

Elementi Di Teoria Degli Insiemi

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

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

Anno Accademico 2022-23

Indice

1	Prologo nel XIX secolo	4
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
2	Il linguaggio della teoria degli insiemi	13
2.1	Le regole di inferenza	15
3	I primi assiomi	17
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
4	Assioma dell'infinito e numeri naturali	34
4.1	Gli assiomi di Peano	36
4.2	L'ordine di omega	38
4.3	Induzione forte e principio del minimo	41
4.4	Ricorsione numerabile	43
5	Cardinalità	51
5.1	Teorema di Cantor-Bernstein	52
5.2	Teorema di Cantor	55
5.3	Operazioni fra cardinalità	55
6	Cardinalità finite	58
6.1	Principio dei cassetti	58
6.2	Operazioni fra le cardinalità finite	61
7	La cardinalità del numerabile	64
7.1	Insiemi numerabili in pratica	68
7.2	Prodotto di numerabili è numerabile	69
7.3	Numeri interi e razionali	70
7.4	Ordini densi numerabili	75
7.5	Il grafo random	78
8	\mathbb{R} e la cardinalità del continuo	80
8.1	Caratterizzazione dei reali come ordine	82
8.2	La cardinalità del continuo è 2^{\aleph_0}	83
8.3	Operazioni che coinvolgono la cardinalità del continuo	83
8.4	Sottrarre un numerabile dal continuo	84
	Stato del corso	85
9	I buoni ordinamenti	86

Premessa

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

Ringraziamenti

Francesco Sorce, Rubens Martino, Lorenzo Picinelli.

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



§1 Prologo nel XIX secolo

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

Problema 1.1. Data una serie trigonometrica:

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

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

Risolto positivamente da **Georg Cantor** nel 1870.

Definizione 1.2. Diciamo che $X \subseteq \mathbb{R}$ è un **insieme di unicità** se, per ogni serie trigonometrica:

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

vale la seguente implicazione:

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

Esempio 1.3

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

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

Fatto 1.5

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

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

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

^bOvvero f non ha punti angolosi.

Esempio 1.6

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

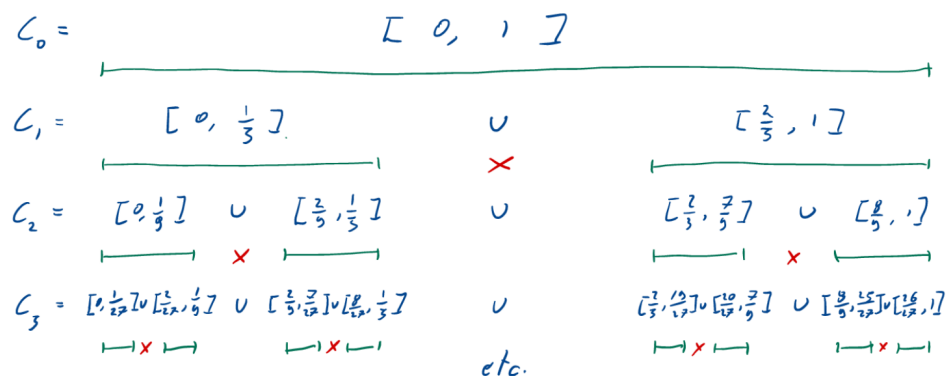
NON Esempio 1.7

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

NON Esempio buffo 1.8

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

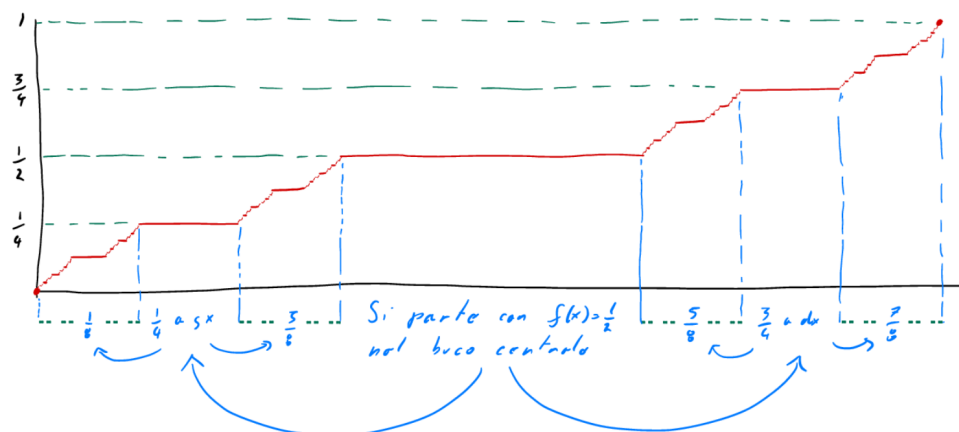
Possiamo costruire l'insieme di Cantor a partire dall'intervallo $C_0 = [0, 1]$ nel seguente modo:



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

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

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

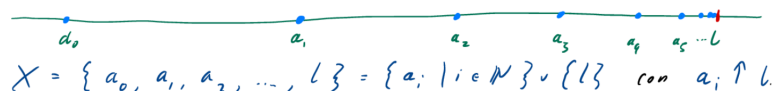


tale funzione si costruisce aggiungendo tratti costanti (prima $\frac{1}{2}$, poi $\frac{1}{4}$, $\frac{3}{4}$ e così via, dividendo l'intervallo $[0, 1]$ sull'asse delle ordinate in parti uguali) alle parti eliminate sull'intervallo $[0, 1]$ sull'asse delle ascisse per costruire l'insieme di Cantor.

Nota 1.9 — Per \mathbb{Q} e \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.

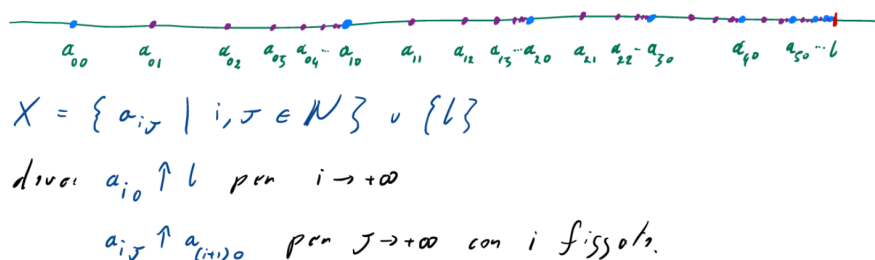


Dimostriamo quindi che X è un insieme di unicità.

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

§1.1 Digressione: insiemi numerabili

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

Esempio 1.13

Alcuni esempi di insiemi numerabili sono:

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

Esempio meno immediato 1.14

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

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

Proposizione 1.15

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

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

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

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

Proposizione 1.16

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

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

Esempio 1.17

\mathbb{Q} è numerabile.

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

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

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

□

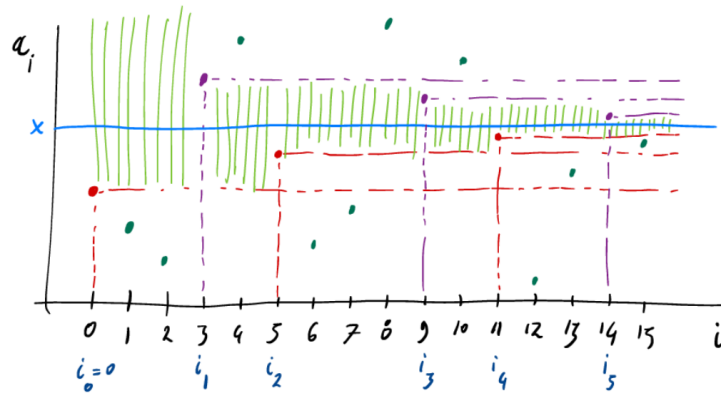
NON Esempio 1.18

\mathbb{R} non è numerabile.

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

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

graficamente:



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

Esercizio 1.19. Completare la dimostrazione nel caso $n < i$.

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

□

²num. = numeratore, den. = denominatore.

§1.2 Tornando agli insiemi di unicità

Teorema 1.21 (Cantor-Lebesgue)

Se $X \subseteq \mathbb{R}$ è chiuso e numerabile, allora X soddisfa il [Fatto 1.5](#), ed è, quindi, di unicità.

La strategia di dimostrazione passa attraverso una definizione.

Definizione 1.22. Dato $X \subseteq \mathbb{R}$, il **derivato di Cantor-Bendixson** di X è:

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

(dove $a \in X$ è un **punto di accumulazione** se $\exists \varepsilon > 0 :]a - \varepsilon, a + \varepsilon[\cap X = \{a\}$).

Osservazione 1.23 — Se X è chiuso e per X' vale il [Fatto 1.5](#), allora anche per X vale il [Fatto 1.5](#).

Dimostriamo questo fatto.

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

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

Corollario 1.24

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

^a n volte.


Dimostrazione. Induzione su n . \square

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

Esempio 1.25

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

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



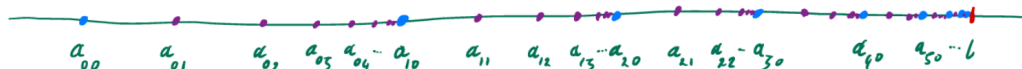
Tutti i punti sono isolati, $X' = \emptyset$.

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

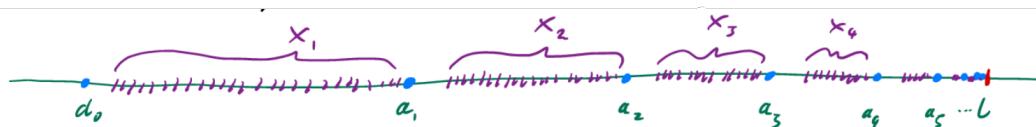


“Successione con punto limite”. Tutti i punti sono isolati salvo l , quindi $X' = \{l\}$ e $X'' = \emptyset$.

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



“Successione di successioni”, $X' = \{a_{10}, a_{20}, \dots, l\}$, $X'' = \{l\}$ e $X''' = \emptyset$.
Si vede che possiamo proseguire, in qualche modo, costruendo una successione di successioni di successioni, etc. n volte, X_n . Avremo $X_n^{(n)} \neq \emptyset$, $X_n^{(n+1)} = \emptyset$. Ora costruiamo X_ω fatto così:



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

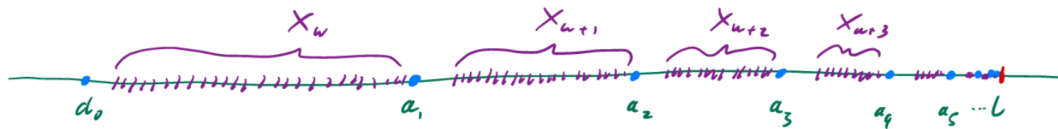
Esercizio 1.26. Perché X_ω è numerabile?

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

Corollario 1.27

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

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



No: occorre un nuovo corollario.

Corollario 1.28

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

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

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

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

No, ogni sforzo di trovare l’induzione a capo delle induzioni è vano. Se ho $X_\omega, X_{\omega^\omega}, X_{\omega^{\omega^\omega}}$, etc., allora, ecco che faccio una successione con queste cose, la battezzo in qualche modo - ad esempio, X_{ε_0} - e si riparte!

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

Esercizio 1.29 (per la fine del corso). Dimostrare il teorema di [Cantor-Lebesgue](#).

§1.3 Giochi di parole

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

Paradosso di Russell

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

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

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

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

Paradosso di Berry

L’italiano annovera un numero finito di parole, è quindi possibile formare solo un numero finito di frasi di meno di cento parole. Alcune di queste descrivono un numero naturale,

altre no. Comunque, solo un numero finito di numeri naturali può essere descritto con meno di cento parole. Per il principio del minimo, esiste:

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

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

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

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

§1.4 Scopi del corso

Questo corso persegue due obiettivi:

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

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

§2 Il linguaggio della teoria degli insiemi

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

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

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

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

- Le formule atomiche si combinano tra loro mediante:
 - connettivi logici** ovvero il “non” la “e” e la “o” (inclusiva):

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

quindi ad esempio:

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

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

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

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

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

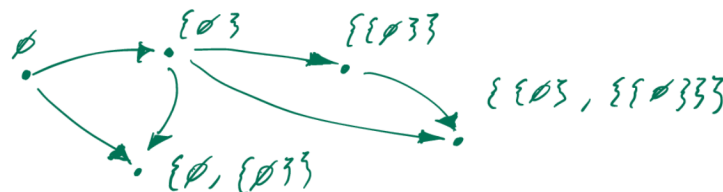
ad esempio:

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

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

Esercizio 2.1. Chiaramente varranno $\forall x x = x$, $\forall x \exists y x = y$, $\neg(\exists x \forall y x = y)$.

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



³ “appartiene a”.

