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

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.

Ringraziamenti

Francesco Sorce.

§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:

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

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 $f : \mathbb{R} \longrightarrow \mathbb{R}$ 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] $f(x) = \alpha x + \beta$.
[b] Ovvero f non ha punti angolosi.

Esempio 1.6
$X = \{\ldots, a_{-2}, a_{-1}, a_0, a_1, a_2, \ldots\} = \{a_i | i \in \mathbb{Z}\}$ con $\ldots < a_{-2} < a_{-1} < a_0 < a_1 < a_2 < \ldots$, $\lim_{i \to +\infty} a_i = +\infty$, $\lim_{i \to -\infty} a_i = -\infty$ ha la proprietà data dal Fatto 1.5, quindi è di unicità.

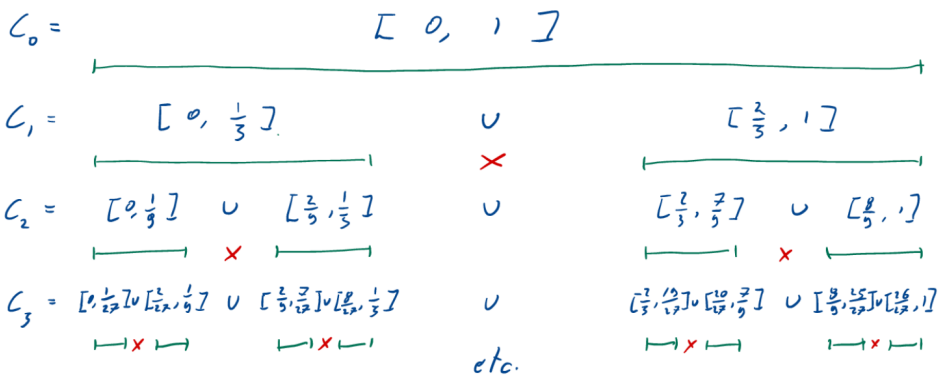
NON Esempio 1.7

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.

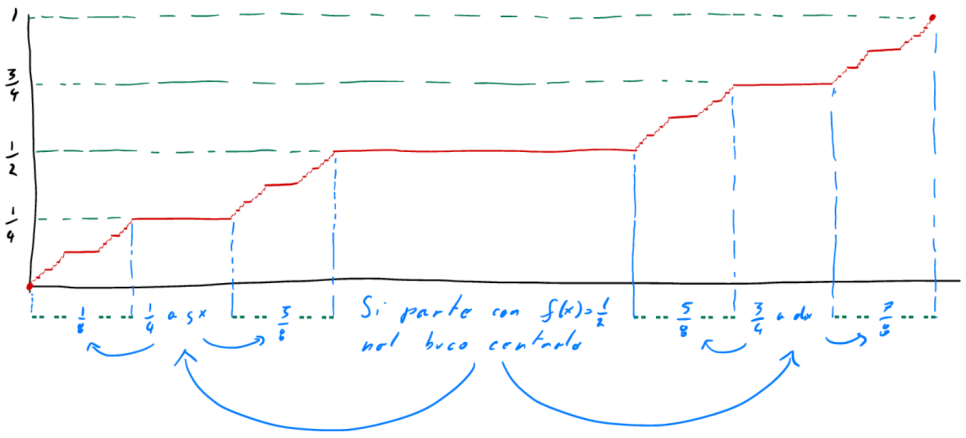
Possiamo costruire l'insieme di Cantor a partire dall'intervallo $C_0 = [0,1]$ nel seguente modo:



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

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

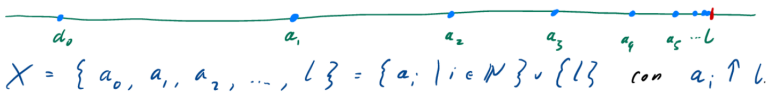
Esiste una funzione continua (e crescente) $f : \mathbb{R} \longrightarrow \mathbb{R}$ detta **scala di Cantor** (o **scala del diavolo**), tale che $f'(x) = 0$ per $x \notin C$ e non è derivabile in $x \in C$.



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

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

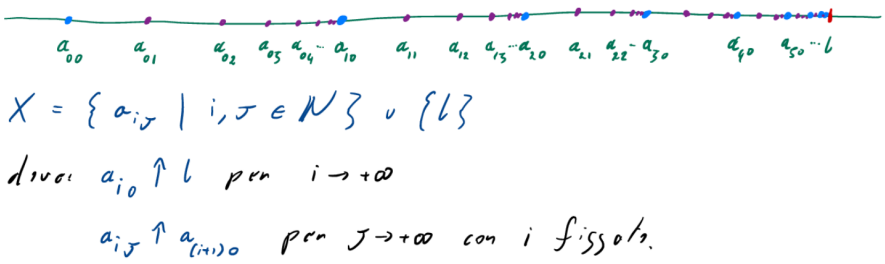
Esempio buffo 1.10
L'insieme degli elementi di una successione crescente col suo limite è un esempio di insieme di unicità.



Dimostriamo quindi che X è un insieme di unicità.

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

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 $a'_i = a_{i0}$. □

§1.1 Digressione: insiemi numerabili

Definizione 1.12. Un insieme X è **numerabile** se è il supporto di una successione, $X = \{a_0, a_1, a_2, \ldots\} = \{a_i | i \in \mathbb{N}\}$, 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 bigezione.
- I numeri dispari, con la bigezione data da $a_i = 2i + 1$.
- I numeri primi, $a_i = p_i$, con p_i i-esimo numero primo.
- $\mathbb{Z}$ l'insieme dei numeri interi, con la bigezione data da $a_i = (-1)^i \left\lceil \frac{i}{2} \right\rceil$.

Esempio meno immediato 1.14

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

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

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:

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

dove i minimi esistono perché Y non è finito. □

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 $X \times Y = \{(a_{i_t}, a_{j_t}) | t \in \mathbb{N}\}$. □

Esempio 1.17

$\mathbb{Q}$ è numerabile.

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

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

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

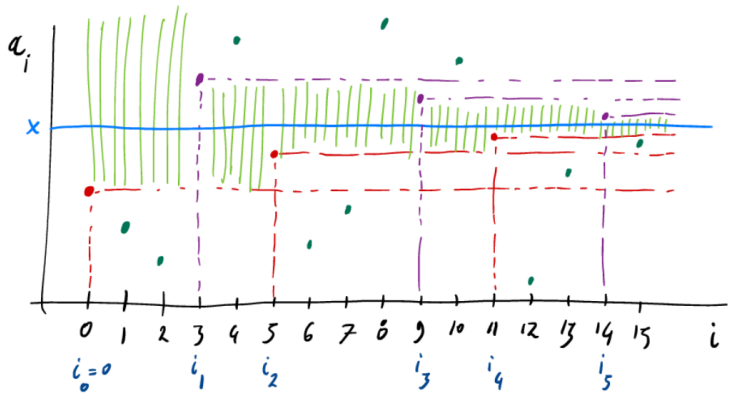
□

NON Esempio 1.18
$\mathbb{R}$ non è numerabile.

