)$, o $q_j > f_i(\alpha_n)$ rispettivamente [dunque possiamo estendere f_i prendendo quest'elemento fuori da associare al nostro $a_i \notin \text{Dom}(f_i)$ (a sua volta fuori), per preservare l'ordinamento]. 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 come prima, possiamo estendere la funzione, preservando l'ordinamento con questo elemento]. \square

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.

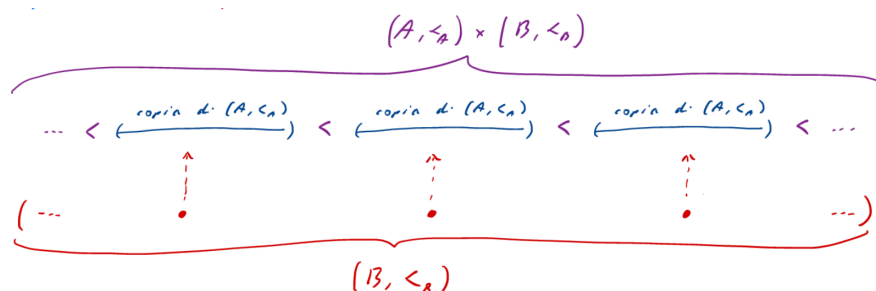
Definizione 7.43 (Prodotto lessicografico di ordini). Dati $(A, <_A)$ e $(B, <_B)$ definiamo il **prodotto lessicografico** di ordini come:

$$(A, <_A) \times (B, <_B) \stackrel{\text{def}}{=} (A \times B, <_{A \times B})$$

dove $(a, b) <_{A \times B} (a', b') \stackrel{\text{def}}{=} (b <_B b') \vee (b = b' \wedge a <_A a')$.

⁷⁸Stiamo estendendo f_i in due passi in modo da poterla estendere prima in avanti [aggiungendo a_i al dominio] e poi all'indietro [aggiungendo q_i all'insieme d'arrivo], che è proprio la tecnica del **back-and-forth**.

Ossia: $(A, <_A) \times (B, <_B)$ è il prodotto cartesiano $A \times B$ munito dell'ordine che CONFRONTA PRIMA LA SECONDA COMPONENTE. Visualmente, si può immaginare $(A, <_A) \times (B, <_B)$ come “ $(A, <_A)$ ripetuto $(B, <_B)$ volte”.



In altre parole, prendiamo l'insieme A , B volte, e disponiamo le sue copie secondo l'ordine degli elementi di B (ogni elemento in una copia di A avrà come prima componente un elemento di A , e come seconda l'elemento di B che corrisponde a quella copia di A). Questa immagine rispetta perfettamente l'ordine dato dal prodotto lessicografico, infatti, confrontando elementi a caso in $A \times B$ si guarda prima la seconda componente (che determina l'ordine delle copie di A), e a parità di quest'ultima (aka siamo nella stessa copia di A) si confronta la prima secondo $<_A$.

Osservazione 7.44 (Ordine totale \implies prodotto ordine totale) — Il prodotto è un ordine. Inoltre se $(A, <_A)$ e $(B, <_B)$ sono ordini totali, allora anche $(A, <_A) \times (B, <_B)$ lo è.

Esercizio 7.45 (Associatività del prodotto lessicografico). Dati $(A, <_A)$, $(B, <_B)$ e $(C, <_C)$ dimostra che:

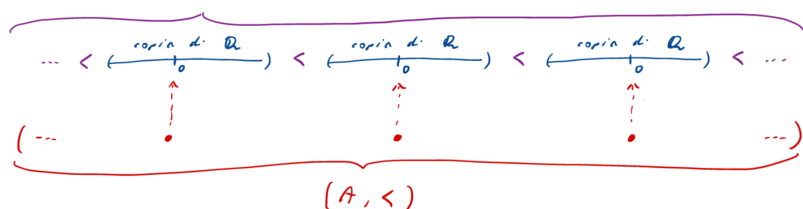
$$((A, <_A) \times (B, <_B)) \times (C, <_C) = (A, <_A) \times ((B, <_B) \times (C, <_C))$$

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 $A \neq \emptyset$ (il caso di $|A|$ finito è anche banale e si può [volendo] trattare separatamente⁷⁹ tuttavia questa dimostrazione copre comunque il caso di A finito). Consideriamo quindi:

$$(S, <) \stackrel{\text{def}}{=} (\mathbb{Q}, <) \times (A, <)$$



⁷⁹Avremmo A in bigezione con n che si immerge in ω che si immerge in \mathbb{Q} , componendo le mappe avremmo che l'immagine con l'ordine indotto da \mathbb{Q} è proprio il sottoinsieme voluto.

L'insieme $S = \mathbb{Q} \times A$ è [in ambo i casi] numerabile. Inoltre, dato $(q, a) \in \mathbb{Q} \times A$ abbiamo:

$$(q-1, a) < (q, a) < (q+1, a)^{80}$$

quindi $\mathbb{Q} \times A$ non ha estremi [né superiori né inferiori]. Per verificare che è denso, consideriamo $(q_1, a_1) < (q_2, a_2)$.

- Se $a_1 < a_2$, allora $(q_1, a_1) < (q_1 + 1, a_1) < (q_2, a_2)$ (per la definizione di ordine nel prodotto lessicografico, ci possiamo spostare come ci pare [sulla prima componente] se le due copie di \mathbb{Q} in cui prendo gli elementi sono distinte, ottenendo elementi nel mezzo).
- Se $a_1 = a_2$ (quindi siamo nella stessa copia di \mathbb{Q}), si ha che $(q_1, a_1) < (\frac{q_1+q_2}{2}, a_1) < (q_2, a_2) = (q_2, a_1)$, ottenendo ancora un elemento nel mezzo.⁸¹

quindi $(S, <)$ è denso e per il [teorema di isomorfismo di Cantor](#) si ha $(S, <) \sim (\mathbb{Q}, <)$. Ma $A \hookrightarrow \mathbb{Q} \times A : a \mapsto (0, a)$, quindi, componendo l'immersione con l'isomorfismo trovato, abbiamo trovato 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 $2 \leq |A| \leq \aleph_0 \implies |A| = \aleph_0$ ⁸². 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 $\mathbb{Q} + n \mapsto \frac{1}{n}$] 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. Pertanto, nel caso in cui A abbia entrambi gli estremi:

$$(A, <) \sim (\mathbb{Q} \cup \{\alpha, \beta\}, <') \sim ([0, 1]_{\mathbb{Q}}, <) = ([0, 1]_{\mathbb{Q}} \cup \{0, 1\}, <)$$

con $f(a) = \alpha$, $f(b) = \beta$ e $<' = \cup(\{\alpha\} \times \mathbb{Q}) \cup (\mathbb{Q} \times \{\beta\})$ ⁸³. Gli altri due casi (A chiuso in un estremo solo) sono analoghi e danno l'isomorfismo con $[0, 1]_{\mathbb{Q}}$ e $]0, 1[_{\mathbb{Q}}$. \square

⁸⁰Ricordiamo che stiamo usando $(A, <)$ come secondo termine del prodotto lessicografico, dunque le copie di $(\mathbb{Q}, <)$ sono ordinate come gli elementi di A .

⁸¹Morale della favola: se ho un ordine non denso, è sufficiente moltiplicarlo per \mathbb{Q} .

⁸²Stiamo escludendo l'insieme denso con un solo elemento

⁸³Per essere precisi, detto f l'isomorfismo tra $(\mathbb{Q}, <)$ e $]0, 1[_{\mathbb{Q}}$, per estenderlo ad un isomorfismo tra $(\mathbb{Q} \cup \{\alpha, \beta\}, <')$ e $([0, 1]_{\mathbb{Q}}, <)$, ci basta porre $f' := f \cup \{(\alpha, 0), (\beta, 1)\}$, in questo modo, componendolo con l'isomorfismo tra $(A, <)$ e $(\mathbb{Q} \cup \{\alpha, \beta\}, <')$, si ottiene l'isomorfismo tra A il chiuso $[0, 1]_{\mathbb{Q}}$ voluto.

§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 irreflessiva $(\forall x \in V (x, x) \notin e)$.

L'idea è che V può essere immaginato come un insieme di punti che possono essere connessi da archi. C'è un arco fra x e y se $(x, y) \in e$.

Partiamo da un'idea intuitiva - chi ha già seguito un corso di probabilità saprà formalizzare questa cosa in termini precisi. Data una probabilità $p \in]0, 1[$ costruiamo un grafo G_p con insieme di vertici ω come segue. Per ogni coppia $(i, j) \in \omega \times \omega$ con $i < j$ [solo per prendere tutte le coppie una volta e non beccare le stesse andando avanti] 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 isomorfismi**⁸⁴, dove, per essere precisi [possiamo definire l'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:

$$\forall v, w \in V_1 (v, w) \in e_1 \iff (f(v), f(w)) \in e_2$$

Vediamo perché. Dati due sottoinsiemi finiti X e Y di ω , e dato un vertice $v \notin X \cup Y$ la probabilità che x sia connesso da un arco a tutti i vertici di X e a nessuno di quelli di Y è $p^{|X|} \cdot (1-p)^{|Y|}$ ⁸⁵ - come che sia, è un certo numero > 0 - e ci sono infiniti [siamo in ω] $v \notin X \cup Y$. Si capisce, quindi, che con probabilità 1 - ossia certamente - almeno uno di questi vincerà questa lotteria (ne abbiamo infiniti, quindi quasi certamente ne troviamo uno), 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) è un **grafo random** se:⁸⁶

$$\forall X \subseteq \omega \forall Y \subseteq \omega \setminus X \quad |X|, |Y| < \aleph_0 \quad \exists v \in \omega \setminus (X \cup Y) \quad \underbrace{X \times \{v\} \subseteq e}_{\forall x \in X (x, v) \in e} \wedge \underbrace{(Y \times \{v\}) \cap e = \emptyset}_{\neg \exists y \in Y (y, v) \in e}$$

(cioè se per ogni coppia di sottoinsiemi 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).

Esercizio 7.50 (Esistenza e unicità del grafo random). Dimostra che esiste un grafo random, ed è unico a meno di isomorfismi.^a

^aHint: Usare il back-and-forth per l'unicità.

⁸⁴A meno di rinominare i vertici, che è quello che diremo nella definizione di isomorfismo.

⁸⁵Eventi 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 $(1-p)^{|Y|}$.

⁸⁶Typo di Mamino.

■

Soluzione.



§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.

^aÈ una facile verifica che passa attraverso la definizione di minimo.

Definizione 8.3 (Ordine totale completo). Un ordine totale $(A, <)$ è **completo** se ogni $B \subseteq A$ superiormente limitato ha un estremo superiore $\sup B \in A$.⁸⁷

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} .

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 8.5 (Segmento iniziale). Sia $(A, <)$ un ordine totale. $B \subseteq A$ è un **segmento iniziale** di A se $\forall x \in B \ \forall y \in A \ y < x \rightarrow y \in B$. [Se contiene un punto, contiene tutti i precedenti, strettamente].

Ossia B è un segmento iniziale di A se, ogniquale volta B contiene un elemento, B contiene altresì tutti gli elementi minori di questo. Un segmento iniziale B di A si dice **proprio** se $B \neq A$.

Esempio 8.6 (Segmento iniziale principale)

Dato $(A, <)$ ordine totale, A stesso e \emptyset sono segmenti iniziali di A . Dato $x \in A$, l'insieme:

$$A_x \stackrel{\text{def}}{=} \{y \in A | y < x\}$$

è un segmento iniziale proprio di A - detto **segmento iniziale principale** determinato da x . Ad esempio $\{x \in \mathbb{Q} | x < 0 \vee x^2 < 2\}$ è un segmento iniziale [proprio] di \mathbb{Q} che non è principale.

⁸⁷Questa definizione [la Dedekind-completezza] è a priori diversa dalla Cauchy-completezza (ovvero che tutte le successioni di Cauchy convergono).

Nota 8.7 — 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 8.8 (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 il punto lo metto nel complementare].

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 8.9 (Insieme ordinato dei numeri reali). Definiamo l'insieme dei **numeri reali** come l'insieme delle sezioni di Dedekind di \mathbb{Q} :

$$\mathbb{R} \stackrel{\text{def}}{=} \{x \in \mathcal{P}(\mathbb{Q}) \mid x \text{ è una sezione su } \mathbb{Q}\}^{88 \ 89}$$

con l'ordine dato da:

$$\forall x, y \in \mathbb{R} \ x \leq y \stackrel{\text{def}}{=} x \subseteq y^{90}$$

Proposizione 8.10 (\mathbb{R} è completo)

$(\mathbb{R}, <)$ è un ordine totale completo.

Prima della dimostrazione, isoliamo un semplice lemma.

Lemma 8.11 (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 $\beta \in A$, con $\beta < \alpha$. Dobbiamo dimostrare che $\beta \in \bigcup X$ [cioè che l'unione è ancora un segmento iniziale]. Siccome $\alpha \in \bigcup X$, esiste $x \in X$, tale che $\alpha \in x$ (cioè α è un elemento di un elemento per definizione di unione). Siccome x è un segmento iniziale di A , allora $\beta < \alpha \rightarrow \beta \in \underbrace{x}_{\in X} \subseteq \bigcup X$ [cioè è un elemento di un

elemento di X (= sottoinsieme dell'unione degli elementi degli elementi), dunque sta nell'unione e quindi questa è un segmento iniziale]. \square

Ora possiamo dimostrare la proposizione come segue.

Dimostrazione. Abbiamo un ordine parziale perché il contenimento \subseteq , è un ordine parziale su \mathcal{P} (quello che sia). Supponiamo per assurdo, che non sia totale, allora esistono $x, y \in \mathbb{R}$ per cui $x \not\subseteq y$ e $y \not\subseteq x$, quindi ci sono $a \in x \setminus y$ e $b \in y \setminus x$ (non essendo contenuti né uguali fare queste sottrazioni di insiemi ci lascia sempre insiemi non vuoti in cui prendere gli elementi). Ora si danno due casi: se $a <_{\mathbb{Q}} b^{91}$ allora [per definizione di segmento iniziale] $b \in y \implies a \in y \nmid$, simmetricamente, se $b < a$ allora $a \in x \implies b \in x \nmid$. Dunque \subseteq è un

⁸⁸Moralmente: sono tutti i modi di prendere \mathbb{Q} e tagliarlo in due (indipendentemente da cosa chiamo numero reale, i.d. la cosa a destra o a sinistra, cioè la sezione di Dedekind o il suo complementare, basta fissare una codifica).

⁸⁹Dunque nella nostra codifica un reale non è altro che una semiretta sinistra di \mathbb{Q} .

⁹⁰Era equivalente definire il $<$ a partire da \subseteq , avremmo ottenuto comunque lo stesso ordine su \mathbb{R} .

⁹¹Le sezioni di Dedekind sono sottoinsiemi di \mathbb{Q} , quindi i loro elementi sono ordinati dall'ordine totale in $(\mathbb{Q}, <)$.

ordine totale. Resta da dimostrare la completezza.

Sia $A \subseteq \mathbb{R}$ non vuoto e superiormente limitato [= ammette un maggiorante] da $m \in \mathbb{R}$. Dimostriamo che $\sup A = \bigcup A \in \mathbb{R}$.

Per il lemma precedente $\bigcup A$ è ancora un segmento iniziale, e siccome A non è vuoto $\bigcup A \neq \emptyset$, inoltre poiché m è un maggiorante di A [quindi per l'ordinamento definito contiene tutti gli elementi e in automatico gli elementi degli elementi], si ha $\bigcup A \subseteq m$, per cui $\bigcup A \neq A$ (ovvero è un segmento iniziale proprio). In definitiva $\bigcup A$ è una sezione di Dedekind di \mathbb{Q} , e, di conseguenza un elemento di \mathbb{R} .

Verifichiamo che $\bigcup A$ è un maggiorante di A . Se $x \in A$, allora $x \subseteq \bigcup A$ [per definizione], cioè, appunto $x \leq \bigcup A$ per come abbiamo definito l'ordine su \mathbb{R} .

Ora, se m è un altro maggiorante di A , allora $\forall x \in A \ x \subseteq m$, ma ciò equivale a $\bigcup A \subseteq m$ (se tutti gli elementi sono contenuti in m , allora lo sono in automatico tutti gli elementi degli elementi), quindi $\bigcup A$ è il minimo dei maggioranti di A . \square

Osservazione 8.12 (\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^a, immerge \mathbb{Q} in \mathbb{R} in maniera strettamente crescente e densa (ossia $\iota(\mathbb{Q}) = \text{Im}(\iota)$ è densa in \mathbb{R}).

^aÈ in automatico ben definita essendo l'oggetto in arrivo una sezione di Dedekind di \mathbb{Q} .

Dimostrazione. Dati $a, b \in \mathbb{Q}$, con $a < b$, abbiamo $\mathbb{Q}_a \subsetneq \mathbb{Q}_b$ (perché ad esempio $a \notin \mathbb{Q}_a$, ma $a \in \mathbb{Q}_b$, dunque vale $\mathbb{Q}_a \subsetneq \mathbb{Q}_b \equiv \mathbb{Q}_a < \mathbb{Q}_b$), quindi ι è strettamente crescente [dunque anche iniettiva]⁹². Dati $x, y \in \mathbb{R}$, con $x < y$, ciò equivale per definizione di ordine su \mathbb{R} a $x \subsetneq y$, dunque esiste $a \in y \setminus x$ ($a \in \mathbb{Q}$ per definizione di sezione).

Siccome y non ha massimo (per definizione di sezione) [e $a \in y$], c'è un $b \in y$ [dunque $b \in \mathbb{Q}$] con $a < b$. Ora per tale b si ha: $x \subsetneq \mathbb{Q}_b \subsetneq y$, dove il primo contenimento⁹³ è stretto perché $a \notin x$ [per definizione di a] e $a \in \mathbb{Q}_b$ [perché $a < b$ per come è definito b], mentre il secondo è stretto perché $b \notin \mathbb{Q}_b$ [per definizione di di segmento iniziale principale] e $b \in y$ [per definizione] (inoltre sono contenimenti di segmenti iniziali, dunque è naturale che tutti gli elementi di quelli più a sinistra siano contenuti da quelli più a destra). Dunque $\text{Im}(\iota)$ densa in \mathbb{R} . \square

⁹²In particolare così abbiamo già che $(\mathbb{Q}, <)$ è isomorfo a $(\iota[\mathbb{Q}], <_{\iota[\mathbb{Q}]}) \subseteq (\mathbb{R}, <)$.

⁹³Per costruzione $a \in y \setminus x$, e $a \in \mathbb{Q}_b$, dunque $x < a$ e per la definizione di segmento iniziale tutti gli elementi di x stanno in \mathbb{Q}_b .

Notazione 8.13 (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 abusare della notazione immaginando che queste siano vere e proprie inclusioni [di insiemi, senza passare per le immagini^a]:

$$\omega \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

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.

^aAnche più immagini visto che per arrivare in \mathbb{R} gli insiemi più a sinistra devono passare per una composizione di funzioni.

Corollario 8.14 (\mathbb{R} è più che numerabile)

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

Dimostrazione. Dall'osservazione sulla notazione di sopra, abbiamo visto che $\mathbb{Q} \xhookrightarrow{\iota} \mathbb{R}$, 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] (per la seconda cosa ci basta che ci sia sempre qualcosa in \mathbb{R} tra due elementi di \mathbb{R} , se questo qualcosa è un elemento di $\iota[\mathbb{Q}]$ poco importa, la proprietà è verificata lo 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 [non vale l'ipotesi 1. dell'isomorfismo di Cantor che avevamo assunto dunque] non può esserci una bigezione $\Rightarrow \aleph_0 < |\mathbb{R}|$. \square

§8.1 Caratterizzazione dei reali come ordine

Abbiamo stabilito che $(\mathbb{R}, <)$ è un ordine completo senza estremi con un sottoinsieme, \mathbb{Q} , denso e numerabile. Queste proprietà, a loro volta, caratterizzano l'insieme ordinato $(\mathbb{R}, <)$ a meno di isomorfismi.

