

# **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

<b>1</b>	<b>Prologo nel XIX secolo</b>	<b>5</b>
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
<b>2</b>	<b>Il linguaggio della teoria degli insiemi</b>	<b>14</b>
2.1	Le regole di inferenza	16
<b>3</b>	<b>I primi assiomi</b>	<b>18</b>
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
<b>4</b>	<b>Assioma dell'infinito e numeri naturali</b>	<b>35</b>
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
<b>5</b>	<b>Cardinalità</b>	<b>52</b>
5.1	Teorema di Cantor-Bernstein	53
5.2	Teorema di Cantor	56
5.3	Operazioni fra cardinalità	56
<b>6</b>	<b>Cardinalità finite</b>	<b>59</b>
6.1	Principio dei cassetti	59
6.2	Operazioni fra le cardinalità finite	63
<b>7</b>	<b>La cardinalità del numerabile</b>	<b>65</b>
7.1	Insiemi numerabili in pratica	69
7.2	Prodotto di numerabili è numerabile	70
7.3	Numeri interi e razionali	72
7.4	Ordini densi numerabili	78
7.5	Il grafo random	84
<b>8</b>	<b><math>\mathbb{R}</math> e la cardinalità del continuo</b>	<b>86</b>
8.1	Caratterizzazione dei reali come ordine	89
8.2	La cardinalità del continuo è $2^{\aleph_0}$	91
8.3	Operazioni che coinvolgono la cardinalità del continuo	92
8.4	Sottrarre un numerabile dal continuo	93
	<b>Stato del corso</b>	<b>96</b>
<b>9</b>	<b>I buoni ordinamenti</b>	<b>97</b>
9.1	Operazioni aritmetiche fra buoni ordinamenti	102

9.2	Gli ordinali di Von Neumann . . . . .	105
9.3	L'assioma del rimpiazzamento . . . . .	110
9.4	Induzione e ricorsione transfinita . . . . .	112
<b>10</b>	<b>Aritmetica ordinale e forma normale di Cantor</b>	<b>117</b>
10.1	Sottrazione e divisione euclidea . . . . .	117
	<b>Bibliografia</b>	<b>118</b>

## Premessa

Queste dispense sono la quasi esatta trascrizione in  $\text{\LaTeX}$  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<sup>a</sup>:

- 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<sup>b</sup>.

<sup>a</sup> $f(x) = \alpha x + \beta$ .

<sup>b</sup>Ovvero  $f$  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.

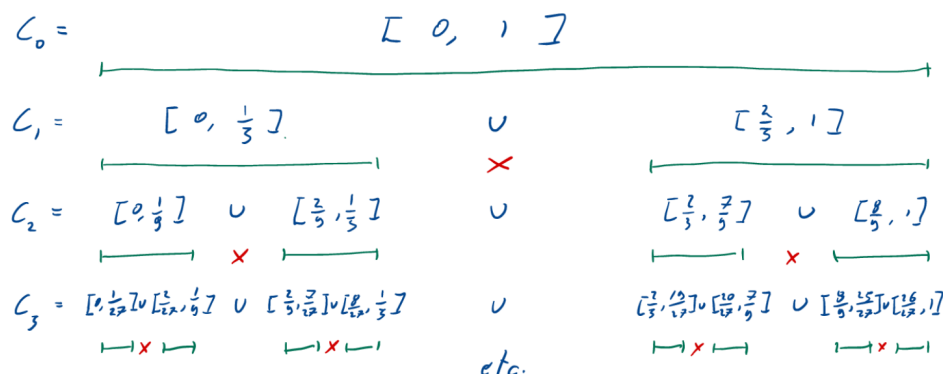
### NON Esempio 1.7

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.

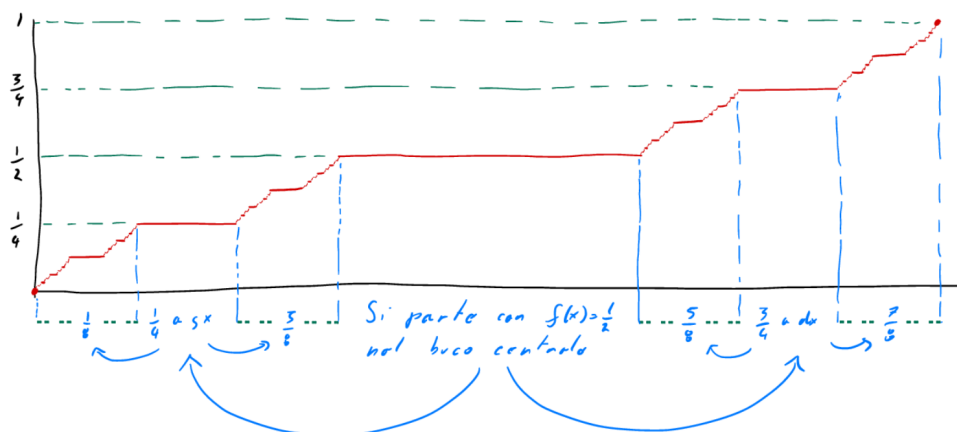
Possiamo costruire l'insieme di Cantor a partire dall'intervallo  $C_0 = [0, 1]$  nel seguente modo:



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  $x \in C$ .

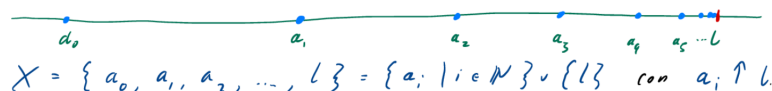


tale funzione si costruisce aggiungendo tratti costanti (prima  $\frac{1}{2}$ , poi  $\frac{1}{4}$ ,  $\frac{3}{4}$  e così via, dividendo l'intervallo  $[0, 1]$  sull'asse delle ordinate in parti uguali) alle parti eliminate sull'intervallo  $[0, 1]$  sull'asse delle ascisse per costruire l'insieme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

**Nota 1.9** — Per  $\mathbb{Q}$  e  $\mathbb{C}$  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.

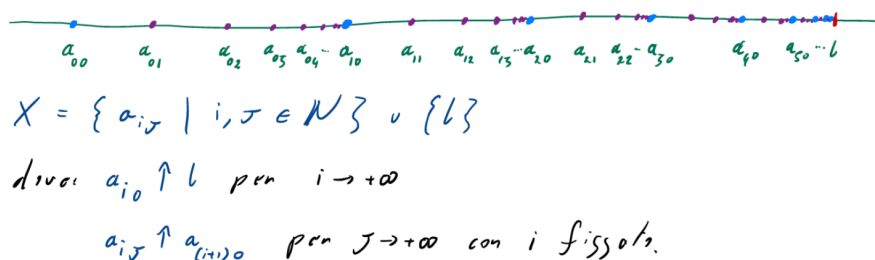


Dimostriamo quindi che  $X$  è un insieme di unicità.

*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  $i \neq j$ .<sup>1</sup>

### Esempio 1.13

Alcuni esempi di insiemi numerabili sono:

- $\mathbb{N}$ , l'insieme dei numeri naturali, infatti, la successione  $a_i = i$  realizza la bigezione.
- I numeri dispari, con la bigezione 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 bigezione 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,  $\mathbb{N} \times \mathbb{N} = \{(i, j) | t \in \mathbb{N}\}$ . Quindi  $X \times Y = \{(a_{i_t}, b_{j_t}) | t \in \mathbb{N}\}$ .  $\square$

### Esempio 1.17

$\mathbb{Q}$  è numerabile.

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



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

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

□

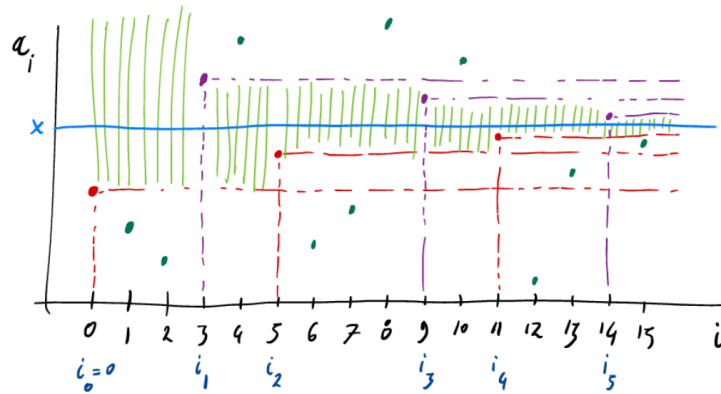
### NON Esempio 1.18

$\mathbb{R}$  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.

□

<sup>2</sup>num. = 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  $\alpha$  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.

<sup>a</sup> $n$  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  $i \rightarrow \infty$ .



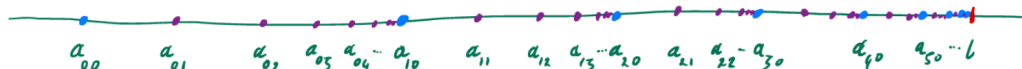
Tutti i punti sono isolati,  $X' = \emptyset$ .

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

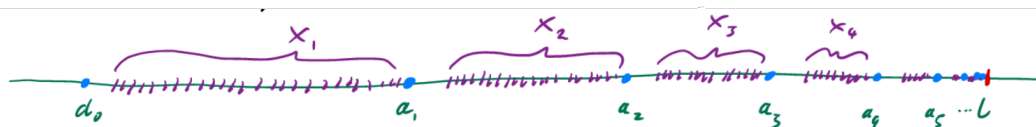


“Successione con punto limite”. Tutti i punti sono isolati salvo  $l$ , quindi  $X' = \{l\}$  e  $X'' = \emptyset$ .