Dimostrazione. Supponendo, per assurdo, che $\mathbb{R} = \{a_i | i \in \mathbb{N}\}$, 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:

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

graficamente:



Si vede facilmente (esercizio!) che la successione $\{a_{i_{2k}}\}_k$ è crescente, $\{a_{i_{2k+1}}\}_k$ è decrescente e $\lim_{k\to+\infty} a_{i_{2k}} \leq \lim_{k\to+\infty} a_{i_{2k+1}}$. Fissiamo x tale che $\lim_{k\to+\infty} a_{i_{2k}} \leq x \leq \lim_{k\to+\infty} a_{i_{2k+1}}$. 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.

□

[2] num. = numeratore, den. = denominatore.

§1.2 Tornando agli insiemi di unicità

Teorema 1.21 (Cantor-Lebesgue)
Se $X \subseteq \mathbb{R}$ è chiuso e numerabile, allora X soddisfa il Fatto 1.5, ed è, quindi, di unicità.

La strategia di dimostrazione passa attraverso una definizione.

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

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

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

Osservazione 1.23 — Se X è chiuso e per X' vale il Fatto 1.5, allora anche per X vale il Fatto 1.5.

Dimostriamo questo fatto.

Dimostrazione. Occorre dimostrare che se f è continua, lineare, ristretta agli intervalli aperti che non intersecano X, e non ha punti angolosi, allora f è lineare ristretta agli intervalli aperti che non intersecano X'. Fatto questo, usando l'ipotesi su X', f è lineare - abbiamo quindi mostrato che per X vale Fatto 1.5.
Sia $]a,b[\cap X' = \emptyset$, dobbiamo dire che $f_{|]a,b[}$ è lineare. Ci basta dire che per ogni $\varepsilon > 0$, $f_{|[a+\varepsilon, b-\varepsilon]}$ è lineare. Siccome $]a,b[\cap X' = \emptyset$, $]a,b[\cap X = \{\text{punti isolati di } X\}$. Quindi $[a+\varepsilon, b-\varepsilon] \cap X$ è finito - se così non fosse, avrebbe un punto di accumulazione 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. □

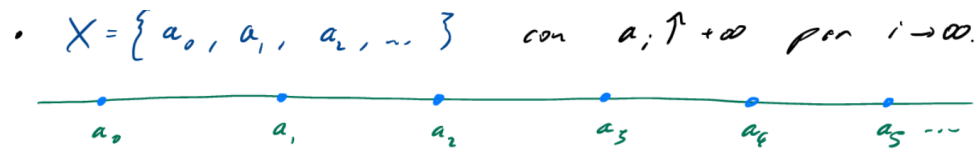
Corollario 1.24
Sia $X^{(n)} = X''^{\cdots}$[a]. Se $X^{(n)} = \emptyset$ per qualche $n \in \mathbb{N}$, allora per X vale il Fatto 1.5.

[a] n volte.

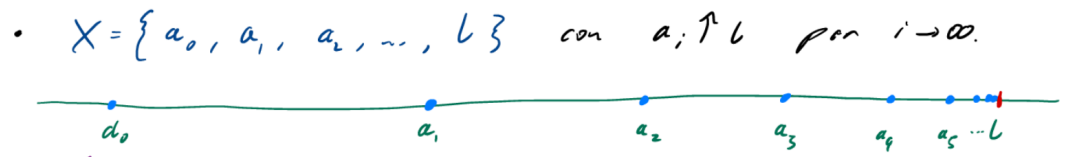
Dimostrazione. Induzione su n. □

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

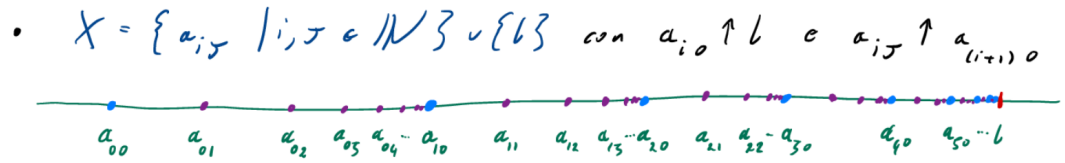
Esempio 1.25
Vogliamo costruire X chiuso e numerabile tale che $X^{(n)} \neq \emptyset$ per ogni $n \in \mathbb{N}$. Cominciamo col rivedere alcuni esempi già visti.



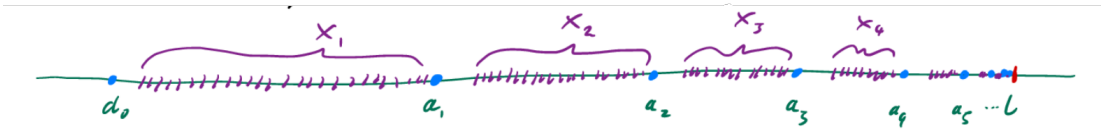
Tutti i punti sono isolati, $X' = \emptyset$.



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



"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:



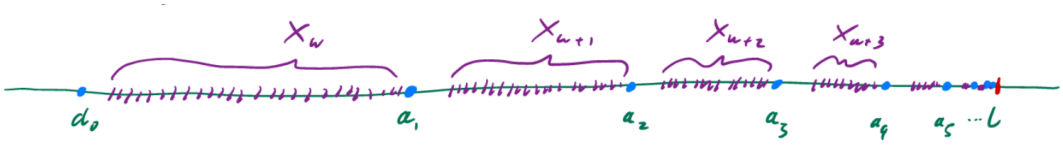
È chiaro che, per ogni n, $X_\omega^{(n)} \neq \emptyset$. D'altro canto, X_ω soddisfa il Fatto 1.5, perché f deve essere lineare in ciascuno degli intervalli $[a_n, a_{n+1}]$, perché X_{n+1} soddisfa il Fatto 1.5, quindi ci si riduce al caso della successione.

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 ω^ω, ω^{ω^ω}, etc. È questa la soluzione allora?
No, ogni sforzo di trovare l'induzione a capo delle induzioni è vano. Se ho X_ω, X_{ω^ω}, $X_{\omega^{\omega^\omega}}$, 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:

$$N = \{\text{collezioni } X \,|\, X \notin X\}$$

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 $\{X|P(X)\}$ - 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 centro parole. Alcune di queste descrivono un numero naturale,

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

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

Il guaio chiaramente, è che lo abbiamo appena descritto con sedici parole.
Quindi non ci si può fidare troppo neppure dell'italiano, o meglio, non è possibile descrivere precisamente cosa sia una descrizione precisa.
In conclusione, occorre fissare un linguaggio formale in cui si esprimano le proposizioni della teoria degli insiemi, e occorre fissare un sistema di assiomi, espressi in questo linguaggio, che 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:

    $\neg\Phi \equiv$ "Φ è falsa"
    $\Phi \wedge \psi \equiv$ "Φ e ψ sono entrambe vere"
    $\Phi \vee \psi \equiv$ "almeno una fra Φ e ψ è vera"

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

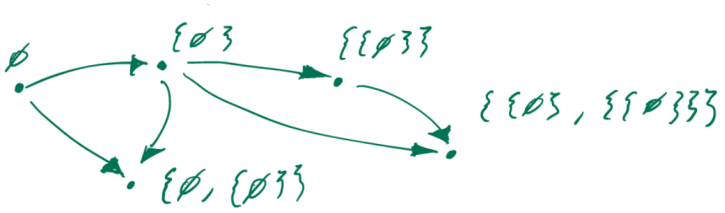
    $$\forall x \,\text{formula} \qquad \exists x \,\text{formula}$$

    ad esempio:

    $\forall x\, \Phi \equiv$ "Φ è vera qualunque sia l'insieme x"
    $\exists x\, \Phi \equiv$ "c'è un insieme x che fa si che Φ sia vera"

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

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



[3] "appartiene a".