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

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

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

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

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

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

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

Parentesi Ad essere precisi, avremmo dovuto definire le formule includendo un mucchio di parentesi, allo scopo di eliminare ogni possibilità di formare una combinazione di simboli ambigua. Per esempio $\Phi_1 \wedge \Phi_2 \vee \Phi_3$ è ambigua, perché si potrebbe leggere $(\Phi_1 \wedge \Phi_2) \vee \Phi_3$ o $\Phi_1 \wedge (\Phi_2 \vee \Phi_3)$. In una notazione completamente parentesizzata, per esempio, la formula per “ a è un sottoinsieme di b ” sarebbe:

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

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

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

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

Nota 2.2 — Il fatto che possiamo dire $C = A \cup B$ o $C = A \cap B$ non significa né che questi oggetti esistano né che siano unici. Dimostreremo fra poco l’esistenza e unicità di unione e intersezione.

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

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

Esercizio 2.3. Esprimi queste proposizioni mediante formule insiemistiche pure:

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

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

§2.1 Le regole di inferenza

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

- 1 Sono argomento del corso di logica.
- 2 In realtà, scrivere le dimostrazioni in maniera formale, le renderebbe lunghissime e particolarmente incomprensibili.
- 3 In pratica, non si sbaglia facendo ragionamenti che non reggono, si sbaglia dicendo cose fumose che non possono essere espresse nel linguaggio della teoria. Per esempio, le parole “e così via” sono pericolose.
- 4 Conoscere le regole - fidatevi - non aiuta né a trovare né a capire le dimostrazioni.

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

Tavole di verità Due combinazioni mediante connettivi logici (\neg , \wedge , \vee , \rightarrow , \leftrightarrow) delle stesse formule - “**combinazioni booleane**” - alle volte, dicono la stessa cosa. Per esempio, $\neg\Phi \vee \neg\psi \equiv \neg(\Phi \wedge \psi)$. Per verificare questo fatto basta considerare tutte le possibili combinazioni di valori di verità che possono assumere le formule combinate - nell'esempio Φ e ψ - compilando una “**tabella di verità**”.

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

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

Conviene tenere a mente alcune delle equivalenze elementari:

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

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

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

⁶ “equivale a”.

⁷ Leggi di De Morgan.

Esercizio 2.4. Dimostrare le equivalenze delle formule elencate sopra.

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

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

Esercizio 2.5. Convinciti della validità delle equivalenze precedenti.

Esercizio 2.6. Dimostra che:

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

Esercizio 2.7. Dimostra che:

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

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

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

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

§3 I primi assiomi

§3.1 Assiomi dell'insieme vuoto e di estensionalità

Assioma 3.1 (Assioma dell'insieme vuoto)

Esiste un insieme vuoto.

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

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

Assioma 3.3 (Assioma di estensionalità)

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

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

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

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

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

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

Proposizione 3.5 (Unicità dell'insieme vuoto)

C'è un unico insieme vuoto.

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

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

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

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

Dimostrazione formale. Questo livello di pedanteria non è necessario, ma, per una volta, proviamo a dimostrare in ogni dettaglio la formula $\exists! x (\forall y (y \notin x))$. Per definizione di $\exists!$, ciò equivale a:

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

Per l'**assioma del vuoto**, $\exists x_1 \forall y y \notin x_1$: fissiamo questo x_1 . Resta da dimostrare che:

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

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

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

Ora prendiamo un x_2 qualunque, dobbiamo dimostrare:

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

Si danno due casi: o $\forall y (y \notin x_2)$ è vera o è falsa. Nel secondo caso, l'implicazione è vera per via della tabella di verità. Nel primo abbiamo sia $\forall y y \notin x_1$, [vera] per costruzione, sia $\forall y y \notin x_2$, [vera] per ipotesi. Quindi, preso un qualunque y , $y \in x_1$ e $y \in x_2$ sono entrambe false. La tabella di verità di \leftrightarrow ci dice quindi che vale $y \in x_1 \leftrightarrow y \in x_2$, e, per l'arbitrarietà di y :

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

Dall'**assioma di estensionalità**:

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

Abbiamo quindi $x_1 = x_2$, da cui segue la verità dell'implicazione iniziale. \square

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

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

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

§3.2 Assioma di separazione

Assioma 3.7 (Assioma di separazione)

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

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

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

Nota 3.8 — Tecnicamente l'assioma di separazione è uno **schema di assiomi**, ossia una regola che, per ogni possibile formula ψ , ci permette di scrivere un assioma.

Proposizione 3.9

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

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

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

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

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

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

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

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

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

Proposizione 3.12 (Insieme di tutti gli insiemi)

Non esiste l'insieme di tutti gli insiemi.

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

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

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

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

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

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

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

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

§3.3 Classi e classi proprie

Sebbene, abbiamo detto che gli unici oggetti della teoria degli insiemi sono gli insiemi, usualmente ci si riferisce alla collezione di tutti gli insiemi che soddisfano una certa formula come ad una specie di insieme: una [classe](#). Più precisamente, data una formula $\psi(x)$, se diciamo: “sia C la classe degli insiemi x tali che $\psi(x)$ ” intendiamo dire che useremo la scrittura $x \in C$ come una semplice abbreviazione per la formula $\psi(x)$.⁹

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

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

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

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

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

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

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

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

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

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

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

che equivale $A = B$ per **estensionalità**. Ha quindi senso, con un leggero abuso di notazione, omettere il cappelletto $\hat{}$ e “identificare” la classe \hat{A} semplicemente con A . In questo senso, abbiamo classi che sono insiemi - formalmente C è un insieme se $C = \hat{A}$ per qualche insieme A - e classi che non sono insiemi. Chiamiamo **classe propria** una classe che non è un insieme.¹¹

Esempio 3.15

V è una classe propria.

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

§3.4 Assioma del paio e coppia di Kuratowski

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

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

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

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

Assioma 3.16 (Assioma del paio)

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

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

Proposizione 3.17 (Unicità del paio)

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

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

Esercizio 3.18. Dimostra la proposizione precedente.

Soluzione. Supponiamo che esistano P_1 e P_2 tali che:

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

da ciò segue che:

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

dunque per [estensionalità](#) l'espressione sopra equivale a $P_1 = P_2$. \square

Proposizione 3.19 (Esistenza dei singoletti)

Dato a , esiste ed è unico $\{a\}$.

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

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

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

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

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

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

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

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

Dimostrazione. Segue dal fatto che \vee è commutativo:

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

quindi per [estensionalità](#) $\{a, b\} = \{b, a\}$. \square

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

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

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

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

Proposizione 3.23 (Proprietà di coppia ordinata)

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

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

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

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

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

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

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

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

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

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

in tal modo abbiamo che:

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

Possiamo quindi ricavare la tesi come segue:

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

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

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

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

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

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

Nota 3.25 — Quest'ultima definizione è, in realtà, uno schema di definizioni: una per ogni n . Per ora, **NON** siamo in grado di scrivere, per esempio, una formula insiemistica che dica “Esiste un n ed una n -upla (a_1, \dots, a_n) tale che...”. Però, per ogni n dato, chissà 92, possiamo scrivere esplicitamente una formula che dice $x = (a_1, a_2, a_3, \dots, a_{92})$.

Proposizione 3.26 (Proprietà di n -upla ordinata)

Si ha che:

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

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

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

§3.5 Assioma dell'unione e operazioni booleane

Assioma 3.28 (Assioma dell'unione)

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

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

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

Proposizione 3.29 (Unicità dell'unione)

Vale l'unicità dell'unione:

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

Dimostrazione. Supponiamo di avere B_1 e B_2 tali che:

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

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

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

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

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

^a “Unione di A ”.

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

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

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

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

Definizione 3.32 (Unione di insiemi). Poniamo:

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

Proposizione 3.33 (Caratterizzazione unione di insiemi)

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

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

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

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

Definizione 3.34 (Intersezione di un insieme). Sia C una **classe**¹⁵ non vuota. L'**insieme** B è l'**intersezione** di C se:

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

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

Proposizione 3.35 (Esistenza e unicità dell'intersezione)

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

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

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

Dimostrazione. L'unicità segue per **estensionalità** al solito modo. Veniamo all'esistenza. Dal momento che C non è vuota [per ipotesi], possiamo prendere $z \in C$. Ora consideriamo (un sottoinsieme di B ottenuto per **separazione** nel modo seguente):

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

¹⁵Quindi, in particolare, C può essere un insieme (in questo caso la definizione è comunque lecita in generale con le classi, i cui elementi sono appunto insiemi).

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

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

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

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

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

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

Proposizione 3.38 (Caratterizzazione intersezione e differenza di insiemi)

Vale che:

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

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

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

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

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

Dimostrazione. Tutte queste proprietà si deducono immediatamente dalle corrispondenti proprietà dei connettivi logici, le quali, a loro volta, si vedono con le tabelle di verità. Per

esempio, dimostriamo la prima delle leggi di De Morgan (facendo uso della corrispondente legge per i connettivi logici):

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

□

Ora possiamo costruire insiemi finiti elencandone gli elementi, come si fa di solito, con la notazione $\{\dots\}$ ¹⁶.

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

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

Proposizione 3.42 (Caratterizzazione di insieme con n elementi)

Vale che:

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

Esercizio 3.43. Dimostrare la proposizione precedente.

§3.6 Assioma delle parti e prodotto cartesiano

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

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

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

Assioma 3.44 (Assioma delle parti)

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

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

¹⁶Paradossalmente prima di aggiungere l'assioma dell'unione alla teoria potevamo costruire n -uple ordinate di lunghezza arbitraria, ma non un insieme con più di due elementi.

Proposizione 3.45 (Unicità delle parti)

Vale che:

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

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

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

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

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

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

Proposizione 3.47 (Esistenza ed unicità del prodotto cartesiano)

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

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

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

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

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

così come scritto, siamo sicuri che è un insieme che contiene coppie ordinate di elementi di A e B , tuttavia dobbiamo dimostrare anche che ogni coppia (x, y) con $x \in A$ e $y \in B$ appartiene a questo insieme. Per fare ciò bisogna dimostrare che tutte queste coppie appartengono a $\mathcal{P}(\mathcal{P}(A \cup B))$:^{17 18}

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

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

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

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

¹⁸Tutte le implicazioni si basano sul fatto che se un oggetto è sottoinsieme di un qualche insieme allora è un elemento del corrispondente insieme delle parti per definizione.

§3.7 Relazioni di equivalenza e di ordine, funzioni

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

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

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

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

Esempio 3.51

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

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

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

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

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

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

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

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

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

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

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

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

Proposizione 3.56 (Corrispondenza tra ordini stretti e larghi)

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

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

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

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

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

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

^bCome la nota sopra.

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

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

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

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

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

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

Esercizio 3.59. Formula la definizione precedente per ordini stretti.

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

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

o anche semplicemente:

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

E per quanto detto possiamo anche pensare che:

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

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

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

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

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

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

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

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

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

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

Definizione 3.63 (Funzione). Chiamiamo **funzione** $f : A \rightarrow B$ una relazione $f \subseteq A \times B$ tale che:

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

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

Notazione 3.64 (Immagine e immagine di un sottoinsieme) — Data una funzione f possiamo indicare la coppia $(x, y) \in f$ con la seguente abbreviazione:

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

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

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

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

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

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

bigettiva se: è sia iniettiva sia surgettiva.

Definizione 3.66 (Funzione inversa). Data f iniettiva:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

assurdo, pertanto $x = y$ ²¹. Se $g \circ f$ è surgettiva, allora g è surgettiva, infatti, per ipotesi, $\forall z \in C \exists x \in A g(f(x)) = z$, e, dato che $f(x) \in B$, abbiamo trovato che per ogni $z \in C$ esiste $y = f(x) \in B$ tale che $g(y) = z$, ovvero g surgettiva.

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

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

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

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

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

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

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

Osserviamo che per ogni $B, C \in A/\sim$, vale che $B \cap C \neq \emptyset \iff B = C$, infatti, se esiste $x \in B \cap C$, allora $x \sim y, \forall y \in B$, e $x \sim z, \forall z \in C$. Da cui $w \in B \iff w \sim x \iff w \in C$ e quindi per l'arbitrarietà di x , vale $B = C$.²²

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

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

Soluzione. Osserviamo che²³ $f(x) = (\tilde{f} \circ i_\sim)(x), \forall x \in A$ se e solo se $f(x) = \tilde{f}(i_\sim(x))$, ora ciò equivale al fatto che l'immagine dell'elemento $x \in A$ al LHS è uguale a quella

²¹Abbiamo dimostrato per assurdo che $f(x) = f(y) \implies x = y$ (sotto l'ipotesi che $g \circ f$ iniettiva), il viceversa è banale e con questo si ha l'equivalenza con la definizione di f iniettiva

²²Essendo che ogni elemento, per quanto detto è in una classe di equivalenza di A/\sim , si ha anche che $\bigcup A/\sim = A$, dunque le classi di equivalenza sono disgiunte e la loro unione dà proprio l'insieme, pertanto si dirà che formano una **partizione** dell'insieme A .