Proposizione 8.15 (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

allora $(A, <)$ è isomorfo a $(\mathbb{R}, <)$.^a

^aCome al solito il teorema è una condizione sufficiente per essere isomorfo ad \mathbb{R} , e l'altra freccia è già stata verificata man mano che si costruiva \mathbb{R} in precedenza.

Dimostrazione. Sia \tilde{A} l'insieme delle sezioni su B . Osserviamo che $(A, \leq) \sim (\tilde{A}, \subseteq)$. L'isomorfismo è infatti dato da:

$$f : A \rightarrow \tilde{A} : a \mapsto B_a = \{x \in B \mid x < a\} \subsetneq B$$

la cui inversa è:

$$g : \tilde{A} \rightarrow A : Y \mapsto \sup Y$$

Verifiche: a è un maggiorante di B_a (per definizione), ed è il minimo perché se $x < a$ fosse un maggiorante, per la densità di B in A , esiste $y \in B$ con $x < y < a$, quindi $y \in B_a$ per la seconda disuguaglianza (cioè per definizione di segmento iniziale), e $x < y$ non può essere ovviamente un maggiorante di B_a [abbiamo appena trovato un elemento in B_a più grande]. Quindi $\sup B_a = a$, ossia $g(f(a)) = a$.

Per ottenere la composizione opposta, $B_{\sup Y} = Y$, dimostriamo che $x \in B_{\sup Y} \leftrightarrow x \in Y$ [che è equivalente per estensionalità].

← Per costruzione, vale che $x \in Y \rightarrow x \leq \sup Y$, perché il sup per definizione è un maggiorante di Y , inoltre non può essere $x = \sup Y$ perché, per definizione di sezione, Y non ha massimo, quindi $x \in B_{\sup Y}$.

→ Per ottenere la freccia opposta, abbiamo $x \in B_{\sup Y} \iff x < \sup Y$, allora x non può essere un maggiorante di Y - perché $\sup Y$ è il minimo di questo e $x < \sup Y$ - quindi esiste $y \in Y$ ⁹⁴ [se non ci fosse y , x sarebbe un maggiorante, ma come detto, ciò è assurdo], con $x < y$, ma Y è un segmento iniziale, quindi per definizione $x \in Y$.

Ora per il [teorema di isomorfismo di Cantor](#) [è numerabile per 3., è denso per lo stesso motivo (se lo è in A , lo è a maggior ragione in se stesso⁹⁵), ed essendo A senza estremi e B denso in A , anche B è senza estremi⁹⁶], B con l'ordine indotto da $(A, <)$ è isomorfo a $(\mathbb{Q}, <)$, quindi le sezioni di Dedekind di $(B, <)$ sono isomorfe alle sezioni di \mathbb{Q} , ossia $(\tilde{A}, \subseteq) \sim (\mathbb{R}, \leq)$ e quindi $(A, \leq) \sim (\mathbb{R}, \leq)$. \square

Nota 8.16 — Come conseguenza della dimostrazione abbiamo ottenuto che le sezioni di Dedekind di \mathbb{R} con l'ordine indotto sono isomorfe a $(\mathbb{R}, <)$.

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 ⁹⁷
- $\forall x, y, z \in F \ x < y \rightarrow x + z < y + z$ (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).

⁹⁴Sarebbe la caratterizzazione del sup di un insieme.

⁹⁵Tutti gli elementi di B sono anche elementi di A .

⁹⁶Se B fosse limitato superiormente o inferiormente, ci sarebbe un elemento di A più grande del limite, e per densità uno di B tra il limite e quello più grande.

⁹⁷Come ribadito più volte è indifferente usare $<$ o \leq .

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.

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 [1], capitolo 10; NOTE DEL PROF. Di Nasso, fascicolo 4 [2]; LEZIONE 16 dell'a.a. 2020-21 [3].

§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 disuguaglianza da dimostrare è $2^{\aleph_0} \leq |\mathbb{R}|$. Esibiamo quindi una funzione iniettiva $\mathcal{P}(\omega) \rightarrow \mathbb{R}$ ⁹⁸ come segue:

$$f : \mathcal{P}(\omega) \rightarrow \mathbb{R} : S \mapsto 0.a_0^S a_1^S a_2^S a_3^S \dots \quad \text{con } a_i^S = \begin{cases} 0 & \text{se } i \notin S \\ 1 & \text{se } i \in S \end{cases} \quad \text{100}$$

per esempio $S = \{2, 3, 5, 7, 11, \dots\}$ dà $f(S) = 0.001101010001 \dots$ è chiaro che:

$$f(S) = f(T) \stackrel{\text{def.}}{\iff} \forall i \in \omega \ a_i^S = a_i^T \stackrel{\text{def.}}{\iff} \forall i \in \omega \ i \in S \leftrightarrow i \in T \stackrel{\text{estensionalità}}{\iff} S = T$$

⁹⁸Ricordando che $|\mathcal{P}(A)| \stackrel{\text{visto}}{=} |A^2| \stackrel{\text{op. card.}}{=} 2^{|A|}$.

⁹⁹Sarebbe la scrittura decimale.

¹⁰⁰Cioè restituisce un numero decimale fatto da soli 0 e 1, che ha gli 1 dove l'indice corrisponde ad una posizione sta nell'insieme S e 0 se la posizione non lo è (naturalmente se l'insieme è finito la sequenza sarà 0 da un certo punto, se non lo fosse non è detto, ad esempio presi i naturali pari avremo una sequenza infinita del tipo 0.1010101010...).

Non è difficile formalizzare questa dimostrazione. Basterebbe definire $0.a_1a_2a_3\dots$ come $\sum_{i=0}^{\infty} a_i 10^{-i}$, poi $\sum_{i=0}^{\infty}$ come $\sup \{\sum_{i=0}^n\}$, poi $\sum_{i=0}^n$ per ricorsione numerabile, poi dimostrare le proprietà aritmetiche rilevanti. Noi sfrutteremo la stessa idea, ma formulando la dimostrazione in termini di ordini.

§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 $(2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0}$, e, ricordando che prodotto di numerabili è numerabile, si ottiene $2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$. \square

Lemma 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:

$$\begin{aligned} \beta &= \beta + 0 && \stackrel{\text{compatib. op. cardin.}}{\leq} && \alpha + \beta && \stackrel{\text{compatib. op. cardin.} + \text{Hp.}}{\leq} && 2\beta = \beta \\ \beta &= \beta \cdot 1 && \stackrel{\text{compatib. op. cardin.}}{\leq} && \alpha \cdot \beta && \stackrel{\text{compatib. op. cardin} + \text{Hp.}}{\leq} && \beta^2 = \beta \end{aligned}$$

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

Lemma 8.24 ($\alpha^{\aleph_0} = 2^{\aleph_0}$)

Se $2 \leq \alpha \leq 2^{\aleph_0}$ 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:

$$2^{\aleph_0} \leq \alpha^{\aleph_0} \leq (2^{\aleph_0})^{\aleph_0} \stackrel{\text{oss. sopra}}{=} 2^{\aleph_0}$$

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 $A \setminus B \subseteq A$, o $|A \setminus B| = \aleph_0$ o $|A \setminus B| < \aleph_0$ (cioè la sottrazione ci dà ancora un sottoinsieme di ω , che quindi è al più numerabile e per una proposizione vista o è finito o è numerabile). Escludiamo che valga la seconda possibilità, se così fosse:

$$A = B \cup (A \setminus B)$$

cioè un insieme numerabile è unione di insiemi finiti, dunque è finito¹⁰² che è assurdo¹⁰³. \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 disuguaglianza opposta. Siccome $2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0}$, esiste una biezione:

$$f : A \rightarrow {}^\omega 2 \times {}^\omega 2$$

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:

$$|\pi \circ f[B]| \leq \aleph_0 < 2^{\aleph_0}$$

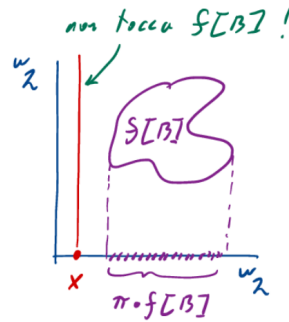
in particolare $|f[B]| = |B| \leq \aleph_0$ perché f biezione, inoltre, essendo $f[B]$ al più numerabile e π surgettiva, $\pi[f[B]]$ è al più numerabile (come visto nell'[esercizio](#)¹⁰⁴).

¹⁰¹Possiamo sempre assumere sia ω WLOG.

¹⁰²Per inclusione-esclusione $|A \cup B| \leq |A| + |B| = n + m \in \omega$.

¹⁰³Volendo ogni cardinalità finita sta in ω [o un qualsiasi altro insieme numerabile], e quindi si immerge in lui, cosa che rende assurda l'uguaglianza trovata.

¹⁰⁴ $|f[B]| \leq \aleph_0$, $f[B] \xrightarrow{\pi} \pi[f[B]]$, quindi $|\pi[f[B]]| \leq \aleph_0$.



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 $f[B]$] $(\{x\} \times \omega_2) \cap f[B] = \emptyset$ (fondamentalmente, trovato l' x in ω_2 , siamo tornati indietro con π^{-1} ¹⁰⁵).

Quindi tornando indietro ad A [via f^{-1}], $f^{-1}(\{x\} \times \omega_2) \cap B = \emptyset$, ossia $f^{-1}(\{x\} \times \omega_2) \subseteq A \setminus B$ [se non sta in B sta nel suo complementare in A], 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 disuguaglianza dal basso e quindi $|A \setminus B| = 2^{\aleph_0}$. \square

Siamo finitamente pronti per dimostrare che $|\mathbb{R}| = 2^{\aleph_0}$.

Dimostrazione. Siccome $\mathbb{R} \subseteq \mathcal{P}(\mathbb{Q})$, la disuguaglianza $|\mathbb{R}| \leq 2^{\aleph_0}$ è immediata. Per dimostrare la disuguaglianza opposta definiamo:

$$A \stackrel{\text{def}}{=} \{X \in \mathcal{P}(\omega) \mid X \neq \emptyset \wedge |\omega \setminus X| \geq \aleph_0\}$$

ossia i sottoinsiemi di ω non vuoti e **co-infiniti**.

Intuitivamente: $X \in A$ rappresenta lo sviluppo in notazione binaria di un $x \in]0, 1[$ - $x = 0.a_1a_2a_3\dots$, $a_i = 1 \leftrightarrow i \in X$ - la condizione $X \neq \emptyset$ serve a escludere lo 0, la condizione di co-infinitesza a escludere l'uno periodico.

Ci basta dimostrare che $|A| = 2^{\aleph_0}$ e che esiste $f : A \rightarrow \mathbb{R}$ iniettiva. La prima cosa è facile:

$$A = \mathcal{P}(\omega) \setminus (\{\emptyset\} \cup \underbrace{\{X \in \mathcal{P}(\omega) : |\omega \setminus X| < \aleph_0\}}_{\stackrel{\text{def}}{=} S})$$

L'insieme S è in corrispondenza biunivoca con $\mathcal{P}^{\text{fin.}}(\omega)$ tramite la funzione "complementare rispetto a ω ":

$$\bar{} : S \rightarrow \mathcal{P}^{\text{fin.}}(\omega) : X \mapsto \bar{X} = \omega \setminus X$$

Quindi $|S| = |\mathcal{P}^{\text{fin.}}(\omega)| = \aleph_0$, e, di conseguenza ¹⁰⁶ $|A| = |\mathcal{P}(\omega) \setminus (\{\emptyset\} \cup S)| = 2^{\aleph_0}$, grazie al lemma precedente. Resta da costruire $f : A \rightarrow \mathbb{R}$ iniettiva.

Cominciamo col definire un ordine totale su A . Dati $X, Y \in A$ (cioè sottoinsiemi non vuoti e co-infiniti di ω):

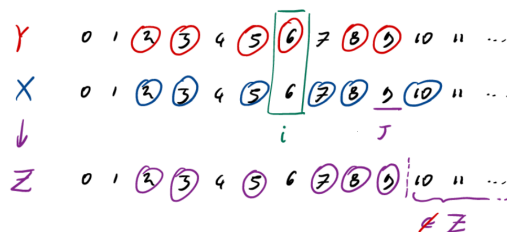
$$X <_A Y \stackrel{\text{def}}{=} \exists i \in \omega \underbrace{(i \cap X = i \cap Y)}_{\forall j < i \ j \in X \leftrightarrow j \in Y} \wedge \underbrace{(i \in Y \setminus X)}_{i \in Y \wedge i \notin X}$$

¹⁰⁵ $\pi^{-1}(x) = \{x\} \times \omega_2$, quindi $x \notin \pi \circ f[B]$ diventa $\pi^{-1}(x) = (\{x\} \times \omega_2) \cap f[B] = \emptyset$, perché se l'intersezione fosse non vuota

¹⁰⁶ $|\{\emptyset\} \cup S| \leq |\emptyset| + |S| = 1 + \aleph_0 = \aleph_0$ e $S \subseteq (\{\emptyset\} \cup S)$, da cui formalmente si ottiene che l'unione è numerabile.

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 ancora un sottoinsieme di ω per cui il minimo esiste], se $i \in Y$ - per cui, chiaramente, $i \notin X$ - allora $X < Y$, se, invece $i \in X$ - per cui $i \notin Y$ - allora $Y < X$ (in altri termini, presa la differenza simmetrica di due insiemi, chi dei due ha il minimo elemento è il maggiore). La verifica del fatto che questo è un ordine totale è immediata. Consideriamo $B \stackrel{\text{def}}{=} \mathcal{P}^{\text{fin.}}(\omega) \setminus \{\emptyset\} \subseteq A$. Chiaramente $|B| = \aleph_0$. Dimostriamo ora che B è denso in A .

Dati $X, Y \in A$, con $X < Y$, sia $i := \min X \Delta Y$ (che c'è per quanto appena scritto e in particolare sta in Y) e $j > i$ minimo tale che $j \notin X$, che esiste perché X è co-infinito. Sia $Z \stackrel{\text{def}}{=} (X \cap j) \cup \{j\}$ (ricordiamo che siamo in ω , quindi stiamo togliendo da X tutte le cose maggiori o uguali a j e poi stiamo riaggiungendo j), Z è finito [perché intersezione con $j \in \omega +$ unione con singoletto], quindi appartiene a B per definizione. Inoltre j è il minimo elemento di $X \Delta Z$ [l'abbiamo preso come il più piccolo non in x e poi lo abbiamo aggiunto a Z] e $j \in Z$, quindi [per come è definito l'ordine] $X < Z$, e, similmente, i è il minimo di $Z \Delta Y$ e $i \in Y$, quindi di nuovo si ha $Z < Y$, pertanto $X < Z < Y$.



Stabilito che B è denso in A , B è, in particolare, denso [numerabile e naturalmente illimitato rispetto all'ordine dato ad A^{107}], quindi, c'è un isomorfismo di ordini $g : B \rightarrow \mathbb{Q}$. Ora, siccome, nuovamente, B è denso in A , la funzione:

$$h : A \rightarrow \text{sezioni [principali] su } B : X \mapsto B_X = \{Y \in B \mid Y < X\}$$

è iniettiva [e sezioni di $B = \mathbb{R}$]. Quindi $f : A \rightarrow \mathbb{R} : X \mapsto g[h(X)]$ è una funzione iniettiva da A a \mathbb{R} (per essere formali dovremmo comporre anche ι alla fine, per quanto osservato sul fatto che $\mathbb{Q} \subseteq \mathbb{R}$). \square

¹⁰⁷Segue dal fatto che ω è illimitato.

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 soli assiomi 1-7. Inoltre ci mancano risultati desiderabili per via delle applicazioni, segnatamente il lemma di Zorn.
3. Vi sono insiemi la cui esistenza vorremmo escludere. Per esempio vorremmo che l'equazione $X = \{X\}$ non avesse soluzioni, e 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, $x \in A_a \xrightarrow{\text{def.}} x < a \xrightarrow{a \text{ min. in } A \setminus I} x \notin A \setminus I \implies x \in I$ (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:

$$\bigcap_{x \in B} B_x^{108}$$

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 [aka $B_m = \emptyset$]. 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 $y < y \not\leq$. 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 [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 non è un buon ordine, come già sapevamo.

¹⁰⁸Ricordiamo che: $\bigcap_{x \in B} B_x = \bigcap \{B_x \mid x \in B\}$.

Lemma 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 $\forall x \in A \ x \leq f(x)$.

Dimostrazione. Per assurdo, assumiamo la negazione della tesi, $\exists x \in A \ x > f(x)$. Quindi l'insieme $B = \{x \in A \mid f(x) < x\}$ 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 $g : A \rightarrow B$ fossero due isomorfismi diversi, allora $g^{-1} \circ f : A \rightarrow A$ 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 ordini. 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 [non necessariamente proprio]¹⁰⁹. Si ha che $g \circ f$ è crescente in quanto composizione di funzioni crescenti. Occorre verificare che $g \circ f[A]$ è un segmento iniziale di C .

Verifica: sia $g(f(a))$ un qualunque elemento di $g \circ f[A]$, se sia $x < g(f(a))$, dobbiamo verificare [per avere la definizione di segmento iniziale] che $x \in g \circ f[A]$. $g(f(a)) \in g[B]$ e [per ipotesi] $g[B]$ è segmento iniziale di C , quindi $g[B] \ni g(f(a)) > x \in g[B]$. Scriviamo $x = g(y)$. Ora, siccome g è un isomorfismo, da $x < g(f(a))$ deduciamo $y < f(a) \in f[A]$. Siccome $f[A]$ è segmento iniziale di B , segue che $y \in f[A]$, quindi possiamo scrivere $y = f(z)$, per qualche $z \in A$. In definitiva 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.

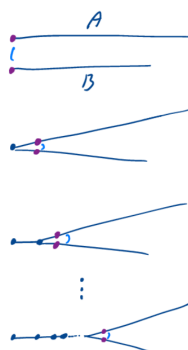
Dimostrazione. Siano $f : A \rightarrow B$ e $g : B \rightarrow A$ isomorfismi fra A e un segmento iniziale di B e fra B e un segmento iniziale di A . Ricordando la dimostrazione dell'osservazione precedente, $g \circ f$ è un isomorfismo fra A e un **segmento iniziale** $g \circ f[A]$ di A . Ma per l'(1) del corollario $g \circ f[A]$ non può essere un segmento iniziale **proprio**, quindi [deve essere tutto A] $g \circ f[A] = A$. Ma allora, per il (2) del medesimo corollario, $g \circ f = \text{id}_A$. Ragionando simmetricamente $f \circ g = \text{id}_B$, quindi f è un isomorfismo fra A e B , con inversa g . \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 teorema 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 .

¹⁰⁹Una definizione alternativa ed equivalente di minore o uguale tra buoni ordini, rispetto a quella data all'inizio, è che un buon ordine sia isomorfo ad un segmento iniziale non necessariamente proprio dell'altro.

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 teorema¹¹⁰, si può verificare al più una delle tre condizioni. Consideriamo ora 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 (cioè 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 $\text{Dom}(f) = A$ 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 $B_b \not\subseteq$ (a causa dell'(1) del corollario).

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 (cioè manda s.i. in s.i. [isomorfi] in arrivo), 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 che $A_{a'} \preceq A_a$ [$\implies A_{a'} \subseteq A_a \implies a' \leq a$] che è assurdo perché A_a è un segmento iniziale proprio di $A_{a'}$ [poiché avevamo assunto $a < a'$].