- $X = \{a_{i,j} \mid i,j \in \mathbb{N}\} \cup \{l\}$  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  $X_\omega$  fatto così:



È chiaro che, per ogni  $n$ ,  $X_\omega^{(n)} \neq \emptyset$ . D'altro canto,  $X_\omega$  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.

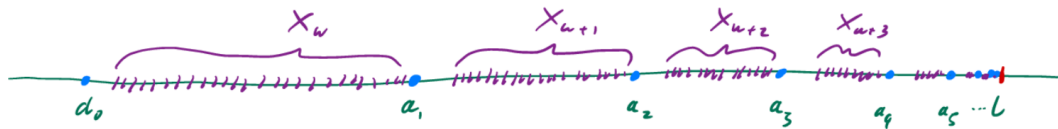
**Esercizio 1.26.** Perché  $X_\omega$  è numerabile?

Ora potremmo pensare che, pazienza se  $X_\omega$  non si smonta a furia di derivati, sarà un caso particolare. Però adesso, possiamo fare una successione di insiemi come  $X_\omega$ , 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  $X_\omega$ ”, allora per  $X$  vale il [Fatto 1.5](#).

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



No: occorre un nuovo corollario.

### Corollario 1.28

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

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

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

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

No, ogni sforzo di trovare l’induzione a capo delle induzioni è vano. Se ho  $X_\omega, X_{\omega^\omega}, X_{\omega^{\omega^\omega}}$ , etc., allora, ecco che faccio una successione con queste cose, la battezzo in qualche modo - ad esempio,  $X_{\varepsilon_0}$  - 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”:

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

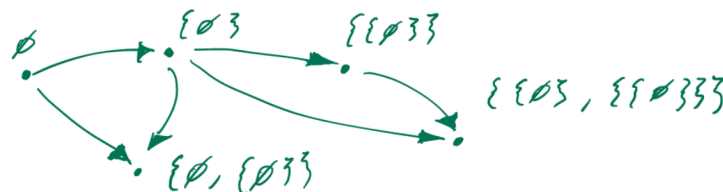
ad esempio:

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

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

**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.



<sup>3</sup> “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. <sup>4</sup>

**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.

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

<sup>5</sup>Cioè “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  $B$ <sup>a</sup>

<sup>a</sup>Qui 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  $\Phi$  e  $\psi$  - compilando una “**tabella di verità**”.

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

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:

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

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

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

<sup>6</sup> “equivale a”.

<sup>7</sup> 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  $\Phi$ . 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<sup>a</sup>.

<sup>a</sup>Nel 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  $\{x \in A \mid \psi(x)\}$ <sup>a</sup> è un insieme.

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

<sup>a</sup>Stiamo 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  $\psi$ , 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 collezione<sup>8</sup>. 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  $\psi(x)$ .<sup>9</sup>

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  $\psi(x)$ .

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

<sup>9</sup>Ovvero 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:

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

<sup>a</sup>Non 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  $\hat{\phantom{x}}$  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.<sup>11</sup>

### 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.

<sup>10</sup>Cioè 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).

<sup>11</sup>Essere 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  $x = a$ <sup>12</sup>.  $\square$

**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](#)  $\{a, b\} = \{b, a\}$ .  $\square$

<sup>12</sup>Stiamo 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  $\exists! x (x \in c)$ <sup>14</sup>:

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

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:

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

<sup>13</sup>Sostanzialmente 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  $a$ ).

<sup>14</sup>Cioè 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  $A$ .

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

<sup>a</sup>Cioè  $x$  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:

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

<sup>a</sup> “Unione di  $A$ ”.



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

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

<sup>a</sup>Cioè 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**<sup>15</sup> 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):

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

<sup>15</sup>Quindi, 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  $\{\dots\}$ <sup>16</sup>.

**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  $A$ .

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

<sup>16</sup>Paradossalmente 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:

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

<sup>a</sup>Ossia, 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  $\mathcal{P}(\mathcal{P}(A \cup B))$ :<sup>17 18</sup>

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

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.

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

<sup>18</sup>Tutte 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.  $\square$

<sup>19</sup> $\forall x_1, \dots, x_n \stackrel{\text{def}}{=} \forall x_1 \dots \forall x_n$ , 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.

<sup>a</sup>Formalmente:  $\{z \in A \times A \mid \exists x, y \in A \ z = (x, y) \wedge \dots\}$ .

<sup>b</sup>Come 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<sup>a</sup> 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.

<sup>a</sup>Altrimenti 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  $\text{id}_A$  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

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



assurdo, pertanto  $x = y$ <sup>21</sup>. 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  $B = C$ .<sup>22</sup>

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 che<sup>23</sup>  $f(x) = (\tilde{f} \circ i_\sim)(x), \forall x \in A$  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

<sup>21</sup>Abbiamo 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

<sup>22</sup>Essendo 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  $A$ .

<sup>23</sup>Per 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 <sup>24</sup>, 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  $\omega$  - come l'intersezione della classe, non vuota per l'assioma dell'infinito, di tutti gli insiemi induttivi. <sup>25</sup>

<sup>24</sup>Ciò non esclude che ci possano essere altri elementi oltre a  $\emptyset$  che non siano successori (questa cosa è sempre falsa in  $\omega$ ).

<sup>25</sup>Aver introdotto l'assioma dell'infinito ci assicura che tale intersezione è non vuota, e ciò basta affinché  $\omega$  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  $\omega$  è l'intersezione di tutti gli insiemi induttivi, ossia  $\omega$  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  $\omega$ , 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  $\omega$  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  $\omega$ .

**Esercizio 4.7.** Dimostra che  $\{\{\emptyset\}\} \notin \omega$ .<sup>a</sup>

<sup>a</sup>**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  $\omega$  non contenga elementi che non sono successori, si ottiene che  $\{\{\emptyset\}\} \notin \omega$ .<sup>28</sup>  $\square$

<sup>26</sup>Cioè  $x$  è in  $\omega$  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).

<sup>27</sup>Volendo 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  $\{\emptyset\}$ ).

<sup>28</sup>Non abbiamo usato l'hint di Mamino e abbiamo usato un fatto non dimostrato.

## §4.1 Gli assiomi di Peano

Per convincerci, però, che  $\omega$  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  $\omega$ <sup>29</sup>. In questo senso<sup>30</sup>, quindi,  $\omega$  codifica legittimamente i numeri naturali.

**Definizione 4.8** (Assiomi di Peano al secondo ordine<sup>31</sup>). Dato un insieme  $\mathbb{N}$ , un elemento  $0 \in \mathbb{N}$ , e una funzione:

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

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

(a) Il successore è iniettivo:

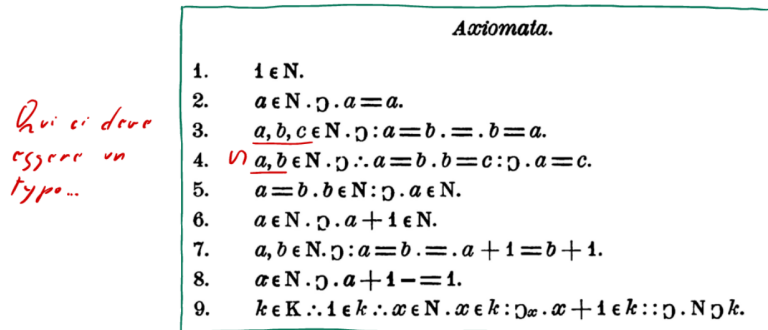
$$\forall n, m \in \mathbb{N} \text{ succ}(m) = \text{succ}(n) \rightarrow m = n$$
<sup>33</sup>

(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** ( $\omega$ 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.

<sup>29</sup>Cioè gli assiomi di Peano diventano enunciati dimostrabili all'interno della ZFC.

<sup>30</sup>Classicamente gli assiomi definivano  $\mathbb{N}$  a meno di isomorfismo, mostrando che  $\omega$  li soddisfa siamo sicuri di avere l'oggetto (insieme)  $\mathbb{N}$  definito da tali assiomi nella ZFC, e tale oggetto è appunto  $\omega$ .

<sup>31</sup>qualunque cosa questo significhi...

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

<sup>33</sup>L'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  $\omega$ ).

Dimostriamo ora che  $\omega$  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  $\omega = A$ <sup>34</sup>, 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  $\omega$  è contenuta nell'elemento:  $\forall n \in \omega \bigcup n \subseteq n$ .

*Dimostrazione.* Avendo dimostrato in (c) che in  $\omega$  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  $y = n$ ).  $\square$

<sup>34</sup>Stiamo costruendo  $A$  come sottoinsieme di  $\omega$  (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  $\omega$  è proprio l'elemento:  $\forall n \in \omega \bigcup s(n) = n$ .

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

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

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  $\omega$ )** — Dati  $m, n \in \omega$ , scriviamo:

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

<sup>a</sup>Per 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  $\Delta_\omega$  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  $\omega$ )**

La relazione  $<$  è un ordine totale su  $\omega$ .

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)**

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

<sup>a</sup>Moralmente: 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  $\omega$  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  $\omega$  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  $\forall b \in \omega (\emptyset \in b) \vee (\emptyset = b) \vee (b \in \emptyset)$ <sup>35</sup>. 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:

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

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

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

<sup>35</sup>Ovviamente 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  $\omega$ ) — Avendo dimostrato che  $<$  è un ordine totale su  $\omega$ , 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  $\omega$  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)

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

<sup>a</sup>Naturalmente il lemma vale anche con  $<$  e  $\subsetneq$ .