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

$$\text{“}a \text{ è un elemento di un certo } b\text{”} \equiv \text{“c'è un percorso di due frecce fra } a \text{ e } b\text{”}$$

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

$$\text{“}a \text{ è un sottoinsieme di } b\text{”} \equiv \text{“ogni elemento di } a \text{ è elemento di } b\text{”} \equiv$$

$$\equiv \text{“non c'è un insieme che è elemento di } a \text{ e non di } b\text{”} \equiv$$

$$\equiv \text{“non c'è un vertice con una freccia verso } a \text{ e non una verso } b\text{”}$$

che corrisponde mediante formule insiemistiche a $\neg\exists x(x \in a \land \neg x \in b)$ (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 $\Phi_1 \land \Phi_2 \lor \Phi_3$ è ambigua, perché si potrebbe leggere $(\Phi_1 \land \Phi_2) \lor \Phi_3$ o $\Phi_1 \land (\Phi_2 \lor \Phi_3)$. In una notazione completamente parentesizzata, per esempio, la formula per “a è un sottoinsieme di b” sarebbe:

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

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

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

$$x \neq y \stackrel{\text{def}}{=} \neg x = y \text{[5]} \qquad x \notin y \stackrel{\text{def}}{=} \neg x \in y \qquad \nexists x\, \Phi \stackrel{\text{def}}{=} \neg\exists x\, \Phi$$

$$\Phi \to \psi \stackrel{\text{def}}{=} \psi \lor \neg\Phi \qquad \Phi \leftrightarrow \psi \stackrel{\text{def}}{=} (\Phi \to \psi) \land (\psi \to \Phi)$$

$$\exists x \in y\ \Phi \stackrel{\text{def}}{=} \exists x(x \in y \land \Phi) \qquad \forall x \in A\ \Phi \stackrel{\text{def}}{=} \forall x(x \in A \to \Phi)$$

$$\exists!\, x\, \Phi(x) \stackrel{\text{def}}{=} \exists x(\Phi(x) \land \forall y(\Phi(y) \to y = a))$$

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

$$A \subseteq B \stackrel{\text{def}}{=} \forall x(x \in A \to x \in B) \qquad A \subsetneq B \stackrel{\text{def}}{=} (A \subseteq B) \land (A \neq B)$$

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

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

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

[4] Mi riservo in queste dispense di modificare un pochino questa regola, qualora alcune formule risultassero più leggibili con le parentesi.
[5] Cioè “non è vero che x è uguale a y”.

Esercizio 2.3. Esprimi queste proposizioni mediante formule insiemistiche pure:

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

[a] Qui assumi che l'unione e intersezione esistano e siano uniche.

§2.1 Le regole di inferenza

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

1 Sono argomento del corso di logica.

2 In realtà, scrivere le dimostrazioni in maniera formale, le renderebbe lunghissime e particolarmente incomprensibili.

3 In pratica, non si sbaglia facendo ragionamenti che non reggono, si sbaglia dicendo cose fumose che non possono essere espresse nel linguaggio della teoria. Per esempio, le parole "e così via" sono pericolose.

4 Conoscere le regole - fidatevi - non aiuta né a trovare né a capire le dimostrazioni.

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

Tavole di verità Due combinazioni mediante connettivi logici ($\neg$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$) delle stesse formule - "**combinazioni booleane**" - alle volte, dicono la stessa cosa. Per esempio, $\neg\Phi \vee \neg\psi \equiv$ [6] $\neg(\Phi \wedge \psi)$. Per verificare questo fatto basta considerare tutte le possibili combinazioni di valori di verità che possono assumere le formule combinate - nell'esempio Φ e ψ - compilando una "**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:

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

$$\neg(\Phi \wedge \psi) \equiv \neg\Phi \vee \neg\psi \qquad \neg(\Phi \vee \psi) = \neg\Phi \wedge \neg\psi \text{ [7]}$$

$$\Phi \to \neg\psi \equiv \psi \to \neg\Phi \qquad \Phi \to \psi \equiv \neg\psi \to \neg\Phi$$

[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.

$$\neg\forall x\,\Phi \equiv \exists x\,\neg\Phi \qquad \neg\forall x\,\neg\Phi \equiv \exists x\,\Phi$$
$$\neg\exists x\,\Phi \equiv \forall x\,\neg\Phi \qquad \neg\exists x\,\neg\Phi \equiv \forall x\,\Phi$$

Esercizio 2.5. Convinciti della validità delle equivalenze precedenti.

Esercizio 2.6. Dimostra che:

$$\neg\forall x \in A\,\Phi \equiv \exists x \in A\,\neg\Phi \qquad \neg\exists x \in A\,\Phi \equiv \forall x \in A\,\Phi$$

Esercizio 2.7. Dimostra che:

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

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

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

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 $a = b \to \forall x(x \in a \leftrightarrow x \in b)$, in realtà, segue dal fatto che se $a = b$ allora a e b sono indistinguibili[a].

[a] Nel senso che abbiamo descritto in precedenza, cioè sono nomi della stessa cosa.

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

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

Proposizione 3.5 (Unicità dell'insieme vuoto)
C'è un unico insieme vuoto.

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

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

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

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

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:

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

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

$$(\forall y \, y \notin x_1) \wedge \forall x_2 (\forall y \, y \notin x_2) \to x_2 = x_1$$

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

$$\forall x_2 (\forall y \, y \notin x_2) \to x_2 = x_1$$

Ora prendiamo un x_2 qualunque, dobbiamo dimostrare:

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

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:

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

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

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:

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

§3.2 Assioma di separazione

Assioma 3.7 (Assioma di separazione)

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

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

[a] Stiamo usando già questa notazione, ma la definiremo a breve.

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

Proposizione 3.9

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

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

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

$$\forall x\, x \in B_1 \leftrightarrow (x \in A \land \psi(x)) \qquad \forall x\, x \in B_2 \leftrightarrow (x \in A \land \psi(x))$$

Allora, $\forall x\, x \in B_1 \leftrightarrow (x \in A \land \psi(x)) \leftrightarrow x \in B_2$, quindi ciò coimplica, per estensionalità, che $B_1 = B_2$. □

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

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

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

Osserviamo che l'assioma di separazione è una forma indebolita del principio di collezione[8]. Rimpiazzando il principio con questo assioma, il Paradosso di Russell diventa una proposizione.

Proposizione 3.12 (Insieme di tutti gli inisemi)
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:

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

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

$$\forall x\, x \in N \leftrightarrow (x \in V \land x \notin x)$$

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. □

§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 $C \in$ 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 $\psi(x)$.

[8] Quel principio che definisce gli insiemi come tutte le cose che soddisfano una certa formula.
[9] Ovvero per tutti gli oggetti (solo gli insiemi in questo caso) che soddisfano una tale formula $\psi(x)$.

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

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

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

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

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

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

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

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

che equivale $A = B$ per estensionalità. Ha quindi senso, con un leggero abuso di notazione, omettere il cappelletto ˆ 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 $\{x|$ 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.

[10] Cioè la classe degli insiemi che soddisfano il predicato $\psi(x) : x = x$ (ovvero tutti gli insiemi per quanto assunto all'inizio della teoria), $V = \{x|\psi(x)\} = \{x|x = x\}$ (dove naturalmente non sto usando separazione ma il principio di collezione perché stiamo definendo una classe).
[11] Essere un insieme per una classe significa quindi moralmente identificarvisi nel senso riportato sopra, se ciò non fosse possibile parliamo di classi proprie.

