

# **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>4</b>  |
| 1.1      | Digressione: insiemi numerabili . . . . .                | 7         |
| 1.2      | Tornando agli insiemi di unicità . . . . .               | 9         |
| 1.3      | Giochi di parole . . . . .                               | 11        |
| 1.4      | Scopi del corso . . . . .                                | 12        |
| <b>2</b> | <b>Il linguaggio della teoria degli insiemi</b>          | <b>13</b> |
| 2.1      | Le regole di inferenza . . . . .                         | 15        |
| <b>3</b> | <b>I primi assiomi</b>                                   | <b>17</b> |
| 3.1      | Assiomi dell'insieme vuoto e di estensionalità . . . . . | 17        |
| 3.2      | Assioma di separazione . . . . .                         | 18        |
| 3.3      | Classi e classi proprie . . . . .                        | 19        |
| 3.4      | Assioma del paio e coppia di Kuratowski . . . . .        | 20        |
| 3.5      | Assioma dell'unione e operazioni booleane . . . . .      | 23        |
| 3.6      | Assioma delle parti e prodotto cartesiano . . . . .      | 26        |
| 3.7      | Relazioni di equivalenza e di ordine, funzioni . . . . . | 28        |
| <b>4</b> | <b>Assioma dell'infinito e numeri naturali</b>           | <b>32</b> |
| 4.1      | Gli assiomi di Peano . . . . .                           | 34        |
| 4.2      | L'ordine di omega . . . . .                              | 36        |
| 4.3      | Induzione forte e principio del minimo . . . . .         | 39        |
| 4.4      | Ricorsione numerabile . . . . .                          | 41        |
| <b>5</b> | <b>Cardinalità</b>                                       | <b>49</b> |
| 5.1      | Teorema di Cantor-Bernstein . . . . .                    | 50        |
| 5.2      | Teorema di Cantor . . . . .                              | 53        |
| 5.3      | Operazioni fra cardinalità . . . . .                     | 53        |
| <b>6</b> | <b>Cardinalità finite</b>                                | <b>56</b> |
| 6.1      | Principio dei cassetti . . . . .                         | 56        |
| 6.2      | Operazioni fra le cardinalità finite . . . . .           | 59        |
| <b>7</b> | <b>La cardinalità del numerabile</b>                     | <b>60</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.

## Ringraziamenti

Francesco Sorce, Rubens Martino.

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.

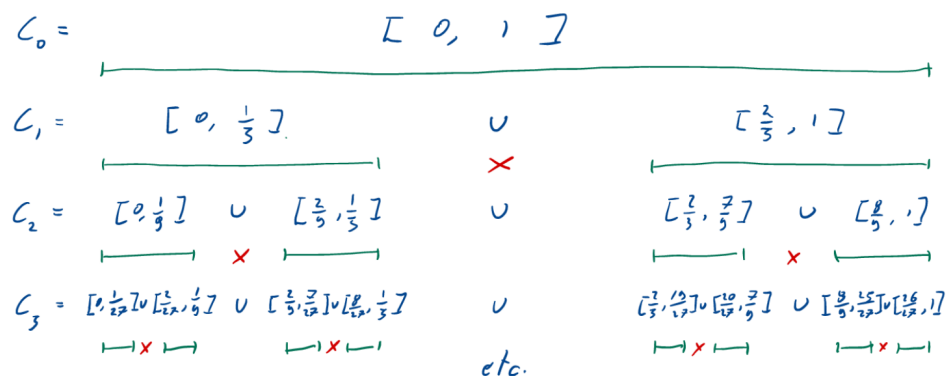
### NON Esempio 1.7

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.