*Dimostrazione.* Siccome  $\omega$  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  $\omega$ , quindi irriflessiva, inoltre, nella dimostrazione del primo caso, si osserva che nel secondo passaggio è indifferente usare  $<$  o  $\leq$  nell'enunciato e dimostrazione del corollario<sup>36</sup>. □

<sup>36</sup>Mamino 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  $\Phi$  del numero precedente. Qui, invece, possiamo far conto di sapere  $\Phi$ , 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  $\forall x < m \Phi(x)$ )<sup>37</sup>.

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  $\omega$  ha un minimo elemento.

<sup>37</sup>Stiamo 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 tesi<sup>38</sup> 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.<sup>39</sup>

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

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<sup>a</sup> per quanto visto nel teorema precedente.

<sup>a</sup>Si 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  $a < b \stackrel{\text{def}}{=} a \in b$ .

<sup>38</sup>Cioè di questo caso della dimostrazione come visto nell'osservazione.

<sup>39</sup>Cioè se vale il principio del minimo c(ome vale in  $\omega$ ).

*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  $a! = 1 \cdot 2 \cdot \dots \cdot (a - 1) \cdot a$ .

<sup>40</sup>Che 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**  $\omega$  - 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  $A \times B$ ).

<sup>41</sup>Cioè 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:

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

<sup>a</sup> $k$  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  $\omega$  ad  $A$ ) usando la formula  $\Phi$ . 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  $\omega$ )

$\forall x \in \omega \exists! g$  “ $g$  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  $\Phi$ :

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

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  $\omega$  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:

$$f'(\emptyset) = k = f''(\emptyset) \quad f'(s(n)) = h(n, f'(n)) \stackrel{\text{Hp. indutt.}}{=} {}^{43}h(n, f''(n)) = f''(s(n))$$

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.

<sup>42</sup>Formalmente  $f = \{(x, y) \in \omega \times A \mid \Phi(x, y)\} = \{(x, y) \in \omega \times A \mid \exists! g \in {}^{s(x)}A \text{ "} g \text{ è una } x\text{-approssimazione" } \wedge g(x) = y\}$ , 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).

<sup>43</sup>E 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  $\omega$  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  $(\omega, \emptyset, s)$  sono strutture isomorfe - **ossia, formalmente, esiste:  $f : \omega \rightarrow \mathbb{N}$  bigettiva** tale che:

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

<sup>a</sup>Cioè 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:

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

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  $\omega$  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:

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

<sup>a</sup>Cioè è un numero di  $\omega$ .

<sup>b</sup>In 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  $\omega$ .

#### 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  $h(g) = g(n-1) + g(n-2)^a$ .

<sup>a</sup>Abbiamo quindi ottenuto  $h$  come funzione di funzioni con dominio in  $\omega$  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 con dominio in  $\omega$ , 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  $\cdot$ .

<sup>44</sup>Esiste 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  $A \hookrightarrow B$ )<sup>45</sup>.

**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<sup>a</sup>):

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

<sup>a</sup>Potrebbe 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  $\text{id}_A$  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

<sup>45</sup>Tale 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 bigettive<sup>46</sup>, per avere  $|A| = |C|$ .  $\square$

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

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

<sup>a</sup>Tali 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  $\text{id}_A$  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:

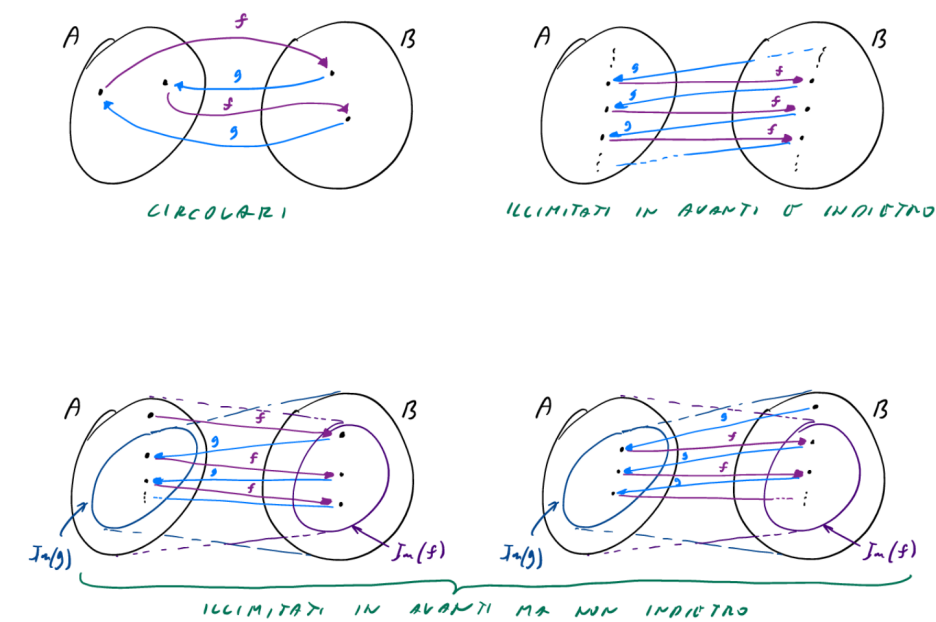
$$a \xrightarrow{f} f(a) \xrightarrow{g} g(f(a)) \xrightarrow{f} f(g(f(a))) \xrightarrow{g} \dots$$

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):

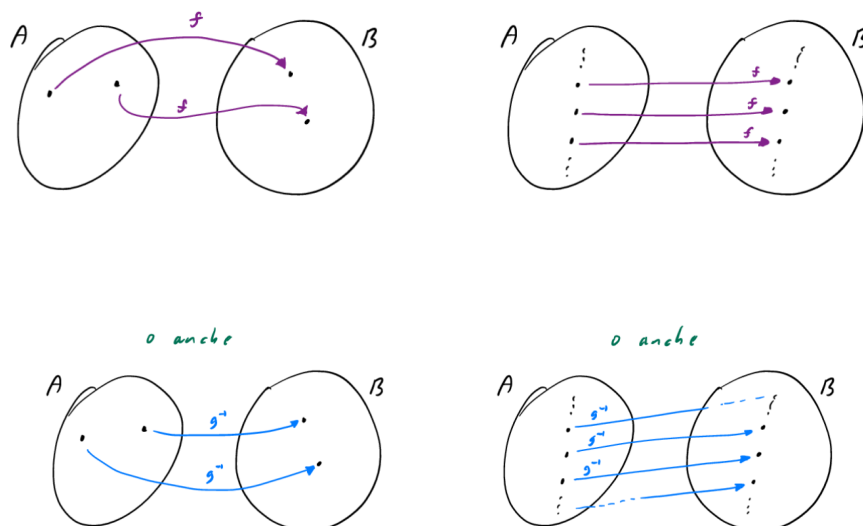
$$f^{-1}(g^{-1}(a)) \xrightarrow{f} g^{-1}(a) \xrightarrow{g} a \xrightarrow{f} f(a) \xrightarrow{g} g(f(a)) \xrightarrow{f} f(g(f(a))) \xrightarrow{g} \dots$$

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:

<sup>46</sup>È una semplice verifica.

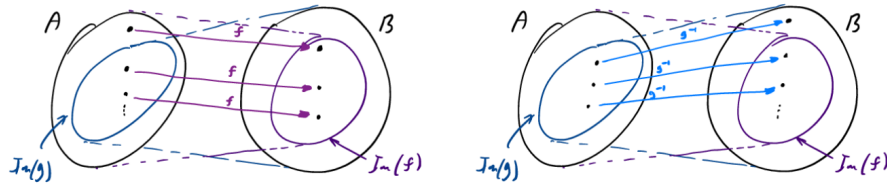


Per gli elementi che si trovano su un percorso circolare, o su un percorso illimitato avanti e indietro,  $f$  fornisce una bigezione, come la fornirebbe anche  $g^{-1}$  - la scelta è arbitraria a patto di usare la medesima funzione per l'intero percorso - nel modo seguente<sup>47</sup>:



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  $g^{-1}$ .

<sup>47</sup>Informalmente, 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:

$$a \in f(a) \subseteq A \iff a \in B \iff a \notin f(a) \quad \text{!}$$

□

## §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.

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

<sup>49</sup> $f(x) \in \mathcal{P}(A)$ , 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  $\alpha, \beta, \gamma$  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). □

<sup>51</sup>Cioè 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  $b \in B$ .

<sup>52</sup>Ovvero 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  $\text{id}_B$  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  $A = n \in \omega$ <sup>53</sup>. 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 surgettiva<sup>54</sup>, quindi non può avere in arrivo tutto  $n$ ). D'altro canto, per l'injectività 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'injectività di  $f$ , si ha  $|C| = |m|$ , quindi, per l'ipotesi induttiva (essendo  $C \subseteq m$ ), vale  $C = m$ . Ma in questo modo  $B = \text{Im}(f) = C \cup \underbrace{\{f(m)\}}_{=m} = m \cup \{m\} = s(m) = n$ .

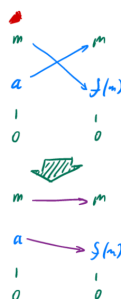
<sup>53</sup>Quello che faremo è proprio portare  $B \subsetneq A$  in  $f[B] \subsetneq f[A] = n$  e qui trovare l'assurdo, che è come assumere sempre che  $A = n$ , perché possiamo sempre spostare il problema in  $\omega$  con una bigezione.

<sup>54</sup>È 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 bigettività 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  $\omega$  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  $\omega$  non è finito, perché la funzione successore stabilisce una corrispondenza biunivoca fra  $\omega$  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  $\omega$  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  $\omega$  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  $\omega$  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  $m < n$ .<sup>a</sup>
- se  $A$  è finito e  $f : A \rightarrow B$ , allora  $f[A]$  è finito.

<sup>a</sup>Fondamentalmente ogni sottoinsieme di  $\omega$  (che non è detto sia un elemento di  $\omega$ ) è in bigezione con un elemento di  $\omega$ .