$\text{Dom}(f)$ è s.i. di A Sia $a \in \text{Dom}(f)$ e $a' < a$, vogliamo dimostrare che $a' \in \text{Dom}(f)$ (che quindi è un segmento iniziale). L'ipotesi $a \in \text{Dom}(f)$ equivale a dire che esiste $b \in B$ tale che $A_a \sim B_b$, quindi, in particolare, $A_a \preceq B_b$ (per la definizione di f abbiamo l'isomorfismo e per l'osservazione sull'antisimmetria possiamo indebolire la cosa a disuguaglianza). Da $a' < a$ segue come al solito che $A_{a'} \subsetneq A_a$, quindi [per definizione di \prec] $A_{a'} \prec A_a$.

Per transitività abbiamo quindi $A_{a'} \prec B_b$ e, siccome ogni segmento iniziale [proprio] è principale [in un buon ordine], esiste $b' \in B_b$, tale che $A_{a'} \sim (B_b)_{b'}$ (stiamo usando la definizione di \prec). Si conclude osservando che $(B_b)_{b'} \sim B_{b'}$ (basta verificare i due contenimenti banali), quindi $A_{a'} \sim B_{b'} \iff f(a') = b' \iff (a', b') \in f \implies a' \in \text{Dom}(f)$.

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

¹¹⁰Typo di Mamino.

$$\begin{array}{l} \text{Dom}(f) = A \\ \text{o } \text{Im}(f) = B \end{array}$$

Se così non fosse, per la terza verifica vista, $\text{Dom}(f) = A_a$ e per la penultima $\text{Im}(f) = B_b$ ¹¹¹, 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 $\text{Im}(f) = B_b$. Ma allora, per definizione di f , $A_a \sim B_b$, cioè $(a, b) \in f$. Quindi $a \in \text{Dom}(f) = A_a \not\subseteq$ (o anche $b \in \text{Im}(f) = B_b \not\subseteq$).

□

Esercizio 9.13 (Ogni sottoinsieme proprio di un buon ordine è isomorfo a un s.i. non necessariamente proprio). Sia $(A, <)$ un buon ordine e sia $B \subsetneq A$. Dimostra che $B \preceq A$, ma non necessariamente $B \prec A$.

Soluzione. Osserviamo che $(B, <|_B)$ è un buon ordine [eredita la totalità di $<$ e tutti i sottoinsiemi di B sono anche sottoinsiemi di A , dunque c'è sempre un minimo], segue che, per il teorema precedente, $(B, <|_B)$ è isomorfo a un segmento iniziale di A , ma non necessariamente proprio, infatti nel caso di cardinalità infinita $B \subsetneq A \not\Rightarrow |B| < |A|$ ¹¹², dunque soltanto $|B| \leq |A|$ (quindi il segmento iniziale in arrivo potrebbe anche essere proprio), e concludiamo [potendo la cardinalità anche essere la stessa che] $B \preceq A$. □

Esercizio 9.14. 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 controesempio eliminando la condizione 2.

Soluzione.

□

§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:

$$\begin{aligned} (x, y) <_+ (x', y') &\stackrel{\text{def}}{=} (y = 0 \wedge y' = 1) \\ &\vee (y = 0 \wedge y' = 0 \wedge x <_A x') \\ &\vee (y = 1 \wedge y' = 1 \wedge x <_B x') \end{aligned}$$

¹¹¹Stiamo negando un OR quindi l'unica possibilità è che siano entrambe false, dunque, visto quanto verificato sopra, abbiamo ottenuto che sono entrambi segmenti iniziali propri e quindi principali.

¹¹²Cioè non vale la Dedekind-finitezza.

L'idea è che $(A, <_A) + (B, <_B)$ si ottiene attaccando $(B, <_B)$ in coda a $(A, <_A)$.

$$\underbrace{(A, <_A) \quad (B, <_B)}_{(A, <_A) + (B, <_B)}$$

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:

$$(x, y) <_{\times} (x', y') \stackrel{\text{def}}{=} (y <_B y') \wedge (y = y' \wedge x <_A x')$$

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).

$$\underbrace{\dots < \underbrace{\text{copia di } (A, <_A)} < \underbrace{\text{copia di } (A, <_A)} < \underbrace{\text{copia di } (A, <_A)} < \dots}_{(B, <_B)} \quad (A, <_A) \times (B, <_B)$$

Per definire l'esponenziale ci serve la nozione di supporto.

Definizione 9.17 (Supporto di una funzione a un buon ordine). Dato un buon ordine $(B, <)$ e $f : A \rightarrow B$, il **supporto** di f è:

$$\text{supp}_B(f) \stackrel{\text{def}}{=} \{x \in A \mid f(x) \neq \min_{<_B} B\}$$

(ometteremo il pedice B quando è chiaro cosa sia B).

Il supporto è quindi l'insieme dei punti sull'insieme [qualsiasi] di partenza, sui quali f verso un buon ordine non assume il minimo di quest'ultimo.

Definizione 9.18 (Esponenziali di ordini totali). Dati $(A, <_A)$ e $(B, <_B)$ ordini totali, definiamo l'**esponenziale di ordini totali**:

$$(A, <_A)^{(B, <_B)} \stackrel{\text{def}}{=} (\{f \in {}^B A : |\text{supp}_A f| < \aleph_0\}, <_{\text{exp}})$$

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 $<_{\text{exp}}$ è definito da:

$$f <_{\text{exp}} g \stackrel{\text{def}}{=} (f \neq g) \wedge (f(m) <_A g(m))$$

dove m è il massimo valore in B su cui f e g sono diverse [dunque stiamo confrontando l'immagine dell'elemento massimo (nell'unione dei supporti) su cui non sono uguali], $m := \max_{<_B} \{x \in B \mid f(x) \neq g(x)\}$.¹¹³

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 ¹¹⁴. Ordinare queste tuple lessicograficamente significa che vince la componente diversa più a destra [se definitivamente c'è il minimo in entrambe le tuple (per la finitezza del supporto non può essere diversamente), basta confrontare l'ultima componente dove sono diverse (questa cosa corrisponde a dire che entrambe le funzioni fanno definitivamente il minimo)], ossia quella corrispondente all'elemento di B più grande (morale: vince chi fa di più prima che f e g siano definitivamente uguali).

Esercizio 9.19. Verificare che $(\omega, <)^{(\omega, <)} \sim (\mathbb{N}[x], <)$, 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 $p(x) < q(x)$ da un certo punto in poi).

Soluzione.

□

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 $<_{\text{exp}}$ è irreflessiva per definizione [richiede $f \neq g$, dunque se sono uguali non sono in relazione]. Occorre, intanto, verificare la transitività. Assumiamo $f <_{\text{exp}} g$ e $g <_{\text{exp}} h$ [naturalmente $f, g \in {}^B A$] con:

$$m_1 = \max_{<_B} \{x \in B \mid f(x) \neq g(x)\}$$

$$m_2 = \max_{<_B} \{x \in B \mid g(x) \neq h(x)\}$$

$$m_3 = \max_{<_B} \{x \in B \mid f(x) \neq h(x)\}$$

Detto $m := \max(m_1, m_2)$, abbiamo [per ipotesi abbiamo le due disuguaglianze con $<_{\text{exp}}$ e stiamo usando il massimo tra i due che rendono vere le disuguaglianze] $f(m) \leq_A g(m) \leq_A h(m)$, dove la prima disuguaglianza è stretta se $m = m_1$, e la seconda se $m = m_2$ (sempre

¹¹³In particolare si ha che le funzioni coincidono (in quanto a supporto finito), $\forall n \in B \ m <_B n \rightarrow f(n) = g(n)$, dunque stiamo confrontando l'ultimo valore su cui differiscono, e prendendo il massimo.

¹¹⁴D'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).

per la definizione di $<_{\text{exp}}$. In ogni caso, almeno una delle due disuguaglianze è stretta e quindi abbiamo $f(m) <_A h(m)$. D'altro canto, se $m <_B x$, allora $f(x) = g(x) = h(x)$ (cioè le funzioni, essendo a supporto finito, sono definitivamente costanti), quindi $m = m_3$ [cioè m è proprio il più grande valore per cui $f < h$ prima che diventino definitivamente costanti, ovvero m_3] e la transitività è dimostrata.

La relazione $<_{\text{exp}}$ è un ordine totale perché, se $f \neq g$ [allora per definizione di ordine stretto totale vogliamo una delle due disuguaglianze strette], allora esiste $m = \max_{<_B} \{x \in B \mid f(x) \neq g(x)\}$, e o $f(m) <_A g(m)$ o $g(m) <_A f(m)$. Nel primo caso $f <_{\text{exp}} g$, nel secondo $g <_{\text{exp}} f$ (quindi prese due funzioni distinte, essendo entrambe a supporto finito, il sottoinsieme di B su cui sono distinte è non vuoto, ed in particolare ha un massimo [è un insieme finito e B è totalmente ordinato], per tale massimo si verifica necessariamente una delle due disuguaglianze strette, pertanto f e g sono necessariamente in una delle due relazioni).

Resta da verificare che l'ordine ottenuto esponenziando è buono. Per assurdo, supponiamo che non lo sia, allora, detto S l'insieme delle funzioni $B \rightarrow A$ a supporto finito, abbiamo:

$$\underbrace{\exists f \in S \exists A \subseteq S (f \in A \wedge \forall g \in A \exists h \in A h <_{\text{exp}} g)}_{\text{c'è un } A \subseteq S \text{ non vuoto}} \quad \underbrace{\hspace{10em}}_{\text{che non ha minimo}}$$

Ora, fissiamo una $f \in S$ tale che $\exists A \subseteq S$ etc. con queste proprietà [possiamo farlo perché stiamo negando la tesi, quindi fissata una f che non la rispetti, esiste il sottoinsieme etc.]: che $\max_{<_B}(\text{supp}_A(f))$ sia minimo, e che, a parità di $m = \max_{<_B}(\text{supp}_A(f))$ il valore di $f(m)$ sia minimo. Fissiamo ora A in modo tale che $f \in A$ ed A non abbia minimo. Il nostro scopo è costruire $\tilde{A} \subseteq S$ che non ha minimo e contiene una funzione \tilde{f} con $\max_{<_B}(\text{supp}_A(f)) <_B m$, in questo modo neghiamo la minimalità di m ed otteniamo la contraddizione voluta.

Osserviamo, intanto che A può essere ripartito in:

$$\begin{aligned} A_1 &= \{g \in A \mid \max_{<_B}(\text{supp}_A(g)) <_B m\} \\ A_2 &= \{g \in A \mid \max_{<_B}(\text{supp}_A(g)) = m \wedge g(m) = f(m)\} \\ A_3 &= \{g \in A \mid \max_{<_B}(\text{supp}_A(g)) = m \wedge f(m) <_A g(m)\} \\ A_4 &= \{g \in A \mid m <_B \max_{<_B}(\text{supp}_A(g))\} \end{aligned}$$

e segue dalla definizione che le funzioni in A_1 , sono $<_{\text{exp}}$ di quelle in A_2 , che sono $<_{\text{exp}}$ etc. fino ad A_4 . 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 . Allora A_2 , che non è vuoto perché contiene f non ha minimo, se, infatti, l'avesse, questo dovrebbe essere anche minimo di A .

Concentriamoci ora su A_2 . Tutte le $g \in A_2$ assumono il medesimo valore su m , quindi, comparando due di queste funzioni con $<_{\text{exp}}$, il valore assunto da entrambe su m è irrilevante. Ossia la funzione:

$$H : A_2 \rightarrow S : g \mapsto \hat{g} \quad \text{con} \quad \hat{g}(x) = \begin{cases} \min A & \text{se } x = m \\ g(x) & \text{altrimenti} \end{cases}$$

è strettamente crescente. Per cui $\tilde{A} \stackrel{\text{def}}{=} H[A_2]$ non ha minimo.

Ora, però, segue dalla definizione che, fissata $g \in A_2$, $\text{supp}(\hat{g}) = \text{supp}(g) \setminus \{m\}$, quindi, ponendo $\tilde{f} \stackrel{\text{def}}{=} \hat{g}$, abbiamo $\max(\text{supp}(\tilde{f})) < m$, e questo contraddice la minimalità di m . \square

Proposizione 9.21 (Buona definizione delle operazioni tra “classi di isomorfismo” di buoni ordini - ovvero le operazioni tra buoni ordini sono definite modulo 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.

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 fa commutare il diagramma seguente:

$$\begin{array}{ccc} B & \xrightarrow{h} & A \\ g^{-1} \uparrow & & \downarrow f \\ B' & \longrightarrow & A' \end{array}$$

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, quindi dove h fa il minimo di A , allora h' dovrà necessariamente fare il minimo, e viceversa, pertanto vale che $\text{supp}_{A'}(f \circ h \circ g^{-1}) = g[\text{supp}_A(f)]$ (e g isomorfismo). \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

$$\begin{aligned} \text{associatività:} \quad & (\mathcal{A} + \mathcal{B}) + \mathcal{C} \sim \mathcal{A} + (\mathcal{B} + \mathcal{C}) \quad (\mathcal{A} \cdot \mathcal{B}) \cdot \mathcal{C} \sim \mathcal{A} \cdot (\mathcal{B} \cdot \mathcal{C}) \\ \text{distributività a sinistra:} \quad & \mathcal{A} \cdot (\mathcal{B} + \mathcal{C}) \sim \mathcal{A} \cdot \mathcal{B} + \mathcal{A} \cdot \mathcal{C} \\ \text{proprietà delle potenze:} \quad & \mathcal{A}^{\mathcal{B} + \mathcal{C}} \sim \mathcal{A}^{\mathcal{B}} \cdot \mathcal{A}^{\mathcal{C}} \quad (\mathcal{A}^{\mathcal{B}})^{\mathcal{C}} \sim \mathcal{A}^{\mathcal{B} \cdot \mathcal{C}} \end{aligned}$$

^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.

È importante notare che 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 $1 + \omega \neq \omega + 1$.

□

Un altro tranello in cui si potrebbe cadere è credere che le operazioni sui buoni ordini generalizzino quelle sulle cardinalità [perché provando le operazioni con gli ordini finiti, valgono tutte le proprietà, comprese quelle false]. Questo è vero per le cardinalità finite, e anche in generale per somma e prodotto - come è ovvio dalla definizione - ma fallisce per l'esponentiale quando è infinito.¹¹⁵

Esercizio 9.26. 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 b}

^aCioè per l'esponentiale di ordini valgono proprietà diverse rispetto a quelle classiche per le cardinalità (proprio perché le cose sono definite in maniera completamente diversa, e qui stiamo considerando solo alcune delle funzioni da ω in ω), quindi ad esempio $|\omega^\omega| = \aleph_0$ (cioè la cardinalità dell'esponentiazione), mentre $|\omega^\omega| = |\omega|^{|\omega|} = \aleph_0^{\aleph_0} = 2^{\aleph_0} > \aleph_0$ (cioè la cardinalità delle funzioni da ω in ω [che abbiamo associato alle ω -uple di elementi di ω]).

^b**Hint:** ricordare che $\mathcal{P}^{\text{fin}}(\omega) = \aleph_0$ e pensare a come si possa identificare ciò con ω^ω .

§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 [abbiamo creato un ordine totale formale tra di essi basato su ciò], 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.¹¹⁶

¹¹⁵Un trucco è ricordare che le proprietà che valgono sono quelle con le parentesi a destra, perché ridefiniremo le operazioni per ricorsione transfinita in maniera analoga a quanto fatto per quelle in ω con la ricorsione numerabile, ed in questo caso le parentesi saranno a destra.

¹¹⁶Vorremo anche fissare un rappresentante canonico per le "classi di equivalenza" dei buoni ordini, viste sopra a meno di isomorfismo, da cui l'idea di introdurre gli ordinali, questa cosa ci richiederà qualcosa

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 insiemi di elementi).¹¹⁷

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:

$$<_\alpha \stackrel{\text{def}}{=} \{(x, y) \in \alpha \times \alpha \mid x \in y\} \quad {}^{118}$$

Denotiamo con Ord la classe degli ordinali¹¹⁹, 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^a

^aE in generale il successore di un ordinale è un ordinale, ciò ci permette di descrivere bene gli elementi di ω senza l'assioma dell'infinito, ci basta prendere gli ordinali finiti, dove finito può essere espresso ad esempio con il principio del massimo, quindi elemento di $\omega =$ insieme ben ordinato, transitivo e con il principio del massimo.

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 il segmento iniziale principale [e in automatico proprio] 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 [tutti gli elementi sono sottoinsiemi], $\beta \subseteq \alpha$, quindi β è bene ordinato da \in [ristretto come ordine a β]. La transitività di β segue dalla transitività della relazione di ordine $<_\alpha$. Prendiamo, infatti, $\delta \in \gamma$, con $\gamma \in \beta$. Dobbiamo dimostrare che $\delta \in \beta$ (che è equivalente al dire $\gamma \subseteq \beta$, e che quindi i suoi elementi sono anche sottoinsiemi).

Siccome $\gamma \in \beta$, per la transitività di α , $\gamma \in \alpha$ [abbiamo usato che β è anche un sottoinsieme di α], e, da questo, nuovamente per la transitività di α [ora che abbiamo $\gamma \in \alpha$,

in più in termini di ipotesi e anche la necessità di introdurre un nuovo assioma, queste cose possono essere aggirate continuando a lavorare con i buoni ordini, ma il tutto verrebbe estremamente più pesante al livello di trattazione.

¹¹⁷ ω è un esempio di insieme transitivo, e naturalmente negli insiemi transitivi, così come ω gli elementi sono sottoinsiemi, ma non tutti i sottoinsiemi sono elementi.

¹¹⁸Esattamente come su ω , $x < y \leftrightarrow x \in y \leftrightarrow (x, y) \in <.$

¹¹⁹Tale classe contiene un elemento per ogni buon ordine, ad esempio, preso $(\omega, <)$, come classe di buoni ordini isomorfi a lui, prenderemo solo ω (il buon ordine transitivo e che ha come ordinamento proprio quello dato dall'appartenenza, e quindi ordinale), come rappresentante della “classe di equivalenza” nella classe dei buoni ordini (attenzione a non confondere i due significati del termine classe).

essendo α transitivo, abbiamo in automatico $\gamma \subseteq \alpha$, $\delta \in \alpha$ (e quindi anche $\delta \subseteq \alpha$ ¹²⁰). Ora $\delta, \gamma, \beta \in \alpha$ (e anche tutti sottoinsiemi), e abbiamo l'ipotesi $\delta \in \gamma \wedge \gamma \in \beta$ (e vogliamo dimostrare $\gamma \subseteq \beta$), ossia [in termini di $<_\alpha$, che ora possiamo usare, perché sono tutti elementi di α] $\delta <_\alpha \gamma \wedge \gamma <_\alpha \beta$, da cui [per transitività della relazione d'ordine] $\delta <_\alpha \beta$. Quest'ultima dice, appunto, che $\delta \in \beta$ (dunque $(\beta, <_{\alpha|\beta})$ è transitivo). Resta da dire che $\beta = \alpha_\beta$, e segue facilmente:

$$x \in \alpha_\beta \stackrel{\text{def. s.i.}}{\iff} x \in \alpha \wedge x <_\alpha \beta \stackrel{\text{def. } <_\alpha}{\iff} x \in \alpha \wedge x \in \beta$$

Ora, $x \in \beta \rightarrow x \in \alpha$ per la transitività di α , quindi l'AND si riduce a un solo termine:

$$x \in \alpha \wedge x \in \beta \iff x \in \beta$$

e concludiamo che $x \in \alpha_\beta \leftrightarrow x \in \beta$, dunque per estensionalità, $\alpha_\beta = \beta$. \square

La proposizione seguente ci dice che due ordinali non possono essere nella stessa classe di isomorfismo di buoni ordini [cioè per ogni classe di isomorfismo 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 uno ed uno solo]. Enunciamo prima 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 $(\alpha, <_\alpha) \sim (\beta, <_\beta)$, allora $\alpha = \beta$.^a

^aLa proposizione ha come conseguenza che per ogni classe di isomorfismo di buoni ordini, 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:

$$\gamma \stackrel{\text{Oss. sull' } \in \text{ degli ord.}}{=} \alpha_\gamma \stackrel{(\star)}{=} f[\alpha_\gamma] \stackrel{\text{Oss. sopra}}{=} \beta_{f(\gamma)} \stackrel{\text{Oss. sull' } \in \text{ degli ord.}}{=} f(\gamma) \not\equiv$$

dove (\star) è vero in quanto, abbiamo preso γ come il più piccolo ordinale per cui f non è l'identità, ma α_γ è fatto da cose strettamente più piccole di γ , dunque $f[\alpha_\gamma] = \alpha_\gamma$. \square

¹²⁰È una specie di bootstrap per chi conoscesse il termine dall'analisi.