Assioma 3.16 (Assioma del paio)
Dati a e b esiste l'insieme $\{a, b\}$.

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

Proposizione 3.17 (Unicità del paio)
Fissati a e b, l'insieme $\{a, b\}$ è univocamente determinato.

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

Esercizio 3.18. Dimostra la proposizione precedente.

Soluzione. Supponiamo che esistano P_1 e P_2 tali che:

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

da ciò segue che:

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

dunque per estensionalità l'espressione sopra equivale a $P_1 = P_2$. □

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]. □

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 $\{a, b\} = \{b, a\}$. □

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

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

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

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

Proposizione 3.23 (Proprietà di coppia ordinata)
La coppia di Kuratowski (a, b) rappresenta la coppia ordinata di a e b, ossia vale che:

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

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

$$x = a \leftrightarrow \forall y \in c(x \in y)$$ [13]

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

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

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:

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

in tal modo abbiamo che:

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

Possiamo quindi ricavare la tesi come segue:

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

(dove nel secondo passaggio abbiamo usato estensionalità per giustificare le uguaglianze). □

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

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

[13] Sostanzialmente stiamo dicendo che preso un elemento x, $x = a$ se e solo se, preso un elemento di $(a, b) = \{\{a\}, \{a, b\}\}$, x appartiene sempre a tale elemento (dovendo appartenere sia ad $\{a\}$ che ad $\{a, b\}$ sarà per forza a).
[14] Cioè sto dicendo la coppia è in realtà un insieme fatto da un solo insieme.

Nota 3.25 — Quest'ultima definizione è, in realtà, uno schema di definizioni: una per ogni n. Per ora, NON siamo in grado di scrivere, per esempio, una formula insiemistica che dica "Esiste un n ed una n-upla $(a_1, \dots, a_n)$ tale che...". Però, per ogni n dato, chessò 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:

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

$$(a_1, \dots, a_n) = (a_1', \dots, a_n') \leftrightarrow a_1 = a_1' \land \dots \land a_n = a_n'$$

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.

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

[a] Cioè x è un elemento di B se e solo se è un elemento di un elemento di A.

Proposizione 3.29 (Unicità dell'unione)
Vale l'unicità dell'unione:

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

Dimostrazione. Supponiamo di avere B_1 e B_2 tali che:

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

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

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

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

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

[a] "Unione di A".

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

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

[a] Cioè per ogni insieme esiste l'insieme di tutti gli elementi degli elementi di A.

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

Definizione 3.32 (Unione di insiemi)**.** Poniamo:

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

Proposizione 3.33 (Caratterizzazione unione di insiemi)
Dati a, b e $a \cup b$ vale che:

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

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

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:

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

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):

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

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

ovvero il sottoinsieme di z di tutti gli elementi che appartengono a tutti gli elementi di C. Chiaramente (per definizione) $x \in B \to \forall y \in C(x \in y)$, d'altro canto, $\forall y \in C(x \in y)$ implica, in particolare (un tale x appartiene a tutti gli elementi della classe e quindi anche a z), $x \in z$, quindi in automatico $x \in B$.
Abbiamo così verificato che $x \in B \leftrightarrow \forall y \in C(x \in y)$, ossia $B = \bigcap C$ (moralmente abbiamo costruito l'intersezione di un insieme per separazione su un elemento della classe C (o insieme se lo è), come il sottoinsieme di tutti gli elementi che stanno in tutti gli elementi della classe). L'ultimo ragionamento può essere pensato anche nel seguente modo:

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

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. □

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

$$a \cap b \overset{\text{def}}{=} \bigcap\{a, b\} \qquad \text{e} \qquad a \setminus b \overset{\text{def}}{=} \{x \in a | x \notin b\}$$

Proposizione 3.38 (Caratterizzazione intersezione e differenza di insiemi)
Vale che:

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

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

Proposizione 3.40 (Proprietà di unione, intersezione e differenza di insiemi)
Alcune proprietà delle operazioni $\cup$, $\cap$, $\setminus$:

commutatività:	$a \cup b = b \cup a \qquad \text{e} \qquad a \cap b = b \cap a$
associatività:	$a \cup (b \cup c) = (a \cup b) \cup c \overset{\text{def}}{=} a \cup b \cup c$
	$a \cap (b \cap c) = (a \cap b) \cap c \overset{\text{def}}{=} a \cap b \cap c$
distributività:	$a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$
	$a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$
leggi di De Morgan:	$a \setminus (b \cup c) = (a \setminus b) \cap (a \setminus c)$
	$a \setminus (b \cap c) = (a \setminus b) \cup (a \setminus c)$

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

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

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

□

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):

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

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 $A \to B$ saranno poi sottoinsiemi di $A \times B$, e vorremo parlare dell'insieme ${}^A B$ delle funzioni $A \to B$. 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.

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

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

Proposizione 3.45 (Unicità delle parti)
Vale che:
$$\forall A\ \exists! B\ \forall x\ x \in B \leftrightarrow x \subseteq A$$

Dimostrazione. Segue come sempre per estensionalità, in quanto, se avessimo B_1, B_2, allora:
$$\forall x(x \in B_1 \leftrightarrow x \subseteq A) \qquad \text{e} \qquad \forall x(x \in B_2 \leftrightarrow x \subseteq A)$$
quindi $\forall x((x \in B_1) \leftrightarrow (x \subseteq A) \leftrightarrow (x \in B_2)) \leftrightarrow \forall x(x \in B_1 \leftrightarrow x \in B_2) \leftrightarrow B_1 = B_2$. □

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

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

Dimostrazione. L'unicità è conseguenza immediata della definizione e dell'assioma di estensionalità (stessa dimostrazione di sempre). Per l'esistenza, definiamo per separazione:
$$A \times B \stackrel{\text{def}}{=} \{z \in \mathcal{P}(\mathcal{P}(A \cup B)) | \exists x \in A\ \exists y \in B\ z = (x, y)\}$$
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. □

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

[17] Poniamo $a, b, \ldots \in z \stackrel{\text{def}}{=} a \in z \wedge b \in z \wedge \ldots$ e $a, b, \ldots \subseteq z \stackrel{\text{def}}{=} a \subseteq z \wedge b \subseteq z \wedge \ldots$
[18] Tutte le implicazioni si basano sul fatto che se un oggetto è sottoinsieme di un qualche insieme allora è un elemento del corrispondente insieme delle parti per definizione.

§3.7 Relazioni di equivalenza e di ordine, funzioni

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

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

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

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

Esempio 3.51

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

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

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

(i) **riflessiva**: $\forall x \in A\ x \sim x$.

(ii) **simmetrica**: $\forall x, y \in A$[19] $x \sim y \leftrightarrow y \sim x$.

(iii) **transitiva**: $\forall x, y, z \in A\ (x \sim y \wedge y \sim z) \to x \sim z$.

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

(i) **riflessiva**: $\forall x \in A\ x \leq x$.

(ii) **antisimmetrica**: $\forall x, y \in A\ (x \leq y \wedge y \leq x) \to x = y$.

(iii) **transitiva**: $\forall x, y, z \in A\ (x \leq y \wedge y \leq z) \to x \leq z$.