*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  $\text{id}_m$ ).<sup>55</sup>

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:

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

<sup>55</sup>Per concludere si può osservare, alternativamente, che  $n$  finito implica Dedekind-finito, dunque non può essere in bigezione 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  $\omega$  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  $h$  bigettive quanto scritto equivale ad  $a = b$ , che, applicando  $f$ , equivale a:

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

per cui  $g$  è iniettiva e vale la 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  $\omega$ )

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  $\omega$  le operazioni tra cardinalità corrispondono alla cardinalità delle operazioni tra gli elementi, già definite per ricorsione su  $\omega$ .

*Dimostrazione.* Dimostriamo, intanto che  $|m| + |1| = |s(m)|$ . A sinistra abbiamo, infatti la cardinalità di  $(m \times \{0\}) \cup \{(0, 1)\}$ <sup>56</sup> 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  $\omega$ .

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

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

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

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

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

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

<sup>56</sup>Typo 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  $f = \emptyset$ <sup>57</sup>).

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 biezione con  $m$ ).

□

**Nota 6.10** — Questa proposizione ci fornisce una dimostrazione delle proprietà aritmetiche elementari delle operazioni su  $\omega$  [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<sup>a</sup>.

<sup>a</sup>E 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.*

□

<sup>57</sup>E 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  $\omega$ .

### 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 (parzialmente<sup>58</sup>) 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).

<sup>58</sup>Dove 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<sup>a</sup>] indotto da  $\omega$  (cioè l'ordine che abbiamo definito su  $\omega$  ristretto a  $n$ ).

<sup>a</sup>Per 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:

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

□

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

**Proposizione 7.9** (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  $\omega$ , 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  $\omega$ ) 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 7.10** (Caratterizzazione di  $\omega$  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  $(A, \prec) \sim (\omega, <)$ .<sup>a</sup>

<sup>a</sup>Questa proposizione completa la caratterizzazione di  $(\omega, <)$  come ordine totale.

Dimostriamo prima un facile lemma.

**Lemma 7.11** (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.

<sup>a</sup>Typo 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  $(A, \prec)$ :

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

dove  $\min_{\prec}$  denota il minimo secondo la relazione d'ordine (buona)  $\prec$  di  $A$ . Occorre dimostrare intanto che  $f$  è ben definita.  $f(0)$  è ben definita, perché  $A \neq \emptyset$ , e quindi vale

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

il principio del minimo (che abbiamo per ipotesi). Per dire che  $f(s(n))$  è ben definita, occorre dire che la funzione  $h : A \rightarrow A$ ,  $h(x) = \min_{\prec} \{a \in A \mid x \prec a\}$  è ben definita (sarebbe la funzione che definisce la ricorsione - prima forma -), ossia che  $\{a \in A \mid x \prec a\}$  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  $\omega$  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  $f(x) \prec y$ , allora  $f[\omega]$  sarebbe [non vuoto e] superiormente limitato da  $y$ , tuttavia non avrebbe massimo perché ogni  $f(x)$  è  $\prec$  di  $f(s(x))$ , il che è assurdo [qui stiamo usando che violerebbe 3.]. Quindi c'è il **minimo**  $x \in \omega$  tale che  $y \preceq f(x)$ . Dimostriamo che, per tale  $x$ ,  $f(x) \preceq y$ , da cui l'uguaglianza (e quindi la surgettività).

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

$x = s(x')$  in questo caso  $f(x') \prec y$  per la minimalità di  $x$  (avendo preso  $x$  come il minimo in  $\omega$  tale che  $f(x) \preceq y$ , tutto ciò che sta sotto non può rispettare l'ultima condizione), ma allora,  $y \in \{a \in A \mid f(x') \prec a\}$ , quindi  $f(x) = f(s(x')) = \min_{\prec} \{a \in A \mid f(x') \prec a\} \preceq y$  (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 7.12 (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  $\omega$  soddisfa le ipotesi della proposizione precedente. 1 e 3<sup>60</sup> valgono in quanto ogni sottoinsieme di  $B$  è in particolare, sottoinsieme di  $\omega$  (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 sottoinsieme di  $\omega$  è infinito, allora è necessariamente numerabile.

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

<sup>60</sup>Typo di Mamino.

**Esercizio 7.13.** 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 7.14** (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  $B$ <sup>62</sup>. 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.  $\square$

<sup>61</sup>Si 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.

<sup>62</sup>Oppure potevamo assumere WLOG che  $B$  fosse proprio contenuto in  $C$  e che la mappa fosse proprio  $\text{id}_B$ , in ogni caso è solo una questione di nomi.

**Osservazione 7.15** (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 7.16** (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 7.17** ( $\aleph_0 \cdot \aleph_0 = \aleph_0$ )

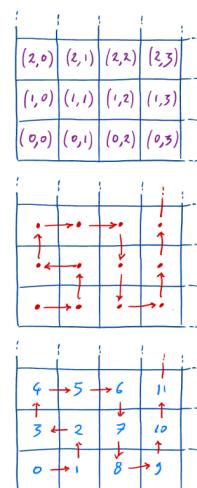
$\aleph_0 \cdot \aleph_0 = \aleph_0$ , ossia esiste una biezione fra  $\omega \times \omega$  e  $\omega$ .

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.

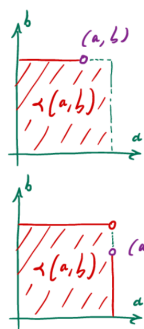
Altrimenti, è possibile esibire delle biezioni esplicite, per esempio:

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

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  $b'$ .<sup>64</sup>

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  $\omega$ , 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  $\omega$  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  $(A \setminus A') \cap (\omega \times \omega)_a =$

<sup>64</sup>Come 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 7.18** ( $\mathbb{Z}$ ). 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 7.19.** Dimostrare che  $\sim_{\mathbb{Z}}$  è una relazione di equivalenza.

#### Esempio 7.20 (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 7.21** ( $\mathbb{Q}$ ). 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 7.22.** Dimostrare che  $\sim_{\mathbb{Q}}$  è una relazione di equivalenza.

<sup>65</sup>Morale: " $(a, b) = a - b$ ".

<sup>66</sup>Morale: " $(n, d) = \frac{n}{d}$ ".



**Esercizio 7.23** (Operazioni su  $\mathbb{Q}$ ). Definisci  $+$ ,  $-$ ,  $\cdot$  e  $\square^{-1}$  su  $\mathbb{Q}$  nella maniera ragionevole e dimostra che  $\mathbb{Q}$  è un campo.

**Esercizio 7.24** (Ordinamento su  $\mathbb{Q}$ ). Definisci la relazione  $<$  su  $\mathbb{Q} \times \mathbb{Q}$  dicendo che  $q \in \mathbb{Q}$  è positivo se  $q = [(n, d)]_{\mathbb{Q}}$ , con  $n, d \in \omega \setminus \{0\}$ , e dicendo che  $a < b$  se e solo se  $b - a$  è positivo. Dimostra che questo è un ordine totale e **denso**, cioè:

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

<sup>a</sup>Typo di Mamino.

**Nota 7.25** — Gli esercizi precedenti sono tedious, 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 risolviamo<sup>67</sup>.

**Corollario 7.26** (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.<sup>a</sup>

<sup>a</sup>Formalmente 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)<sup>68</sup>.

Per l'inverso, supponiamo  $A$  al più numerabile e mostriamo che c'è sempre una mappa surgettiva tra  $\omega$  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  $\omega$  in  $A$  (cioè estendiamo la funzione che già c'è con  $n$  a tutti i naturali maggiori o uguali ponendola come  $g(0)$ ).  $\square$

<sup>67</sup>La soluzione riportata è quella di Mamino.

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

**Notazione 7.27 (Successione)** — Con **successione** (numerabile) intendiamo semplicemente una funzione con dominio  $\omega$ , per cui:

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

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

<sup>a</sup>Stiamo abbreviando la successione elencando direttamente i suoi elementi indicizzati.

<sup>b</sup>Moralmente: 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 7.28 (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 numerabile<sup>69</sup> 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 7.29 (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  $\alpha_i$  per ogni  $i \in \omega$ . Usando l'assioma della scelta potremo farlo, ma, per ora, non abbiamo modo, in generale, di procurarci la funzione

<sup>69</sup> $|\omega \times \omega| = \aleph_0 \cdot \aleph_0 = \aleph_0$ .

$i \mapsto \alpha_i$  (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 7.30** ( $|A| \leq \aleph_0 \implies |\bigcup A| \leq \aleph_0$ )

Sia  $A = \{a_i \in A \mid i \in \omega\}$  e sia  $\{\alpha_i\}_{i \in \omega}$  una **successione di funzioni**<sup>a</sup> tali che, per ogni  $i \in \omega$ ,  $\alpha_i : \omega \rightarrow a_i$  è una enumerazione di  $a_i$ <sup>b</sup>. Allora  $|\bigcup A| \leq \aleph_0$ .

<sup>a</sup>Come 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.

<sup>b</sup>Cioè 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 7.31** — 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 7.32** (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 7.33** (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  $\mathcal{P}^{\text{fin.}}(A) = \bigcup_{n \in \omega} \mathcal{P}^{\leq n}(A)$ <sup>70</sup>, basta esibire una successione di enumerazione  $\alpha_n$  di  $\mathcal{P}^{\leq n}(A)$  (cioè una mappa surgettiva da  $\omega$  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

<sup>70</sup>Ricordiamo 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  $\omega$  ad un altro insieme è un fatto equivalente al fatto che il secondo insieme sia al più numerabile).