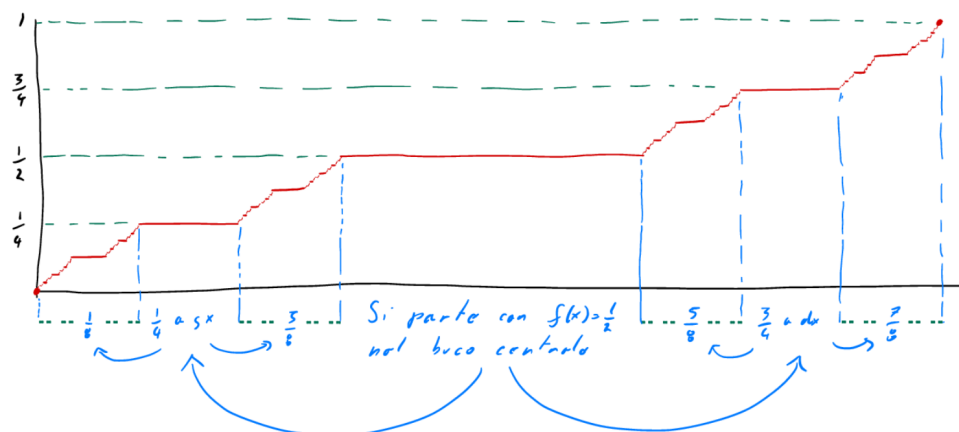
Possiamo costruire l'insieme di Cantor a partire dall'intervallo  $C_0 = [0, 1]$  nel seguente modo:



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  $x \in C$ .

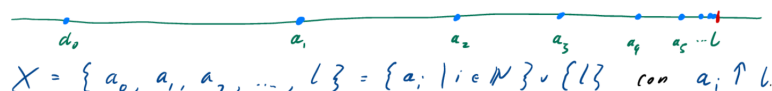


tale funzione si costruisce aggiungendo tratti costanti (prima  $\frac{1}{2}$ , poi  $\frac{1}{4}$ ,  $\frac{3}{4}$  e così via, dividendo l'intervallo  $[0, 1]$  sull'asse delle ordinate in parti uguali) alle parti eliminate sull'intervallo  $[0, 1]$  sull'asse delle ascisse per costruire l'insieme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

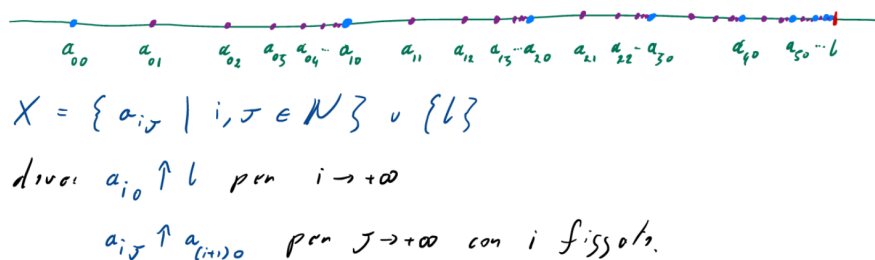


Dimostriamo quindi che  $X$  è un insieme di unicità.

*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,  $\mathbb{N} \times \mathbb{N} = \{(i, j) | i, j \in \mathbb{N}\}$ . Quindi  $X \times Y = \{(a_{i_t}, b_{j_t}) | t \in \mathbb{N}\}$ .  $\square$

### Esempio 1.17

$\mathbb{Q}$  è numerabile.

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

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

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

□

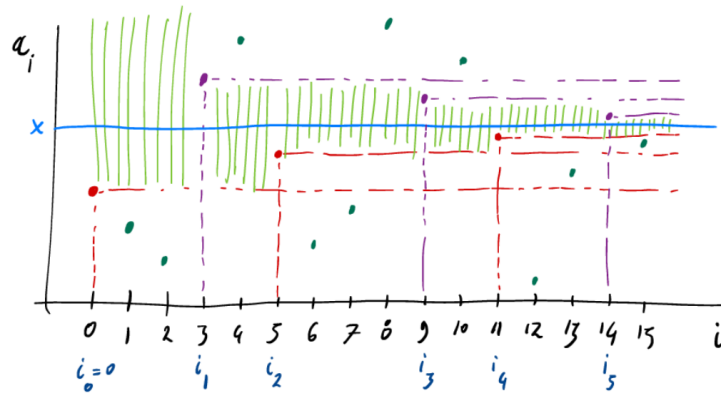
### NON Esempio 1.18

$\mathbb{R}$  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  $i \rightarrow \infty$ .

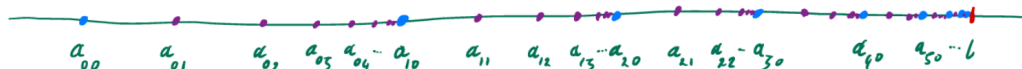
Tutti i punti sono isolati,  $X' = \emptyset$ .