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

(i) **irriflessiva**: $\forall x \in A\ \neg(x < x)$.

(ii) **transitiva**: $\forall x, y, z \in A\ (x < y \wedge y < z) \to x < z$.

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

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

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

[19] $\forall x_1, \ldots, x_n \stackrel{\text{def}}{=} \forall x_1 \ldots \forall x_n$, 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:

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

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

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

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

[a] Formalmente: $\{z \in A \times A | \exists x, y \in A \; z = (x,y) \wedge \ldots\}$.
[b] Come la nota sopra.

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

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

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. □

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:

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

□

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. □

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

$$\mathrm{Dom}(\mathcal{R}) \stackrel{\text{def}}{=} \{x \in A | \exists y \in B \; x\mathcal{R}y\} \qquad \textbf{dominio} \text{ di } \mathcal{R}$$
$$\mathrm{Im}(\mathcal{R}) \stackrel{\text{def}}{=} \{y \in B | \exists x \in A \; x\mathcal{R}y\} \qquad \textbf{immagine} \text{ di } \mathcal{R}$$

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

Definizione 3.63 (Funzione)**.** Chiamiamo **funzione** $f : A \to B$ 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 $S \subseteq \mathrm{Dom}(f)$, indichiamo l'immagine di un sottoinsieme (ovvero l'insieme delle immagini del sottoinsieme) come:

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

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

iniettiva se: $\forall y \in \mathrm{Im}(f) \; \exists! \, x \in \mathrm{Dom}(f) \; f(x) = y$
suriettiva se: $B = \mathrm{Im}(f)$ 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:

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

Osservazione 3.67 — Se f iniettiva, $f^{-1} : \mathrm{Im}(f) \to \mathrm{Dom}(f)$ 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 $x \in \mathrm{Dom}(f)$ tale che $y = f(x)$). In particolare se $f : A \to B$ è bigettiva, allora f^{-1} è bigettiva.

[a] Altrimenti è la semplice controimmagine di un sottoinsieme dell'immagine (che non è una funzione).

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

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

"f **ristretta** ad A'" è una funzione: $A' \to B$.

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

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

"f **composta** con g" è una funzione: $A \to C$.

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

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

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

$$g = f^{-1} \qquad g \circ f = \mathrm{id}_A \qquad f \circ g = \mathrm{id}_B$$

Esercizio 3.72. Data $g : A \to B$ e $f : B \to C$, sotto quali condizioni $f \circ g$ è iniettiva, suriettiva, bigettiva?

Esercizio 3.73. Data una relazione di equivalenza $\sim$ su A, dimostra che esiste un insieme $A/\sim$ ed una funzione surgettiva $i_\sim$ da A a $A/\sim$ tale che:

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

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

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

§4 Assioma dell'infinito e numeri naturali

Il nostro prossimo obiettivo è definire i numeri naturali. I soli oggetti della teoria degli insiemi sono gl 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:

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

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

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, 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.

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

$$\forall x(x \in \omega \leftrightarrow (\forall A \text{ “}A \text{ è induttivo”} \rightarrow x \in A))^{21}$$

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

Definizione 4.5. Definiamo:

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

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

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 $\{\{\emptyset\}\}$.

§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. In questo senso, quindi, ω codifica legittimamente i numeri naturali.

Definizione 4.8 (Assiomi di Peano al secondo ordine (qualunque cosa questo significhi...))**.** Dato un insieme $\mathbb{N}$, un elemento $0 \in \mathbb{N}$, e una funzione:

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

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

(a) Il successore è iniettivo:

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

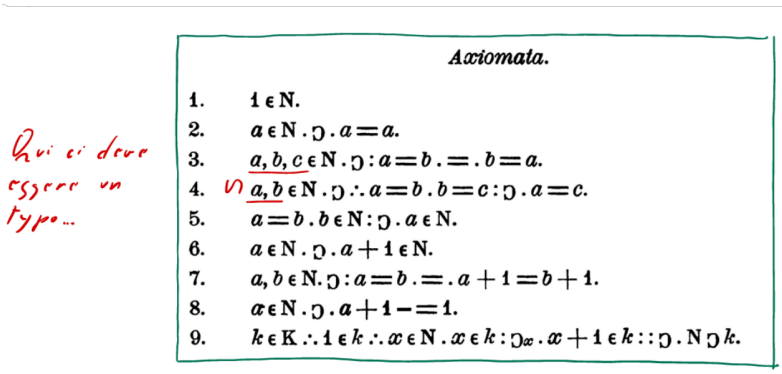
(b) Lo zero non è un successore:

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

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

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

[21] Cioè 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).



Axiomata.

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

Qui ci deve essere un typo...

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

Teorema 4.9
La funzione succ : $\omega \longrightarrow \omega$, $\text{succ}(n) = s(n)$, è ben definita e $(\omega, \emptyset, \text{succ})$ soddisfa gli assiomi di Peano.

Dimostrazione. Per controllare che succ sia ben definita, occorre assicurarsi che se $n \in \omega$, allora $s(n) \in \omega$. 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 $s(n) \in \omega$. 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:

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

contro la definizione di $\emptyset$.

(c) Dimostriamo che l'insieme $A = \{n \in \omega | \Phi(n)\}$ è induttivo, da cui $\omega = A$[22], quindi $\forall n \in \omega \ \Phi(n)$.

1. Per ipotesi abbiamo che $\Phi(\emptyset)$, quindi $\emptyset \in A$.
2. $n \in A \underbrace{\Longrightarrow}_{\text{per ipotesi}} \Phi(n) \implies \Phi(s(n)) \underbrace{\Longrightarrow}_{\text{perché } n \in \omega \to s(n) \in \omega} s(n) \in A$

(a) La dimostrazione passa attraverso due lemmi.

Lemma 4.10 (Lemma 1)
$\forall n \in \omega \ \bigcup n \subseteq n$.

Dimostrazione. Per induzione (c) con $\Phi(n) \overset{\text{def}}{=} \bigcup n \subseteq n$.

$$\Phi(\emptyset): \qquad \bigcup \emptyset = \emptyset \subseteq \emptyset$$

$$\Phi(n) \to \Phi(s(n)): \qquad \bigcup(s(n)) = \bigcup(n \cup \{n\}) = \left(\bigcup n\right) \cup n = n \subseteq s(n)$$

[22] Stiamo costruendo A come sottoinsieme di ω.

Dove la penultima uguaglianza vale in quanto:

$$\begin{aligned} x \in \bigcup(n \cup \{n\}) &\iff \exists y\, x \in y \wedge y \in n \cup \{n\} \\ &\iff \exists y\, x \in y \wedge (y \in n \vee y = n) \\ &\iff \exists y\, (x \in y \wedge y \in n) \vee (x \in y \wedge y = n) \\ &\iff \exists y\, (x \in y \wedge y \in n) \vee \exists y (x \in y \wedge y = n) \\ &\iff x \in \bigcup n \vee x \in N \\ &\iff x \in \left(\bigcup n\right) \cup n \end{aligned}$$

Mentre l'ultima in quanto, per ipotesi induttiva, $\bigcup n \subseteq n$, quindi $(\bigcup n) \cup n \subseteq n \cup n = n$. □

Lemma 4.11 (Lemma 2)
$\forall n \in \omega\ \bigcup s(n) = n$.