Costruiamo una enumerazione<sup>71</sup>  $\{\alpha_n\}_{n \in \omega}$  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  $\alpha_0$  è la costante [funzione vuota]  $\emptyset$  (cioè la successione  $\alpha_0$  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  $\alpha_m$  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 surgettiva<sup>72</sup>, cioè che la nostra successione di successioni, è in particolare una successione di enumerazioni:

caso  $n = 0$  la successione vuota  $\alpha_0$  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  $\alpha_m$  è surgettiva, quindi  $Y$  è immagine di qualche  $t \in \omega$ ). Per la surgettività di  $f$ , la funzione surgettiva da  $\omega$  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  $\alpha_0$ , da  $\alpha_{s(m)}$  e aggiungere ricorsivamente tutti gli elementi a  $Y$  a partire dal vuoto).  $\square$

<sup>71</sup>In questo caso è una successione di enumerazioni, cioè una successione di funzioni surgettive.

<sup>72</sup>In 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  $\mathbb{A}_R$ <sup>73</sup> 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):

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

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:

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

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.

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

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

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).

<sup>73</sup>Sarebbe  $\overline{\mathbb{Q}} \cap \mathbb{R}$ .

<sup>74</sup>Può essere pensata come funzione da  $d$  in  $\mathbb{Q}$ .

<sup>75</sup>Cioè, abbiamo visto che un polinomio può essere pensato come una funzione da un qualche elemento di  $\omega$  (= anche sottoinsieme) a  $\mathbb{Q}$ , in particolare ogni elemento di  $\omega$  né è un sottoinsieme finito, quindi tutti i polinomi a coefficienti in  $\mathbb{Q}$  saranno funzioni da un sottoinsieme (in particolare funzioni) finito di  $\omega$  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  $\omega \times \mathbb{Q}$ .

<sup>76</sup>Nell'ordine di  $\mathbb{R}$  che prima non avevamo.

**Esercizio 7.34.** 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 7.35** (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 7.36** ( $(\mathbb{Q}, <)$  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 7.37** ( $(\omega, <)$  non è denso in se stesso)

L'insieme  $\omega$  con il suo ordinamento naturale non è denso, perché  $\nexists z \in \omega \ 0 < z < 1$ .

**Teorema 7.38** (Teorema di isomorfismo di Cantor)

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

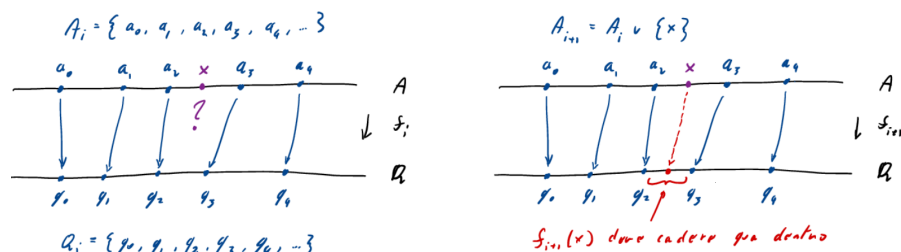
1.  $|A| = \aleph_0$
2.  $(A, <)$  è denso
3.  $(A, <)$  non ha **estremi**, ossia non ha né massimo né minimo elemento

allora  $(A, <) \sim (\mathbb{Q}, <)$ .<sup>a</sup>

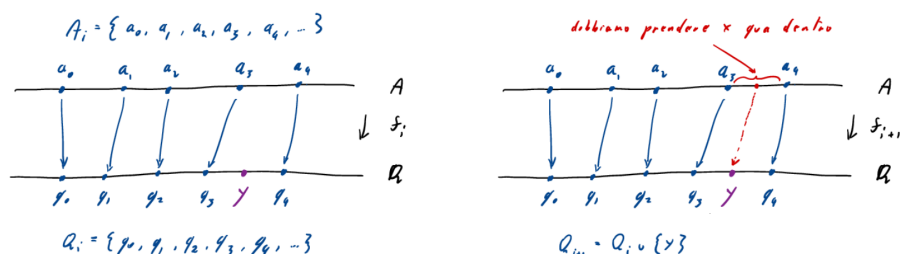
<sup>a</sup>Questa è una condizione sufficiente, quella necessaria consisterebbe nel verificare che  $(\mathbb{Q}, <)$  soddisfa le tre proprietà, ma sono ovvie per osservazioni precedenti.

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 7.39** (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  $B$ :<sup>a</sup>

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

<sup>a</sup>Moralmente 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  $|A_i| = |Q_i| < \aleph_0$ <sup>77</sup>
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  $\omega$  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:

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

<sup>77</sup>Ricordiamo 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  $q_i \in \text{Im}(f_{i+0.5})$ <sup>78</sup> [ $q_i$  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 isomorfo 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 7.40 (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 7.41** — 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.

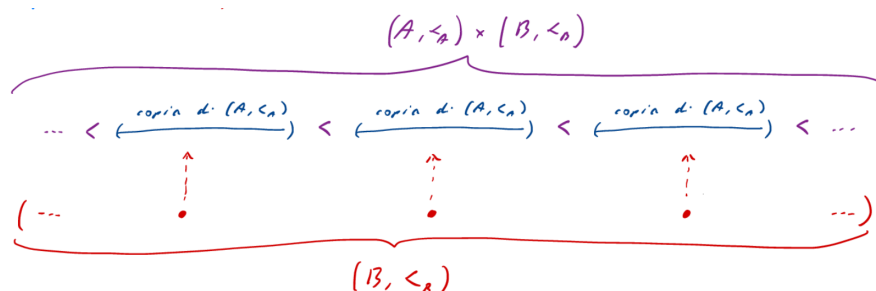
**Definizione 7.42** (Prodotto lessicografico di ordini). Dati  $(A, <_A)$  e  $(B, <_B)$  definiamo il **prodotto lessicografico** di ordini come:

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

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

<sup>78</sup>Stiamo 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 7.43** (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 7.44** (Associatività del prodotto lessicografico). Dati  $(A, <_A)$ ,  $(B, <_B)$  e  $(C, <_C)$  dimostra che:

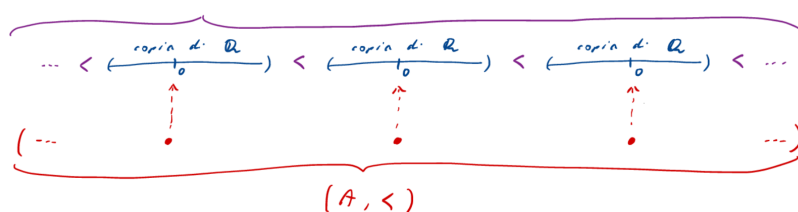
$$((A, <_A) \times (B, <_B)) \times (C, <_C) = (A, <_A) \times ((B, <_B) \times (C, <_C))$$

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 separatamente<sup>79</sup> tuttavia questa dimostrazione copre comunque il caso di  $A$  finito). Consideriamo quindi:

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



<sup>79</sup>Avremmo  $A$  in bigezione con  $n$  che si immerge in  $\omega$  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.<sup>81</sup>

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 7.45** (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  $2 \leq |A| \leq \aleph_0 \implies |A| = \aleph_0$ <sup>82</sup>. 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  $<' = \cup(\{\alpha\} \times \mathbb{Q}) \cup (\mathbb{Q} \times \{\beta\})$ <sup>83</sup>. Gli altri due casi ( $A$  chiuso in un estremo solo) sono analoghi e danno l'isomorfismo con  $[0, 1]_{\mathbb{Q}}$  e  $]0, 1[_{\mathbb{Q}}$ .  $\square$

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

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

<sup>82</sup>Stiamo escludendo l'insieme denso con un solo elemento

<sup>83</sup>Per 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 7.46** (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  $\omega$  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**<sup>84</sup>, dove, per essere precisi [possiamo definire l'isomorfismo tra grafi].

**Definizione 7.47** (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  $\omega$ , 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  $p^{|X|} \cdot (1-p)^{|Y|}$ <sup>85</sup> - come che sia, è un centro numero  $> 0$  - e ci sono infiniti [siamo in  $\omega$ ]  $v \notin X \cup Y$ . 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 7.48** (Grafo random). Il grafo  $(\omega, e)$  è un **grafo random** se:<sup>86</sup>

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

(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 7.49** (Esistenza e unicità del grafo random). Dimostra che esiste un grafo random, ed è unico a meno di isomorfismi.<sup>a</sup>

<sup>a</sup>Hint: Usare il back-and-forth per l'unicità.

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

<sup>85</sup>Eventi 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  $(1-p)^{|Y|}$ .

<sup>86</sup>Typo 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<sup>a</sup>.

<sup>a</sup>È 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  $\sup B \in A$ .<sup>87</sup>

**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.

<sup>87</sup>Questa 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  $\alpha$  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

<sup>88</sup>Moralmente: 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).

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

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

<sup>91</sup>Le 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<sup>a</sup>, immerge  $\mathbb{Q}$  in  $\mathbb{R}$  in maniera strettamente crescente e densa (ossia  $\iota(\mathbb{Q}) = \text{Im}(\iota)$  è densa in  $\mathbb{R}$ ).

<sup>a</sup>È 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  $\iota$  è strettamente crescente [dunque anche iniettiva]<sup>92</sup>. 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 contenimento<sup>93</sup> 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  $\mathbb{R}$ .  $\square$

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

<sup>93</sup>Per 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<sup>a</sup>]:

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

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  $\iota$ , con  $\mathbb{Q}$ , e questa corrispondenza preserva tutta la struttura rilevante - l'ordine come abbiamo verificato, ma anche le operazioni di campo.