²³Per essere formalissimi, staremmo usando che $f = \tilde{f} \circ i_\sim \iff f(x) = (\tilde{f} \circ i_\sim)(x), \forall x \in A$, ovvero l'estensionalità per funzioni vista in un'osservazione precedente.

della classe di equivalenza (che è un sottoinsieme di A) $i_{\sim}(x)$ tramite \tilde{f} al RHS. Per rispettare la relazione richiesta (che sarebbe poi la commutatività di un diagramma) possiamo definire $\tilde{f}(C)$, $C \in A/\sim$, come $f(z)$ per un qualunque $z \in C$.

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

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

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

§4 Assioma dell'infinito e numeri naturali

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

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

Sceglieremo, invece, quest'altra codifica:

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

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

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

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

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

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

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

Definizione 4.2 (Insiemi induttivi). Diciamo che A è un **insieme induttivo** se contiene \emptyset ed è chiuso per successori ²⁴, ossia:

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

Assioma 4.3 (Assioma dell'infinito)

Esiste un insieme induttivo.

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

Finalmente definiamo l'insieme dei numeri naturali - che, per qualche buffa ragione, chiamiamo ω - come l'intersezione della classe, non vuota per l'assioma dell'infinito, di tutti gli insiemi induttivi. ²⁵

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

²⁵Aver introdotto l'assioma dell'infinito ci assicura che tale intersezione è non vuota, e ciò basta affinché ω sia un insieme (in caso contrario avremmo avuto l'intersezione del vuoto, che, come visto, non è un insieme).

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

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

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

Definizione 4.5 (Codifica dei numeri naturali). Definiamo:

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

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

Soluzione. Avendo definito ω come:

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

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

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

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

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

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

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

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

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

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

Avendo dimostrato che $\{\{\emptyset\}\}$ non è né un successore né (ovviamente) il vuoto, ci basta mostrare che non appartiene ad un insieme induttivo A che non ha altri elementi (oltre a \emptyset) che non sono successori. Dando per buono che ω non contenga elementi che non sono successori, si ottiene che $\{\{\emptyset\}\} \notin \omega$.²⁸ \square

²⁶Cioè x è in ω se e solo se è elemento di qualsiasi insieme induttivo (nella classe degli insiemi induttivi), e, inoltre, essendo l'intersezione di una classe, è in particolare un insieme (perché per definizione stiamo intersecando gli elementi di una classe, che sono insiemi).

²⁷Volendo essere pignoli possiamo usare la definizione dell'unione come il prendere gli elementi degli elementi: $\{\emptyset\} \cup \{\{\emptyset\}\} = \bigcup \{\{\emptyset\}, \{\{\emptyset\}\}\}$, e l'unione di tale insieme è formata appunto da tutti gli elementi degli elementi (quindi naturalmente il vuoto \emptyset e anche $\{\emptyset\}$).

²⁸Non abbiamo usato l'hint di Mamino e abbiamo usato un fatto non dimostrato.

§4.1 Gli assiomi di Peano

Per convincerci, però, che ω è, a buon diritto, l'insieme dei numeri naturali, serve qualcosa di più. Classicamente, i numeri naturali si definiscono per mezzo degli **assiomi di Peano**. Questi assiomi, che caratterizzano a meno di isomorfismi l'insieme \mathbb{N} dotato della funzione di successore, **per noi diventano dei teoremi** che dimostreremo a proposito dell'insieme ω ²⁹. In questo senso³⁰, quindi, ω codifica legittimamente i numeri naturali.

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

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

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

(a) Il successore è iniettivo:

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

(b) Lo zero non è un successore:

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

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

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

Axiomata.

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

Qui ci deve essere un typo...

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

Teorema 4.9 (ω soddisfa gli assiomi di Peano)

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

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

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

³¹qualunque cosa questo significhi...

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

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

Dimostrazione. Per controllare che succ sia ben definita, occorre assicurarsi che se $n \in \omega$, allora $\text{succ}(n) = s(n) \in \omega$. Fissiamo $n \in \omega$ e consideriamo un qualunque insieme induttivo A . Siccome A è induttivo $\omega \subseteq A$, quindi $n \in A$, e, di conseguenza $s(n) \in A$. Per l'arbitrarietà di A , allora, $s(n)$ appartiene a ogni insieme induttivo (quindi all'intersezione, ovvero ω).

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

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

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

contro la definizione di \emptyset .

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

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

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

- (a) La dimostrazione passa attraverso due lemmi.

Lemma 4.10 (Lemma 1)

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

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

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

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

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

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

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

Lemma 4.11 (Lemma 2)

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

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

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

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

Finalmente abbiamo che, per il Lemma 2:

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

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

§4.2 L'ordine di omega

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

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

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

^aPer essere precisi non stiamo usando \in come una relazione (visto che abbiamo assunto all'inizio che fosse un simbolo del linguaggio della teoria degli insiemi), ma stiamo definendo $< \stackrel{\text{def}}{=} \{(m, n) \in \omega \times \omega \mid m \in n\}$.

Proposizione 4.13 (Ordinamento totale di ω)

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

Per dimostrare questa proposizione, sono comodi alcuni lemmi.

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

- (1) $m \in n \rightarrow m \in s(n)$, infatti $n \subseteq n \cup \{n\} = s(n)$ (banalmente se m è contenuto in n allora è contenuto anche nel suo successore).
- (2) $m \in s(n) \rightarrow (m \in n \vee m = n)$, cioè se m è nel successore di n , allora è n stesso o un suo elemento, infatti:

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

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

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

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

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

Dimostrazione. Procediamo per induzione su b .

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

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

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

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

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

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

□

Possiamo ora dimostrare la proposizione iniziale.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

caso $a = 0$ La tesi diventa $\forall b \in \omega (\emptyset \in b) \vee (\emptyset = b) \vee (b \in \emptyset)$ ³⁵. Procediamo quindi per induzione su b :

* **caso $b = 0$** La tesi diventa $(\emptyset \in \emptyset) \vee (\emptyset = \emptyset)$, dove naturalmente la prima affermazione è sempre falsa, mentre la seconda è sempre vera, dunque la tesi è vera.

* **caso $b = s(m)$** La tesi è $(\emptyset \in s(m)) \vee (\emptyset = s(m))$, con ipotesi induttiva $(\emptyset \in m) \vee (\emptyset = m)$. Abbiamo quindi due casi in base all'ipotesi induttiva:

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

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

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

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

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

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

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

³⁵Ovviamente quest'ultimo caso è sempre falso e quindi può essere escluso.

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

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

Corollario 4.17 (Rappresentazione dei numeri naturali)

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

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

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

Corollario 4.18 (Più piccolo = contenuto)

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

Dimostrazione. Siccome ω è totalmente ordinato, si danno due casi (nel primo dimostro \rightarrow , nel secondo dimostro che la negazione della premessa implica la negazione della conseguenza, che è equivalente 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 ω , 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 Φ del numero precedente. Qui, invece, possiamo far conto di sapere Φ , non solo per il precedente, ma per tutti i numeri minori di n .

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

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

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

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

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

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

- Nel caso $x < n$ abbiamo $\Phi(x)$ per ipotesi induttiva.
- Nel caso $x = n$, l’ipotesi induttiva, combinata con l’antecedente ci dà $\Phi(n)$, ossia $\Phi(x)$ (perché abbiamo che $\forall x < n \Phi(x) \rightarrow \Phi(n)$, ma tutta l’espressione è vera per ipotesi e per ipotesi induttiva l’antecedente è vero, quindi anche $\Phi(n)$ lo è). (Per l’arbitrarietà di $x < m$ abbiamo dimostrato $\forall x < m \Phi(x)$)³⁶.

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

Teorema 4.21 (Principio del minimo)

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

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

³⁶Stiamo solo giustificando formalmente il per ogni.

$x = n$ è già contemplato nell'osservazione dicendo che $x \notin A$). Osserviamo che la contronominale della nostra tesi³⁷ 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.³⁸

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

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

Esempio 4.25

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

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

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

Soluzione. \square

§4.4 Ricorsione numerabile

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

³⁷Cioè di questo caso della dimostrazione come visto nell'osservazione.

³⁸Cioè se vale il principio del minimo c(ome vale in ω).

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** ω - sono definite nella maniera più naturale proprio per ricorsione.

Esempio 4.30 (Esempio di applicazione della ricorsione)

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

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

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

$$F_n = F_{n-1} + F_{n-2}^{39}$$

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:

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

^a k sarà il caso base della ricorsione.

Esempio 4.34 (Potenza e fattoriale con la ricorsione numerabile)

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

³⁹Cioè 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, cioè 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 ω ad A) usando la formula Φ .

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

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

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

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

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

Dimostrazione. Induzione su x .

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

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

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

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

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

□

Stabilito il lemma, introdurremo la formula Φ :

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

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**:

$$f(x) = y \stackrel{\text{def}}{=} \Phi(x, y)^{40}$$

Occorre verificare che f soddisfa le condizioni della ricorsione.

⁴⁰Formalmente $f = \{(x, y) \in \omega \times A \mid \Phi(x, y)\} = \{(x, y) \in \omega \times A \mid \exists! g \in {}^{s(x)}A \text{ “} g \text{ è una } x\text{-approssimazione”} \wedge g(x) = y\}$, 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 ω è $\{(0, k)\}$ (cioè soddisfa semplicemente il caso base), quindi $f(\emptyset) = g(\emptyset) = k$.

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

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

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:

$$f'(\emptyset) = k = f''(\emptyset) \quad f'(s(n)) = h(n, f'(n)) \stackrel{\text{Hp. indutt. } 41}{=} h(n, f''(n)) = f''(s(n))$$

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 ω è a buon diritto, l'insieme dei numeri naturali.

⁴¹E 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 (ω, \emptyset, s) sono strutture isomorfe - **ossia, formalmente, esiste: $f : \omega \rightarrow \mathbb{N}$ bigettiva** tale che:

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

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

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

Fa comodo isolare la seguente osservazione.

Osservazione 4.39 (Ogni numero in $\omega \setminus \emptyset$ è successore) — $\forall x \in \omega \quad x \neq 0 \rightarrow \exists y \in \omega \quad x = s(y)$, 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 ω a $\omega \times \omega$. È comodo, però, disporre di una versione più versatile del teorema di ricorsione numerabile.

Teorema 4.40 (Ricorsione numerabile - seconda forma)

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

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

^aCioè è un numero di ω .

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

Esempio 4.41 (Esempio di applicazione)

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

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

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

$$f'(\emptyset) = \emptyset \quad f'(s(n)) = f'(n) \cup \{(n, h(f'(n)))\}^{42}$$

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

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:

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

⁴²Esiste 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:

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

ossia $\exists f \in {}^A B$ “ f è iniettiva” (la definizione ci dice proprio che esiste un sottoinsieme di B che è in bigezione con A , e per definizione di iniettività, si ha proprio che $A \hookrightarrow B$)⁴³.

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

- La scrittura $|A| = |B|$ suggerisce che esistono insiemi - o oggetti di qualche genere - denotati $|A|$ e $|B|$ di cui si predica l'uguaglianza. Effettivamente costruiamo questi oggetti, ma, per ora, la scrittura $|A| = |B|$ è inscindibile, come $\clubsuit[A, B]$ (nel senso che per ora è solo un'abbreviazione per dire bigezione, pertanto non possiamo separare quei simboli o farci qualcosa).
- Potrebbe sorgere il sospetto che se $|A| < |B|$ quando $A \subsetneq B$, ma non è così, come mostra l'esempio di $A = \{x \in \omega \mid x > 0\}$ e $B = \omega$, infatti $A \subsetneq B$, ma $|A| = |B|$.

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

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

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

Esercizio 5.4. Dimostrare l'osservazione.

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

⁴³Tale relazione sarà anche una relazione di ordine tra cardinalità quando queste ultime saranno singoli oggetti della teoria.

è sufficiente osservare che $g \circ f : A \rightarrow C$ è bigettiva in quanto composizione di funzioni bigettive⁴⁴, per avere $|A| = |C|$. \square

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

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

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

Esercizio 5.6. Dimostrare l'osservazione.