Dimostrazione. Come nel passo induttivo della dimostrazione precedente:

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

dove l'ultima uguaglianza abbiamo $\bigcup n \subseteq n$, non per ipotesi induttiva, ma per il Lemma 1. □

Finalmente abbiamo che, per il Lemma 2:

$$s(m) = s(n) \implies m = \bigcup s(m) = \bigcup s(n) = n$$

□

§4.2 L'ordine di omega

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

Notazione 4.12 — Dati $m, n \in \omega$, scriviamo:

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

Proposizione 4.13
La relazione $<$ è un ordine totale su ω.

Per dimostrare questa proposizione, sono comodi alcuni lemmi.

Osservazione 4.14 — Si osserva che:

1. $m \in n \to m \in s(n)$, infatti $n \subseteq n \cup \{n\} = s(n)$.

2. $m \in s(n) \to (m \in n \vee m = n)$, infatti:

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

Lemma 4.15
$\forall a, b \in \omega\ a \in b \to (s(a) \in b \vee s(a) = b)$.

Dimostrazione. Induzione su b.

- Caso $b = 0$: $a \in \emptyset \to \ldots$ vera a vuoto, perché $a \in \emptyset$ è falsa.
- Caso $b = s(n)$: l'ipotesi induttiva è $a \in n \to (s(a) \in n \vee s(a) = n)$. Dobbiamo dimostrare:
$$a \in s(n) \to (s(a) \in s(n) \vee s(a) = s(n))$$
abbiamo che $a \in s(n) \implies a \in n \cup \{n\} \implies a \in n \vee a = n$. Quindi abbiamo due casi:
$$\begin{aligned} a \in n &\implies s(a) \in n \vee s(a) = n \implies s(a) \in s(n) \\ a = n &\implies s(a) = s(n) \end{aligned}$$

□

Possiamo roa dimostrare la proposizione.

Dimostrazione. Verifichiamo le tre proprietà richieste da un ordinamento totale:
transitività: $a \in b \wedge b \in c \to a \in c$. Induzione su c:

- caso $c = 0$: la premessa $b \in c$ è falsa, quindi l'implicazione è vera a vuoto.
- caso $c = s(n)$: assumiamo per ipotesi induttiva $a \in b \wedge b \in n \to a \in n$. Sapendo $a \in b \wedge b \in s(n)$ vogliamo dedurre $a \in s(n)$. Abbiamo due casi:
$$\begin{aligned} b = n &\implies a \in b = n \implies a \in s(n) \\ b \in n &\implies a \in b \in n \implies a \in n \implies a \in s(n) \end{aligned}$$

irriflessività: $\neg\, a \in a$. Per induzione:

- caso $a = 0$: $\neg\, \emptyset \in \emptyset$ per definizione di $\emptyset$.
- caso $a = s(n)$: assumiamo l'ipotesi induttiva $\neg\, n \in n$. Per assurdo supponiamo $s(n) \in s(n)$ ed abbiamo due casi:
$$\begin{aligned} s(n) = n &\implies n \in n \lightning \\ s(n) \in n &\implies n \in s(n) \in n \implies n \in n \lightning \end{aligned}$$

totalità: $a \in b \vee a = b \vee b \in a$. Per induzione su a:

- caso $a = 0$: $\emptyset \in b \vee \emptyset = b \vee b \in \emptyset$[23]. Procediamo per induzione su b:

[23] Ovviamente quest'ultimo caso è impossibile.

- caso $b = 0$: $0 \in \emptyset \vee \emptyset = \emptyset$, dove naturalmente la prima affermazione è falsa, mentre la seconda è vera.
- caso $b = s(m)$: ipotesi induttiva $\emptyset \in m \vee \emptyset = m$. Abbiamo due casi:

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

- caso $a = s(n)$: L'ipotesi induttiva è $n \in b \vee n = b \vee b \in n$. Abbiamo tre casi:

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

□

Corollario 4.16

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

$$\forall m \in \omega \; m = \{n \in \omega | n < m\}$$

Dimostrazione. Vogliamo dire che $m = \{n \in \omega | n \in m\}$, ossia che $m \subseteq \omega$. Per induzione: $\emptyset \subseteq \omega$ è vera; assumiamo $m \subseteq \omega$, allora $s(m) = m \cup \{m\}$ (con $\{m\} \subseteq \omega$ in quanto $m \in \omega$), quindi $s(m) \subseteq \omega$. □

Corollario 4.17

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

Dimostrazione. Siccome ω è totalmente ordinato, si danno due casi:

$$m \leq n \implies \forall x \in \omega \; x < m \to x < n \implies \forall x \in \omega \; x \in m \to x \in n \implies m \subseteq n$$

$$n < m \implies n \in m \quad \text{tuttavia} \quad n \notin n \implies m \not\subseteq n$$

□

§4.3 Induzione forte e principio del minimo

Teorema 4.18 (Principio di induzione - forma forte)

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

$$(\forall n \in \omega (\forall x < n \; \Phi(x)) \to \Phi(n)) \to \forall n \in \omega \; \Phi(n)$$

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

Osservazione 4.19 — 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 [e dimostriamo il conseguente]:

$$\forall n \in \omega\, (\forall x < n\ \Phi(x)) \to \Phi(n)$$

Inizialmente, dimostriamo per induzione $\forall m \in \omega\ \psi(m)$ dove:

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

- caso $m = 0$: $\forall x < \emptyset\ \Phi(x)$ è vera a vuoto.
- caso $m = s(n)$: per ipotesi induttiva abbiamo $\forall x < n\ \Phi(x)$. Se $x < m = s(n)$, sappiamo già che $x < n \vee x = n$. Si danno 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 $\Phi(x)$. Per l'arbitrarietà di $x < m$ abbiamo dimostrato $\forall x < m\ \Phi(x)$.

Ora sappiamo che $\forall m \in \omega\ \forall x < m\ \Phi(x)$. Dato un $n \in \omega$ qualunque, considerando $m = n + 1$ e $x = n$ otteniamo $\Phi(n)$ (grazie a quanto abbiamo dimostrato). □

Teorema 4.20 (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 4.21 (Idea 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, oppure $\forall x < n\ x \notin A$, ma allora n è il minimo di A.

Dimostrazione. Considerando la contronominale, dobbiamo dimostrare che se A non ha un minimo elemento, allora A è vuoto. Assumiamo quindi $\forall n \in A\ \exists x \in A\ x < n$ (ovvero che A non ha minimo), dobbiamo dimostrare che $\forall n \in \omega\ n \notin A$ (quindi A vuoto). Procediamo per induzione in forma forte. Ci serve dire che $(\forall x < n\ x \not\in nA) \to n \notin A$. QUesto, però, è immediato, perché equivale a:

$$\begin{aligned}
&(\neg\exists x < n\ x \in A) \to n \notin A \\
\iff &(\neg\exists x < n \wedge x \in A) \to n \notin A \\
\iff &(\neg\exists x \in A\ x < n) \to n \notin A \\
\iff &n \in A \to \exists x \in A\ x < n
\end{aligned}$$

che è appunto l'assunto. □

Definizione 4.22. Un insieme totalmente ordinato $(S, <)$ si dice **bene ordinato** se ogni sottoinsieme non vuoto ha un minimo.[24]

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

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 4.23
$(\omega, <)$ è un insieme bene ordinato.

Esercizio 4.24. Dimostra che $X = s(s(s(\omega)))$ è bene ordinato dalla relazione $a < b \overset{\text{def}}{=} a \in b$.