<sup>a</sup>Anche 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  $(\mathbb{R}, <)$ .<sup>a</sup>

<sup>a</sup>Come 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  $y \in Y$ <sup>94</sup> [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 stesso<sup>95</sup>), ed essendo  $A$  senza estremi e  $B$  denso in  $A$ , anche  $B$  è senza estremi<sup>96</sup>],  $B$  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 <sup>97</sup>
- $\forall x, y, z \in F \ x < y \rightarrow x + z < y + z$  (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  $F$ ).

<sup>94</sup>Sarebbe la caratterizzazione del sup di un insieme.

<sup>95</sup>Tutti gli elementi di  $B$  sono anche elementi di  $A$ .

<sup>96</sup>Se  $B$  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.

<sup>97</sup>Come 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  $\mathcal{P}(\omega) \rightarrow \mathbb{R}$ <sup>98</sup> come segue:

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

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

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

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

<sup>99</sup>Sarebbe la scrittura decimale.

<sup>100</sup>Cioè 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  $\alpha, \beta$  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  $\beta$ ). Nel caso di  $2\beta$ , 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  $\beta$  come massimo).  $\square$

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

Se  $2 \leq \alpha \leq 2^{\aleph_0}$  allora  $\alpha^{\aleph_0} = 2^{\aleph_0}$ .

<sup>a</sup>Per 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  $\omega$ , 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 finito<sup>102</sup> che è assurdo<sup>103</sup>.  $\square$

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:

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

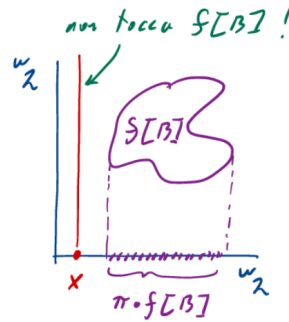
in particolare  $|f[B]| = |B| \leq \aleph_0$  perché  $f$  biezione, inoltre, essendo  $f[B]$  al più numerabile e  $\pi$  surgettiva,  $\pi[f[B]]$  è al più numerabile (come visto nell'[esercizio](#)<sup>104</sup>).

<sup>101</sup>Possiamo sempre assumere sia  $\omega$  WLOG.

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

<sup>103</sup>Volendo ogni cardinalità finita sta in  $\omega$  [o un qualsiasi altro insieme numerabile], e quindi si immerge in lui, cosa che rende assurda l'uguaglianza trovata.

<sup>104</sup> $|f[B]| \leq \aleph_0$ ,  $f[B] \xrightarrow{\pi} \pi[f[B]]$ , 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  $\omega_2$ , siamo tornati indietro con  $\pi^{-1}$  <sup>105</sup>).

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  $\omega$  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  $\omega$ ”:

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

Quindi  $|S| = |\mathcal{P}^{\text{fin.}}(\omega)| = \aleph_0$ , e, di conseguenza <sup>106</sup>  $|A| = |\mathcal{P}(\omega) \setminus (\{\emptyset\} \cup S)| = 2^{\aleph_0}$ , 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  $\omega$ ):

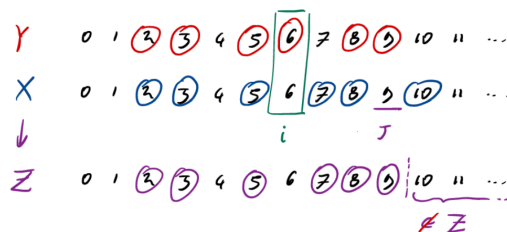
$$X <_A Y \stackrel{\text{def}}{=} \exists i \in \omega \underbrace{(i \cap X = i \cap Y)}_{\forall j < i \ j \in X \leftrightarrow j \in Y} \wedge \underbrace{(i \in Y \setminus X)}_{i \in Y \wedge i \notin X}$$

<sup>105</sup>  $\pi^{-1}(x) = \{x\} \times \omega_2$ , 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

<sup>106</sup>  $|\{\emptyset\} \cup S| \leq |\emptyset| + |S| = 1 + \aleph_0 = \aleph_0$  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  $\omega$  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  $\omega$ , 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  $\iota$  alla fine, per quanto osservato sul fatto che  $\mathbb{Q} \subseteq \mathbb{R}$ ).  $\square$

<sup>107</sup>Segue dal fatto che  $\omega$  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  $(B, <_B)$ <sup>a</sup> 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  $(A, <_A)$

<sup>a</sup>Nel 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  $\omega$ , 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  $\omega$  è principale [corrisponde a  $\omega_0$ ], 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.

<sup>108</sup>Ricordiamo 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.

<sup>a</sup>Ricordare 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]<sup>109</sup>. 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<sup>a</sup>

<sup>a</sup>I 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.

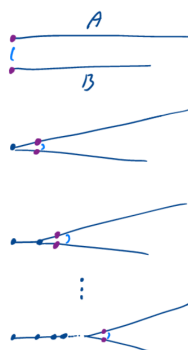
*Dimostrazione.* Siano  $f : A \rightarrow B$  e  $g : B \rightarrow A$  isomorfismi fra  $A$  e un segmento iniziale di  $B$  e fra  $B$  e un segmento iniziale di  $A$ . Ricordando la dimostrazione dell'osservazione precedente,  $g \circ f$  è un isomorfismo fra  $A$  e un **segmento iniziale**  $g \circ f[A]$  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  $\omega$  passaggi avremo identificato un segmento iniziale di  $A$ , diciamo  $A_x$ , isomorfo a  $\omega$ , con un  $B_y$ , anch'esso ovviamente isomorfo a  $\omega$ . 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  $y$ .

<sup>109</sup>Una 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 teorema<sup>110</sup>, 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.

<sup>110</sup>Typo di Mamino.

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

Se così non fosse, per la terza verifica vista,  $\text{Dom}(f) = A_a$  e per la penultima  $\text{Im}(f) = B_b$ <sup>111</sup>, 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  $B \subsetneq A \not\Rightarrow |B| < |A|$ <sup>112</sup>, 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:

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

<sup>111</sup>Stiamo 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.

<sup>112</sup>Cioè 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).

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

Per definire l'esponentiale 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** (Esponentiali di ordini totali). Dati  $(A, <_A)$  e  $(B, <_B)$  ordini totali, definiamo l'**esponentiale 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],  $m := \max_{<_B} \{x \in B \mid f(x) \neq g(x)\}$ .<sup>113</sup>

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  $B$ <sup>114</sup>. 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 siano definitivamente uguali).

**Esercizio 9.19.** Verificare che  $(\omega, <)^{(\omega, <)} \sim (\mathbb{N}[x], \prec)$ , dove  $\mathbb{N}[x]$  denota l'insieme dei polinomi a coefficienti in  $\mathbb{N}$ , e definiamo:

$$p \prec q \stackrel{\text{def}}{=} \exists N \in \mathbb{N} \forall x \in \mathbb{N} \ x > N \rightarrow p(x) < q(x)$$

(ossia  $p \prec q$  se  $p(x) < q(x)$  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**.

□

**Proposizione 9.21** (Buona definizione delle operazioni tra "classi di equivalenza" di buoni ordini)

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.<sup>a</sup>

<sup>a</sup>In 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.

<sup>113</sup>In 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.

<sup>114</sup>D'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).



*Dimostrazione.*

□

### Proposizione 9.22 (Proprietà delle operazioni sui buoni ordini)

Siano  $\mathcal{A} = (A, <_A)$ ,  $\mathcal{B} = (B, <_B)$  e  $\mathcal{C} = (C, <_C)$  buoni ordini. Allora:<sup>a</sup>

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

<sup>a</sup>Valgono in realtà anche l'esistenza e le proprietà degli elementi neutri per  $\cdot$  e  $+$ .

*Dimostrazione.* Facili verifiche.

□

**Esercizio 9.23.** Fare qualcuna delle verifiche delle proprietà sopra.

È importante notare che non tutte le proprietà delle operazioni aritmetiche su  $\omega$  valgono per i buoni ordini.

**Esercizio 9.24** (Proprietà **false** delle operazioni tra buoni ordini). Esibire controesempi alle seguenti:

$$\begin{aligned} \mathcal{A} + \mathcal{B} &\sim \mathcal{B} + \mathcal{A} & (\mathcal{A} + \mathcal{B}) \cdot \mathcal{C} &\sim \mathcal{A} \cdot \mathcal{C} + \mathcal{B} \cdot \mathcal{C} \\ \mathcal{A} \cdot \mathcal{B} &\sim \mathcal{B} \cdot \mathcal{A} & (\mathcal{A} \cdot \mathcal{B})^{\mathcal{C}} &\sim \mathcal{A}^{\mathcal{C}} \cdot \mathcal{B}^{\mathcal{C}} \end{aligned}$$

ovvero non valgono: **commutatività**, **distributività a destra** e **potenza di un prodotto**.

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'esponenziale quando è infinito.<sup>115</sup>

**Esercizio 9.25.** 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  $|C| = \aleph_0$ .<sup>a b</sup>

<sup>a</sup>Cioè per l'esponenziale 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  $\omega$  in  $\omega$ ), quindi ad esempio  $|\omega^\omega| = \aleph_0$  (cioè la cardinalità dell'esponenziazione), mentre  $|\omega^\omega| = |\omega|^{|\omega|} = \aleph_0^{\aleph_0} = 2^{\aleph_0} > \aleph_0$  (cioè la cardinalità delle funzioni da  $\omega$  in  $\omega$  [che abbiamo associato alle  $\omega$ -uple di elementi di  $\omega$ ].)

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

## §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 classe di isomorfismo di questi

<sup>115</sup>Un 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  $\omega$  con la ricorsione numerabile, ed in questo caso le parentesi saranno a destra.