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

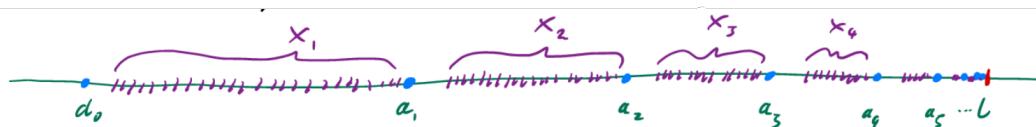


“Successione con punto limite”. Tutti i punti sono isolati salvo  $l$ , quindi  $X' = \{l\}$  e  $X'' = \emptyset$ .

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



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

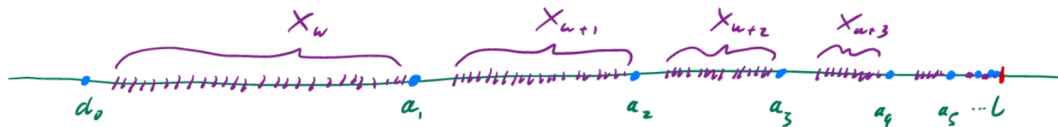
**Esercizio 1.26.** Perché  $X_\omega$  è numerabile?

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  $X_{\omega \cdot 2}$ ?



No: occorre un nuovo corollario.

### Corollario 1.28

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

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

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

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

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

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

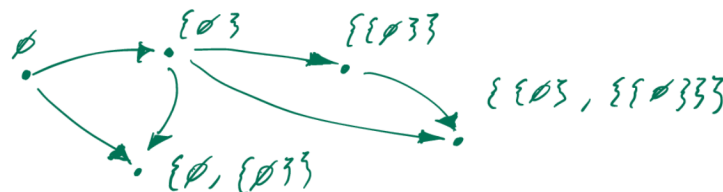
ad esempio:

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

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

**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:

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

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:

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

<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:

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

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.** Data  $g : A \rightarrow B$  e  $f : B \rightarrow C$ , sotto quali condizioni  $f \circ g$  è iniettiva, suriettiva, bigettiva?

*Soluzione.*

□

**Esercizio 3.73.** 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:

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

*Soluzione.*

□

**Esercizio 3.74.** Data una relazione di equivalenza  $\sim$  su  $A$  e  $f : A \rightarrow B$ , affinché esista  $\tilde{f} : A/\sim \rightarrow B$  tale che  $f = \tilde{f} \circ i_\sim$ , è necessario e sufficiente che  $\forall x, y \in A \quad x \sim y \rightarrow f(x) = f(y)$ .

*Soluzione.*

□

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

## §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:

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

Sceghlieremo, invece, quest'altra codifica:

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

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

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

L'ostacolo è ora parlare di questi oggetti in maniera precisa nel linguaggio della teoria degli insiemi. A dire il vero, potremmo già scrivere una formula  $\Phi(n)$  che dice " $n$  è un numero naturale" si tratta di un **esercizio** difficile, che sarà reso più facile da idee che vedremo più avanti. Noi non scriviamo questa formula, ma, anche a farlo, non potremmo comunque dimostrare che esiste un insieme i cui elementi sono i numeri naturali, questo perché gli assiomi visti finora non permettono di uscire dalla classe degli insiemi finiti (degli insiemi "ereditariamente finiti", ad essere precisi: definiremo questi concetto a tempo debito).

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

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

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

**Definizione 4.2** (Insiemi induttivi). Diciamo che  $A$  è un **insieme induttivo** se contiene  $\emptyset$  ed è chiuso per successori <sup>21</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>22</sup>

<sup>21</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>22</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:

$$\forall x(x \in \omega \leftrightarrow (\forall A \text{ "A è induttivo"} \rightarrow x \in A))^{23}$$

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:

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

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

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

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

Un esercizio un po' più difficile è esibire insiemi che non appartengono a  $\omega$ .

**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  $s(x) = s(\{\emptyset\}) = \{\emptyset\} \cup \{\{\emptyset\}\} =$

<sup>24</sup> $\{\emptyset, \{\emptyset\}\}$ , 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>25</sup>  $\square$

<sup>23</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>24</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>25</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>26</sup>. In questo senso<sup>27</sup>, quindi,  $\omega$  codifica legittimamente i numeri naturali.