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

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

§5.1 Teorema di Cantor-Bernstein

Teorema 5.7 (Cantor-Bernstein)

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

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

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

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

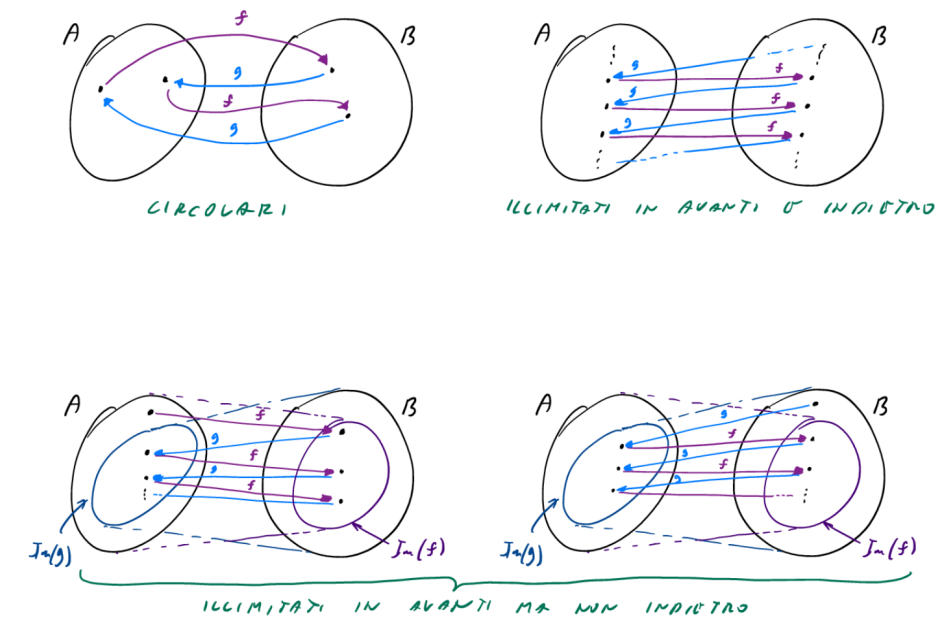
$$a \xrightarrow{f} f(a) \xrightarrow{g} g(f(a)) \xrightarrow{f} f(g(f(a))) \xrightarrow{g} \dots$$

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

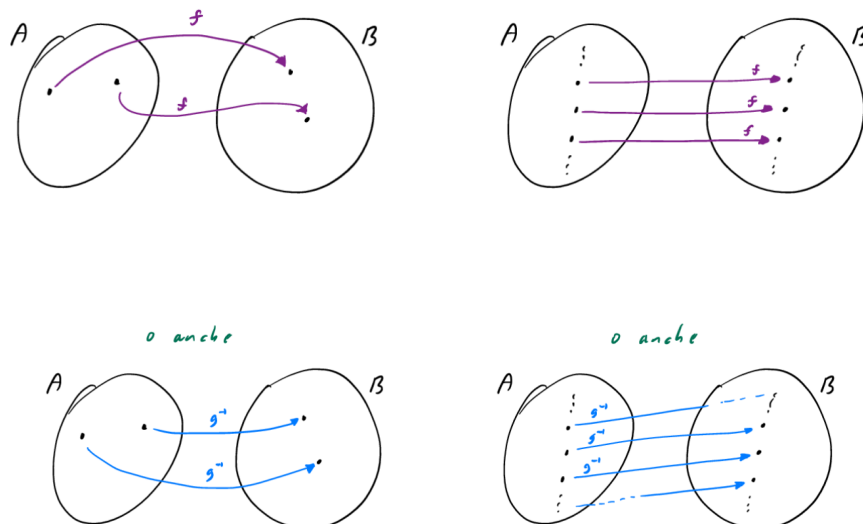
$$f^{-1}(g^{-1}(a)) \xrightarrow{f} g^{-1}(a) \xrightarrow{g} a \xrightarrow{f} f(a) \xrightarrow{g} g(f(a)) \xrightarrow{f} f(g(f(a))) \xrightarrow{g} \dots$$

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

⁴⁴È una semplice verifica.

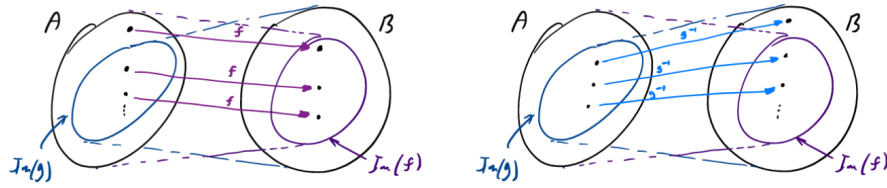


Per gli elementi che si trovano su un percorso circolare, o su un percorso illimitato avanti e indietro, f fornisce una bigezione, come la fornirebbe anche g^{-1} - la scelta è arbitraria a patto di usare la medesima funzione per l'intero percorso - nel modo seguente⁴⁵:



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} .

⁴⁵Informalmente, 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:

$$|A| < |B| \stackrel{\text{def}}{=} |A| \leq |B| \wedge |A| \neq |B| \quad ^{46}$$

§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:

$$B = \{x \in A \mid x \notin f(x)\} \quad ^{47}$$

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.

⁴⁶Dove ricordiamo che $|A| \neq |B| \stackrel{\text{def}}{=} \neg(|A| = |B|)$.

⁴⁷ $f(x) \in \mathcal{P}(A)$, ovvero è un sottoinsieme di A , quindi stiamo considerando il sottoinsieme degli elementi di A che non stanno nelle loro immagini (dei sottoinsiemi di A).

Proposizione 5.11 (Buona definizione delle operazioni)

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

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

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

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

ed equivalgono alle uguaglianze di cardinalità nella tesi. \square

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

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

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

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

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

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

Proposizione 5.14 (Proprietà delle operazioni fra cardinalità)

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

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

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

Dimostriamo che $(|A|^{|D|})^{|C|} = |A|^{|C| \cdot |B|}$. Dobbiamo esibire una bigezione fra l'insieme ${}^C({}^B A)$ delle funzioni che ad ogni elemento di C associano una funzione $B \rightarrow A$, e l'insieme ${}^{C \times B} A$, delle funzioni che ad ogni coppia di elementi in $C \times B$ associano un elemento di A . Associamo a $f \in {}^C({}^B A)$ la funzione $\tilde{f} \in {}^{C \times B} A$ definita da:

$$\tilde{f}(c, b) = \underbrace{(f(c))}_{\in {}^B A} \underbrace{(b)}_{\in B} \quad 49$$

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:

$$\bar{g}(c) : B \longrightarrow A : b \longmapsto g(c, b) \quad 50$$

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). □

⁴⁹Cioè 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 $b \in B$.

⁵⁰Ovvero la mappa $-$ associa una mappa di ${}^{C \times B} A$ con la mappa $\bar{g} \in {}^C({}^B A)$, che valutata in $c \in C$, dà una funzione da B in A , che ad ogni $b \in B$ associa $g(c, b)$.

§6 Cardinalità finite

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

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

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

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

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

§6.1 Principio dei cassetti

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

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

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

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

Supponiamo per assurdo che $|B| = |A|$. Osserviamo che, senza perdita di generalità, possiamo assumere $A = n \in \omega$ ⁵¹. 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 surgettiva⁵², 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 $B = \text{Im}(f) = C \cup \underbrace{\{f(m)\}}_{=m} = m \cup \{m\} = s(m) = n$.

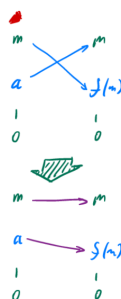
⁵¹Quello che faremo è proprio portare $B \subsetneq A$ in $f[B] \subsetneq f[A] = n$ e qui trovare l'assurdo, che è come assumere sempre che $A = n$, perché possiamo sempre spostare il problema in ω con una bigezione.

⁵²È conseguenza del fatto che B sia un sottoinsieme proprio e che f è bigettiva.



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

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



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

□

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

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

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

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

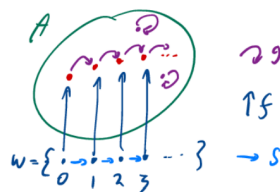
Se adesso volessimo dimostrare il viceversa: [che formulato in versione contronominale è] che un insieme infinito non è Dedekind-finito, quale sarebbe l'ostacolo? Abbiamo già osservato che ω non è finito, perché la funzione successore stabilisce una corrispondenza biunivoca fra ω e $\omega \setminus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

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

Dimostrazione. Basta considerare la funzione iniettiva:

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

È immediato vedere che $\text{Im}(g) = A \setminus \{f(0)\} \subsetneq A$ (l'unico escluso è lo 0, perché non può esserci un elemento che ha come controimmagine un elemento di ω il cui successore sia 0, perché per quanto visto non esiste), dunque A è in biezione con un suo sottoinsieme proprio.



□

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

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

Dov'è l'errore? Nell'ultima riga! Noi sappiamo che, data $f|_n$, esistono degli $a \in A$ con $a \notin \text{Im}(f|_n)$, questo è corretto. È anche corretto che ci basterebbe porre $f(n) = \text{"uno qualunque di questi } a\text{"}$. Il guaio è che, per applicare il teorema di ricorsione, ci serve una funzione che fissa (nel senso che la h del teorema di ricorsione essendo un insieme deve avere tutti gli elementi già fissati, cosa che non può avvenire in questo caso) uno degli a . A patto di averne una, ne andrebbe bene una qualunque.

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

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

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

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

Dimostrazione. Basta dimostrare il \leq , infatti $|n| < |n+1| \leq |A|$. Dimostriamo per induzione su n che c'è una funzione iniettiva da n ad A .

caso $n = 0$ La funzione vuota, $f = \emptyset$.

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

□

Corollario 6.7 (Ovvietà)

Un sottoinsieme di un insieme finito è finito.

Dimostrazione. Sia A finito e $B \subseteq A$. Se, per assurdo B fosse infinito, avremmo $|A| < |B| \leq |A|$ (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 (Le operazioni tra cardinalità finite possono essere definite in funzione delle operazioni su ω)

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

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

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

Dimostrazione. Dimostriamo, intanto che $|m| + |1| = |s(m)|$. A sinistra abbiamo, infatti la cardinalità di $(m \times \{0\}) \cup \{(0, 1)\}$ ⁵³ e a destra abbiamo la cardinalità di $m \cup \{m\}$. Quest'ultimo insieme si mappa bigettivamente nel primo, mandando $x \in m$ in $(x, 0)$ e m in $(0, 1)$. Ora, le uguaglianze asserite seguono, per induzione su n , dalle proprietà delle operazioni sulle cardinalità e dalla definizione ricorsiva delle operazioni su ω .

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

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

⁵³Typo del prof. Mamino sui suoi appunti in quanto $1 = \{0\}$.

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

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

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

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

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

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

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

caso $n = 0$ $|m|^{|0|} = |{}^0m| = |1| = |m^0|$ (l'unica funzione possibile dal vuoto a m è $f = \emptyset^{54}$).

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

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

□

⁵⁴E quindi ${}^0m = \{f : \emptyset \rightarrow m\} = \{\emptyset\} = 1$, o in alternativa si può pensare che $f \subseteq \emptyset \times m = \emptyset \implies f \in \mathcal{P}(\emptyset) = \{\emptyset\}$ e quindi $f = \emptyset \implies {}^0m = \{f\} = \{\emptyset\} = 1$.

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

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

Esercizio 6.11. Dimostra che se $m, n \in \omega$ e $m \leq n$, 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 bigezione con ω .

Proposizione 7.3

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

Ossia: $|A| < \aleph_0$ se e solo se A è finito [non è altro che una formulazione equivalente della proposizione sopra].

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

In generale, per costruire una bigezione fra due insiemi A e B - ossia per dimostrare $|A| = |B|$ - occorre appoggiarsi a qualche struttura definita sugli insiemi A e B . Per esempio, una funzione successore. In questo corso, giocheranno un ruolo importante, in questa direzione, le relazioni d'ordine, e, in particolare - l'idea è di Cantor - i **buoni ordini**. Ricordiamo la definizione.

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

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

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

Definizione 7.5 (Isomorfismo). Due insiemi (parzialmente⁵⁵) ordinati $(A, <_A)$ e $(B, <_B)$ sono **isomorfi**, in simboli $(A, <_A) \sim (B, <_B)$ se esiste una bigezione $f : A \rightarrow B$ tale che:

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

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

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

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

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

⁵⁵Dove parziale indica l'assenza della proprietà di totalità nella definizione di relazione d'ordine.

Esercizio 7.7. Dimostrare la proposizione enunciata sopra.

Osservazione 7.8 (Ogni insieme finito è isomorfo alla sua cardinalità) — Sia $(A, <_A)$ totalmente ordinato con $|A| = n \in \omega$. Allora $(A, <_A) \sim (n, <)$, dove $<$ denota l'ordinamento indotto da ω (cioè l'ordine che abbiamo definito su ω ristretto a n).

Dimostrazione. Procediamo per induzione su n .

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

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

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

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

è l'isomorfismo cercato.