- 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.<sup>116</sup>

**Definizione 9.26** (Insieme transitivo). L'insieme  $\alpha$  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  $\alpha$  è transitivo se gli elementi degli elementi di  $\alpha$  sono, a loro volta, elementi di  $\alpha$  (cioè se gli elementi sono a loro volta insiemi di elementi).<sup>117</sup>

**Definizione 9.27** (Ordinali di Von Neumann). L'insieme  $\alpha$  è un **ordinale** se è **transitivo e bene ordinato dalla relazione di appartenenza**. Formalmente, l'insieme transitivo  $\alpha$  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  $\text{Ord}$  la classe degli ordinali<sup>119</sup>, per cui:

$$\alpha \in \text{Ord} \stackrel{\text{def}}{=} \text{“}\alpha \text{ è transitivo e ben ordinato da } \in \text{”}$$

### Esempio 9.28 (Esempi di ordinali)

Alcuni esempi di ordinali già incontrati:

- $\omega$  è un ordinale
- gli elementi di  $\omega$  sono ordinali
- $s(\omega) = \omega \cup \{\omega\}$  è un ordinale<sup>a</sup>

<sup>a</sup>E in generale il successore di un ordinale è un ordinale, ciò ci permette di descrivere bene gli elementi di  $\omega$  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 9.29** (Ord è [una classe] transitiva) — Se  $\alpha \in \text{Ord}$  e  $\beta \in \alpha$ , allora  $\beta \in \text{Ord}$  e  $\beta = \alpha_\beta$  (ovvero  $\beta$  è il segmento iniziale principale [e in automatico proprio] di  $\alpha$ , determinato da  $\beta$ ). In particolare la classe degli ordinali  $\text{Ord}$  è transitiva.<sup>a</sup>

<sup>a</sup>Cioè tutti gli ordinali sono a loro volta insiemi di ordinali.

*Dimostrazione.* Siccome  $\beta \in \alpha$ , per la transitività di  $\alpha$  [tutti gli elementi sono sottoinsiemi],  $\beta \subseteq \alpha$ , quindi  $\beta$  è bene ordinato da  $\in$  [ristretto come ordine a  $\beta$ ]. La transitività di

<sup>116</sup>Vorremo 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 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.

<sup>117</sup> $\omega$  è un esempio di insieme transitivo, e naturalmente negli insiemi transitivi, così come  $\omega$  gli elementi sono sottoinsiemi, ma non tutti i sottoinsiemi sono elementi.

<sup>118</sup>Esattamente come su  $\omega$ ,  $x < y \leftrightarrow x \in y \leftrightarrow (x, y) \in <_\omega$ .

<sup>119</sup>Tale classe contiene un elemento per ogni buon ordine, ad esempio, preso  $(\omega, <)$ , come classe di buoni ordini isomorfi a lui, prenderemo solo  $\omega$  (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).

$\beta$  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  $\alpha$ ,  $\gamma \in \alpha$  [abbiamo usato che  $\beta$  è anche un sottoinsieme di  $\alpha$ ], e, da questo, nuovamente per la transitività di  $\alpha$  [ora che abbiamo  $\gamma \in \alpha$ , essendo  $\alpha$  transitivo, abbiamo in automatico  $\gamma \subseteq \alpha$ ],  $\delta \in \alpha$  (e quindi anche  $\delta \subseteq \alpha$ <sup>120</sup>). 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  $\alpha$ ]  $\delta <_\alpha \gamma \wedge \gamma <_\alpha \beta$ , 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  $\alpha$ , 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 9.30** (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:

$$\begin{aligned} x \in B_{f(a)} &\iff x <_B f(a) \\ &\iff f^{-1}(x) <_A a \\ &\iff f^{-1}(x) \in A_a \\ &\iff x \in f[A_a] \end{aligned}$$

$\square$

### Proposizione 9.31

Dati  $\alpha, \beta \in \text{Ord}$ , se  $(\alpha, <_\alpha) \sim (\beta, <_\beta)$ , allora  $\alpha = \beta$ .

*Dimostrazione.* Sia  $f : \alpha \rightarrow \beta$  un isomorfismo. Ci basta dimostrare che  $\forall \gamma \in \alpha \ f(\gamma) = \gamma$ . Sia, per assurdo,  $\gamma$  il minimo elemento di  $\alpha$  tale che  $f(\gamma) \neq \gamma$ . Allora:

$$\gamma = \alpha_\gamma = f[\alpha_\gamma] = \beta_{f(\gamma)} = f(\gamma) \nmid$$

$\square$

<sup>120</sup>È una specie di bootstrap per chi conoscesse il termine dall'analisi.

Possiamo ora chiederci come si rifletta l'ordinamento totale delle classi di isomorfismo di buoni ordini, dato dalla relazione “essere segmento iniziale di”, sugli ordinali. La risposta è che diventa la relazione di appartenenza.

### Teorema 9.32

Dati  $\alpha, \beta \in \text{Ord}$ , vale **una e una sola** delle seguenti:

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

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

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

Notazione: d'ora in poi [avendo dimostrato che per ogni classe di isomorfismo di buoni ordini c'è (al più) un ordinale<sup>121</sup> corrispondente], porremo per comodità:  $\alpha \prec \beta \stackrel{\text{def}}{=} (\alpha, <_\alpha) \prec (\beta, <_\beta)$ , e analogamente  $\alpha \sim \beta$  e  $\beta \prec \alpha$ .

*Dimostrazione.* □

**Notazione 9.33** (Ordine della classe degli ordinali) — Dati  $\alpha, \beta \in \text{Ord}$ , poniamo:

$$\alpha < \beta \stackrel{\text{def}}{=} \alpha \in \beta$$

Il teorema precedente ci dice che la relazione  $<$  gode delle proprietà di un ordine totale stretto sulla classe degli ordinali.

### Proposizione 9.34 (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.* □

Ricordiamo che  $s(\alpha) \stackrel{\text{def}}{=} \alpha \cup \{\alpha\}$ . La proposizione segue dice che  $s(\alpha)$  è, a buon diritto, il successore di  $\alpha$ , anche quando  $\alpha$  è un ordinale.

### Proposizione 9.35

Dato  $\alpha \in \text{Ord}$ ,  $s(\alpha)$  è il minimo ordinale  $> \alpha$ .

*Dimostrazione.* □

### Corollario 9.36

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

<sup>121</sup>Per il viceversa serve l'assioma del rimpiazzamento.

### Proposizione 9.37

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  $X$ .

<sup>a</sup>Gli  $\alpha \in \text{Ord}$  tali che  $\forall \beta \in X \beta \leq \alpha$ .

*Dimostrazione.*

□

### Corollario 9.38

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

*Dimostrazione.*

□

### Corollario 9.39 (Paradosso di Burali-Forti)

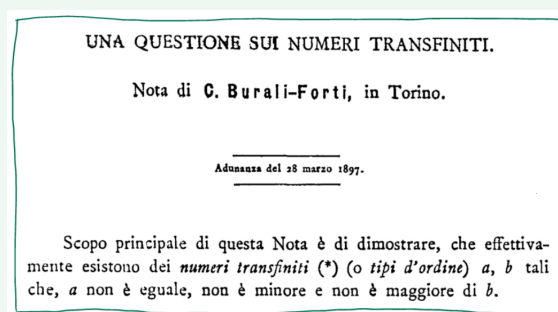
Ord è una classe propria.

Ossia non esiste l'insieme di tutti gli ordinali.

*Dimostrazione.* Per il punto 3. della proposizione, se Ord fosse un insieme, esisterebbe un ordinale che non vi appartiene, che è assurdo.

□

**Nota 9.40** (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, ma allora  $\Omega \stackrel{\text{def}}{=} [(\text{Ord}, <)]$ , la classe di isomorfismo di  $(\text{Ord}, <)$ , sarebbe uno dei membri della classe Ord, e, considerando il suo successore  $s(\Omega)$ , avremmo  $\Omega < s(\Omega)$ , ma anche  $s(\Omega) < \Omega$ , 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  $\omega$  con un numero finito di applicazioni della mappa successore.

**Esercizio 9.41.** Dimostra che la classe descritta sopra è effettivamente una classe, ossia è definita da una formula.

Se vogliamo poter rispondere alla domanda “quanti ordinali esistono?” occorre un nuovo assioma: l'assioma del rimpiazzamento. Sotto questa ipotesi addizionale, la risposta sarà “tutti quelli che potrebbero esistere”, ossia avremo un ordinale per ogni classe di isomorfismo di buoni ordini.

Per formulare l'assioma, ci serve il concetto di funzione classe.

**Definizione 9.42** (Funzione classe). Date due classi  $A$  e  $B$  una **funzione classe** da  $A$  a  $B$  è una formula insiemistica  $\varphi(x, y)$  tale che:

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

Ossia, una funzione classe è una proprietà, espressa nel linguaggio della teoria degli insiemi, che ad ogni  $x \in A$  associa un **unico**  $y \in B$ .

**Notazione 9.43** (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 9.44** (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 9.45** (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.<sup>a</sup>

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

(cioè per ogni insieme esiste un insieme i cui elementi sono immagini di quelli di  $A$  rispetto alla funzione classe  $F$ ).

<sup>a</sup>Come per la separazione, anche questo è uno **schema di assiomi**, uno per ogni possibile funzione classe  $F$ .

**Proposizione 9.46** (Unicità del rimpiazzo)

Data una funzione classe  $F : V \rightarrow V$  vale che:

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

*Dimostrazione.* Estensionalità. □

**Osservazione 9.47** (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:

$$\forall y \forall x (y \in G[A] \leftrightarrow \exists x \in A \ y = G(x))$$

*Dimostrazione.* Applicando l'**assioma del rimpiazzamento** appena enunciato, applicato alla funzione classe  $F : V \rightarrow V$ , abbiamo:

$$y = F(x) \stackrel{\text{def}}{=} (x \in A \wedge y = G(x)) \vee (x \notin A \wedge y = \emptyset)$$

ossia:

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

Infatti  $x \in A$  implica  $G(x) = F(x)$ , per cui  $G[A] = F[A]$ . □

**Esercizio 9.48.** 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**.

**Teorema 9.49** (Ogni buon ordine è isomorfo ad un unico ordianle)

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

<sup>a</sup>Questo 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, e quindi ce n'è esattamente uno corrispondente.