**Definizione 4.8** (Assiomi di Peano al secondo ordine<sup>28</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>29</sup> soddisfa gli assiomi di Peano se:

(a) Il successore è iniettivo:

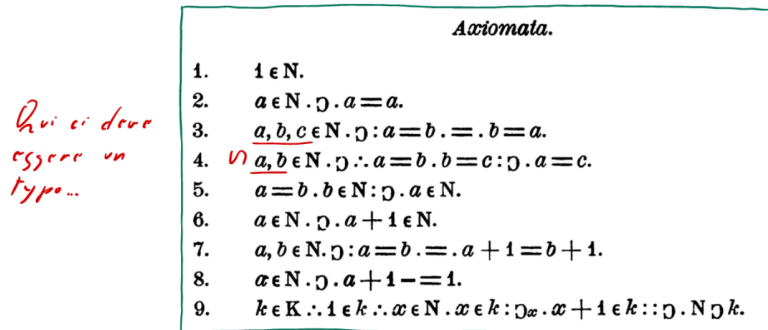
$$\forall n, m \in \mathbb{N} \text{ succ}(m) = \text{succ}(n) \rightarrow m = n$$
<sup>30</sup>

(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>26</sup>Cioè gli assiomi di Peano diventano enunciati dimostrabili all'interno della ZFC.

<sup>27</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>28</sup>qualunque cosa questo significhi...

<sup>29</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>30</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>31</sup>, quindi varrà che  $\forall n \in \omega \Phi(n)$ .

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

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

- (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  $\Phi(n) \stackrel{\text{def}}{=} \bigcup n \subseteq n$ .

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

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

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

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

<sup>31</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  $< \stackrel{\text{def}}{=} \{(m, n) \in \omega \times \omega \mid m \in n\}$ .

**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>32</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>32</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.  $\square$

**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  $s(m) \subseteq \omega$ .  $\square$

**Corollario 4.18** (Più piccolo = contenuto)

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

*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 a  $\leftarrow$ ):

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

( $n \notin n$  perché abbiamo dimostrato che  $<$  è di ordine stretto su  $\omega$ , quindi irreflessiva).  $\square$

### §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>33</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.

**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

<sup>33</sup>Stiamo solo giustificando formalmente il per ogni.



$x = n$  è già contemplato nell'osservazione dicendo che  $x \notin A$ ). Osserviamo che la contronominale della nostra tesi<sup>34</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>35</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  $a < b \stackrel{\text{def}}{=} a \in b$ .

*Soluzione.*  $\square$

## §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.

<sup>34</sup>Cioè di questo caso della dimostrazione come visto nell'osservazione.

<sup>35</sup>Cioè se vale il principio del minimo c(come vale in  $\omega$ ).

**Esempio 4.27** (Operazioni aritmetiche)

Possiamo definire somma e prodotto come:

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

anziché  $a + b = s(\underbrace{s(\dots a \dots)}_{b \text{ successori}})$  (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:

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

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

**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 ...).

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  $n$ :

$$F_n = F_{n-1} + F_{n-2}^{36}$$

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  $A \times B$ ).

*Dimostrazione.* Si osserva che:

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

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

<sup>36</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  $n$ .

**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  $\Phi$ :

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

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**:

$$f(x) = y \stackrel{\text{def}}{=} \Phi(x, y)^{37}$$

Occorre verificare che  $f$  soddisfa le condizioni della ricorsione.

<sup>37</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).

$f(\emptyset) = k$  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:

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

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:

$$f'(\emptyset) = k = f''(\emptyset) \quad f'(s(n)) = h(n, f'(n)) \stackrel{\text{Hp. indutt. } 38}{=} h(n, f''(n)) = f''(s(n))$$

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

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

#### Esempio 4.37 (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:

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

Scriviamo quindi:

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

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.

<sup>38</sup>E usando l'estensionalità per funzioni su  $h$ .

**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:

$$(i) \quad f(\emptyset) = 0.$$

$$(ii) \quad \forall n \in \omega \quad f(s(n)) = \text{succ}(f(n)).^a$$

<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) —  $\forall x \in \omega \quad x \neq 0 \rightarrow \exists y \in \omega \quad x = s(y)$ , 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  $\forall n \in \omega \quad f(s(n)) = \text{succ}(f(n))$ . 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  $\forall y \in \mathbb{N} \quad \exists x \in \omega \quad f(x) = y$ .