Possiamo ora chiederci [avendo modo di ordinare questi particolari buoni ordini, detti ordinali] 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 (cioè gli ordinali sono proprio tutti ordinati dall'appartenenza, d'altronde abbiamo già visto come sono ordinati i buoni ordini, nel caso di questa particolare classe di buoni ordini transitivi, abbiamo appena visto che non ci sono classi di isomorfismo ma direttamente uguaglianze, è naturale quindi che l'essere isomorfo ad un segmento iniziale di un altro buon ordine, diventi in questo caso essere proprio esattamente quel segmento iniziale, quindi, venuto via l'isomorfismo abbiamo direttamente l'appartenenza come ordine).

Morale: ci piacerebbe ordinare gli ordinali usando \in , gli ordinali in quanto buoni ordini sono già ordinati dalla “relazione d'ordine sulle classi di isomorfismo di buoni ordini”, ebbene si scopre proprio che il fatto che i buoni ordini siano ordinati totalmente da $<$ è equivalente al fatto che gli ordinali delle corrispondenti classi di isomorfismo [che per ora non sappiamo esserci, ma se ci sono, sono unici] sono ordinati totalmente secondo \in .

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

$$\alpha \in \beta \text{ che vale se e solo se } (\alpha, <_\alpha) < (\beta, <_\beta)$$

$$\alpha = \beta \text{ che vale se e solo se } (\alpha, <_\alpha) \sim (\beta, <_\beta)$$

$$\beta \in \alpha \text{ che vale se e solo se } (\beta, <_\beta) < (\alpha, <_\alpha)$$

(l'implicazione \Leftarrow tra i due fatti in mezzo la abbiamo già dimostrata con la proposizione precedente).

^aSiamo in una classe, dunque ordinare gli ordinali è impreciso perché non abbiamo mai parlato di relazioni sulle classi, tuttavia, li stiamo ordinando nello stesso senso [ed a partire proprio] dall'ordinamento dei buoni ordini, usando in questo caso l'appartenenza.

Notazione: d'ora in poi porremo per comodità: $\alpha < \beta \stackrel{\text{def}}{=} (\alpha, <_\alpha) < (\beta, <_\beta)$, e analogamente $\alpha \sim \beta$ e $\beta < \alpha$.

Dimostrazione. Dimostriamo il primo caso [il terzo sarà simmetrico a questo]. Se $\alpha < \beta$ allora, per definizione di $<$, esiste $\gamma \in \beta$ tale che $\alpha \sim \beta_\gamma$. Però, β è un ordinale e per quanto visto in un'osservazione precedente, si ha $\beta_\gamma = \gamma$, da cui $\alpha \sim \gamma$, ma dalla proposizione precedente sappiamo che due ordinali isomorfi sono proprio uguali, ovvero $\alpha \sim \gamma \rightarrow \alpha = \gamma$.

Abbiamo quindi che $\alpha = \gamma \in \beta$ [e ciò dimostra che se vale l'ordinamento come buon ordine vale l'appartenenza di ordinali]. D'altro canto, se $\alpha \in \beta$, allora $\alpha = \beta_\alpha$ (sempre per la solita osservazione), quindi $\alpha < \beta$ (esattamente per la definizione di $<$ visto che α diventa proprio un segmento iniziale di β).

Se $\alpha \sim \beta$, come detto, la proposizione precedente ci assicura l'uguaglianza, il viceversa è immediato per la definizione di isomorfismo tra ordini totali. \square

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 $\alpha \in \omega$.

Proposizione 9.36 (Ordine largo sulla classe degli ordinali)

Siano $\alpha, \beta \in \text{Ord}$, allora:

$$\alpha \leq \beta \leftrightarrow \alpha \subseteq \beta$$

con $\alpha \leq \beta \stackrel{\text{def}}{=} \alpha < \beta \vee \alpha = \beta$.

Dimostrazione. Vediamo le due implicazioni:

\rightarrow Se $\alpha < \beta$ allora $\alpha \in \beta$ per la definizione di ordine sugli ordinali, quindi $\alpha \subseteq \beta$ per la transitività di β . Se $\alpha = \beta$, allora in particolare $\alpha \subseteq \beta$.

\leftarrow Dato $\alpha \subseteq \beta$, supponiamo per assurdo che $\beta < \alpha$. Allora $\beta \in \alpha$, ma per ipotesi si ha $\beta \in \alpha \subseteq \beta$. Per la transitività di β [nel senso che gli elementi degli elementi sono elementi], si ha $\beta \in \beta \not\vdash$ [per definizione (se $\beta \in \beta$ allora $\beta < \beta \not\vdash$) o anche perché abbiamo dimostrato con la proposizione precedente che è un ordine stretto e totale sugli ordinali, dunque irreflessiva].¹²¹

□

Ricordiamo che $s(\alpha) \stackrel{\text{def}}{=} \alpha \cup \{\alpha\}$. La proposizione segue 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 $\beta \in s(\alpha)$, o $\beta \in \alpha$ o $\beta = \alpha$ (per la definizione di successore). Nel secondo caso è ovviamente transitivo, nel ugualmente per quanto visto nell'*osservazione*.

buon ordine Siccome $s(\alpha)$ è un insieme di ordinali, \in è un ordine totale su $s(\alpha)$ [per quanto già dimostrato]. Dato $X \subseteq s(\alpha) = \alpha \cup \{\alpha\}$, con $X \neq \emptyset$, abbiamo che o $X = \alpha$ o $X \cap \alpha = \emptyset$ [α è un elemento dell'insieme unione ed è a sua volta un insieme di ordinali]. Nel primo caso X ha chiaramente un minimo, nel secondo, $\min(X \cap \alpha)$ è il minimo di X [gli elementi di X fuori dall'intersezione sono ordinali di α e quindi più piccoli].

¹²¹Segnalo che sulle dispense originali di Mamino c'è un divertente riferimento a buona fondazione.

Supponiamo, ora $\alpha < \beta$, dobbiamo dimostrare $s(\alpha) \leq \beta$. Sappiamo che $\alpha < \beta \implies \alpha \in \beta \implies \alpha \subseteq \beta$, allora dalla prima implicazione si ottiene $\{\alpha\} \subseteq \beta$ [transitività di β], e ciò, unito alla seconda implicazione, dà $s(\alpha) = \alpha \cup \{\alpha\} \subseteq \beta$, pertanto [per la proposizione sopra] $s(\alpha) \leq \beta$. \square

Corollario 9.38 (Successore del primo termine in una disuguaglianza tra ordinali)

$\forall \alpha, \beta \in \text{Ord} \quad \beta \leq \alpha \leftrightarrow \beta < s(\alpha)$.

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 $\min X = \bigcap X$.
2. Esiste il minimo dei maggioranti di X^a , detto $\sup X$, inoltre $\sup X = \bigcup X$.
3. C'è un ordinale che non appartiene a X .^b

^aI maggioranti di un insieme di ordinali sono definiti allo stesso modo di quanto visto per i reali, ovvero sono gli $\alpha \in \text{Ord}$ tali che $\forall \beta \in X \quad \beta \leq \alpha$.

^bQuesta cosa ci garantisce che non esiste un insieme di tutti gli ordinali, perché ci sarebbe sempre un ordinale fuori.

Dimostrazione. Vediamo i vari punti.

1. Dimostriamo, prima, che il minimo esiste. Sia $\alpha \in X$ fissato, che c'è perché supponiamo $X \neq \emptyset$. Consideriamo $\mu \stackrel{\text{def}}{=} \min_{<_{s(\alpha)}} (X \cap s(\alpha))$. Questo esiste perché $X \cap s(\alpha) \neq \emptyset$ in quanto α vi appartiene [e l'intersezione è sottoinsieme di $s(\alpha)$ che è ben ordinato, avendo dimostrato sopra che $s(\alpha)$ è un ordinale].

Vediamo che $\mu = \min X$. Infatti, preso $\beta \in X$, se $\beta \leq \alpha$ allora [per il corollario sopra $\beta \in s(\alpha)$] $\beta \in s(\alpha) \cap X$, dunque $\beta \leq \mu$ [cioè partecipa alla scelta per il minimo nell'intersezione]. Se però $\alpha < \beta$ (cioè $s(\alpha) \leq \beta$), allora $\mu < s(\alpha) \leq \beta$, dove la prima disuguaglianza è stretta perché c'è anche α in $s(\alpha) \cap X$ (e quindi μ è minimo per tutti gli ordinali in X che sono maggiori o uguali ad α).

Ora verifichiamo che $\mu = \bigcap X$. Chiaramente $\forall \gamma \in X \quad \mu \leq \gamma$, quindi $\forall \gamma \in X \quad \mu \subseteq \gamma$, cioè μ è un sottoinsieme di ogni elemento di X , dunque è un sottoinsieme degli elementi comuni degli elementi, ossia $\mu \subseteq \bigcap X$. D'altro canto $\mu \in X$, quindi [poiché si prendono gli elementi comuni anche a μ , necessariamente l'intersezione è un sottoinsieme] $\bigcap X \subseteq \mu$.

2. Dimostriamo in primis che $\bigcup X$ è un ordinale.

transitività Dato $\alpha \in \bigcup X$, esiste $\beta \in X$ tale che $\alpha \in \beta$. Per transitività di β si ha $\alpha \subseteq \beta$. Da cui [α è un sottoinsieme degli elementi di β , quindi unendo questi elementi ad altri, α rimarrà ancora un sottoinsieme dei nuovi elementi] $\alpha \subseteq X$.

buon ordine Ogni $\alpha \in \bigcup X$ appartiene a qualche $\beta \in X$, ed è, quindi, un ordinale (per la solita **osservazione**). Stabilito che $\bigcup X$ è un insieme di ordinali, è chiaro che ogni suo sottoinsieme non vuoto è un insieme non vuoto di ordinali. Quindi ha minimo per il punto 1.

Dimostriamo ora che $\sigma \in \text{Ord}$ è un maggiorante per X se e solo se $\bigcup X \leq \sigma$ (in questo modo sappiamo che $\bigcup X$ è più piccolo di tutti i maggioranti, e si vede facilmente che è a sua volta un maggiorante in quanto $\forall x \in X$ si ha che un elemento di un insieme è naturalmente un sottoinsieme della sua unione [in altre parole, unendo un insieme stiamo prendendo tutti gli elementi degli elementi, dunque un elemento dell'insieme iniziale sarà un sottoinsieme dell'unione, in quanto ne abbiamo preso gli elementi nell'unione], pertanto segue $x \subseteq \bigcup X \leftrightarrow x \leq \bigcup X$).

$$\underbrace{\forall \alpha \in X \alpha \leq \sigma}_{\sigma \text{ è un maggiorante}} \iff \forall \alpha \in X \alpha \subseteq \sigma \iff \bigcup X \subseteq \sigma \iff \bigcup X \leq \sigma$$

dove l'equivalenza centrale deriva dal fatto che se tutti gli elementi di X sono contenuti in σ , allora i loro elementi appartengono a σ , e dunque ovviamente la loro unione [degli elementi degli elementi] è un sottoinsieme di σ .

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, per definizione di estremo superiore, necessariamente 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, dunque la definizione di ordinale in questo caso si riduce al richiedere la transitività dell'insieme. □

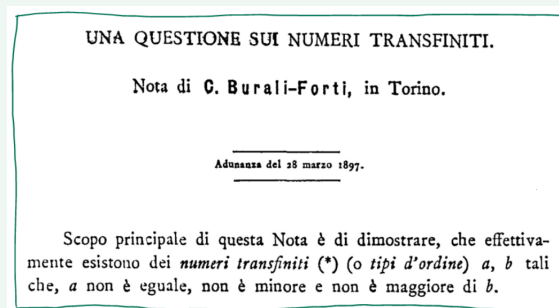
Corollario 9.41 (Paradosso di Burali-Forti)

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 $<$ fosse un ordine totale su queste classi.



Burali-Forti credette di poter negare la totalità dell'ordine $<$ ragionando per assurdo. Se $<$ fosse un ordine totale, si può dimostrare che sarebbe buono [esattamente come abbiamo visto sopra, un insieme di ordinali è sempre ben ordinato], ma allora $\Omega \stackrel{\text{def}}{=} [(\text{Ord}, <)]$, la classe di isomorfismo di $(\text{Ord}, <)$, sarebbe [a sua volta una classe di isomorfismo di un buon ordine e quindi] uno dei membri della classe Ord stessa, e, considerando il suo successore $s(\Omega)$, avremmo $\Omega < s(\Omega)$, ma anche $s(\Omega) < \Omega$ [per definizione], perché $s(\Omega) \in \text{Ord}$ \nmid .

Il guaio è che, nello stesso anno, Cantor pubblicò una dimostrazione del fatto che la relazione $<$ 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 ordine, 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 correttezza di buon ordine, e fu così che il paradosso di Burali-Forti acquisì il suo nome. E tutti vissero felici e contenti.

§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 che descrive O è:

$$\forall x \, x \in O \leftrightarrow ((x = \emptyset) \vee (x = \omega) \vee (\exists n \in \omega \wedge (x = s^n(\emptyset) \vee x = s^n(\omega))))$$

avendo una formula, 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 (che è proprio quello che vorremmo avendo dimostrato che per ogni classe ce n’è al più uno). Per formulare l’assioma, ci serve il 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 $x \in A$ [= elemento che soddisfa la formula che definisce A] associa un **unico** $y \in B$ [= elemento che soddisfa la formula che definisce 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

$$\forall A \exists B \forall y \forall x (y \in B \leftrightarrow \exists x \in A y = F(x))$$

(cioè per ogni insieme [che ricordiamo essere le uniche variabili del nostro linguaggio] esiste un insieme i cui elementi sono immagini di quelli di A rispetto alla funzione classe F).

^aCome per la separazione, anche questo è uno **schema di assiomi**, uno per ogni possibile funzione classe F .

Proposizione 9.48 (Unicità del rimpiazzo)

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 [in termini meno formali]:

$$F(x) \stackrel{\text{def}}{=} \begin{cases} G(x) & \text{se } x \in A \\ \emptyset & \text{altrimenti} \end{cases}$$

infatti se $x \in A$ si ha $G(x) = F(x)$, altrimenti c'è il vuoto, per cui $G[A] = F[A]$ ¹²². □

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. [FALSA, DA SISTEMARE] Ci basta considerare la funzione classe $F : \mathcal{P}(\mathcal{P}(A \cup B)) \rightarrow V$ definita come:

$$F(z) \stackrel{\text{def}}{=} \begin{cases} (x, y) & \exists x \in A \exists y \in B \ z = (x, y) \\ \emptyset & \text{altrimenti} \end{cases}$$

a questo punto $F[\mathcal{P}(\mathcal{P}(A \cup B))]$ è un insieme ed è proprio uguale a $A \times B$. □

Teorema 9.51 (Ogni buon ordine è isomorfo ad un unico ordianle)

Dato un buon ordine $(A, <)$, esiste un unico ordinale α tale che $(A, <) \sim \alpha$.^a

^aQuesto conclude il discorso sull'identificazione tra ordinali e buoni ordini, infatti prima abbiamo dimostrato che per ogni classe di isomorfismo di buoni ordini c'è al più un ordinale, e ora che ce n'è sempre uno, che è appunto unico.

¹²²Per la precisione $F[A]$, con $F : V \rightarrow V$, dà l'insieme $G[A] \cup \emptyset = G[A]$

Dimostrazione. L'unicità segue per quanto abbiamo già visto, cioè $\alpha \sim \alpha' \rightarrow \alpha = \alpha'$. Basta quindi dimostrare l'esistenza di α . Sia:

$$A' = \{x \in A \mid \exists \gamma \in \text{Ord} \ A_x \sim \gamma\}$$

ovvero gli elementi nel buon ordine i cui segmenti iniziali sono isomorfi ad un ordinale (dopo questa dimostrazione potremo assumere che ce n'è uno per segmento iniziale, ma per ora, non lo sappiamo). Consideriamo la funzione classe $F : A' \rightarrow \text{Ord}$:

$$F(x) = \text{l'unico } \gamma \in \text{Ord} \text{ tale che } A_x \sim \gamma$$

(cioè quella che associa ad ogni elemento di A l'ordinale isomorfo al suo segmento iniziale), l'unicità vale perché:

$$A_x \sim \gamma \wedge A_x \sim \gamma' \implies \gamma \sim \gamma' \implies \gamma = \gamma'$$

Vogliamo dimostrare che $\alpha \stackrel{\text{def}}{=} F[A'] \sim (A, <)$ (in altre parole l'immagine della funzione classe di A' [che è un insieme per rimpiazzamento] è proprio l'ordinale corrispondente alla classe di isomorfismo del buon ordine $(A, <)$).

Dimostriamo dunque che α è un ordinale, A' è un segmento iniziale di A e $\alpha \sim A'$. Infine concludiamo dimostrando che $A' = A$ e quindi si ha proprio che $\alpha \sim A$.

α è un ordinale α è definito come l'insieme degli ordinali isomorfi ai segmenti iniziali corrispondenti agli elementi di A' , dunque è un insieme di ordinali, e per quanto visto, ci basta dimostrare che è transitivo affinché sia un ordinale a sua volta. Supponiamo $\beta < \gamma \in \alpha$, dobbiamo dimostrare che $\beta \in \alpha$ [cioè che β è un sottoinsieme di α]. Sia $f : \gamma \rightarrow A_x$ un isomorfismo [che abbiamo perché $\gamma \in \alpha$ significa che è isomorfismo a qualche segmento iniziale principale di un $x \in A$], allora $f|_\beta : \beta \rightarrow A_{f(\beta)}$ è un isomorfismo [la restrizione dell'isomorfismo deve necessariamente essere ancora iniettiva e preservare l'ordinamento, dunque l'unica cosa da osservare è che $f[\beta] = A_{f(\beta)}$, che è vero in quanto, dato $x \in A$ con $x \in f[\beta]$ e, preso $y \in A$, con $y <_A x$, allora $f^{-1}(y) < f^{-1}(x)$ e $f^{-1}(x) \in \beta$ (perché f isomorfismo), dunque per transitività $f^{-1}(y) \in \beta$, per cui tornando indietro con f si ottiene che $y \in f[\beta]$, dunque l'immagine di β via f è proprio il segmento iniziale determinato su A da $f(\beta)$], quindi β è l'ordinale corrispondente al segmento iniziale su A determinato da $f(\beta)$, ovvero $\beta = F(f(\beta)) = F(A_{f(\beta)})$, pertanto sta in $\alpha = F[A']$.

A' s.i. di A Se $y < x \in A'$, allora esiste un isomorfismo $f : A_x \rightarrow \gamma$, quindi $f|_{A_y} : A_y \rightarrow \gamma_{f(y)}$ è un isomorfismo [poiché gli isomorfismi di ordini totali mandano segmenti iniziali in segmenti iniziali si ha che $f(A_y) = \gamma_{A_y}$, inoltre come sopra nella restrizione si mantengono iniettività e ordinamento] e, siccome [per le solite proprietà degli ordinali] $\gamma_{f(y)} = f(y)$, abbiamo quindi proprio per f ristretta che $\gamma_{A_y} = A_y \sim f(y)$. Per cui, per definizione di A' , essendo A_y isomorfo ad un ordinale, si ha proprio $y \in A'$ ¹²³, dunque A' è un segmento iniziale di A .