*Dimostrazione.* □

Una conseguenza del risultato precedente è che possiamo definire le operazioni sugli ordinali come semplice riflesso di quelle sui buoni ordini.

**Definizione 9.50** (Operazioni sugli ordinali - v.1). Dati  $\alpha, \beta \in \text{Ord}$ , definiamo  $\alpha + \beta$ ,  $\alpha \cdot \beta$ ,  $\alpha^\beta$  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 9.51** (Esistenza del prodotto cartesiano via rimpiazzamento). 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 9.52.** 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. La soluzione è poco sotto.

*Soluzione.* □



**Proposizione 9.53** (Induzione transfinita - v.1)

Data una formula insiemistica  $\varphi(x)$ . Se vale [l'ipotesi dell'induzione]<sup>a</sup>:

$$\forall \alpha \in \text{Ord} (\forall \beta < \alpha \varphi(\beta)) \rightarrow \varphi(\alpha)$$

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

<sup>a</sup>Come nell'induzione normale, il difficile è mostrare 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  $\forall \alpha \in \text{Ord} (\forall \beta < \alpha \varphi(\beta)) \rightarrow \alpha \in C$ <sup>122</sup>, allora  $\forall \alpha \in \text{Ord} \varphi(\alpha)$ , oppure, in forma più coincisa:

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

(in altre parole, assumere che  $\alpha$  è un sottoinsieme di  $C$  e da questo dimostrare che ne è un elemento, ci assicura che la classe degli ordinali è contenuta nella classe degli oggetti che soddisfano la formula che definisce  $C$ ).

*Dimostrazione.* Per assurdo, assumiamo [la negazione della tesi]  $\neg \varphi(\alpha)$ <sup>123</sup>, essendo l'ipotesi vera e [per ipotesi assurda]  $\varphi(\alpha)$  falsa, l'ipotesi [come formula insiemistica] diventa una implicazione<sup>124</sup> vera, con conseguente falso, quindi l'unica possibilità è che anche l'antecedente sia falso, ovvero  $\neg(\forall \beta < \alpha \varphi(\beta))$ , cioè  $\exists \beta < \alpha \neg \varphi(\beta)$ .

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  $\alpha$  dei  $\beta$  per cui  $\varphi$  è falsa è non vuoto, quindi possiamo considerare<sup>125</sup>  $\beta_0 := \min\{\beta \in \alpha \mid \neg \varphi(\beta)\}$ . Ora, usando  $\beta_0$  nell'ipotesi [come fatto all'inizio con  $\alpha$ ] (essendo un altro ordinale per cui la formula è falsa), si ottiene che  $\exists \beta < \beta_0 \neg \varphi(\beta)$  (cioè la formula ci procura un ordinale più piccolo per cui la formula è falsa), contro la minimalità di  $\beta_0$ , che è assurdo.  $\square$

**Nota 9.54** (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  $\varphi$ .

C'è una chiara ideologia 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 9.55** (Ordinale successore). Diciamo che  $\alpha \in \text{Ord}$  è un **ordinale successore** se  $\exists \beta \in \text{Ord} \alpha = s(\beta)$ . Un ordinale  $\alpha > 0$  che non è successore è detto **ordinale limite**.

<sup>122</sup>Ricordiamo  $\alpha$  in una classe  $= \alpha$  soddisfa la formula che definisce tale classe.

<sup>123</sup>Formalmente  $\neg(\forall \alpha \in \text{Ord} \varphi(\alpha)) = \exists \alpha \in \text{Ord} \neg \varphi(\alpha)$ , e stiamo considerando un  $\alpha$  per cui la formula è falsa.

<sup>124</sup>Materiale (qualunque cosa significhi).

<sup>125</sup>Perché ora possiamo scrivere un insieme per separazione da cui prendere il minimo, prima sarebbe stato il minimo preso su qualcosa definito per separazione sulla classe degli ordinali, e poteva essere problematico, così invece non abbiamo alcun problema.

**Osservazione 9.56** — Un ordinale  $\alpha$  è successore se e solo se ha un massimo elemento.

*Dimostrazione.*  $\beta$  è il massimo di  $\alpha$  **se e solo se**  $\alpha$  è il minimo ordinale  $> \beta$  **se e solo se**  $\alpha = s(\beta)$ .  $\square$

**Proposizione 9.57** (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  $\lambda$ ,  $(\forall \beta < \lambda \varphi(\beta)) \rightarrow \varphi(\lambda)$  (caso limite)

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

*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:

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

Se  $\alpha$  è limite o 0 abbiamo questa formula tout court. Altrimenti  $\alpha = s(\gamma)$  e abbiamo:

$$\forall \beta < \alpha \varphi(\beta) \implies \varphi(\gamma) \implies \varphi(s(\gamma)) = \varphi(\alpha)$$

$\square$

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

**Notazione 9.58** (Restrizione di una funzione classe) — Data una funzione classe  $F : A \rightarrow B$  e un insieme  $X \subseteq A$  esiste la funzione:

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

**Teorema 9.59** (Ricorsione transfinita - v.1)

Data una funzione classe  $G : V \rightarrow V$  esiste un'unica<sup>a</sup> funzione  $F : \text{Ord} \rightarrow V$  tale che:

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

<sup>a</sup>Dove l'unicità va intesa nel senso seguente: date  $F_1, F_2$  come sopra, vale  $\forall \alpha \in \text{Ord } F_1(\alpha) = F_2(\alpha)$ .

*Dimostrazione.*  $\square$

Come per l'induzione, possiamo esprimere la ricorsione transfinita separando i casi zero, successore e limite.

**Definizione 9.60** (Prodotto cartesiano di classi). Date due classi  $A, B$  definiamo la classe  $A \times B$  come:

$$x \in A \times B \stackrel{\text{def}}{=} \exists a \in A \exists b \in B x = (a, b)$$

(cioè  $x$  è uguale a una coppia di elementi ciascuno in una classe, ovvero ciascuno soddisfa un predicato).

**Corollario 9.61** (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.*

□

**Corollario 9.62** (Operazioni tra ordinali (definizione ricorsiva))

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

$$\begin{aligned} \alpha + 0 &= \alpha & \alpha \cdot 0 &= 0 \\ \alpha + s(\beta) &= s(\alpha + \beta) & \alpha \cdot s(\beta) &= \alpha \cdot \beta + \alpha \\ \alpha^\lambda &= \sup\{\alpha + \beta \mid \beta < \lambda\} & \alpha \cdot \lambda &= \sup\{\alpha \cdot \beta \mid \beta < \lambda\} \\ \alpha^0 &= 1 \\ \alpha^{s(\beta)} &= \alpha^\beta \cdot \alpha \\ \alpha^\lambda &= \sup\{\alpha^\beta \mid \beta < \lambda\} \end{aligned}$$

Ossia, le operazioni aritmetiche sugli ordinali si possono definire in modo analogo alle operazioni aritmetiche su  $\omega$  nei casi 0 e successore, estendendole **con continuità** nel caso limite.

**Definizione 9.63** (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  $\lambda$  vale  $F(\lambda) = \sup F|_\lambda$ .

**Notazione 9.64** — 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  $\alpha$ , possiamo costruire ricorsivamente la funzione classe " $\alpha +$ "  $\text{Ord} \rightarrow \text{Ord}$ , ma abbiamo, a quanto pare, una diversa funzione per ogni possibile  $\alpha$ . 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  $\alpha$ . 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  $\alpha$ . 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  $\alpha$ , questa variabile comparirà altresì nella formula di  $F$ , ed avremo così, in realtà, una funzione classe di due argomenti:  $\alpha$  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 9.65** (Le operazioni fra ordinali definite ricorsivamente sono equivalenti alle corrispondenti sui 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.*

□

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 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  $\alpha$  si scrive, in modo unico, nella forma:

$$\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n$$

con  $n \in \omega$ ,  $k_1, k_2, \dots, k_n \in \omega \setminus \{0\}$  e  $\beta_1 > \beta_2 > \dots > \beta_n$ . Con queste forme normali di Cantor è possibile calcolare le operazioni aritmetiche in modo esplicito.

**Nota 10.1** — Per procederemo con ordine, assumeremo la definizione ricorsiva delle operazioni ordinali e procederemo unicamente da quella.

### Proposizione 10.2

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  $\alpha^\beta$  assumendo  $1 < \alpha$  - e **ma decrescenti nel primo argomento**.

Per dimostrare la proposizione ci serviranno queste note.

**Nota 10.3** — Dati due insiemi di ordinali  $X, Y$  non vuoti.

$$\forall \alpha \in X \exists \beta \in Y \alpha \leq \beta \rightarrow \sup X \leq \sup Y$$

*Dimostrazione.*

□

**Nota 10.4** — La funzione  $\alpha \mapsto s(\alpha)$  è crescente.

*Dimostrazione.*  $\alpha < \beta \leftrightarrow s(\alpha) \leq \beta \leftrightarrow s(\alpha) < s(\beta)$ .

□

Possiamo quindi dimostrare la proposizione.

*Dimostrazione.*

□

### §10.1 Sottrazione e divisione euclidea

Introduciamo, ora, due lemmi che serviranno per calcolare la forma normale di Cantor: la sottrazione e la divisione di ordinali.

## 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.