□

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

Proposizione 7.9 (Proprietà di $(\omega, <)$)

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

- (1) $(\omega, <)$ è un buon ordine.
- (2) $(\omega, <)$ è **illimitato** - ossia $\forall x \in \omega \exists y \in \omega x < y$.
- (3) Ogni $A \subseteq \omega$ superiormente limitato e non vuoto ha un massimo, ossia:

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

Dimostrazione. Abbiamo che (1) è il principio del minimo che abbiamo già dimostrato su ω , per (2) basta prendere $y = s(x)$ (e $x \in s(x) \implies x < y$). Per (3) se A è superiormente limitato da $L \in \omega$, allora $A \subseteq s(L)$, quindi A è finito. Siccome A è finito, l'ordinamento totale su A definito da:

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

è buono, quindi, in particolare, c'è il minimo di A secondo l'ordinamento \prec . Questo è il massimo di A (secondo l'ordinamento $<$). □

Proposizione 7.10 (Caratterizzazione di ω come ordine)

Sia (A, \prec) , con $A \neq \emptyset$, un ordinamento:

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

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

Dimostriamo prima un facile lemma.

Lemma 7.11 (Stretta crescita col successore \implies stretta crescita)

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

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

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

^aTypo di Mamino nelle dispense.

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

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

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

Possiamo ora dimostrare la proposizione.

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

$$f(0) = \min_{\prec} A \quad f(s(n)) = \min_{\prec} \{a \in A \mid f(n) \prec a\} \text{ }^{56}$$

dove \min_{\prec} denota il minimo secondo la relazione d'ordine (buona) \prec . Occorre dimostrare intanto che f è ben definita. $f(0)$ è ben definita, perché $A \neq \emptyset$, dunque (essendo ben ordinato per ipotesi ha un minimo⁵⁷). Per dire che $f(s(n))$ è ben definita, occorre dire che la funzione $h : A \rightarrow A$, $h(x) = \min_{\prec} \{a \in A \mid f(n) \prec a\}$ è ben definita (sarebbe la funzione che definisce la ricorsione - prima forma -), ossia che $\{a \in A \mid x \prec a\}$ è non vuoto (e quindi di nuovo esiste il minimo perché stiamo supponendo A ben ordinato). Ma questo avviene, qualsiasi sia $x \in A$, perché altrimenti A sarebbe limitato [superiormente] da x (e non illimitato superiormente come abbiamo supposto nelle ipotesi).

⁵⁶Cioè la funzione manda il successore nel più piccolo termine in (A, \prec) che sta "sopra" a $f(n)$ (in pratica la stiamo costruendo apposta affinché sia strettamente crescente).

⁵⁷Per essere precisi essendo $A \in \mathcal{P}(A)$ tecnicamente il principio del buon ordinamento si applica anche ad A stesso (oltre che ai suoi sottoinsiemi propri), che quindi ha minimo.

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

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

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

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

□

Tornando alla proposizione iniziale.

Proposizione 7.12 (Caratterizzazione insiemi al più numerabili)

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

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

Sia $B \subseteq \omega$ infinito, dimostriamo che B , con l'ordinamento indotto dall'ordine naturale di ω soddisfa le ipotesi della proposizione precedente. 1 e 3⁵⁸ valgono in quanto ogni sottoinsieme di B è in particolare, sottoinsieme di ω (dunque abbiamo buon ordinamento ed esistenza del massimo). Per ottenere 2 dobbiamo dire che B non ha un massimo elemento (cioè è illimitato). Se, infatti, ci fosse un $M \in B$ tale che $\forall b \in B \ b \leq M$, allora avremmo che $B \subseteq s(M)$, B sarebbe dunque finito, contro l'ipotesi. Pertanto $(B, <|_B) \sim (\omega, <) \implies |B| = \aleph_0$, dunque se un sottoinsieme di ω è infinito, allora è necessariamente numerabile.

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

Esercizio 7.13. Dimostra che se $|A| \leq \aleph_0$ e $f : A \twoheadrightarrow B$ è surgettiva, allora $|B| \leq \aleph_0$.

Soluzione. Mostriamo che sotto queste ipotesi esiste $h : B \hookrightarrow \omega$ (iniettiva), sia $g : A \hookrightarrow \omega$ e poniamo:

$$h(b) = \min(g[\underbrace{\{a \in A \mid f(a) = b\}}_{= "f^{-1}(b)"}])^{59}$$

l'insieme tra graffe è non vuoto per surgettività di f , dunque il minimo è ben definito. Inoltre, se $h(b) = h(b')$, allora i minimi [che chiamiamo] $g(a)$ e $g(a')$ sono uguali, ma a e

⁵⁸Typo di Mamino.

⁵⁹Si noti che, essendo f non necessariamente iniettiva, f^{-1} denota la controimmagine, non la funzione inversa, da cui la scelta delle parentesi quadre quando si applica g , per evidenziare che stiamo facendo l'immagine di un'insieme.

a' sono elementi nelle controimmagini rispettivamente di b e b' , cioè tali che $f(a) = b$ e $f(a') = b'$. Sappiamo quindi per ipotesi che $g(a) = g(a')$ e per l'iniettività di g segue $a = a'$, da cui $f(a) = f(a')$ (ovviamente sono lo stesso elemento), da cui $b = f(a) = f(a') = b'$. \square

§7.1 Insiemi numerabili in pratica

Sapere che, se $|A| \leq \aleph_0$, allora o A è finito o è numerabile, ci fornisce lo strumento essendo per dimostrare la numerabilità di molti insiemi concreti. Spesso, infatti, è facile dimostrare che un insieme infinito è tale. Rimane poi da gestire un discorso di disuguaglianze per dire che esso è al più numerabile.

Cominciamo quindi con qualche considerazione generale a proposito delle disuguaglianze fra cardinalità.

Osservazione 7.14 (Compatibilità tra operazioni e “ordinamento” fra cardinalità) — Dati gli insiemi A, B, C con $|B| \leq |C|$ allora vale:

$$\begin{aligned} |A| + |B| &\leq |A| + |C| & |A|^{|B|} &\leq |A|^{|C|} \\ |A| \cdot |B| &\leq |A| \cdot |C| & |B|^{|A|} &\leq |C|^{|A|} \end{aligned}$$

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

Dimostrazione. Detta $f : B \rightarrow C$ la funzione iniettiva che testimonia che $|B| \leq |C|$ e detto $B' = f[B]$ abbiamo che $|B| = |B'|$ (come al solito per definizione di disuguaglianza tra cardinalità), quindi basta dimostrare le disuguaglianze asserite con B' al posto di B . Ora, giocando sul fatto che $B' \subseteq C$ (abbiamo fatto apposta lo scambio tra B e B' per poter usare i contenimenti), si vede che queste disuguaglianze rappresentano, in realtà, relazioni di contenimento fra RHS e LHS. Per esempio:

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

Le altre si ottengono allo stesso modo. \square

Osservazione 7.15 (Disuguaglianza di inclusione-esclusione) — $|A \cup B| \leq |A| + |B|$.

Dimostrazione. Basta osservare che la seguente funzione è iniettiva:

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

\square

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

Proposizione 7.16 (Operazioni aritmetiche con \aleph_0)
 $\aleph_0 + \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0^n = \aleph_0$, con $n \in \omega \setminus \{0\}$.

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

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

Da cui per il [Cantor-Bernstein](#):

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

Ora è facile vedere per induzione che $n \in \omega \setminus \{0\} \rightarrow \aleph_0^n = \aleph_0$, infatti $\aleph_0^1 = \aleph_0$ e $\aleph_0^{n+1} = \aleph_0^n \cdot \aleph_0 \stackrel{\text{Hp. indutt.}}{=} \aleph_0 \cdot \aleph_0 = \aleph_0$. \square

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

§7.2 Prodotto di numerabili è numerabile**Lemma 7.17** ($\aleph_0 \cdot \aleph_0 = \aleph_0$)

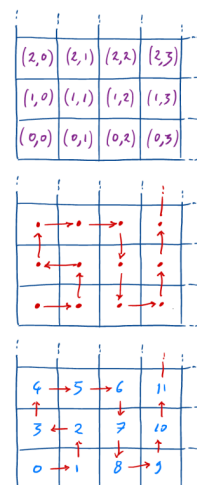
$\aleph_0 \cdot \aleph_0 = \aleph_0$, ossia esiste una biezione fra $\omega \times \omega$ e ω .

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

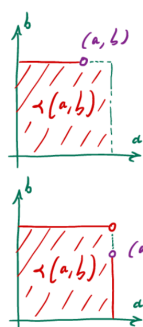
Altrimenti, è possibile esibire delle biezioni esplicite, per esempio:

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

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



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



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

(dove per \max sulla coppia si intende il \max tra a e b) ossia per confrontare (a, b) con (a', b') , si confrontano prima $\max(a, b)$ e $\max(a', b')$; a parità si confrontano a ed a' (cioè se hanno una delle due componenti con lo stesso modulo massimo, si passa a confrontare il valore delle

prime componenti); se anche queste coincidono, allora si confrontano b e b' .⁶⁰

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

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

Per dire che l'ordine è totale osserviamo che se (a, b) e (a', b') non sono né \prec né \succ allora dobbiamo avere $\max(a, b) = \max(a', b')$, $a = a'$, $b = b'$, ovvero $(a, b) = (a', b')$, dunque l'ordine stretto è anche totale. Ora vogliamo dire che $(\omega \times \omega, \prec) \sim (\omega, <)$ (in questo modo, avendo un'isomorfismo di ordini, avremmo in particolare una biezione tra ω e $\omega \times \omega$, dunque il prodotto di cardinalità numerabili è numerabile).

Partiamo dall'osservazione che se $(a, b) \in \omega \times \omega$ allora:

$$(\omega \times \omega)_{(a,b)} \stackrel{\text{def}}{=} \{(x, y) \in \omega \times \omega \mid (x, y) \prec (a, b)\}$$

detto il “**segmento iniziale** determinato da (a, b) su $(\omega \times \omega, \prec)$ ”, è finito⁶¹. Infatti $(\omega \times \omega)_{(a,b)} \subseteq s(\max(a, b)) \times s(\max(a, b))$. Ci serve dire 1. $(\omega \times \omega, \prec)$ è bene ordinato 2. $(\omega \times \omega, \prec)$ è illimitato 3. ogni sottoinsieme non vuoto e superiormente limitato di $\omega \times \omega$ ha un massimo.

1. Dato $A \subseteq \omega \times \omega$ con $A \neq \emptyset$, considero $a \in A$. Se $(\omega \times \omega)_a \cap A = \emptyset$ (stiamo considerando il segmento iniziale rispetto a un generico elemento $a \in \omega \times \omega$), allora a è il minimo di A (sta in a e non c'è nulla più piccolo nell'insieme perché l'intersezione col segmento iniziale di a (= cose strettamente più piccole in $(\omega \times \omega, \prec)$) è vuota). Altrimenti $A' = (\omega \times \omega)_{(a,a)} \cap A$ è non vuoto e finito, quindi ha minimo m (perché \prec è un ordine totale). Questo deve essere anche il minimo di A , perché se $x \in A \setminus A'$, allora $m \prec a \preceq x$ (dove la seconda disuguaglianza segue per quanto detto nel caso dell'intersezione vuota, mentre la prima perché sia a che m stanno nell'intersezione in cui abbiamo preso il minimo).
2. Dato $(a, b) \in \omega \times \omega$, $(a, b) \prec (s(a), s(b))$, dunque $\omega \times \omega$ è illimitato.
3. Dato $A \subseteq \omega \times \omega$ non vuoto e superiormente limitato da $(a, b) \in \omega \times \omega$, abbiamo che $A \subseteq (\omega \times \omega)_{(a+1, b+1)}$ è finito (per quanto osservato sopra), quindi ammette massimo perché \prec è totale (abbiamo un numero finito di elementi da confrontare).

□

§7.3 Numeri interi e razionali

Usando la proposizione appena dimostrata, potremmo dimostrare, per esempio, che \mathbb{Z} e \mathbb{Q} sono numerabili, se non fosse che non abbiamo ancora definito questi oggetti. Allo

⁶⁰Come si vede nella figura a lato, nel primo caso, avendo b modulo massimo, ci sono anche punti più a destra, che in quest'ordinamento sono più piccoli (perché hanno un valore più piccolo come massima componente).

⁶¹È quello che abbiamo detto sopra sulla definizione di \prec , pensando alle due figure.

scopo, ricordiamo che - [esercizio 3.73](#) - una relazione di equivalenza induce un insieme di classi di equivalenza.

Definizione 7.18 (\mathbb{Z}). Definiamo \mathbb{Z} come l'insieme delle classi di equivalenza su $\omega \times \omega$ indotte dalla relazione:

$$(a, b) \sim_{\mathbb{Z}} (a', b') \stackrel{\text{def}}{=} a + b' = b + a' \quad {}^{62}$$

Esercizio 7.19. Dimostrare che $\sim_{\mathbb{Z}}$ è una relazione di equivalenza.