§4.4 Ricorsione numerabile

La ricorsione è il procedimento per cui si costruisce una funzione $f : \omega \longrightarrow$ 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 $(\dots)$. Vediamo qualche esempio.

Esempio 4.25 (Operazioni aritmetiche)
Possiamo definire somma e prodotto come:

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

anziché $a + b = \underbrace{s(s(\dots a \dots))}_{b \text{ successori}}$ e $a \cdot b = \underbrace{a + a + \dots + a}_{b \text{ volte}}$.

Esempio 4.26 (Potenza e fattoriale)
Possiamo definire ricorsivamente potenze e fattoriali come segue:

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

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

[24] Cioè se vale il principio del minimo.

Esempio 4.27 (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 $\sum_{i=0}^{a} f(i) = f(0) + f(1) + \ldots + f(a)$.

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

Esempio 4.28

In quanti modi posso coprire una sequenza di n caselle $\underbrace{\square\square\square\ldots\square\square}_{n}$ 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}. Quindi:

$$F_n = F_{n-1} + F_{n-2}$$[25]

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

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 4.29 (Estensionalità per funzioni) — Date $f, g : A \longrightarrow B$, allora:

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

Dimostrazione. Si osserva che:

$$(x, y) \in f \iff y = f(x) \iff y = g(x) \iff (x, y) \in g$$

□

[25] Cioè il numero totale di modi di ricoprire la sequenza di n caselle deriva dalla somma dei due casi, che rappresentano i modi di ricoprire le altre caselle fissata quella/e iniziale/i.

Notazione 4.30 — Indichiamo con ${}^{A}B$ l'insieme delle funzioni da A a B, che esiste per separazione in $\mathcal{P}(A \times B)$.

Teorema 4.31 (Ricorsione numerabile - prima forma)
Dato un insieme A, un elemento $k \in A$ e una funzione:

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

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

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

Esempio 4.32
Per definire a^b considero $k = 1$, $h(n, x) = a \cdot x$. Per definire il fattoriale $k = 1$, $h(n, x) = s(n) \cdot x$.

Esercizio 4.33. 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 - più semplicemente otteniamo f per separazione nell'insieme $\omega \times A$ usando la formula Φ. Per dire "$y = f(x)$" dire "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:

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

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

Lemma 4.34
$\forall x \in \omega \; \exists! \, g$ "g è una x-approssimazione".

Dimostrazione. Induzione su x.

- caso $x = \emptyset$: Basta osservare che l'unica $\emptyset$-approssimazione è $\{(\emptyset, k)\}$. Infatti il dominio è $\{\emptyset\}$ per definizione, e abbiamo la condizione $g(\emptyset) = k$.

- caso $x = s(a)$: Per ipotesi induttiva 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. Per verificare l'unicità, osserviamo che, data $s(a)$-approssimazione g' e g'', la loro restrizione a $s(a)$ è una a-approssimazione, quindi,

per ipotesi induttiva $g'_{|s(a)} = g = g''_{|s(a)}$. D'altro canto il dominio di una $s(a)$-approssimazione è $s(s(a)) = s(a) \cup \{s(a)\}$, abbiamo detto che g' e g'' coincidono su $s(a)$, e:

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

□

Stabilito il lemma, introdurremo la formula Φ:

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

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

$$f(x) = y \overset{\text{def}}{=} \Phi(x, y)^{26}$$

Occorre verificare che f soddisfa le condizioni della ricorsione.

- $f(\emptyset) = k$: immediata.
- $f(s(n)) = \ldots$: Per costruzione $f(s(n)) = g(s(n))$ per una $s(n)$-approssimazione g. D'altro canto $g(s(n)) = h(n, g(n))$. Ora $g_{|s(n)}$ è una n-approssimazione, quindi $g(n) = g_{|s(n)}(n) = f(n)$. Mettendo tutto insieme:

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

  L'unicità di f segue facilmente per induzione, Date f' e f'' che soddisfano la ricorsione abbiamo:

  $$f'(\emptyset) = k = f''(\emptyset) \qquad f'(s(n)) = h(n, f'(n)) = {}^{27}h(n, f''(n)) = f''(s(n))$$

□

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 4.35 (Costruzione di $+ : \omega \times \omega \to \omega$)
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 $f : \omega \to \omega$ tale che:

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

Scriviamo quindi:

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

[26] Formalmente $f = \{(x, y) \in \omega \times A | \Phi(x, y)\}$.
[27] Per ipotesi induttiva.

L'applicazione che segue chiude il conto che abbiamo lasciato aperto con gli assiomi di Peano. Dimostriamo che essi identificano un'unica struttura a meno di isomorfismi, quindi ω è a buon diritto, l'insieme dei numeri naturali.

Teorema 4.36 (Unicità dei numeri naturali)
Supponiamo che $(\mathbb{N}, 0, \text{succ})$ soddisfi gli assiomi di Peano, allora $(\mathbb{N}, 0, \text{succ})$ **e** $(\omega, \emptyset, s)$ sono strutture isomorfe - **ossia, formalmente, esiste** $f : \omega \longrightarrow \mathbb{N}$ **bigettiva tale che** $f(\emptyset) = 0$ e $\forall n \in \omega\ f(s(n)) = \text{succ}(f(n))$.[a]

[a] Cioè è una bigezione tra insiemi, che rispetta lo 0 e la funzione successore che abbiamo definito.

Fa comodo isolare la seguente osservazione.

Osservazione 4.37 — $\forall x \in \omega\ x \neq 0 \to \exists y \in \omega\ x = s(y)$.[a]

[a] Moralmente, 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 $x = s(y)$. □

Dimostriamo ora il teorema.

Dimostrazione. Per il teorema di ricorsione c'è un'unica f che soddisfa le condizioni $f(\emptyset) = 0$ e $\forall n \in \omega\ f(s(n)) = \text{succ}(f(n))$. Resta da constatare che f è bigettiva.
Surgettività Per ipotesi $(\mathbb{N}, 0, \text{succ})$ soddisfa il principio di induzione. Dimostriamo quindi per induzione in $(\mathbb{N}, 0, \text{succ})$ che $\forall y \in \mathbb{N}\ \exists x \in \omega\ f(x) = y$.

- caso $y = 0$: basta osservare che $f(\emptyset) = 0$ per costruzione.
- caso $y = \text{succ}(n)$: per ipotesi induttiva c'è $x \in \omega$ tale che $f(x) = n$, quindi $f(s(x)) = \text{succ}(n)$.

Iniettività Consideriamo, per assurdo, il minimo $x \in \omega$ tale che, per qualche $y \in \omega$ con $y \neq x$, $f(x) = f(y)$. Osserviamo che, per la minimalità di x, $x < y$, quindi, in particolare $y \neq \emptyset$, e possiamo scrivere $y = s(y')$.

- Se $x = \emptyset$, allora $\text{succ}(f(y')) = f(s(y')) = f(y) = f(x) = 0$, contraddicendo il (b) per $(\mathbb{N}, 0, \text{succ})$.
- Se $x \neq \emptyset$ allora 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) in $(\mathbb{N}, 0, \text{succ})$, $f(x') = f(y')$. Allora, per la minimalità di x, siccome $x' < x$, dobbiamo avere $x' = y'$. Ma da questo seguirebbe $x = s(x') = s(y') = y$ ↯.