$\alpha \sim A'$ Sia $f : A' \rightarrow \alpha$, la funzione, tra insiemi, definita da $f(x) = F(x)$, che esiste per l'[assioma di separazione](#) applicato ad $A' \times \alpha$ (quindi con la funzione classe abbiamo ottenuto l'insieme α , ed ora possiamo proprio prendere una funzione tra i due insiemi, che faccia le stesse cose che faceva F). Dimostriamo quindi che f è un isomorfismo di ordini.

¹²³Typo di Mamino.

La surgettività è immediata perché, per costruzione, abbiamo che $\alpha = F[A'] = f[A']$. Verifichiamo la monotonia:

$$x < y \xrightarrow{\text{def. s.i.}} A_x \prec A_y$$

ora, essendo che f è definita tramite F , associa ad ogni elemento di A l'ordinale a cui è isomorfo il suo segmento iniziale, cioè $f(x) \sim A_x$ e $f(y) \sim A_y$, dunque, avendo la relazione \prec in partenza (che ci ricordiamo definita mediante isomorfismo), componendo gli isomorfismi troviamo che $f(x) \prec f(y)$, ovvero $f(x)$ è un segmento iniziale proprio di $f(y)$ mediante l'isomorfismo, ma, essendo $f(x)$ e $f(y)$ ordinali, sappiamo che la relazione d'ordine dei buoni ordini, coincide su di essi con l'appartenenza, pertanto $f(x) < f(y)$ (e con la monotonia stretta dimostrata abbiamo gratis l'iniettività).

$A' = A$ Se così non fosse A' [che per 3. è un s.i.] sarebbe un segmento iniziale proprio di A , avremmo quindi $A' = A_k$ per qualche $k \in A$.

Ma allora, per i punti 1-3, $A_k = A' \sim \alpha \in \text{Ord}$, quindi, per definizione stessa di A' , $k \in A'$ [perché $k \in A$ sarebbe un elemento il cui s.i. principale è isomorfo ad un ordinale]. Però questo contraddice $A' = A_k \not\vdash$ (perché un s.i. principale non può contenere l'elemento da cui è determinato).

□

Una conseguenza del risultato precedente è che possiamo definire le operazioni sugli ordinali come semplice riflesso di quelle sui buoni ordini (perché a questo punto abbiamo 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:

$$\alpha + \beta \sim (\alpha, <_\alpha) + (\beta, <_\beta) \quad \alpha \cdot \beta \sim (\alpha, <_\alpha) \cdot (\beta, <_\beta)$$

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

Esercizio 9.53. Dimostra che l'insieme introdotto all'inizio della sezione è effettivamente $\omega + \omega$, ossia, più precisamente:

$$\forall x \, x \in \omega + \omega \leftrightarrow (\exists m \in \omega \, x = m) \vee (\exists n \in \omega \, x = \omega + n)$$

§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:

$$\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \dots\}$$

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.

Soluzione.

□

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 $\forall \alpha \in \text{Ord} \varphi(\alpha)$.

^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 $\forall \alpha \in \text{Ord} (\forall \beta < \alpha \varphi(\beta)) \rightarrow \alpha \in C$ ¹²⁴, allora $\forall \alpha \in \text{Ord} \alpha \in C$, oppure, in forma più coincisa:

$$(\forall \alpha \in \text{Ord} (\alpha \subseteq C \rightarrow \alpha \in C)) \rightarrow \text{Ord} \subseteq C$$

cioè, assumendo che per tutti gli ordinali valga che $\forall \beta < \alpha \beta \in C \iff \forall \beta \in \alpha \beta \in C \iff \alpha \subseteq C$ implica $\alpha \in C$ [cioè se tutti gli elementi di un ordinale stanno in C , allora anche l'ordinale stesso lo è], allora la classe degli ordinali è contenuta in C , ovvero tutti gli ordinali soddisfano la formula che definisce C .

Dimostrazione. Per assurdo, assumiamo [la negazione della tesi] $\neg \varphi(\alpha)$ ¹²⁵, e consideriamo un α per cui la formula è falsa. Essendo l'ipotesi vera e [per ipotesi assurda] $\varphi(\alpha)$ falsa, l'antecedente dell'ipotesi [che come formula insiemistica è un'implicazione materiale] deve essere necessariamente falso, cioè vale $\neg(\forall \beta < \alpha \varphi(\beta))$, ovvero $\exists \beta < \alpha \neg \varphi(\beta)$.

Quindi il ragionamento per assurdo ci ha portato a dire che esiste almeno un $\beta < \alpha$ per cui la proposizione è falsa, in particolare il sottoinsieme di α dei β per cui φ è falsa è non vuoto, quindi possiamo considerare¹²⁶ $\beta_0 := \min\{\beta \in \alpha \mid \neg \varphi(\beta)\}$, che esiste in quanto α è un buon ordine. Ora, usando β_0 nell'ipotesi [come fatto all'inizio con α] (essendo un altro ordinale per cui la formula è falsa), si ottiene che $\exists \beta < \beta_0 \neg \varphi(\beta)$ (cioè l'antecedente dell'ipotesi ci procura un'ordinale più piccolo per cui la formula è falsa), contro la minimalità di β_0 , che è assurdo. □

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 schermo di teoremi - o metateorema - che ci permette di costruire un diverso teorema per ogni possibile formula φ [non essendo le classi oggetti della teoria degli insiemi non possono essere quantificate con i quantificatori

¹²⁴Ricordiamo che avere α in una classe corrisponde al fatto che α soddisfa la formula per mezzo della quale è definita tale classe.

¹²⁵Formalmente $\neg(\forall \alpha \in \text{Ord} \varphi(\alpha)) = \exists \alpha \in \text{Ord} \neg \varphi(\alpha)$.

¹²⁶Perché ora possiamo scrivere un insieme non vuoto da cui, per separazione, prendere il minimo. Prima sarebbe stato il minimo α preso su qualcosa definito per separazione sulla classe degli ordinali, e poteva essere problematico, così invece non abbiamo alcun problema.

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 (Ordinale successore). Diciamo che $\alpha \in \text{Ord}$ è un **ordinale successore** se $\exists \beta \in \text{Ord} \ \alpha = s(\beta)$. Un ordinale $\alpha > 0$ ¹²⁷ che non è successore è detto **ordinale limite**.

Osservazione 9.58 (Un ordinale è successore se e solo se ha max) — Un ordinale α è successore se e solo se ha un massimo elemento.^a

^aEquivalentemente questo ci dice anche che un ordinale è non successore [quindi limite tranne nel caso 0] se e solo se non ha un massimo

Dimostrazione. β è il massimo di α **se e solo se** α è il minimo ordinale $> \beta$, poiché:

$$\begin{aligned} \beta \text{ è il massimo di } \alpha &\iff \forall x \in \alpha \ x \leq \beta \wedge \beta \in \alpha \\ &\stackrel{\text{trans.}}{\iff} \forall x \in \alpha \ x \leq \beta \wedge \beta \not\subseteq \alpha \\ &\stackrel{(\star)}{\iff} \beta \not\subseteq \alpha \wedge \forall \gamma \in \text{Ord} \ \beta \subseteq \gamma \rightarrow \alpha \subseteq \gamma \end{aligned}$$

dove (\star) vale perché, se vale che se β è contenuto in un ordinale, allora anche α lo è, significa che se tutti gli elementi di β stanno in γ , allora anche tutti quelli di α stanno in γ , ovvero $\alpha \subseteq \beta \leftrightarrow \forall x \in \alpha \ x \subseteq \alpha \rightarrow x \subseteq \beta \leftrightarrow x \leq \beta$, dunque $\forall x \in \alpha \ x \leq \beta$ e quindi β è un massimo [perché $\beta \in \alpha$]. Viceversa, $\forall x \in \alpha \ x \leq \beta \leftrightarrow x \subseteq \beta \implies x \subseteq \gamma$, ma questo, per ogni x , equivale a $\alpha \subseteq \gamma$.

Quando dimostrato è equivalente a dire che α è il minimo ordinale più grande di β . Si conclude osservando che ciò è vero **se e solo se** $\alpha = s(\beta)$ [per quanto visto sul successore di un ordinale, questo è per definizione il più piccolo ordinale più grande (a cui cioè appartiene l'ordinale iniziale)]. \square

Proposizione 9.59 (Induzione transfinita - v.2)

Sia $\varphi(x)$ una formula insiemistica. Se:

- $\varphi(0)$ (caso base)
- $\forall \gamma \in \text{Ord} \ \varphi(\gamma) \rightarrow \varphi(s(\gamma))$ (caso successore)
- per ogni ordinale limite λ , $(\forall \beta < \lambda \ \varphi(\beta)) \rightarrow \varphi(\lambda)$ ^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, dunque, fissato $\alpha \in \text{Ord}$ bisogna mostrare che vale:

$$(\forall \beta < \alpha \ \varphi(\beta)) \rightarrow \varphi(\alpha)$$

¹²⁷Quindi tutti gli ordinali limite devono contenere lo 0, e lo 0 NON è un ordinale limite a sua volta.

Se α è limite o 0 abbiamo questa formula tout court [nel caso di 0 la formula sopra è sempre vera, nel caso degli ordinali limite abbiamo assunto che è vera nelle ipotesi]. Ci resta da vedere che la formula sopra è vera nel caso in cui $\alpha = s(\gamma)$, in questo caso abbiamo:

$$\gamma < \alpha \xrightarrow{\text{antecedente Hp. induttiva}} \varphi(\gamma) \xrightarrow{\text{Hp. prop.}} \varphi(\alpha)$$

dunque anche in questo caso vale l'ipotesi della prima forma dell'induzione transfinita, che quindi vale $\forall \alpha \in \text{Ord}$, pertanto per la prima forma vale $\varphi(x)$ per tutti gli $x \in \text{Ord}$. \square

Ora possiamo dimostrare il teorema di ricorsione transfinita. Faremo uso della notazione seguente.

Notazione 9.60 (Restrizione di una funzione classe) — Data una funzione classe $F : A \rightarrow B$ e un insieme $X \subseteq A$ esiste la funzione [di insiemi]^a:

$$f = F|_X : X \rightarrow F[X] : a \mapsto F[a]$$

(che è in automatico surgettiva).

^aIn partenza ci stiamo restringendo ad un insieme, ed anche in arrivo, infatti $F[X]$ è un'insieme per [rimpiazzamento](#).

Teorema 9.61 (Ricorsione transfinita - v.1)

Data una funzione classe $G : V \rightarrow V^a$ esiste un'unica^b funzione $F : \text{Ord} \rightarrow V$ tale che:

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

^aAnche in questo caso, questo è uno **schema di teoremi**, uno per ogni formula G , per la solita ragione che le formule delle classi non sono oggetti della teoria degli insiemi e quindi non sono quantificabili [inoltre la dimostrazione sarà uno schema di dimostrazioni].

^bDove l'unicità va intesa nel senso seguente: date F_1, F_2 come sopra, vale $\forall \alpha \in \text{Ord} \quad F_1(\alpha) = F_2(\alpha)$, cioè date due formule che rispettano entrambe quanto scritto, queste danno la stessa cosa [anziché richiedere che la formula sia unica, visto che le formule possono essere scritte in tanti modi equivalenti].

^cSi osserva che $F|_\alpha$ è proprio una funzione tra insiemi $\alpha \rightarrow F[\alpha]$, come osservato sopra, per [rimpiazzamento](#).

Dimostrazione. \square

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:

$$x \in A \times B \stackrel{\text{def}}{=} \exists a \in A \exists b \in B \quad x = (a, b)$$

(cioè x è uguale a una coppia di elementi ciascuno in una classe, ovvero ciascuno soddisfa un predicato).

Corollario 9.63 (Ricorsione transfinita - v.2)

Date le funzioni classe $G_1 : \text{Ord} \times V \rightarrow V$ e $G_2 : V \rightarrow V$. Detto x_0 un insieme, esista un'unica funzione classe F tale che:

$$\begin{aligned} F(0) &= x_0 \\ \forall \alpha \in \text{Ord} \quad F(s(\alpha)) &= G_1(\alpha, F(\alpha)) \\ \forall \lambda \in \text{Ord} \quad \lambda \text{ limite} &\rightarrow F(\lambda) = G_2(F|_\lambda) \end{aligned}$$

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:

$$G(f) = \begin{cases} \emptyset & \text{se } f \text{ NON è una funzione con } \text{Dom}(f) \in \text{Ord} \\ x_0 & \text{se } f = \emptyset \\ G_1(\alpha, f(\alpha)) & \text{se } \text{Dom}(f) = \alpha + 1 \text{ per qualche } \alpha \in \text{Ord} \\ G_2(f) & \text{altrimenti} \end{cases}$$

(dove abbiamo definito $G(f)$, come G di una certa troncata di F). □

Corollario 9.64 (Operazioni tra ordinali (definizione ricorsiva))

Esistono le funzioni (classe) di somma, prodotto e potenza di ordinali, così definite:^a

$$\begin{aligned} \alpha + 0 &= \alpha & \alpha \cdot 0 &= 0 \\ \alpha + s(\beta) &= s(\alpha + \beta) & \alpha \cdot s(\beta) &= \alpha \cdot \beta + \alpha \\ \alpha^\lambda &= \sup\{\alpha + \beta \mid \beta < \lambda\} & \alpha \cdot \lambda &= \sup\{\alpha \cdot \beta \mid \beta < \lambda\} \end{aligned}$$

$$\begin{aligned} \alpha^0 &= 1 \\ \alpha^{s(\beta)} &= \alpha^\beta \cdot \alpha \\ \alpha^\lambda &= \sup\{\alpha^\beta \mid \beta < \lambda\} \end{aligned}$$

^aRicordiamo che l'estremo superiore di un insieme di ordinali esiste sempre ed è l'unione dell'insieme.

Ossia, le operazioni aritmetiche sugli ordinali si possono definire in modo analogo alle operazioni aritmetiche su ω nei casi 0 e successore, **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 $F(\lambda) = \sup F|_\lambda$.¹²⁸

¹²⁸L'idea è la stessa dell'estensione continua di una funzione fuori dal suo dominio, ovvero quella di far valere la funzione subito fuori l'estremo superiore dell'immagine dell'insieme subito prima.

Notazione 9.66 (Sulle definizioni ricorsive di funzioni classe) — 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 [perché stiamo costruendo una funzione classe da Ord a Ord fissato il primo termine, e in questo caso, essendo la funzione una classe, essa cambia qualsiasi sia il primo termine fissato della somma, e come già visto le classi non possono essere quantificate all'interno della teoria degli insiemi, pertanto, abbiamo necessità di una funzione diversa per ogni fissato ordinale 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, tuttavia, osservare che il teorema si trova già in forma parametrica, anche se non si vede. Una funzione classe non è, infatti, altro che una formula insiemistica - con determinate proprietà - e nulla vieta che questa formula contenga una variabile libera α . Il teorema di [ricorsione transfinita](#) dice che, se una certa formula - quella che definisce G - è una funzione classe, allora un'altra formula - quella di F - scritta esplicitamente nella dimostrazione è anch'essa una funzione classe. Ebbene se la formula per G ha una variabile libera α [e nulla ci vieta di inserirla], 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.

Proposizione 9.67 (Le definizioni ricorsive delle operazioni tra ordinali sono equivalenti alle definizioni mediante le operazioni tra buoni ordini)

Vale che:

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

ossia: che si definiscano le operazioni sugli ordinali per ricorsione o che lo si faccia mediante le corrispondenti operazioni sui buoni ordini, il risultato è il medesimo.

Dimostrazione. Si procede per [induzione transfinita v.2](#) su β (in modo da avere i casi esattamente corrispondenti alla definizione ricorsiva).

$$\alpha + \beta \sim (\alpha, <_\alpha) + (\beta, <_\beta)$$

$\boxed{\beta = 0}$ 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:

$$(\alpha, <_\alpha) + (0, <_0) = (\alpha \sqcup 0, <_+) = ((\alpha \times \{0\}) \cup \underbrace{(\emptyset \times \{1\})}_{=\emptyset}, <_+) = (\alpha \times \{0\}, <_+)$$

con $(a, b) <_+ (a', b') = (b = 0 \wedge b' = 1) \vee ((b = 0 \wedge b' = 0) \wedge a <_\alpha a') \vee ((b = 1 \wedge b' = 1) \wedge a <_\alpha a')$, ma, visto che ci rimane solo $\alpha \times \{0\}$, non ci possono essere coppie

ordinate con seconda componente 1, dunque $<_+$ si riduce al secondo caso [ovvero a confrontare solo coppie con seconda componente 0], pertanto è immediato che $(\alpha \times \{0\}, <_+) \sim (\alpha, <_\alpha)$ ¹²⁹. A questo punto sappiamo già che $\alpha \sim (\alpha, <_\alpha)$, perché semplicemente stiamo considerando l'uno come buon ordine e l'altro come ordinale, ma sono proprio la stessa cosa [isomorfismo di buoni ordini o no].

$\beta = s(\gamma)$ Assumiamo come ipotesi induttiva che $\alpha + \beta \sim (\alpha, <_\alpha) + (\beta, <_\beta)$ e dimostriamo che $\alpha + s(\beta) = (\alpha, <_\alpha) + (s(\beta), <_{s(\beta)})$. Per la definizione ricorsiva $\alpha + s(\beta) = s(\alpha + \beta)$, e per ipotesi induttiva:

$$s(\alpha + \beta) \sim s((\alpha, <_\alpha) + (\beta, <_\beta))$$

(abbiamo semplicemente applicato il successore al LHS e al RHS), osserviamo ora che:

$$s((\alpha, <_\alpha) + (\beta, <_\beta)) = ((\alpha, <_\alpha) + (\beta, <_\beta)) + (1, <) \quad ^{130}$$

a questo punto, si applica la proprietà associativa della somma dei buoni ordini, ottenendo $(\alpha, <_\alpha) + ((\beta, <_\beta) + (1, <))$, e, di nuovo per la verifica [non fatta], si ottiene $(\alpha, <_\alpha) + (s(\beta), <_{s(\beta)})$. A questo punto si ottiene l'isomorfismo voluto.

$\beta = \lambda$ limite Vogliamo dimostrare che $\alpha + \lambda \sim (\alpha, <_\alpha) + (\lambda, <_\lambda)$, con λ ordinale limite. Per definizione di somma tra buoni ordini abbiamo:

$$(\alpha, <_\alpha) + (\lambda, <_\lambda) = (\alpha \sqcup \lambda, <_+)$$

che come sappiamo è un nuovo buon ordine [in particolare una classe di isomorfismo di buoni ordini], pertanto possiamo considerare l'ordinale associato alla classe di isomorfismo $\gamma \sim (\alpha \sqcup \lambda, <_+)$ e l'isomorfismo $f : \alpha \sqcup \lambda \rightarrow \gamma$. Vogliamo calcolare $\alpha + \lambda = \sup\{\alpha + \beta \mid \beta < \lambda\} = \bigcup\{\alpha + \beta \mid \beta < \lambda\}$ (la somma è definita ricorsivamente così + abbiamo visto che l'estremo superiore di un insieme di ordinali è l'unione dell'insieme). Dunque la tesi iniziale da dimostrare si riduce a verificare che¹³¹

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

Ora, per ipotesi induttiva (nel caso limite in un'induzione transfinita, ricordiamo che assumiamo l'ipotesi induttiva per tutti gli ordinali più piccoli di quello limite), se $\beta < \lambda$, allora vale la somma $\alpha + \beta \sim (\alpha \sqcup \beta, <_+)$, e siccome $\alpha \sqcup \beta$ è un segmento iniziale di $\alpha \sqcup \lambda$ ($\beta < \lambda \leftrightarrow \beta \in \lambda$, dunque $\alpha \sqcup \beta \hookrightarrow \alpha \sqcup \lambda$ con un'immersione strettamente monotona), si ha che $f[\alpha \sqcup \beta] = \alpha + \beta$ (perché f è l'isomorfismo che associa l'ordinale $\alpha \sqcup \lambda$ al suo ordinale γ , dunque manda il segmento iniziale $\alpha \sqcup \beta$ nel segmento iniziale $\gamma_{\alpha \sqcup \beta}$, ma $\alpha \sqcup \beta \sim \alpha + \beta$ per ipotesi induttiva, quindi $\gamma_{\alpha \sqcup \beta} \sim \gamma_{\alpha + \beta}$ ^{prop. ordinali} $\alpha + \beta$, e poiché ordinali isomorfi sono uguali si ha proprio che $f[\alpha \sqcup \beta] = \gamma_{\alpha \sqcup \beta} = \alpha + \beta$). Ora, siccome λ è limite, $\lambda = \bigcup\{\beta \mid \beta < \lambda\}$, quindi si vede che:

$$\alpha \sqcup \lambda \stackrel{\lambda \text{ limite}}{=} \bigcup\{\alpha \sqcup \beta \mid \beta < \lambda\}$$

¹²⁹Formalmente l'isomorfismo manda semplicemente $(\alpha \ni x) \mapsto (x, 0) (\in \alpha \times \{0\})$, è facile vedere che è iniettiva e surgettiva, ed è strettamente monotona in quanto, dati $x <_\alpha y$, si ha che $(x, 0) <_+ (y, 0) \equiv ((0 = 0) \wedge x <_\alpha y)$, che è vero per ipotesi.