Esempio 7.20 (Operazioni su \mathbb{Z})

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

$$\begin{aligned} [(a, b)]_{\mathbb{Z}} + [(a', b')]_{\mathbb{Z}} &\stackrel{\text{def}}{=} [(a + a', b + b')]_{\mathbb{Z}} \\ -[(a, b)]_{\mathbb{Z}} &\stackrel{\text{def}}{=} [(b, a)]_{\mathbb{Z}} \\ [(a, b)]_{\mathbb{Z}} \cdot [(a', b')]_{\mathbb{Z}} &\stackrel{\text{def}}{=} [(a \cdot a' + b \cdot b', a \cdot b' + a' \cdot b)]_{\mathbb{Z}} \end{aligned}$$

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

Definizione 7.21 (\mathbb{Q}). Definiamo \mathbb{Q} come l'insieme delle classi di equivalenza su $\mathbb{Z} \times (\omega \setminus \{0\})$ indotte dalla relazione:

$$(n, d) \sim_{\mathbb{Q}} (n', d') \stackrel{\text{def}}{=} n \cdot d' = n' \cdot d \quad {}^{63}$$

Esercizio 7.22. Dimostrare che $\sim_{\mathbb{Q}}$ è una relazione di equivalenza.

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

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

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

^aTypo di Mamino.

Nota 7.25 — Gli esercizi precedenti sono tediosi, ma non sono difficili. Nel resto del corso daremo per scontate le proprietà aritmetiche elementari di \mathbb{Z} e \mathbb{Q} . D'ora innanzi scriveremo:

$$a - b \stackrel{\text{def}}{=} [(a, b)]_{\mathbb{Z}} \quad \frac{n}{d} \stackrel{\text{def}}{=} [(n, d)]_{\mathbb{Q}}$$

Per dimostrare la numerabilità di \mathbb{Z} e \mathbb{Q} , è comodo richiamare ancora un [esercizio](#), però, questa volta, lo risolviamo⁶⁴.

⁶²Morale: “ $(a, b) = a - b$ ”.

⁶³Morale: “ $(n, d) = \frac{n}{d}$ ”.

⁶⁴La soluzione riportata è quella di Mamino.

Corollario 7.26 (Definizione di al più numerabile al contrario)

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

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

Dimostrazione. La freccia \Leftarrow deriva dall'esercizio citato prima con $A = \omega$ e $B = A$ ⁶⁵. Per l'inverso, supponiamo A al più numerabile e mostriamo che c'è sempre una mappa surgettiva tra ω ed A . Sappiamo che se un insieme è al più numerabile, o è finito o è numerabile, se $|A| = \aleph_0$ allora c'è f bigettiva (e quindi in particolare surgettiva), se $|A| < \aleph_0$ allora c'è [per definizione] $g : n \rightarrow A$ bigettiva per qualche $n \in \omega \setminus \{0\}$, da questa definiamo:

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

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

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

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

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

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

^bMoralmente: una successione surgettiva.

Il corollario sopra, quindi, non ci dice altro che $A \neq \emptyset$ è al più numerabile se e solo se ha almeno un'enumerazione.

Esempio 7.28 (L'insieme dei numeri interi è numerabile)

\mathbb{Z} è numerabile.

Dimostrazione. La funzione $\omega \times \omega : (a, b) \mapsto a - b$ è surgettiva per definizione (è la proiezione al quoziente di $\omega \times \omega$ modulo $\sim_{\mathbb{Z}}$, che sappiamo essere sempre surgettiva, in questo caso stiamo indicando le classi $[(a, b)]_{\mathbb{Z}}$ con $a - b$, ma sono sempre classi di equivalenza), e $\omega \times \omega$ è numerabile⁶⁶ dunque $|\mathbb{Z}| \leq \aleph_0$.

D'altro canto, la funzione $\omega \rightarrow \mathbb{Z} : n \mapsto [(n, 0)]_{\mathbb{Z}}$ è iniettiva, infatti $[(n, 0)]_{\mathbb{Z}} = [(m, 0)]_{\mathbb{Z}} \iff (n, 0) \sim (m, 0) \iff n = m$ (per definizione di $\sim_{\mathbb{Z}}$), dunque $\aleph_0 \leq |\mathbb{Z}|$, pertanto [per Cantor-Bernstein] $|\mathbb{Z}| = \aleph_0$. \square

⁶⁵Quelli al LHS sono quelli nell'enunciato dell'esercizio, quelli al RHS sono quelli presi dalle ipotesi del corollario.

⁶⁶ $|\omega \times \omega| = \aleph_0 \cdot \aleph_0 = \aleph_0$.

Esempio 7.29 (L'insieme dei numeri razionali è numerabile) \mathbb{Q} è numerabile.

Dimostrazione. Come nell'esempio precedente, la proiezione al quoziente $\mathbb{Z} \times (\omega \setminus \{0\}) \rightarrow \mathbb{Q} : (n, d) \mapsto \frac{n}{d}$ (dove la frazione è un'abbreviazione per la classe di equivalenza $[(n, d)]_{\mathbb{Q}}$), è surgettiva per costruzione, inoltre $|\mathbb{Z} \times (\omega \setminus \{0\})| = |\mathbb{Z}| \cdot |\omega \setminus \{0\}| = \aleph_0 \cdot \aleph_0 = \aleph_0$, dunque vale il [corollario](#) sulla disuguaglianza tra cardinalità, pertanto $\aleph_0 \geq |\mathbb{Q}|$.

Viceversa, la funzione $\omega \rightarrow \mathbb{Q} : n \mapsto \frac{n}{1}$ è iniettiva, infatti $\frac{n}{1} = \frac{m}{1} \iff n \cdot 1 = m \cdot 1 \iff m = n$, dunque per definizione si ha $\aleph_0 \leq |\mathbb{Q}|$. Da cui per [Cantor-Bernstein](#) $|\mathbb{Q}| = \aleph_0$. \square

Adesso, ci piacerebbe poter dire che, se abbiamo un insieme A al più numerabile, e tutti i suoi elementi sono, a loro volta, insiemi al più numerabili, allora $\bigcup A$ è al più numerabile. D'altro canto è ragionevole: se esiste una enumerazione $\{a_i\}_{i \in \omega}$ di A ($= A$ è al più numerabile), e, per ogni $i \in \omega$, esista una enumerazione $\alpha_i = \{a_{i,j}\}_{j \in \omega}$ ($=$ per ogni elemento $a_i \in A$ esiste una enumerazione, dunque ogni elemento ($=$ insieme) è a sua volta al più numerabile) di a_i , allora possiamo mandare surgettivamente $\omega \times \omega$ in $\bigcup A$: $(i, j) \mapsto \alpha_{i,j}$, e, siccome $\omega \times \omega$ è al più numerabile, lo è anche A (per il solito [corollario](#)). L'errore è credere di poter fissare una α_i per ogni $i \in \omega$. Usando l'assioma della scelta potremo farlo, ma, per ora, non abbiamo modo, in generale, di procurarci la funzione $i \mapsto \alpha_i$. Possiamo però assumere di averla, così si corregge il ragionamento impreciso di prima.

Proposizione 7.30 ($|A| \leq \aleph_0 \implies |\bigcup A| \leq \aleph_0$)

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

^aCome prima stiamo supponendo di averle già, altrimenti ci vuole scelta.

Dimostrazione. Basta osservare che la funzione:

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

è surgettiva e vale quindi il solito [corollario](#). \square

Notazione 7.31 — Data una funzione $f : I \rightarrow S$ definiamo:

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

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

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

(cioè gli elementi degli elementi pescati attraverso l'enumerazione data).

Definizione 7.32 (Parti finite). Definiamo:

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

Proposizione 7.33 (Insieme al più numerabile \implies parti finite al più numerabile)

$$|A| \leq \aleph_0 \rightarrow |\mathcal{P}^{\text{fin.}}(A)| \leq \aleph_0.$$

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

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

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

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

Per $n = 0$ abbiamo $\mathcal{P}^{\leq 0}(A) = \{\emptyset\}$, dunque α_0 è la costante [funzione vuota] \emptyset .

Per $n = s(m)$ poniamo:

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

Dimostriamo per induzione che, per ogni $n \in \omega$, $\alpha_n : \omega \rightarrow \mathcal{P}^{\leq n}(A)$ è surgettiva.

caso $n = 0$ Immediato.

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

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

□

Applicazione Dimostriamo che l'insieme dei numeri reali algebrici \mathbb{A}_R ⁶⁷ è numerabile. Per questa applicazione, assumiamo le proprietà elementari di \mathbb{R} . L'insieme \mathbb{A}_R è definito come l'insieme degli $x \in \mathbb{R}$ che sono zeri di qualche polinomio a coefficienti razionali:

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

I numeri reali che non sono algebrici si dicono **trascendenti** ($= \mathbb{R} \setminus (\overline{\mathbb{Q}} \cap \mathbb{R})$), siccome - formalmente, vedremo questo risultato in seguito - \mathbb{R} non è numerabile, deduciamo dalla numerabilità di \mathbb{A}_R che ci sono numeri reali trascendenti.

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

Possiamo identificare un polinomio:

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

⁶⁷Sarebbe $\overline{\mathbb{Q}} \cap \mathbb{R}$.

con l'insieme dei suoi monomi:

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

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

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

Formalmente, come accade per i numeri, le coppie ordinate, le funzioni, etc., anche i polinomi non sono oggetti atomici della teoria degli insiemi: occorre, in qualche modo, fissare una codifica. Quella appena descritta è una codifica ragionevole. Rappresentando i polinomi in questo modo:

$$\mathbb{Q}[x] \subseteq \mathcal{P}^{\text{fin.}}(\omega \times \mathbb{Q})^{68}$$

per cui, essendo che $|\omega \times \mathbb{Q}| = \aleph_0 \implies |\mathcal{P}^{\text{fin.}}(\omega \times \mathbb{Q})| = \aleph_0$, e che $\mathbb{Q}[x]$ si immerge in quest'ultimo insieme (ad esempio con $\text{id}_{\mathbb{Q}[x]}$), si ha $|\mathbb{Q}[x]| \leq \aleph_0$. Inoltre è elementare che $\mathbb{Q} \hookrightarrow \mathbb{Q}[x]$ (ad esempio mandato tutti i razionali nel polinomio (scritto o meno nella forma codificata con le coppie ordinate non importa) costante, con $a_0 = q$), in tal modo si ha anche l'altra disuguaglianza di cardinalità e quindi $|\mathbb{Q}[x]| = \aleph_0$.

Venendo ad \mathbb{A}_R abbiamo una facile surgezione:

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

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

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

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

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

Esercizio 7.34. Dato un insieme X , una funzione $f : X^2 \rightarrow X$, e un sottoinsieme $A \subseteq X$ al più numerabile, dimostra che esiste un $\bar{A} \subseteq X$ al più numerabile tale che $f[\bar{A} \times \bar{A}] \subseteq \bar{A}$. Concludi che un gruppo finitamente generato è al più numerabile.

§7.4 Ordini densi numerabili

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

Definizione 7.35 (Densità). Sia $(A, <)$ totalmente ordinato, e $B \subseteq A$. B è **denso in** $(A, <)$ se:

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

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

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

(cioè tra due elementi di A c'è sempre qualche elemento di A).

⁶⁸Cioè un sottoinsieme finito (i polinomi hanno grado finito) di un insieme fatto da oggetti del tipo (grado, elemento).