**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  $f(s(x)) = \text{succ}(n)$ .

**Inieltività** 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) (inieltività 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  $\nexists$

□

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:

$$f'(\emptyset) = \emptyset \quad f'(s(n)) = f'(n) \cup \{(n, h(f'(n)))\}^{39}$$

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

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:

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

<sup>39</sup>Esiste ed è unica per il primo teorema di ricorsione

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  $\cdot$ .



## §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:

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

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>40</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  $|B| = |A|$ .

<sup>40</sup>Tale relazione sarà anche una relazione di ordine tra cardinalità quando queste ultime saranno singoli oggetti della teoria.

Infine,  $|A| = |B| \iff \exists f : A \rightarrow B$  bigettiva,  $|B| = |C| \iff \exists g : B \rightarrow C$  bigettiva, ora è sufficiente osservare che  $g \circ f : A \rightarrow C$  è bigettiva in quanto composizione di funzioni bigettive<sup>41</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:

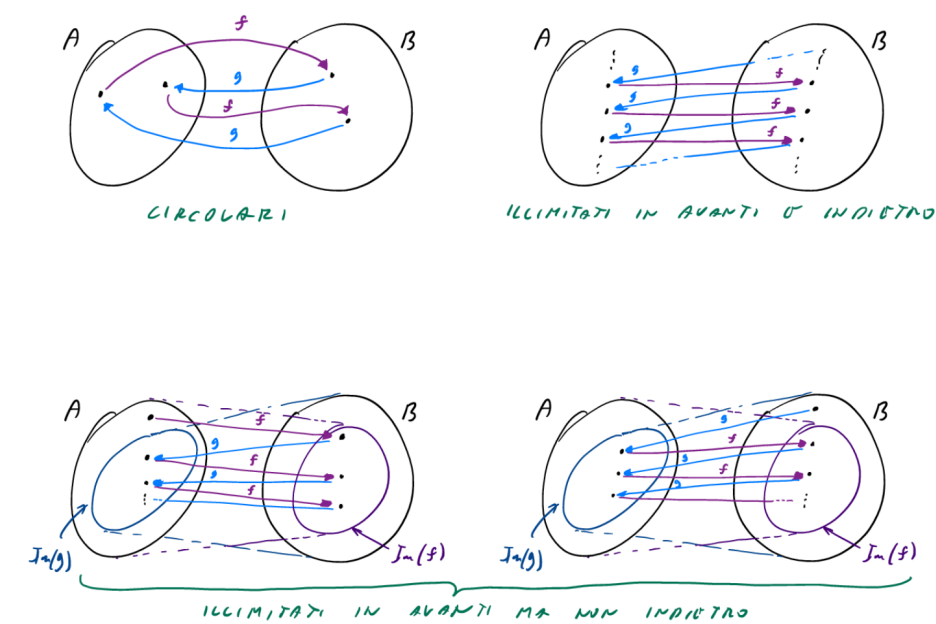
$$a \xrightarrow{f} f(a) \xrightarrow{g} g(f(a)) \xrightarrow{f} f(g(f(a))) \xrightarrow{g} \dots$$

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):

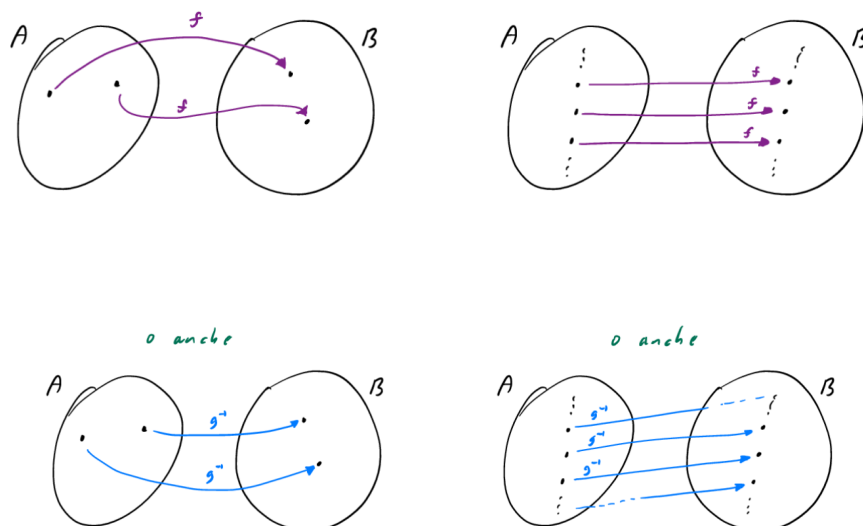
$$f^{-1}(g^{-1}(a)) \xrightarrow{f} g^{-1}(a) \xrightarrow{g} a \xrightarrow{f} f(a) \xrightarrow{g} g(f(a)) \xrightarrow{f} f(g(f(a))) \xrightarrow{g} \dots$$