¹³⁰Andrebbe verificato.

¹³¹Avendo dimostrato che la somma tra buoni ordini è isomorfa all'ordinale γ , possiamo sfruttare la transitività dell'isomorfismo e scrivere la tesi come $\gamma \sim \alpha + \lambda$, e, dovendo al RHS essere un'ordinale [per la definizione ricorsiva], si ha proprio l'uguaglianza (per quanto osservato sul fatto che ordinali isomorfi sono proprio uguali), dunque dobbiamo verificare esattamente che $\gamma = \alpha + \lambda$.

da cui la tesi:

$$\begin{aligned} \gamma &\stackrel{\text{def. } f}{=} f[\alpha \sqcup \lambda] \stackrel{\text{appena visto}}{=} \bigcup \{f[\alpha \sqcup \beta] \mid \beta < \lambda\} \\ &\stackrel{\text{oss. sopra}}{=} \bigcup \{\alpha + \lambda \mid \beta < \lambda\} \stackrel{\text{def. ord. limite}}{=} \alpha + \lambda \end{aligned}$$

Per le altre verifiche (che sono circa sulla stessa linea), riportiamo solo il caso successore dell'induzione transfinita.

$$\alpha \cdot \beta \sim (\alpha, <_\alpha) \cdot (\beta, <_\beta)$$

$\beta = \lambda$ limite Si procede come prima, prendendo $\gamma \sim (\alpha, <_\alpha) \cdot (\lambda, <_\lambda)$ e $f : \alpha \times \lambda \rightarrow \gamma$ isomorfismo. Nuovamente $\lambda = \bigcup \{\beta \mid \beta < \lambda\} \implies \alpha \cdot \lambda = \bigcup \{\alpha \cdot \beta \mid \beta < \lambda\}$, e per ipotesi induttiva si ha che $\alpha \cdot \beta \sim \alpha \times \beta$ [come buon ordine], da cui $f[\alpha \times \beta] = \alpha \cdot \beta$ [con un ragionamento analogo a quanto visto sopra]. Infine si conclude con:

$$\begin{aligned} \gamma &= f[\alpha \times \lambda] = \bigcup \{f[\alpha \times \beta] \mid \beta < \lambda\} \\ &= \bigcup \{\alpha \cdot \beta \mid \beta < \lambda\} = \alpha \cdot \beta \end{aligned}$$

e dal fatto che $\alpha \cdot \lambda = \gamma \sim (\alpha, <_\alpha) \cdot (\lambda, <_\lambda)$, si conclude che $\alpha \cdot \lambda \sim (\alpha, <_\alpha) \cdot (\lambda, <_\lambda)$.

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

$\beta = \lambda$ 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 $g : \beta \rightarrow \alpha$ con 0 su $\alpha \setminus \beta$.

È chiaro che... (DA COMPLETARE)

□

Per la proposizione predente, 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 [quella basta sulla costruzione di nuovi **buoni ordini**] 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 **ma decrescenti 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 se γ è un maggiorante di Y , allora è un maggiorante di X . Infatti, preso $\alpha \in X$ per ipotesi esiste $\beta \in Y$ con $\alpha \leq \beta$, e, siccome $\beta \leq \gamma \implies \alpha \leq \gamma$. Ora $\sup Y$ è un maggiorante di Y [quindi in automatico, per quanto appena visto, domina tutti gli elementi di X], dunque $\sup Y$ è un maggiorante di X , pertanto è maggiore o uguale a $\sup X$ [per definizione]. \square

Nota 10.4 (Il successore è crescente) — La funzione classe $\alpha \mapsto s(\alpha)$ è crescente.

Dimostrazione. $\alpha < \beta \leftrightarrow s(\alpha) \leq \beta \leftrightarrow s(\alpha) < s(\beta)$ [dove entrambe le equivalenza 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** su γ .

caso $\gamma = 0$ Vera a vuoto [$\beta < 0 \leftrightarrow \beta \in \emptyset$].

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 si ha:

$$\alpha + \beta \leq \alpha + \delta <^{132} s(\alpha + \delta) \stackrel{\text{def. ric.}}{=} \alpha + s(\delta) = \alpha + \gamma$$

dove la prima disuguaglianza si ha perché o $\beta = \delta$ o $\beta < \delta$. Nel primo caso naturalmente $\alpha + \beta = \alpha + \gamma$, nel secondo vale l'ipotesi induttiva, cioè $\alpha + \beta < \alpha + \delta$.

caso $\gamma = \lambda$ limite Dato $\beta < \lambda$, abbiamo $s(\beta) < \lambda$ [successore di una disuguaglianza + ordinale limite, quindi non può essere uguale], dunque, possiamo applicare l'ipotesi induttiva sia a β che a $s(\beta)$ e ottenere:

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

dove il minore o uguale vale per la definizione di sup (e per l'osservazione iniziale, cioè prendere β sotto λ , e di conseguenza anche il suo successore sta sotto λ).

$\alpha \mapsto \alpha + \beta$ è non decrescente

Dobbiamo dire che $\alpha < \gamma$, allora $\alpha + \beta \leq \gamma + \beta$. Procediamo ancora una volta per induzione transfinita v.2 su β .

caso $\beta = 0$ Banale per le definizioni delle operazioni [sia ricorsiva sia coi buoni ordini].

caso $\beta = s(\delta)$ Per ipotesi induttiva, vale che $\alpha < \gamma \rightarrow \alpha + \delta \leq \gamma + \delta$, per l'osservazione precedente ci basta applicare la funzione successore a LHS e RHS per ottenere:

$$\alpha + \beta = \alpha + s(\delta) = s(\alpha + \delta) \leq s(\gamma + \delta) = \gamma + s(\delta) = \gamma + \beta$$

caso $\beta = \lambda$ limite Dobbiamo dimostrare che:

$$\alpha + \lambda = \sup\{\alpha + \delta \mid \delta < \lambda\} \leq \sup\{\gamma + \delta \mid \delta < \lambda\} = \gamma + \lambda$$

Basta applicare la prima nota, osservando che vale $\alpha + \delta \leq \gamma + \delta$ per 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?

Osservazione 10.6 (Controesempio alla stretta crescita 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

¹³²Questa disuguaglianza è letteralmente la definizione di $<$ come appartenenza, che col successore è ovvia.

strettamente crescente nella prima componente.

Proposizione 10.7 (Proprietà delle operazioni fra ordinali)

Dati $\alpha, \beta, \gamma \in \text{Ord}$ valgono le seguenti proprietà:

$$\begin{aligned} \text{associatività:} \quad & (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \quad (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma) \\ \text{distributività a sinistra:} \quad & \alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma \\ \text{proprietà delle potenze:} \quad & \alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma \quad (\alpha^\beta)^\gamma = \alpha^{\beta \cdot \gamma} \end{aligned}$$

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.

Lasciamo 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 $X \subseteq \text{Ord}$, se $\sup X \notin X$, allora $\sup X$ è limite.

Dimostrazione. Se per assurdo $\sup X = s(\alpha)$, siccome $\sup X$ non è elemento di X , ciò equivale a $\forall \beta \in X \beta < \sup X$, quindi abbiamo anche $\forall \beta \in X \beta \leq \alpha < \sup X$ [non può accadere mai che $\beta > \alpha$, perché $s(\alpha)$ è il più piccolo ordinale più grande di α come abbiamo visto, in tal caso dovrebbe accadere per forza che $s(\alpha) \leq \beta \implies s(\alpha) \in X$ (in ogni caso), ma $s(\alpha) = \sup X$, quindi è assurdo], per cui α è un maggiorante di X più piccolo di $\sup X$. \square

Osservazione 10.10 (Le operazioni tra ordinali sono continue - ovvero commutano con il sup a destra) — Dato $X \subseteq \text{Ord}$ e $\alpha \in \text{Ord}$ vale che [indipendentemente dal fatto che $\sup X$ sia o meno in X]:

$$\begin{aligned} \alpha + \sup X &= \sup\{\alpha + \beta \mid \beta \in X\} \\ \alpha \cdot \sup X &= \sup\{\alpha \cdot \beta \mid \beta \in X\} \\ \alpha^{\sup X} &= \sup\{\alpha^\beta \mid \beta \in X\} \end{aligned}$$

(quindi quando si ha un ordinale limite, che sappiamo essere sempre della forma $\lambda = \sup\{\beta \mid \beta < \lambda\}$, vale in automatico quanto scritto sopra).

Dimostrazione. Le dimostrazioni sono uguali. Vediamo la prima. Se $\sup X \in X$, l'enunciato è immediato, infatti, come visto, se un insieme di ordinali ha un massimo, allora è in automatico un ordinale [successore], quindi ai LHS diventano le normali operazioni fra ordinali, mentre al RHS gli estremi superiori diventano proprio i massimi, che si raggiungono appunto con $\sup X = \max X$ nelle operazioni.

Supponiamo dunque che $\lambda = \sup X \notin X$ [per quanto visto nell'osservazione sopra sappiamo quindi che $\sup X$ è un ordinale limite]. Dobbiamo dimostrare che:

$$\alpha + \lambda \stackrel{\text{definizione}}{=} \sup \underbrace{\{\alpha + \gamma \mid \gamma < \lambda\}}_A = \sup \underbrace{\{\alpha + \beta \mid \beta \in X\}}_B$$

Dobbiamo verificare la seconda uguaglianza, basta dire che dato $\gamma_1 < \lambda$ esiste $\beta_1 \in X$ con $\alpha + \gamma_1 \leq \alpha + \beta_1$ [dunque $\sup A \leq \sup B$], e, viceversa, dato $\beta_2 \in X$ esiste $\gamma_2 < \lambda$ con $\alpha + \beta_2 \leq \alpha + \gamma_2$ [dunque $\sup A \geq \sup B$] (stiamo usando il lemma visto prima sulla disuguaglianza dei sup).

Preso $\gamma_1 < \lambda = \sup X$, γ_1 ¹³³ non è un maggiorante di X , quindi esiste $\beta_1 \in X$ con $\gamma_1 < \beta_1$ (sarebbe la caratterizzazione del sup), per la monotonia stretta sulla seconda componente, segue $\alpha + \gamma_1 \leq \alpha + \beta_1$ [e la disuguaglianza stretta implica quella larga].

Preso $\beta_2 \in X$, siccome $\lambda = \sup X$ è limite, $\beta_2 < s(\beta_2) < \lambda$ [successore + λ limite], quindi, ponendo $\gamma_2 = s(\beta_2)$, sempre per la stretta monotonia nella prima componente, si ha $\alpha + \beta_2 < \alpha + \gamma_2$ [e ancora una volta la disuguaglianza stretta implica quella larga]. \square

Possiamo quindi dimostrare la proposizione sulle proprietà delle operazioni tra ordinali.

Dimostrazione. Sono tutte facili induzioni su γ . Vediamo la prima, le altre restano come esercizio. Conviene affrontarle nell'ordine in cui sono scritte, sinistra - destra, alto-basso. Dimostriamo $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ per induzione su γ .

caso $\gamma = 0$ 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:

$$\begin{aligned} (\alpha + \beta) + s(\delta) &\stackrel{\text{def. ricors.}}{=} s((\alpha + \beta) + \delta) \\ &\stackrel{\text{Hp. indutt.}}{=} s(\alpha + (\beta + \delta)) \\ &\stackrel{\text{def. ricors.}}{=} \alpha + s(\beta + \delta) \\ &\stackrel{\text{def. ricors.}}{=} \alpha + (\beta + s(\delta)) \end{aligned}$$

caso $\gamma = \lambda$ limite Ancora una volta segue dall'ipotesi induttiva e dalla definizione ricorsiva della somma nel caso limite:

$$\begin{aligned} (\alpha + \beta) + \lambda &\stackrel{\text{def. ricors.}}{=} \sup\{(\alpha + \beta) + \delta \mid \delta < \lambda\} \\ &\stackrel{\text{Hp. indutt.}}{=} \sup\{\alpha + (\beta + \delta) \mid \delta < \lambda\} \\ &= \alpha + (\sup\{\beta + \delta \mid \delta < \lambda\}) \\ &\stackrel{\text{def. ricors.}}{=} \alpha + (\beta + \lambda) \end{aligned}$$

\square

§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 di ordinali)

Dati $\alpha, \gamma \in \text{Ord}$, con $\alpha \leq \gamma$, esiste un unico $\beta \in \text{Ord}$ tale che $\alpha + \beta = \gamma$.

¹³³Typo di Mamino.

Intuitivamente $\gamma \sim \alpha \sqcup (\gamma \setminus \alpha)$ [per la somma di ordinali definita mediante i buoni ordini], dove $\gamma \setminus \alpha = \{\delta \in \gamma \mid \delta \notin \alpha\}$.



Vediamo ora una dimostrazione formale.

Dimostrazione. Abbiamo l'unicità perché la funzione $+$ è crescente nel secondo argomento, come visto nel lemma, dunque è iniettiva, e quindi β è unico. Dimostriamo l'esistenza. Se $\alpha = \gamma$ l'enunciato è ovvio [basta usare l'ordinale 0]. Assumiamo quindi $\alpha < \gamma$. Consideriamo il minimo δ tale che [la somma supera γ] $\gamma < \alpha + \delta$ - δ esiste poiché $\gamma < s(\gamma) \leq \alpha + s(\gamma)$ [la seconda disuguaglianza è la debole monotonia sulla prima componente, dove al LHS usiamo 0 e al RHS α , ciò dimostra che l'insieme di cui stiamo prendendo il minimo è non vuoto]. Se δ è successore, sia $\delta = s(\beta)$, allora [essendo δ minimo per cui $\alpha + \beta > \gamma$, si ha $\alpha + \beta \leq \gamma$] e $\alpha + \beta \leq \gamma < s(\alpha + \beta) = \alpha + s(\beta) = \alpha + \delta$ (che quindi equivale alla cosa presa per ipotesi), da cui segue:

$$\alpha + \beta \leq \gamma < s(\alpha + \beta) \implies \alpha + \beta \leq \gamma \leq \alpha + \beta$$

E quindi [le due disuguaglianze corrispondono a due contenimenti, dunque l'uguaglianza¹³⁴] $\gamma = \alpha + \beta$. Ci basta quindi mostrare che δ non è limite (ovviamente non è 0). Se lo fosse avremmo $\gamma \stackrel{\text{def. } \delta}{<} \alpha + \delta \stackrel{\text{def. ric.}}{=} \sup\{\alpha + \varepsilon \mid \varepsilon < \delta\}$, ma allora, non essendo l'insieme non vuoto, perché vale quanto appena scritto esiste $\varepsilon < \delta$ tale che $\gamma < \alpha + \varepsilon$ [il sup prende l'elemento più piccolo tra i più grandi di tutto l'insieme, quindi basta prendere ε nell'insieme] contro la minimalità di δ . \square

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 Per il lemma precedente, fissato β, ρ è unico [per unicità della differenza appunto]. Dobbiamo quindi dimostrare solo l'unicità di β . Supponiamo per assurdo:

$$\alpha \cdot \beta + \rho = \alpha \cdot \beta' + \rho' \quad \text{con (WLOG) } \beta < \beta' \text{ e } \rho, \rho' < \alpha$$

allora, per la stretta monotonia nella seconda componente della somma, vale che:

$$\begin{aligned} \alpha \cdot \beta + \rho &< \alpha \cdot \beta + \alpha \\ &\stackrel{\text{def. ric.}}{=} \alpha \cdot s(\beta) \\ &\stackrel{\beta < \beta'}{\leq} \alpha \cdot \beta' \\ &\stackrel{2^{\text{a comp.}}}{\leq} \alpha \cdot \beta' + \rho' \\ &\stackrel{\text{Hp. ass.}}{=} \alpha \cdot \beta + \rho \quad \textcolor{red}{\downarrow} \end{aligned}$$

¹³⁴Abbiamo un doppio contenimento vero, quindi per tavola di verità dell'AND devono essere necessariamente veri gli uguali.

esistenza Come nella dimostrazione del lemma precedente, consideriamo il minimo δ tale che $\gamma < \alpha \cdot \delta$ - che esiste in quanto $\gamma \leq \alpha \cdot \gamma < \alpha \cdot s(\alpha)$ [nella prima disuguaglianza c'è la debole monotonia della prima componente con 1 e α , nell'altra, quella stretta della seconda componente con $\gamma < s(\gamma)$, quindi abbiamo preso δ come minimo di un insieme non vuoto]. Se δ è successore, $\delta = s(\beta)$, allora $[\alpha \cdot \beta, \text{essendo } \beta < \delta, \text{ non può essere strettamente più grande di } \gamma] \alpha \cdot \beta \leq \gamma$, quindi [essendo $\alpha \cdot \beta \leq \gamma$], per il lemma precedente, esiste ρ tale che $\alpha \cdot \beta + \rho = \gamma$. Per concludere il caso δ successore, ci basta quindi dimostrare che $\rho < \alpha$ [così da avere tutta la tesi]. Se, per assurdo, fosse $\alpha \leq \rho$, allora si avrebbe:

$$\begin{aligned} \gamma &\stackrel{s(\beta)=\delta}{<} \alpha \cdot s(\beta) \\ &= \alpha \cdot \beta + \alpha \\ &\leq \alpha \cdot \beta + \rho = \gamma \quad \textcolor{red}{\text{!}} \end{aligned}$$

(dove nell'ultima disuguaglianza si è usato appunto che $\alpha \leq \rho$, e quindi si ha la monotonia [debole, data la disuguaglianza debole] sulla seconda componente).

Dobbiamo infine escludere che δ sia limite. Se lo fosse, avremmo $\gamma < \alpha \cdot \delta \stackrel{\text{def. ric.}}{=} \sup\{\alpha \cdot \varepsilon \mid \varepsilon < \delta\}$, ma allora esisterebbe $\varepsilon < \delta$ tale che $\gamma < \alpha \cdot \varepsilon$ [per la solita storia che δ è il sup di questo insieme], contro la minimalità di δ .

□

§10.2 La forma normale di Cantor

Teorema 10.13 (Forma normale di Cantor)

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 $n \in \omega \setminus \{0\}$.