Esempio 7.36 $((\mathbb{Q}, <))$ è denso in se stesso)

Abbiamo già osservato, in un esercizio, che \mathbb{Q} è denso, infatti:

$$x < y \rightarrow x < \frac{x+y}{2} < y$$

NON Esempio 7.37 $((\omega, <))$ non è denso in se stesso)

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

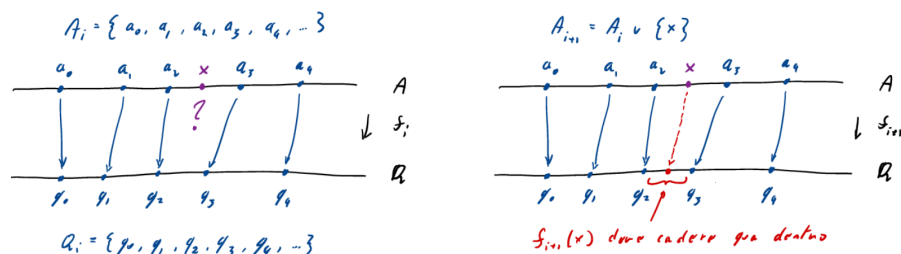
Teorema 7.38 (Teorema di isomorfismo di Cantor)

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

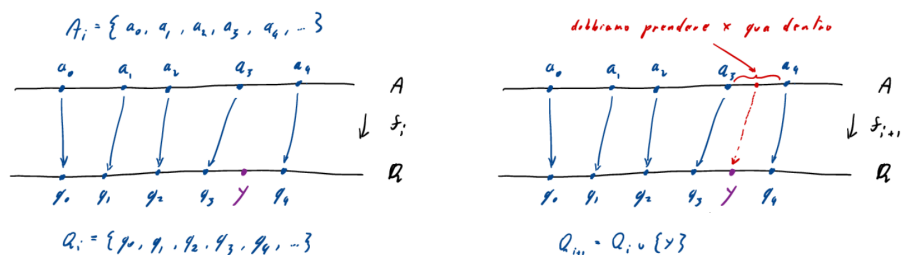
1. $|A| = \aleph_0$
2. $(A, <)$ è denso
3. $(A, <)$ non ha **estremi**, ossia non ha né massimo né minimo elemento

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

L'idea è di costruire l'isomorfismo per ricorsione. Ad ogni passo della ricorsione avremo $f_i : A_i \rightarrow Q_i$ isomorfismo con $A_i \subseteq A$ finito e $Q_i \subseteq \mathbb{Q}$. Dovremo quindi estendere f_i ingrandendo il suo dominio. Supponiamo, per esempio, di



voler definire $f_{i+1}(x)$ con $x \notin A_i$. Allora, siccome A_i è finito, per sapere la posizione di x a ciascuno degli elementi di A_i , ci basta sapere quale sia l'ultimo elemento prima di x , e quale sia il primo dopo x - diciamo che, per esempio, sono a_2 e a_3 rispettivamente. Dovremo allora mandare x in un $f_{i+1}(x)$ con $f_i(a_2) < f_{i+1}(x) < f_i(a_3)$, e questo esiste per la densità di \mathbb{Q} . Ragionando simmetricamente, possiamo anche estendere f_i , dato un $y \in \mathbb{Q}$ con $y \notin Q_i$, in modo tale che $y \in \text{Im}(f_{i+1})$.



In definitiva, ci basta quindi fissare un'enumerazione di A e una di \mathbb{Q} , e fare questi passi di estensione in maniera alternata, assicurandoci così di aggiungere al dominio della

f , uno per uno, tutti gli elementi di A , e di aggiungere all'immagine, uno per uno, tutti gli elementi di \mathbb{Q} . Ci farà comodo la segue osservazione.

Osservazione 7.39 (L'unione di un insieme di funzioni è una funzione se...) — Sia $F \subseteq \mathcal{P}(A \times B)$ un insieme di funzioni. Se:

$$\forall f_1, f_2 \in F \quad f_1|_{\text{Dom}(f_1) \cap \text{Dom}(f_2)} = f_2|_{\text{Dom}(f_1) \cap \text{Dom}(f_2)}$$

ossia $\forall x \in \text{Dom}(f_1) \cap \text{Dom}(f_2) \quad f_1(x) = f_2(x)$, allora $\bigcup F$ è una funzione: $\bigcup \{\text{Dom}(f) | f \in F\} \rightarrow B$.

Dimostrazione. □

Siamo ora pronti per dimostrare formalmente il teorema.

Dimostrazione. □

Corollario 7.40

Sia $(A, <)$ un ordine totale con $|A| \leq \aleph_0$. Allora esiste $B \subseteq \mathbb{Q}$ tale che $(A, <) \sim (B, <)$ con l'ordinamento indotto su B da \mathbb{Q} .

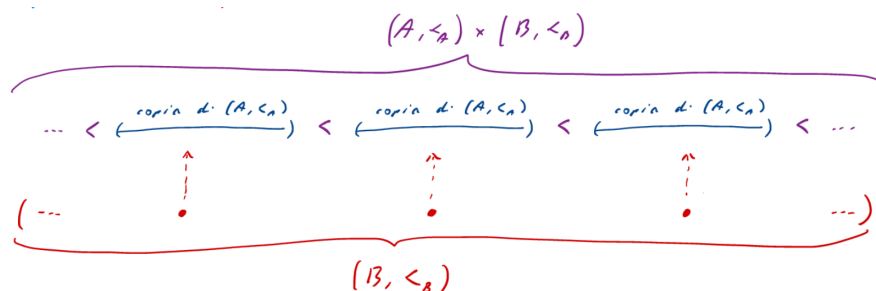
Nota 7.41 — Volendo, si potrebbe dimostrare questo corollario ripetendo, con qualche variazione, la dimostrazione del teorema. Ora daremo, però, un argomento che, invece, applica il teorema. È comodo definire, prima, il prodotto di ordini.

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

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

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

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



Osservazione 7.43 — Il prodotto è un ordine. Inoltre se $(A, <_A)$ e $(B, <_B)$ sono ordini totali, allora anche $(A, <_A) \times (B, <_B)$ lo è.

Esercizio 7.44 (Associatività del prodotto lessicografico). Dati $(A, <_A)$, $(B, <_B)$ e $(C, <_C)$ dimostra che:

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

ossia che il prodotto lessicografico di ordini è associativo a meno di isomorfismi.

Veniamo ora alla dimostrazione del corollario

Dimostrazione. □

Esercizio 7.45. Dimostra che se $(A, <)$ è denso e $2 \leq |A| \leq \aleph_0$, allora $(A, <)$ è isomorfo a uno dei seguenti intervalli di \mathbb{Q} :

$$[0, 1]_{\mathbb{Q}} \quad]0, 1]_{\mathbb{Q}} \quad [0, 1[_{\mathbb{Q}} \quad]0, 1[_{\mathbb{Q}}$$

§7.5 Il grafo random

La tecnica di estendere indefinitamente isomorfismi parziali che ci ha permesso di dimostrare il teorema di isomorfismo di Cantor si chiama **back-and-forth**, ed è un metodo fondamentale per trovare isomorfismi fra strutture.

Cogliamo questa occasione per suggerire un esercizio di applicazione della medesima tecnica che è un po' complicato. Si tratta di definire il **grafo random** o **grafo di Rado**.

Definizione 7.46 (Grafo). Un **grafo** (V, e) sull'insieme di vertici V è dato da una relazione e simmetrica ($\forall x, y \in V (x, y) \in e \leftrightarrow (y, x) \in e$) e irreflessiva ($\forall x \in V (x, x) \notin e$).

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

Partiamo da un'idea intuitiva - chi ha già seguito un corso di probabilità saprà formalizzare questa cosa in termini precisi. Data una probabilità $p \in]0, 1[$ costruiamo un grafo G_p con insieme di vertici ω come segue. Per ogni coppia $(i, j) \in \omega \times \omega$ con $i < j$ lanciamo una moneta **che fa testa con probabilità p** - tutte queste monete indipendentemente - e, se viene testa, mettiamo un arco fra i e j .

Potremmo pensare che i grafi $G_{0.01}$ e $G_{0.99}$ debbano venire molto diversi: uno ha l'1% degli archi possibili, l'altro ha il 99%, insomma uno è quasi vuoto, l'altro quasi completo. Avviene, tuttavia, che, con probabilità 1, questi grafi sono isomorfi, dove, per essere precisi [possiamo definire l'isomorfismo tra grafi].

Definizione 7.47 (Isomorfismo fra grafi). I grafi (V_1, e_1) e (V_2, e_2) sono **isomorfi** se esiste una bigezione $f : V_1 \rightarrow V_2$ tale che:

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

Vediamo perché. Dati due sottoinsiemi finiti X e Y di ω , e dato un vertice $v \notin X \cup Y$ la probabilità che x sia connesso da un arco a tutti i vertici di X e a nessuno di quelli di Y è $p^{|X|} \cdot (1-p)^{|Y|}$ - come che sia, è un centro numero > 0 - e ci sono infiniti $v \notin X \cup Y$. Si capisce, quindi, che con probabilità 1 - ossia certamente - almeno uno di questi vincerà questa lotteria, ossia sarà connesso a tutti gli X e a nessuno degli Y . Usiamo l'esistenza di questo v per definire un grafo random.

Definizione 7.48 (Grafo random). Il grafo (ω, e) è un **grafo random** se:

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

Esercizio 7.49. Dimostra che esiste un grafo random, ed è unico a meno di isomorfismi.

§8 \mathbb{R} e la cardinalità del continuo

In questa sezione daremo una definizione di \mathbb{R} come insieme ordinato. Estenderemo, poi, la definizione ad includere le operazioni di campo, ma senza svolgere le verifiche.

Definizione 8.1 (Maggiorante, insieme superiormente limitato ed estremo superiore). Sia $(A, <)$ un ordine totale, allora:

- $m \in A$ è un **maggiorante** di $B \subseteq A$ se $\forall x \in B \ x \leq m$
- $B \subseteq A$ è **superiormente limitato** se ha un maggiorante
- $s \in A$ è l'**estremo superiore** di B - denotato con $\sup B$ - se s è il minimo dei maggioranti di B .

Nota 8.2 — Non sempre gli estremi superiori esistono, e, se B ha un estremo superiore, questo è unico^a.

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

Definizione 8.3 (Ordine totale completo). Un ordine totale $(A, <)$ è **completo** se ogni $B \subseteq A$ superiormente limitato ha un estremo superiore $\sup B \in A$.⁶⁹

Esercizio 8.4 (\mathbb{Q} non è completo). Dimostra, usando solo le proprietà di \mathbb{Q} , che l'insieme $\{x \in \mathbb{Q} | x^2 < 2\}$ non ha estremo superiore in \mathbb{Q} .

In conseguenza dell'esercizio, possiamo dire che \mathbb{Q} non è completo. Costruiamo ora un ordine completo $(\mathbb{R}, <)$ che contiene una copia isomorfa di \mathbb{Q} come sottoinsieme denso.

Definizione 8.5 (Segmento iniziale). Sia $(A, <)$ un ordine totale. $B \subseteq A$ è un **segmento iniziale** di A se $\forall x \in B \ \forall y \in A \ y < x \rightarrow y \in B$.⁷⁰

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

Esempio 8.6 (Segmento iniziale principale)

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

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

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

Nota 8.7 — Useremo nuovamente il concetto di segmento iniziale studiando gli ordinali. Il prossimo concetto, quello di sezione di Dedekind, invece, ci serve unicamente per definire \mathbb{R} .

⁶⁹L'Assioma di Dedekind sarà poi ciò che ci permetterà di dire che i numeri reali sono completi.

⁷⁰Moralmente: un insieme di cose strettamente più piccole.

Definizione 8.8 (Sezioni di Dedekind). Una **sezione** sull'insieme totalmente ordinato $(A, <)$ è un segmento iniziale **proprio** e **non vuoto** di A che **non ha un massimo elemento**.

Ossia B segmento iniziale di A è una sezione se $B \neq A$, $B \neq \emptyset$ e $\forall x \in B \exists y \in B x < y$.

Definizione 8.9 (Insieme ordinato dei numeri reali). Definiamo i numeri reali come insieme:

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

con l'ordine dato da:

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

Proposizione 8.10 (\mathbb{R} è completo)

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

Prima della dimostrazione, isoliamo un semplice lemma.

Lemma 8.11 (L'unione di segmenti iniziali è un segmento iniziale)

Sia $(A, <)$ un ordine totale e X un insieme di segmenti iniziali di A . Allora $\bigcup X$ è un segmento iniziale di A .

Dimostrazione.

□

Ora possiamo dimostrare la proposizione come segue.

Osservazione 8.12 (\mathbb{Q} si immerge in maniera ordinata e densa in \mathbb{R}) — La funzione $\iota : \mathbb{Q} \rightarrow \mathbb{R} : a \mapsto \mathbb{Q}_a = \{x \in \mathbb{Q} \mid x < a\}$ immerge \mathbb{Q} in \mathbb{R} in maniera strettamente crescente e densa (ossia $\iota(\mathbb{Q}) = \text{Im}(\iota)$ è densa in \mathbb{R}).

Dimostrazione.

□

Notazione 8.13 (Abuso di immersioni) — Siccome le immersioni:

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

sono tutte iniettive e crescente, quando non c'è pericolo di confusione, possiamo abusare della notazione immaginando che queste siano vere e proprie inclusioni [di insiemi, senza passare per le immagini^a]:

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

In realtà non è vero: per esempio è $\iota[\mathbb{Q}]$, non \mathbb{Q} , a essere sottoinsieme di \mathbb{R} , ma $\iota[\mathbb{Q}]$ è in corrispondenza biunivoca, in maniera canonica, tramite appunto ι , con \mathbb{Q} , e questa corrispondenza preserva tutta la struttura rilevante - l'ordine come abbiamo verificato, ma anche le operazioni di campo.

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

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

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

Dimostrazione. Dall'osservazione sulla notazione di sopra, abbiamo visto che $\mathbb{Q} \hookrightarrow \mathbb{R}$, da cui $\aleph_0 = |\mathbb{Q}| \leq |\mathbb{R}|$, inoltre \mathbb{Q} è denso in \mathbb{R} , pertanto \mathbb{R} è denso [in se stesso] (per la seconda cosa ci basta che ci sia sempre qualcosa in \mathbb{R} tra due elementi di \mathbb{R} , se questo qualcosa è un elemento di $\iota[\mathbb{Q}]$ poco importa, la proprietà è verificata lo stesso).