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>41</sup>È una semplice verifica.

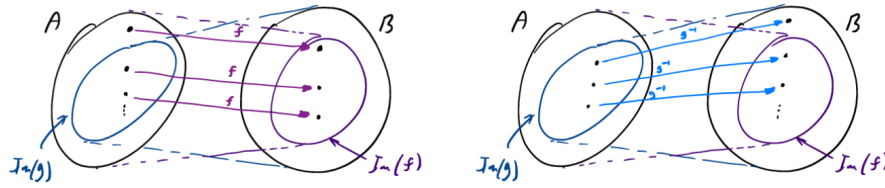


Per gli elementi che si trovano su un percorso circolare, o su un percorso illimitato avanti e indietro,  $f$  fornisce una bigezione, come la fornirebbe anche  $g^{-1}$  - la scelta è arbitraria a patto di usare la medesima funzione per l'intero percorso - nel modo seguente<sup>42</sup>:



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>42</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:

$$|A| < |B| \stackrel{\text{def}}{=} |A| \leq |B| \wedge |A| \neq |B| \quad ^{43}$$

## §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:

$$B = \{x \in A \mid x \notin f(x)\} \quad ^{44}$$

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>43</sup>Dove ricordiamo che  $|A| \neq |B| \stackrel{\text{def}}{=} \neg(|A| = |B|)$ .

<sup>44</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:

$$\tilde{f}(c, b) = \underbrace{(f(c))}_{\in {}^B A} \underbrace{(b)}_{\in B} \quad {}^{46}$$

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:

$$\bar{g}(c) : B \longrightarrow A : b \longmapsto g(c, b) \quad {}^{47}$$

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>46</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>47</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>48</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>49</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  $f(m) = m$ , 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>48</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.

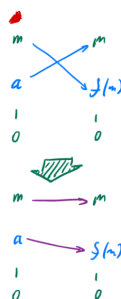
<sup>49</sup>È conseguenza del fatto che  $B$  sia un sottoinsieme proprio e che  $f$  è bigettiva.





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. □

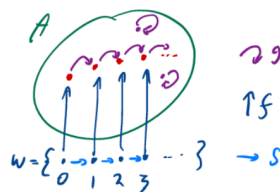
Se adesso volessimo dimostrare il viceversa: [che formulato in versione contronominale è] che un insieme infinito non è Dedekind-finito, quale sarebbe l'ostacolo? Abbiamo già osservato che  $\omega$  non è finito, perché la funzione successore stabilisce una corrispondenza biunivoca fra  $\omega$  e  $\omega \setminus \{0\} \subsetneq \omega$  (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  $A$  è in biezione con un suo sottoinsieme proprio.



□

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  $A \hookrightarrow B$ ) □

**Esercizio 6.8.** Dimostrare che:

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

## §6.2 Operazioni fra le cardinalità finite

### Proposizione 6.9

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.*

□

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

**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.

## §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 biezione 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 biezione 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.

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

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

**Definizione 7.5** (Isomorfismo). Due insiemi (parzialmente<sup>50</sup>) ordinati  $(A, <_A)$  e  $(B, <_B)$  sono **isomorfi**, in simboli  $(A, <_A) \sim (B, <_B)$  se esiste una biezione  $f : A \rightarrow B$  tale che:

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

**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:

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

**Esercizio 7.7.** Dimostrare la proposizione enunciata sopra.

<sup>50</sup>Dove parziale indica l'assenza della proprietà di totalità nella definizione di relazione d'ordine (stretta o larga che sia).

**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 indotto da  $\omega$ .

*Dimostrazione.*

□