Dimostrazione. Dividiamo la dimostrazione in esistenza ed unicità.

esistenza Per induzione transfinita, supponiamo che ogni ordinale $< \alpha$ abbia una forma normale, dobbiamo dimostrare che α ha una forma normale. Sia γ il minimo tale che $\alpha < \omega^\gamma$, che c'è perché [l'insieme su cui prendiamo il minimo è non vuoto in quanto vale sempre almeno che] $\alpha < \omega^{s(\alpha)}$. Come nei lemmi precedenti, consideriamo il caso γ successore. Sia $\gamma = s(\beta_1)$, allora, per il lemma sulla divisione euclidea, dato che $\omega^{\beta_1} < \alpha$ [γ era il minimo per cui α era minore...], possiamo fare la divisione euclidea ottenendo:

$$\alpha = \omega^{\beta_1} \cdot k_1 + \rho \quad \text{con } \rho < \omega^{\beta_1}$$

Osserviamo intanto che $0 < k_1 < \omega$. Infatti:

$$0 = k_1 \implies \alpha = \rho < \omega^{\beta_1} \quad \text{contro la minimalità di } \gamma \text{!}$$

$$\omega \leq k_1 \implies \omega^\gamma = \omega^{s(\beta_1)} \stackrel{2^{\text{a comp. prodotto}}}{\leq} \omega^{\beta_1} \cdot k_1 + \rho = \alpha \text{!}$$

(dove il secondo assurdo c'è in quanto avevamo preso $\alpha < \omega^\gamma$). Ora $\rho < \omega^{\beta_1} \leq \alpha$ [lemma divisione + $\beta_1 < \gamma$], quindi, per ipotesi induttiva, ρ si può scrivere come somma finita:

$$\rho = \omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n$$

Siccome $\rho < \omega^{\beta_1}$, abbiamo $\beta_2 < \beta_1$, quindi, sostituendo ρ nell'espressione iniziale si ottiene:

$$\alpha = \omega^{\beta_1} \cdot k_1 + \rho = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n$$

che è una forma normale. Come al solito non resta che escludere quindi che γ sia limite, e ciò lo si può fare, osservando che, altrimenti, $\alpha < \omega^\gamma = \sup\{\omega^\varepsilon \mid \varepsilon < \gamma\}$, e questo implica che $\alpha < \omega^\varepsilon$, con $\varepsilon < \gamma$ [essendo γ il sup dell'insieme], contro la minimalità di γ .

unicità Sia α minimo che non ha un'unica forma normale. Supponiamo che vi siano due forme normali:

$$\begin{aligned} \alpha &= \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n \\ &= \omega^{\beta'_1} \cdot k'_1 + \omega^{\beta'_2} \cdot k'_2 + \dots + \omega^{\beta'_{n'}} \cdot k'_{n'} \end{aligned}$$

(notare che abbiamo usato anche n' al posto di n , perché la lunghezza della forma normale può essere diversa). Ci basta dire che $\beta_1 = \beta'_1$ e $k_1 = k'_1$, infatti allora:

$$\omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n = \omega^{\beta'_2} \cdot k'_2 + \dots + \omega^{\beta'_{n'}} \cdot k'_{n'} < \omega^{\beta_1}$$

contro la minimalità di α . Supponiamo $\beta_1 = \beta'_1$, allora $\omega^{\beta_1} \cdot k_1 + \overbrace{\dots}^{< \omega^{\beta_1}} = \omega^{\beta_1} \cdot k'_1 + \overbrace{\dots}^{< \omega^{\beta_1}}$ quindi $k_1 = k'_1$ per la divisione euclidea.

Se infine $\beta_1 < \beta'_1$ abbiamo:

$$\omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n < \omega^{s(\beta_1)} \leq \omega^{\beta'_1} \cdot k'_1 + \dots \nless$$

□

Esercizio 10.14. Dimostrare le disuguaglianze in viola (sono tutte uguali).

§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 $\varepsilon_0 = \omega^{\varepsilon_0}$ ¹³⁵. La forma normale di Cantor di ε_0 è quindi, chiaramente, ω^{ε_0} , e procedere ricorsivamente sull'esponente $\omega^{\omega^{\varepsilon_0}}$, $\omega^{\omega^{\omega^{\varepsilon_0}}}$, 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.

¹³⁵Notare che in questo caso non vale che $\alpha > \beta_1$

Proposizione 10.15 (Ogni funzione ordinale continua ha un punto fisso $\geq \alpha$)

Sia $F : \text{Ord} \rightarrow \text{Ord}$ una funzione classe [debolmente] crescente e continua - ossia $F(\lambda) = \sup F[\lambda]$ per λ limite. Allora, per ogni $\alpha \in \text{Ord}$, F ha un punto fisso $\geq \alpha$.
Ossia:

$$\exists \pi \in \text{Ord} \quad \alpha \leq \pi \wedge F(\pi) = \pi$$

Dimostrazione. Definiamo per ricorsione transfinita (stiamo usando la ricorsione per mezzo di una funzione classe) $\pi_0 = \alpha$, $\pi_{s(n)} = F(\pi_n)$ per $n \in \omega$.

Se $F(0) = 0$, allora $\pi = 0$ è un punto fisso.

Se $0 < F(0)$, allora, induzione, $\forall n \in \omega \quad \pi_n < \pi_{s(n)}$ per cui la funzione $n \mapsto \pi_n$ è crescente. Di conseguenza:

$$\pi \stackrel{\text{def}}{=} \sup\{\pi_n | n \in \omega\}$$

è limite (perché $\pi \notin \{\pi_n | n \in \omega\}$, dunque vale il lemma sugli insiemi di ordinali in cui il sup non appartiene all'insieme). Quindi:

$$F(\pi) = \sup F[\pi] = \sup\{F(\pi_n) | n \in \omega\} = \sup\{\pi_{s(n)} | n \in \omega\} = \pi$$

(la dimostrazione ci mostra anche che i punti fissi sono una classe propria di ordinali [se fossero un insieme ci sarebbe un sup, e gli ordinali sarebbero segmenti iniziali dell'ordinale che necessariamente ne viene fuori]). \square

Esempio 10.16

Sia ε un punto fisso di $x \mapsto \omega^x$, allora la forma normale di ε è $\varepsilon = \omega^\varepsilon$.

Esercizio 10.17. Sia $\varepsilon_0 = \sup\{1, \omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \dots\}$. Formalmente definiamo per ricorsione $\alpha_0 = 1$, $\alpha_{n+1} = \omega^{\alpha_n}$, allora $\varepsilon_0 = \sup\{\alpha_n | n \in \omega\}$. Dimostrare che ε_0 è il più piccolo punto fisso della funzione $x \mapsto \omega^x$.

Esercizio 10.18. Sia $F : \text{Ord} \rightarrow \text{Ord}$ crescente e continua. Allora esiste $G : \text{Ord} \rightarrow \text{Ord}$ crescente tale che:

$$\forall \alpha \in \text{Ord} \quad F(\alpha) = \alpha \leftrightarrow \exists \beta \in \text{Ord} \quad \alpha = G(\beta)$$

(ossia F ha una classe propria di punti fissi).

Esercizio 10.19. La G dell'esercizio precedente è univocamente determinata da F ed è continua.

Definizione 10.20 (ε -numbers). Se negli esercizi precedenti $F(\alpha) = \omega^\alpha$, allora $\varepsilon_\alpha \stackrel{\text{def}}{=} G(\alpha)$ ¹³⁶.

L' α -esimo ε -number è L' α -esimo punto fisso di $x \mapsto \omega^x$.

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.¹³⁷

¹³⁶E quindi ce n'è uno per ogni ordinale.

¹³⁷Ricordare 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.

Esercizio 10.21 (★ 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.

Esercizio 10.22 (★★ Ostico). Sia ζ_0 minimo tale che $\varepsilon_{\zeta_0} = \zeta_0$, allora $|\zeta_0| = \aleph_0$.

Esercizio 10.23. Sia ω 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) e $k_1, \dots, k_n < \gamma$.

§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 10.24 (Assorbimento a destra dell'ordinale più grande)

Siano $\alpha, \beta, \gamma \in \text{Ord}$ tali che $\alpha < \omega^\beta \leq \gamma^a$, allora:

$$\alpha + \gamma = \gamma$$

^aNaturalmente $\beta > 0$.

Ossia fare $\alpha + \gamma$ assorbe tutti gli α abbastanza piccoli, ossia quelli minori di qualche potenza di ω che sia a sua volta minore o uguale a γ .¹³⁸

Dimostrazione. Ci basta dimostrare che $\alpha + \gamma \leq \gamma$ (l'altra disuguaglianza è automatica per debole monotonia della prima componente, $0 + \gamma \leq \alpha + \gamma$ ¹³⁹). Scrivendo α in forma normale di Cantor otteniamo:

$$\alpha = \omega^{\beta_1} \cdot k_1 + \dots + \omega^{\beta_n} \cdot k_n$$

con gli ordinali $\beta_1 > \beta_2 > \dots > \beta_n$. Quindi si ha che $\alpha \leq \omega^{\beta_1} \cdot k$, per qualche $k \in \omega$, infatti [iterando la debole monotonia sulla prima componente sia di somma che del prodotto, dal termine n -esimo al secondo, si ottiene]:

$$\alpha = \omega^{\beta_1} \cdot k_1 + \dots + \omega^{\beta_n} \cdot k_n \leq \alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_1} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n = \omega^{\beta_1} \cdot (k_1 + \dots + k_n)$$

con $k := k_1 + \dots + k_n$. Ora, da [l'ipotesi] $\alpha < \omega^\beta$, deduciamo $\beta_1 < \beta$ [basta fare il confronto tra la forma normale di α e la disuguaglianza per ipotesi usando la monotonia delle potenze], quindi $s(\beta_1) \leq \beta$ e possiamo scrivere [usando la sottrazione, visto che il primo termine sta ancora in γ che] $\gamma = \omega^{s(\beta_1)} + \gamma' = \omega^{\beta_1} \cdot \omega + \gamma'$, $\gamma' < \gamma$. Da cui:

$$\alpha + \gamma \stackrel{\text{sopra} + \text{monot.}}{\leq} \omega^{\beta_1} \cdot k + \omega^{\beta_1} \cdot \omega + \gamma = \omega^{\beta_1} (k + \omega) = \omega^{\beta_1} \cdot \omega + \gamma' = \gamma$$

¹³⁸È falso tuttavia che $\gamma + \alpha = \gamma$, infatti per la stretta monotonia nella seconda componente della somma non si può avere $\gamma + 0 < \alpha$ al RHS, perché $0 < \alpha$.

¹³⁹Naturalmente escludiamo il caso $\alpha = 0$, perché in questo caso si ottiene ancora banalmente la tesi.

dove l'uguaglianza in **rosso** segue da $k + \omega = \omega$ [ricordiamo $k \in \omega \setminus \{0\}$], che a sua volta segue da:

$$k + \omega = \sup\{k + n \mid n < \omega\} = \omega$$

□

Proposizione 10.25 (Regole di calcolo in forma normale di Cantor)

Per le somme ($c \neq 0$, $d \neq 0$) vale che:

$$\omega^\alpha \cdot c + \omega^\beta \cdot d = \begin{cases} \omega^\beta \cdot d & \text{se } \alpha < \beta \\ \omega^\alpha \cdot (c + d) & \text{se } \alpha = \beta \\ \omega^\alpha \cdot c + \omega^\beta \cdot d & \text{se } \beta < \alpha^a \end{cases}$$

Per i prodotti si applica la proprietà distributiva, e poi le regole seguenti:

$$\begin{aligned} \beta > 0 &\rightarrow (\omega^{\alpha_1} \cdot k_1 + \dots \omega^{\alpha_2} \cdot k_2 + \dots) \cdot \omega^\beta = \omega^{\alpha_1 + \beta} \\ n \in \omega \setminus \{0\} &\rightarrow (\omega^{\alpha_1} \cdot k_1 + \dots \omega^{\alpha_2} \cdot k_2 + \dots) \cdot n = \omega^{\alpha_1} \cdot k_1 \text{ **rosso** } + \dots \omega^{\alpha_2} \cdot k_2 + \dots \end{aligned}$$

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

$$\begin{aligned} k \in \omega \setminus \{0\} & \quad k^{\omega^{1+\alpha}} = \omega^{\omega^\alpha} \\ \beta > 0 \wedge \alpha_1 > 0 & \rightarrow (\omega^{\alpha_1} \cdot k_1 + \dots \omega^{\alpha_2} \cdot k_2 + \dots)^{\omega^\beta} = \omega^{\alpha_1 \cdot \omega^\beta} \end{aligned}$$

^aÈ già in forma normale, poiché $\beta < \alpha$, le operazioni cancellano solo cose scritte con ω con esponenti non tutti in ordine strettamente decrescente, ovvero non già completamente in forma normale.

Dimostrazione. La regole per la somma sono immediate: la prima è il lemma precedente, infatti se $\alpha < \beta$, allora $\omega^\alpha \cdot c < \omega^{\text{rosso}(\alpha)} \leq \omega^\beta \cdot d$, e quindi nella somma si salva solo il termine di destra; la seconda è la proprietà distributiva a sinistra valida per tutti gli ordinali, e la terza è la stessa 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 intanto il caso particolare $n \cdot \omega = \omega$ per $n \in \omega \setminus \{0\}$:

$$\omega \leq n \cdot \omega = \sup\{n \cdot i \mid i \in \omega\} \leq \sup\{j \mid j^{140} \in \omega\} \leq \omega$$

(la prima disuguaglianza è la solita debole monotonia sulla prima componente del prodotto, la seconda disuguaglianza è il lemma sulla disuguaglianza dei sup¹⁴¹, in particolare il lemma si può applicare al contrario e ottenere proprio uguaglianza dei sup, infine, l'ultima è proprio un'uguaglianza data dal fatto che ω è limite e quindi uguale al sup delle cose più piccole). Ora, scrivendo $\beta = 1 + \gamma$ (abbiamo supposto $\beta > 0$, quindi vale il lemma sulla

¹⁴⁰Typo di Mamino.

¹⁴¹Se per ogni elemento del primo insieme ne trovo sempre uno del secondo che lo domina, allora c'è la disuguaglianza tra gli estremi superiori.

sottrazione, ed otteniamo un'unico $\gamma \in \text{Ord}$ per cui vale quella somma), si ottiene:¹⁴²

$$\begin{aligned}
 \omega^{\alpha_1+\beta} &= \omega^{\alpha_1} \omega^\beta \\
 &\leq (\omega^{\alpha_1} \cdot k_1 + \omega^{\alpha_2} \cdot k_2 + \dots) \cdot \omega^\beta \\
 &\leq (\omega^{\alpha_1} \cdot k_1 + \omega^{\alpha_2} \cdot k_2 + \dots + \omega^{\alpha_1}) \cdot \omega^\beta \\
 &\leq \omega^{\alpha_1} (k_1 + 1) \cdot \omega^\beta \\
 &= \omega^{\alpha_1} \underbrace{(k_1 + 1)\omega}_\omega \omega^\gamma \\
 &= \omega^{\alpha_1} \cdot \omega \cdot \omega^\gamma \\
 &= \omega^{\alpha_1+\beta}
 \end{aligned}$$

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 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 [sarebbe il lemma sopra applicato alle coppie da destra verso sinistra man mano], 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 quanto visto sopra, cioè $\beta = 1 + \gamma$ e le solite proprietà delle potenze; la sesta uguaglianza è il caso particolare visto sopra [$n \cdot \omega = \omega$], essendo $k_1 + 1 \in \omega$; infine, nell'ultima uguaglianza usiamo ancora che $\beta = 1 + \gamma$.

La seconda regola, del prodotto di un ordinale in forma normale e un naturale:

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

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 [usato per una doppia disuguaglianza], è uguale all'estremo superiore ad esempio di $\{n | n \in \omega\}$, 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 $(\omega^\alpha \cdot k)^\omega = \omega^{\alpha \cdot \omega}$:

$$\begin{aligned}
 \omega^{\alpha \cdot \omega} &\leq (\omega^\alpha \cdot k)^\omega \\
 &= \sup (\omega^\alpha \cdot k)^n | n \in \omega \\
 &= \sup \{\omega^{\alpha \cdot n} \cdot k^n | n \in \omega\} \\
 &\leq \sup \{\omega^{\alpha \cdot (n+1)} | n \in \omega\} \\
 &\leq (\omega^\alpha)^\omega = \omega^{\alpha \cdot \omega}
 \end{aligned}$$

¹⁴²Typo Mamino al primo uguale dopo le tre disuguaglianze.

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 terza uguaglianza deriva dal fatto che $n \cdot \omega = \omega$ per quanto visto, quindi, facendo la potenza tutti i k davanti agli ω^α scompaiono e rimane solo l'ultimo; la quarta disuguaglianza è la stretta monotonia sulla seconda componente del prodotto, usando $k < \omega^\alpha$, e poi sono semplicemente le proprietà delle potenze degli ordinali; la quinta disuguaglianza è in realtà un'uguaglianza per la definizione ricorsiva delle potenze nel caso limite, e, infine l'ultima uguaglianza è data dalle proprietà delle potenze degli ordinali.

Siccome $\beta > 0$, allora $\beta \geq 1$, dunque possiamo scrivere $\beta = 1 + \gamma$, per un unico $\gamma \in \text{Ord}$, dunque abbiamo $\omega^\beta = \omega \cdot \omega^\gamma$ ¹⁴³, 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 [ovvero il primo argomento]; per la seconda ci basta aggiungere ai termini della somma ω^{α_1} alla fine (o sostituirlo all'ultimo termine, è indifferente) e poi [dopo aver usato la regola per la somma], si ha la monotonia sulla seconda componente e sulla base della potenza; la terza uguaglianza sono le proprietà delle potenze; la quarta uguaglianza è il caso particolare; 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

¹⁴³Typo di Mamino che si porta dietro tutto il conto.

Esempio 10.26 (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.
- $(\omega + 1)^n = \omega^n + \omega^{n-1} + \dots + 1 = \sum_{i=n}^0 \omega^{i^a}$, $n \in \omega$. 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:

$$(\omega + 1)^{n+1} = (\omega + 1)^n \cdot (\omega + 1) \stackrel{\text{Hp. indutt.}}{=} \left(\sum_{i=n}^n \omega^i \right) \cdot (\omega + 1) = \left(\sum_{i=n}^n \omega^i \right) \cdot \omega + \sum_{i=n}^n \omega^i$$

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 infinita¹⁴⁴. Definiremo la scrittura $|X| = \aleph_\alpha$, come $|X| = |\omega_\alpha|$ (o molto più semplicemente $|\omega_\alpha| \stackrel{\text{def}}{=} \aleph_\alpha$). 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 aleph¹⁴⁵. Resterà quindi da dimostrare che ogni cardinalità è la cardinalità di qualche ordinale [cioè tutte finite e infinite sono realizzate da un ω_α e quindi sono un aleph], 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 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 $\forall \beta < \alpha \quad |\beta| < |\alpha|$.

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, allora esiste $\beta \in \text{Ord}$ tale che $\alpha = s(\beta) = \beta \cup \{\beta\}$ e $\beta < s(\beta) = \alpha$, da cui, essendo α iniziale si ottiene $|\beta| < |s(\beta)| = |\alpha|$. Osserviamo allora che, usando la disuguaglianza di inclusione-esclusione si ottiene:

$$|\alpha| = |\beta \cup \{\beta\}| \leq |\beta| + |\{\beta\}| = |\beta| + 1$$

e, unendo questa disuguaglianza a quella iniziale, si ha: $|\beta| < |\alpha| \leq |\beta| + 1 \implies |\beta| < |\beta| + 1$. \square

§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 bigezione) ad alcun sottoinsieme di X , ossia $|\alpha| \not\leq |X|$.

¹⁴⁴In realtà, senza scelta non lo possiamo ancora dire, quindi ci limitiamo a dimostrare qualcosa di più debole, almeno in questa sezione.

¹⁴⁵Quindi in realtà senza scelta, sapremo solo questo, cioè che tutti gli ordinali infiniti hanno come cardinalità un aleph, in altre parole: scriviamo una funzione che produce degli ordinali, gli ω_α , le cui cardinalità [che sono tutte infinite] chiamiamo aleph, \aleph_α , e mostriamo che tutti gli ordinali infiniti hanno come cardinalità uno di questi.