Si vede facilmente che \mathbb{R} non ha massimo né minimo, quindi se \mathbb{R} fosse numerabile sarebbe isomorfo, per l'**isomorfismo di Cantor**, a \mathbb{Q} . D'altro canto \mathbb{R} è completo e \mathbb{Q} no, dunque non possono essere isomorfi, e quindi non può esserci una bigezione $\implies \aleph_0 < |\mathbb{R}|$. \square

§8.1 Caratterizzazione dei reali come ordine

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

Proposizione 8.15 (Caratterizzazione di $(\mathbb{R}, <)$)

Sia $(A, <)$ un ordine totale completo senza estremi, supponiamo che esista $B \subseteq A$ numerabile e denso in A , allora $(A, <)$ è isomorfo a $(\mathbb{R}, <)$.

Dimostrazione. \square

Per completezza, definiamo ora la struttura di campo di \mathbb{R} . Non verificheremo le proprietà, e neanche la correttezza di queste definizioni.

Definizione 8.16 (Campo ordinato). $(F, 0, 1, +, \cdot, \leq)$ è un **campo ordinato** se:

- $(F, 0, 1, +, \cdot)$ è un campo
- $(F, <)$ è un'ordine totale⁷¹
- $\forall x, y, z \in F \ x < y \rightarrow x + z < y + z$
- $\forall x, y \in F (0 < x \wedge 0 < y) \rightarrow 0 < x \cdot y$

(le ultime due richieste sono le proprietà di **compatibilità** della struttura di campo [= compatibilità delle operazioni] con l'ordinamento $<$ di F).

Definizione 8.17 (Somma su \mathbb{R}). Dati $x, y \in \mathbb{R}$ definiamo:

$$x + y \stackrel{\text{def}}{=} \{a + b \mid a \in x \wedge b \in y\}$$

Definizione 8.18 (Prodotto su \mathbb{R}). Dati $x, y \in \mathbb{R}$ con $x > 0$ e $y > 0$ definiamo:

$$x \cdot y \stackrel{\text{def}}{=} \{q \in \mathbb{Q} \mid q \leq 0\} \cup \{a \cdot b \mid a \in x \wedge b \in y \wedge a > 0 \wedge b > 0\}$$

Definiamo quindi $-x$ tramite l'inverso additivo ed il prodotto nei casi $x < 0$, $y > 0$ etc. tramite l'uso della regola dei segni.

⁷¹Come ribadito più volte è indifferente usare $<$ o \leq .

Teorema 8.19 (Unicità di $(\mathbb{R}, 0, 1, +, \cdot, \leq)$)

\mathbb{R} dotato delle operazioni definite, è l'unico campo ordinato completo a meno di isomorfismo.

La dimostrazione di questo teorema, talvolta, si vede nei corsi di analisi 1, noi non la studieremo, Per chi fosse interessato: LIBRO DI TESTO, capitolo 10; NOTE DEL PROF. Di Nasso, fascicolo 4; LEZIONE 16 dell'a.a. 2020-21.

§8.2 La cardinalità del continuo è 2^{\aleph_0}

Torniamo ad una questione più strettamente insiemistica.

Teorema 8.20 (Cardinalità del continuo)

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

Questo teorema ci dice, in un modo ancora diverso, che \mathbb{R} è più che numerabile - poiché $\aleph_0 < 2^{\aleph_0}$ (per Cantor) - ma, in più, caratterizza anche esattamente la cardinalità di \mathbb{R} .

Prima della dimostrazione formale, vediamo Intuitivamente perché il risultato è vero. Per definizione $\mathbb{R} \subseteq \mathcal{P}(\mathbb{Q})$, quindi si immerge nelle parti, da cui $|\mathbb{R}| \leq 2^{\aleph_0}$, mentre la disuguaglianza da dimostrare è $2^{\aleph_0} \leq |\mathbb{R}|$.

Esibiamo una funzione iniettiva $\mathcal{P}(\omega) \rightarrow \mathbb{R}$:

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

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

$$f(S) = f(T) \iff \forall i \in \omega \ a_i^S = a_i^T \iff \forall i \in \omega \ i \in S \leftrightarrow i \in T \iff S = T$$

Non è difficile formalizzare questa dimostrazione. Basterebbe definire $0.a_1 a_2 a_3 \dots$ come $\sum_{i=0}^{\infty} a_i 10^{-i}$, poi $\sum_{i=0}^{\infty}$ come $\sup \{\sum_{i=0}^n\}$, poi $\sum_{i=0}^n$ per ricorsione numerabile, poi dimostrare le proprietà aritmetica rilevanti. Noi sfrutteremo la stessa idea, ma formulando la dimostrazione in termini di ordini.

§8.3 Operazioni che coinvolgono la cardinalità del continuo

Prima di dimostrare il teorema, sviluppiamo un po' di aritmetica della cardinalità 2^{\aleph_0} . Questi lemmi sono importanti, e serviranno per calcolare la cardinalità di insiemi concreti.

Osservazione 8.21 — $(2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0}$.

Dimostrazione. Basta osservare che per le proprietà delle operazioni sulla cardinalità $(2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0}$, e, ricordando che prodotto di numerabili è numerabile, si ottiene $2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$. \square

⁷²Sarebbe la scrittura decimale.

Lemma 8.22 (Assorbimento della cardinalità al più continua)

Siano α, β abbreviazioni per o “finito” o \aleph_0 o 2^{\aleph_0} , allora:

$$\alpha + \beta = \alpha \cdot \beta = \max(\alpha, \beta)$$

eccetto il caso $\alpha \cdot 0 = 0 \cdot \beta = 0$.

Dimostrazione. Somme e prodotti di cardinalità finite sono finite (per il [teorema](#) sulle operazioni con cardinalità finite, la somma di cardinalità finite è la cardinalità dalla somma in ω che per definirne è finita, idem prodotto e potenza). Supponiamo quindi $\aleph_0 \leq \beta$ e, senza perdita di generalità, $\alpha < \beta$. Abbiamo:

$$\beta = \beta + 0, \beta \cdot 1 \stackrel{\text{compatib. op. cardin.}}{\leq} \alpha + \beta, \alpha \cdot \beta \stackrel{\text{compatib. op. cardin.}}{\leq} 2\beta, \beta^2 = \beta$$

dove l’ultima uguaglianza vale perché sia $\aleph_0^2 = \aleph_0$ (e siamo nel caso in cui β o è \aleph_0 o è 2^{\aleph_0}), sia $2^{\aleph_0} \leq (2^{\aleph_0})^2 \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0}$ (le disuguaglianze sono al solito tutte giustificate dall’osservazione sulla compatibilità di \leq con le operazioni fra cardinalità). Pertanto si conclude l’enunciato usando Cantor-Bernstein nella serie di disuguaglianze sopra, che ci danno proprio la tesi (ricordando che avevamo scelto WLOG β come massimo). \square

Lemma 8.23 ($\alpha^{\aleph_0} = 2^{\aleph_0}$)

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

§8.4 Sottrarre un numerabile dal continuo

Stato del corso

È un dato di fatto - il primo teorema di incompletezza di Gödel - che ogni teoria **calcolabile** - i cui assiomi possano, cioè, essere elencati in maniera meccanica - è necessariamente incompleta. L'incompletezza non è quindi un difetto, o meglio, che lo sia oppure no è irrilevante, perché non può essere evitata.

Tuttavia, gli assiomi che abbiamo introdotto fino ad ora lasciano aperte lacune che sarebbe desiderabile colmare.

1. Sarebbe ragionevole che questi insiemi esistessero:

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

$$\{\omega, s(\omega), s(s(\omega)), s(s(s(\omega))), \dots\}$$

Però gli assiomi 1-7 non bastano né per dimostrarne l'esistenza, né - e questo sarebbe disastroso - permettono di escluderla.

2. Alcune questioni sulle cardinalità, come per esempio la confrontabilità, non possono essere decise sulla base dei soli assiomi 1-7. Inoltre ci mancano risultati desiderabili per via delle applicazioni, segnatamente il lemma di Zorn.
3. Vi sono insiemi la cui esistenza vorremmo escludere. Per esempio vorremmo che l'equazione $X = \{X\}$ non avesse soluzioni, e farebbe comodo escludere l'esistenza di qualcosa del tipo $Y = \{\{\{\{\dots\}\}\}\}$ con infinite parentesi annidate. Il guaio qui non è grave, ma questi oggetti contraddicono, in parte, l'intuizione che vorremmo concretizzare negli assiomi della teoria degli insiemi. Noi vorremmo che un insieme fosse identificabile dalla sua struttura. Mi spiego, per esempio \emptyset è identificato dal fatto di non avere elementi, $\{\emptyset\}$ è identificato dal fatto di avere un solo elemento che non ha elementi etc. per tutti gli insiemi che conosciamo, ma cosa dire di Y ? Y ha un elemento Y_1 , che ha un elemento Y_2 , che ha ... e la stessa descrizione si potrebbe applicare anche a Y_1 , e anche a Y_2 ... Sono tutti uguali?

Queste tre lacune saranno colmate dai tre assiomi che ancora ci mancano: rispettivamente l'assioma del rimpiazzamento, l'assioma della scelta e l'assioma di buona fondazione. La teoria risultante sarà, inevitabilmente, incompleta - per esempio non decide il problema del continuo: l'esistenza di cardinalità intermedie fra \aleph_0 e 2^{\aleph_0} - ma è la fondazione meglio accettata della matematica.

§9 I buoni ordinamenti

Il nostro prossimo obiettivo è definire e studiare la classe dei **numeri ordinali**. Questa può essere pensata come la più vasta classe - dotata di un ordinamento totale definito per mezzo di una formula - su cui sia corretto ragionare per induzione forte. Conteremo, quindi, sugli ordinali per formulare l'induzione e la ricorsione transfinita, procedimenti che superano la forza dimostrativa dell'induzione e della ricorsione aritmetica - per esempio permettendo di ottenere il teorema di Cantor-Lebesgue sugli insiemi di unicità. Siccome l'induzione forte equivale al principio del minimo, studieremo i buoni ordini. In questa sezione, dimostreremo il risultato seguente.

Teorema 9.1 (Isomorfismo di buoni ordini)

Siano $(A, <_A)$ e $(B, <_B)$ ^a insiemi bene ordinati, allora vale **una e una sola** delle seguenti:

- $(A, <_A)$ è isomorfo a un segmento iniziale proprio di $(B, <_B)$
- $(A, <_A)$ e $(B, <_B)$ sono isomorfi
- $(B, <_B)$ è isomorfo a un segmento iniziale di $(A, <_A)$

^aNel seguito scriveremo semplicemente $(A, <)$ e $(B, <)$ per comodità.

Ossia se definiamo:

$$(A, <_A) \prec (B, <_B) \stackrel{\text{def}}{=} \exists C \text{ } C \text{ segmento iniziale proprio di } (B, <_B) \text{ e } (A, <_A) \sim C$$

allora \prec soddisfa le proprietà formali di un ordinamento totale fra le classi di isomorfismo di buoni ordini. Definiamo altresì:

$$(A, <_A) \preceq (B, <_B) \stackrel{\text{def}}{=} (A, <_A) \prec (B, <_B) \vee (A, <_A) \sim (B, <_B)$$

ossia “ $(A, <_A)$ è isomorfo a un segmento iniziale [proprio o meno] di $(B, <_B)$ ”.

Richiamiamo le definizioni fondamentali.

Definizione 9.2 (Buon ordinamento). $(A, <)$ è un **buon ordinamento** se ogni $B \subseteq A$ non vuoto ha un minimo elemento.

Definizione 9.3 (Segmento iniziale). Dato un ordine totale $(A, <)$, $B \subseteq A$ è un **segmento iniziale** se $\forall b \in B \forall x \in A \ x < b \rightarrow x \in B$.

Definizione 9.4 (Segmenti iniziali propri e principali). Il segmento iniziale B è **proprio** se $B \neq A$. Il segmento iniziale B è **principale** se [è della forma]:

$$B = A_a \stackrel{\text{def}}{=} \{x \in A \mid x < a\}$$

per qualche $a \in A$, e, in questo caso, si dice **segmento iniziale principale determinato da a** .

È chiaro che un segmento iniziale principale, A_a , è **sempre** proprio, perché $a \notin A_a$, e nel caso dei buoni ordini questa è una doppia implicazione (quindi se è proprio è anche principale).

Proposizione 9.5 (proprio \implies principale nei buoni ordini)

Ogni segmento iniziale proprio di un buon ordine è principale.