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 su X] dato da:

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

cioè il sottoinsieme delle parti di $X \times X$, degli insiemi che sono buoni ordini [nel senso proprio di relazione, essendo che $R \subseteq X \times X$] su un sottoinsieme di X , quindi stiamo considerando tutte le relazioni d'ordine su $X \times X$, che ristrette ad un sottoinsieme di X sono bene ordinate.

Sia F la funzione classe che associa, ad ogni buon ordine, l'unico ordinale isomorfo¹⁴⁶. Per **rimpiazzamento**, esiste l'insieme $F[Y]$ (ovvero gli ordinali corrispondenti a tutti i buoni ordini, dati dalle relazioni in Y sui sottoinsiemi di X), il nostro obiettivo è dimostrare che c'è almeno un ordinale che non è in bigezione con alcun sottoinsieme di X .

Sia α un ordinale con $\alpha \notin F[Y]$ [possiamo prenderlo perché sappiamo che ogni insieme di ordinali ne ha sempre almeno uno che non gli appartiene]. Mostriamo che tale ordinale non è in bigezione ad alcun sottoinsieme di X , per assurdo, $|\alpha| = |X'|$, per qualche $X' \subseteq X$. Allora, per definizione, abbiamo una bigezione $f : X' \rightarrow \alpha$. Questa, però, ci fornisce un buon ordinamento [indotto] su X' , che lo rende isomorfo ad α - basta porre $x < y \stackrel{\text{def}}{=} f(x) <_\alpha f(y)$ - contrariamente al fatto che $\alpha \notin F[Y]$, ossia non è isomorfo ad alcun buon ordinamento su un sottoinsieme di X , dunque assurdo. Ciò significa che tale $\alpha \notin F[Y]$ non è in bigezione con alcune sottoinsieme di X , ovvero $|\alpha| \not\leq |X|$. \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 l'insieme degli ordinali non equipotenti ad alcun sottoinsieme di X è non vuoto ed è un insieme di ordinali, pertanto, per quanto visto, ammette sempre minimo, di conseguenza il numero di Hartogs di un insieme è sempre ben definito.

Osservazione 11.7 ($H(X)$ 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 $|\beta| = |H(X)|$, avremmo, per minimalità di $H(X)$ [$H(X)$ è il minimo ordinale che non si immerge in X , quindi qualsiasi ordinale più piccolo vi si immerge], $|\beta| \geq |X|$, da cui $|H(X)| = |\beta| \leq |X| \not\leq$. \square

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.

¹⁴⁶Cioè $F : Y \rightarrow \text{Ord} : R \mapsto \gamma$, tale che $\gamma \sim (X', R)$, e da quanto sappiamo γ esiste ed è unico quindi la funzione classe F è ben definita.

Dimostrazione. Se, per assurdo, esistesse l'insieme X degli ordinali iniziali, allora per ogni ordinale iniziale $|\alpha| \leq |\bigcup X|$ [cioè ogni ordinale iniziale è un sottoinsieme dell'unione dell'insieme degli ordinali iniziali], ma [prendendo il numero di Hartogs di tale unione, otteniamo un ordinale iniziale che non è un sottoinsieme dell'unione di X , ovvero non è un elemento di X , che è assurdo] $|\bigcup X| < |H(\bigcup X)| \not\leq$. \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:

$$|H(\alpha)| < |\alpha| \leftrightarrow |H(\alpha)| \not\leq |\alpha|$$

dunque la cosa al RHS, che è la definizione di numero di Hartogs, è equivalente alla disuguaglianza a sinistra, in quanto, essendo tutte le cardinalità degli ordinali confrontabili, come visto, se sono false sia $<$ che $=$, per l'osservazione fatta deve essere vero il $>$ [quindi $\alpha \hookrightarrow H(\alpha)$ non surgettivamente].

Inoltre, per definizione, tutti gli ordinali più piccoli di $H(\alpha)$, non rispettano il fatto che $|H(\alpha)| \not\leq |\alpha|$, in quanto abbiamo definito $H(\alpha)$ come il minimo per cui accade questa cosa, pertanto $H(\alpha)$ è proprio l'ordinale più piccolo in cui si immerge α . \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 $\alpha \stackrel{\text{def}}{=} \sup\{\beta \in \text{Ord} \mid |\beta| \leq \aleph_0\}$. Se per assurdo $|\alpha| \leq \aleph_0$, allora $|s(\alpha)| = |\alpha| + 1 \leq \aleph_0$, quindi, per la definizione di α , $s(\alpha) \leq \alpha \not\leq$.

Soluzione. \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 (Unicità degli isomorfismi tra classi proprie di ordinali)

Sia C una classe propria di ordinali, allora esiste un'unica $F : \text{Ord} \rightarrow C$ crescente e biunivoca.

Dimostrazione. Sia $G : \text{Ord} \rightarrow C$ definita per ricorsione transfinita da:

$$G(\alpha) = \text{il minimo } \beta \in C \text{ maggiore di tutti gli elementi di } G[\alpha]^{147}$$

Ci basta dire che F soddisfa la richiesta se e solo se $F(\alpha) = G(\alpha)$ per ogni $\alpha \in \text{Ord}$, infatti, dopo aver dimostrato che G è crescente e biunivoca avremo che tutte le funzioni da Ord a C coincideranno con G e quindi saranno proprio uguali a G per estensionalità di funzioni¹⁴⁸ [aka c'è un'unica funzione che rispetta tutte le richieste della tesi].

¹⁴⁷In simboli $G(\alpha) := \min\{\beta \in C \mid \forall x \in G[\alpha] \ x < \beta\}$.

¹⁴⁸Anche se in questo caso dovremmo usarne una versione per funzioni classe, che è il discorso già fatto su quando e in che senso due funzioni classe sono uguali.

Si vede immediatamente che G è crescente [per definizione], quindi in automatico iniettiva. Per verificare la surgettività, sia $\beta \in C$, siccome G è crescente $\beta < s(\beta) \leq G(s(\beta))$ [abbiamo visto che le funzioni crescenti di buoni ordini stanno sopra le bisettrici]. Quindi, per la minimalità di $G(s(\beta))$ [cioè il più piccolo che sta sopra tutti gli elementi di $G[s(\beta)]$ per definizione di G , e in questo caso sta sopra a β], si ha necessariamente che $\beta \in G[s(\beta)]$, ed in particolare si ha proprio che β è nell'immagine di G , dunque G è anche surgettiva. Ci resta da dimostrare che $F(\alpha) = G(\alpha)$, $\forall \alpha \in \text{Ord}$. Data F come nell'enunciato, $F(\alpha)$ è maggiore di tutti gli elementi di $F[\alpha]$ poiché F è crescente (per ipotesi). Vorremmo vedere che $F(\alpha)$ fosse proprio il minimo più grande di $F[\alpha]$, infatti, se ci fosse $\beta \in C$ minore di $F(\alpha)$ con questa proprietà [più grande di tutti gli elementi di $F[\alpha]$], allora avremmo $\beta > F(\gamma)$ per $\gamma < \alpha$ (perché $F(\gamma) \in F[\beta]$, e per come abbiamo preso β) e $\beta < F(\gamma)$ per $\gamma \geq \alpha$ [abbiamo preso $\beta < F(\gamma)$ e F è strettamente crescente per ipotesi]¹⁴⁹, quindi $\beta \neq F(\gamma)$ per ogni γ , contro la surgettività di F . Di conseguenza F soddisfa proprio la definizione ricorsiva di G , e, per il teorema di ricorsione transfinita coincidono [il teorema garantisce unicità] $\forall \alpha \in \text{Ord} \ F(\alpha) = G(\alpha)$. \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 è ben definita e unica appunto per il lemma appena visto].¹⁵⁰

Proposizione 11.13 (Definizione ricorsiva della funzione degli aleph)

Definiamo per **ricorsione transfinita v.2** la funzione aleph citata sopra:^a

$$\begin{aligned}\omega_0 &= \omega \\ \omega_{s(\alpha)} &= H(\omega_\alpha) \\ \omega_\lambda &= \sup\{\omega_\alpha \mid \alpha \in \lambda\} \text{ per } \lambda \text{ limite}\end{aligned}$$

^aDi fatto dobbiamo solo dimostrare che sia ben definita, cioè che l'insieme di arrivo sia effettivamente quello degli ordinali iniziali infiniti.

Dimostrazione. I casi 0 e successore sono immediati, vediamo il caso limite. Per la dimostrazione del lemma precedente, ω_λ deve essere il minimo ordinale **iniziale** di ogni $\alpha \in \lambda$ per la definizione ricorsiva datane.

Basta quindi dimostrare che $\beta \stackrel{\text{def}}{=} \sup\{\omega_\alpha \mid \alpha \in \lambda\}$ è iniziale [in questo modo la definizione ricorsiva data sopra della funzione, coincide necessariamente con la funzione degli aleph definita sopra, infatti, in questo caso avremmo una funzione classe dagli ordinali agli ordinali iniziali (cosa che ci manca da verificare), e per il lemma precedente è unica, dunque le due definite coincidono¹⁵¹]. Se così non fosse, cioè se β non fosse iniziale, esisterebbe $\gamma < \beta$ con $|\gamma| = |\beta|$. Ma per definizione di estremo superiore, dovrebbe esistere $\alpha \in \lambda$ tale che si abbia $\gamma < \omega_\alpha \implies \gamma \leq \omega_\alpha$ [è la caratterizzazione del sup, per averla stretta, poi quella stretta implica quella larga], dunque vale:

$$|\gamma| \leq |\omega_\alpha| < |\omega_{s(\alpha)}| \leq |\beta| \nmid$$

e la disuguaglianza stretta [vera per il caso successore, poiché usiamo l'Hartogs] in mezzo ci dà l'assurdo, in quanto avevamo supposto $|\gamma| = |\beta|$, dunque β è un ordinale iniziale e la definizione ricorsiva è ben posta. \square

¹⁴⁹Typo di Mamino, ha invertito entrambe le disuguaglianze.

¹⁵⁰Per come è definita questa funzione prende in arrivo tutti gli ordinali più piccoli associati alle cardinalità **infinite** [non sappiamo ancora che sono tutte], che sono i rappresentanti canonici che cercavamo.

¹⁵¹Anche se la prima non l'abbiamo mai definita esplicitamente.

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 $\aleph_\alpha, \aleph_\beta$ e $n \in \omega \setminus \{0\}$ vale che:

$$\begin{aligned}\aleph_\alpha + \aleph_\beta &= \aleph_\alpha \cdot \aleph_\beta = \max(\aleph_\alpha, \aleph_\beta) = \aleph_{\max(\aleph_\alpha, \aleph_\beta)} \\ \aleph_\alpha + |n| &= \aleph_\alpha \cdot |n| = \aleph_\alpha\end{aligned}$$

Assumiamo per un istante il seguente lemma.

Lemma 11.16 ($\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$)

$\forall \alpha \in \text{Ord} \quad \aleph_\alpha^2 = \aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$.^a

^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 $\aleph_0 \leq \aleph_\alpha$, che deriva dalla definizione ricorsiva data della funzione degli aleph (che poi sarebbe l'ordinamento totale degli ordinali), e il fatto che $|n| < \aleph_0 \implies |n| \leq \aleph_0$, dove la prima disuguaglianza è il fatto che $n \in \omega$. \square

Osservazione 11.17 (Ogni cardinalità infinita \leq un aleph è un aleph) — Se $|X| = \aleph_\alpha$ e $\aleph_0 \leq |Y| \leq |X|$ La prima disuguaglianza è equivalente a dire che Y è infinito una volta assunto scelta., allora $|Y| = \aleph_\beta$, per qualche $\beta \leq \alpha$.

Dimostrazione. Senza perdita di generalità possiamo assumere $X = \omega_\alpha$ [a meno di bigezione] e $Y \subseteq X$ [a meno di bigezione]. Allora Y è ben ordinato dall'ordinamento indotto da $\omega_\alpha = X$.

Sia γ il minimo ordinale tale che $|\gamma| = |Y|$ - che esiste perché l'ordinale di $(Y, <_{|\omega_\alpha|})$ ha questa proprietà. Siccome γ è il minimo della sua cardinalità, allora γ è iniziale, quindi esiste β tale che $\gamma = \omega_\beta$ (ovvero sta nell'immagine della funzione degli aleph, che

ricordiamo essere una funzione classe bigettiva, dunque surgettiva, vero la classe propria degli ordinali iniziali infiniti, dunque essere un ordinale iniziale equivale ad essere proprio uguale a ω_{qualcosa}). La monotonia della funzione $x \mapsto \omega_x$ [sempre la funzione degli aleph, ma scritta con una definizione diversa], implica $\beta \leq \alpha$, e quindi $|\omega_\beta| = \aleph_\beta \leq \aleph_\alpha$. \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 $\aleph_0^2 = \aleph_0$.

In pratica, per confrontare (a, b) con (a', b') , si confrontano prima $\max(a, b)$ e $\max(a', b')$; a parità si confrontano a 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 identiche). 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 $(\omega_\alpha \times \omega_\alpha, \prec)$. Dobbiamo mostrare, visto che siamo passati agli ordinali che $\beta = \omega_\alpha$. Siccome $|\omega_\alpha| \leq |\omega_\alpha \cdot \omega_\alpha| = |\beta|$ (dove la prima disuguaglianza è un'ovvia mappa iniettiva, oppure semplicemente l'osservazione sulla compatibilità delle operazioni fra cardinalità con il loro "ordinamento"), e ω_α è iniziale, abbiamo, per quanto detto sugli ordinali iniziali, necessariamente che $|\omega_\alpha| \leq |\beta| \leftrightarrow \omega_\alpha \subseteq \beta \leftrightarrow \omega_\alpha \leq \beta$, resta quindi da dimostrare che $\omega_\alpha \not\leq \beta$, ossia che ω_α non è isomorfo ad un segmento iniziale proprio di X , e dunque vale proprio l'uguaglianza.

Fissiamo un segmento iniziale proprio $X_{(a,b)}$ di X e dimostriamo che $|X_{(a,b)}| < \aleph_\alpha$ - quindi, necessariamente [viene impossibilitata la bigezione], $X_{(a,b)} \not\sim \omega_\alpha$, pertanto vale proprio, come ordinali, $\omega_\alpha \not\leq \beta$.

Sia $\mu := \max(a, b)$, siccome $\mu < \omega_\alpha$ [$a, b \in \omega_\alpha$ per costruzione] e ω_α è un ordinale iniziale [infinito e limite], allora, essendo un ordinale limite, accade per forza che $s(\mu) < \omega_\alpha$ [non può esserci l'uguale perché ω_α è iniziale e infinito, dunque limite], quindi $|s(\mu)| < \aleph_\alpha$.

Di conseguenza, o $|s(\mu)| = \aleph_\gamma$ per qualche $\gamma < \alpha$ [dunque la cardinalità è un aleph più piccolo di α], oppure $s(\mu) \in \omega$ [ovvero $s(\mu)$ è un ordinale finito]. Nel primo caso

$|s(\mu) \times s(\mu)| = \aleph_\gamma^2 \stackrel{\text{Hp. induttiva}}{=} \aleph_\gamma$ per ipotesi, nel secondo $|s(\mu) \times s(\mu)|$ è finito (proprio come accadeva nella dimostrazione di \aleph_0), dunque, in ogni caso $|s(\mu) \times s(\mu)| < \aleph_\alpha$. Siccome [il segmento iniziale principale è contenuto nel prodotto dei due successive degli elementi che lo determinano] $X_{(a,b)} \subseteq s(\mu) \times s(\mu)$, abbiamo allora che $|X_{(a,b)}| \leq |s(\mu) \times s(\mu)| < \aleph_\alpha$.

E questo conclude perché ora ω_α non può essere isomorfo ad un segmento iniziale proprio di X , per questioni di cardinalità. \square

Esercizio 11.18. Dimostrare che $\forall \alpha \in \text{Ord}$ [COMPLETARE]

§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.

Assioma 12.1 (Assioma 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:

$$\forall X (\emptyset \notin X) \rightarrow (\exists f \in {}^X \left(\bigcup X \right) \forall a \in X \ f(a) \in a)^b$$

^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**:

$$X = \{[n, +\infty] \mid n \in \mathbb{N}\}$$

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 . In questo senso, la possibilità di fissare un oggetto - cioè dare un nome ad un oggetto - è una legge del pensiero: una caratteristica del modo in cui ragioniamo.

Tecnicamente, questa legge è vendicata¹⁵² 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.

¹⁵²Nel senso di rivendicata.

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'espedito di **fissare una singola funzione di scelta**. 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. Dobbiamo verificare che l'enunciato nella nota sopra è un fatto equivalente all'assioma della scelta. Mostriamo prima che da scelta segue la proprietà richiesta e poi viceversa.

\Rightarrow Consideriamo:

$$Z \stackrel{\text{def}}{=} \{A \in \mathcal{P}(X) \mid \exists y \in Y \ \overbrace{\forall x \in X \ x \in A \leftrightarrow f(x) = y}^{A=f^{-1}(y)}\}$$

cioè l'insieme di tutte le controimmagini degli elementi di Y , e ovviamente sono tutte sottoinsiemi di X .

Per la surgettività di f gli elementi di Z sono tutti non vuoti [ogni $y \in Y$ ha controimmagine non vuota], dunque per AC esiste $h : Z \rightarrow X$ ¹⁵³ 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 immediatamente da questa definizione 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 viene proprio y :

$$f(z) = y \quad \text{con } z \in f^{-1}(y)$$

\Leftarrow 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:

$$f : X' \rightarrow X : (a, A) \mapsto A$$

¹⁵³ $\bigcup Z = X$ in quanto l'unione di tutti gli $A \in Z$ ricopre completamente X , infatti, tutti gli elementi di X hanno come immagine un elemento di Y e quindi sono tutti contenuti in una controimmagine, ovvero in un certo $A \in Z$.

è surgettiva [verifica ovvia], quindi per ipotesi ha un'inversa destra $g : X \hookrightarrow X'$ che manda A in una coppia (a, A) per qualche $a \in A$ ¹⁵⁴. 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 [quindi non so chi sia, ma è determinata dalla funzione inversa], cioè $h(A) \in A$.

□

L'assioma della scelta forma, insieme ai due enunciati seguenti - il teorema del buon ordinamento ed il lemma di Zorn - una terna classica di proposizioni equivalenti, nel senso che gli assiomi 1-8, unitamente ad una qualunque delle tre proposizioni, implicano le altre due.

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 (AC \iff buon ordinamento \iff 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.

¹⁵⁴Tale che $f \circ g(A) = f((a, A)) = A$, per un $a \in A$, e g **iniettiva** in quanto funzione inversa, dunque $g(A) = g(B) \implies A = B \wedge a = b$. Dunque la funzione g **sta fissando un certo** $a \in A$ [fissato], **senza scriverlo esplicitamente**, ma visto che l'assunto ci dice che è inversa, dunque iniettiva, g deve necessariamente farlo, qui sta il fatto che genera la funzione di scelta h , il fissare una prima componente perché per ipotesi non può che essere così, sapere che è un elemento di A , ma non sapere necessariamente chi sia.

§12.1 Buon ordinamento \rightarrow AC

Dimostrazione. (Buon ordinamento \rightarrow 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)

§A Soluzioni di altri esercizi e cardinalità note

Riferimenti bibliografici

- [1] Karel Hrbacek, Thomas Jech, *Introduction to Set Theory, Revised and Expanded*, CRC Press, Boca Raton, Florida, 3rd edition, 1999.
- [2] Mauro Di Nasso, *Elementi di teoria degli insiemi, Dispensa 4*, Università di Pisa, Pisa, 2019-20.
- [3] Marcello Mamino, *Elementi di teoria degli insiemi*, Università di Pisa, Pisa, 2020-21.