□

Se, infine, volgiamo la nostra attenzione all'esempio dei numeri di Fibonacci, vediamo che non è possibile definire questa sequenza applicando il teorema di ricorsione in maniera diretta, perché F_n non dispense solo dal termine precedente della sequenza, F_{n-1}, ma anche da F_{n-2}.
Ce la si potrebbe cavare con un trucco, per esempio definendo la funzione $n \longmapsto (F_n, F_{n+1})$ da ω a $\omega \times \omega$. È comodo, però, disporre di una versione più versatile del teorema.

Teorema 4.38 (Ricorsione numerabile - seconda forma)

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

$$\forall n \in \omega \; f(n) = h(f_{|n})^a$$

[a] In altre parole, $f(n)$, può dipendere in maniera arbitraria dai valori assunti da f sui numeri minori di n.

Esempio 4.39 (Esempi di applicazione)

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

Dimostrazione. L'idea è di definire, mediante la prima forma del teorema di ricorsione, la successione della troncata di f. Ossia la funzione $f' : n \longmapsto f_{|n}$. Un modo alternativo, sarebbe ripetere la dimostrazione della prima forma.
Costruiamo per ricorsione - prima forma - la funzione $f' : \omega \to A^*$ tale che:

$$f(\emptyset) = \emptyset \qquad f'(s(n)) = f'(n) \cup \{(n, h(f'(n)))\}$$

Ora poniamo $f(n) = f'(s(n))(n)$. Verifichiamo per induzione che $\forall n \in \omega \; f_{|n} = f'(n)$.

- caso $n = 0$: immediato.
- caso $n = s(m)$: abbiamo:

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

Infine, quindi, $f(n) = f'(s(n))(n) = h(f'(n)) = h(f_{|n})$. □

Abbiamo roa 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 4.40. 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. Dati due insiemi A e B:

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

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

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

ossia: $\exists f \in {}^{A}B$ “f è iniettiva”.

Nota 5.2 — 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 $\clubsuit[A, B)$.
- Potrebbe sorgere il sospetto che se $|A|<|B|$ quando $A \subsetneq B$, ma non è così, come mostra l'esempio di $A = \{x \in \omega | x > 0\}$ e $B = \omega$.

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

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

Esercizio 5.4. Dimostrare l'osservazione.

Osservazione 5.5 — La relazione $|\cdot| \leq |\cdot|$ è:

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

Esercizio 5.6. Dimostrare l'osservazione.

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

Teorema 5.7 (Cantor-Bernstein)
Se c'è una funzione iniettiva $A \to B$ e una funzione iniettiva $B \to A$, allora esiste una bigezione fra A e B.

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

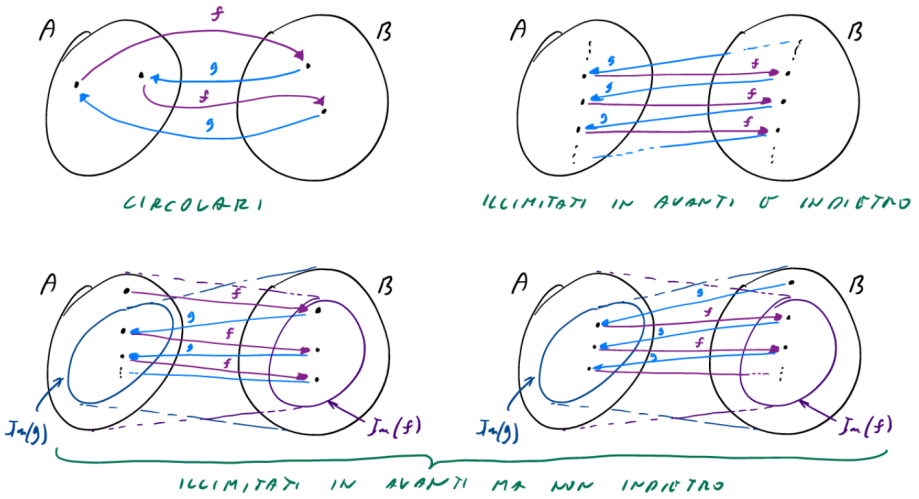
Dimostrazione. Siano $f : A \longrightarrow B$ e $g : B \longrightarrow A$ iniettive. Il nostro obiettivo è costruire una nuova funzione $h : A \longrightarrow B$ bigettiva.
L'idea è che ogni elemento, poniamo, di A, è una tappa di un percorso:

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

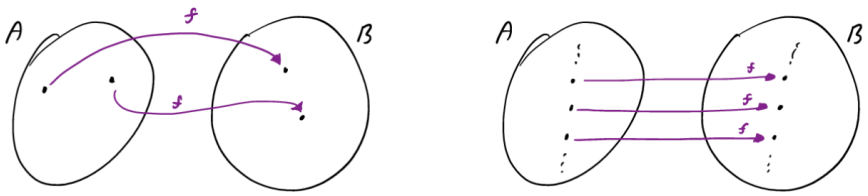
Siccome f e g sono iniettive, questo percorso ha altresì un'unica estensione all'indietro[28]:

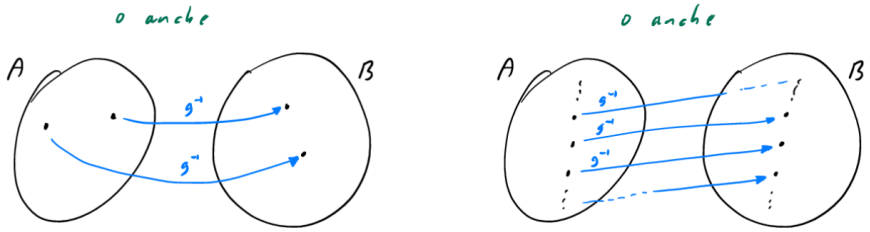
$$f^{-1}(g^{-1}(a)) \xrightarrow{f} g^{-1}(a) \xrightarrow{g} a \xrightarrow{f} f(a) \xrightarrow{g} g(f(a)) \xrightarrow{f} f(g(f(a))) \xrightarrow{g} \dots$$

a patto che $a \in \mathrm{Im}(g)$, $g^{-1} \in \mathrm{Im}(f)$, etc. Quando, e se, non possiamo più applicare la funzione inversa, il percorso si interrompe. Ci sono quindi percorsi di tre tipi:

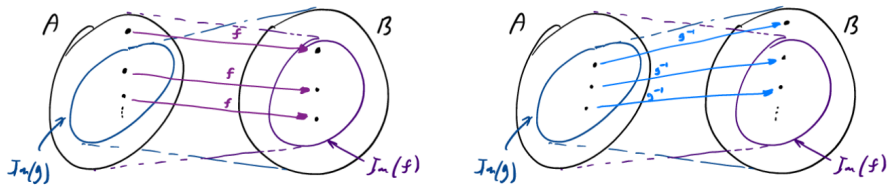


Per gli elementi che si trovano su un percorso circolare, o su un percorso illimitato avanti e indietro, f fornisce una bigezione, come la fornirebbe anche g^{-1} - la scelta è arbitraria a patto di usare la medesima funzione per l'intero percorso -.





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 da g^{-1}.



Per comodità poniamo $h(x) = f(x)$ in ogni caso, eccetto quando x è lungo un percorso che porta da B, nel cui caso poniamo $h(x) = g^{-1}(x)$.
Formalmente, definiamo per ricorsione le seguenti successioni di sottoinsiemi di B e A rispettivamente - ossia, tecnicamente, la funzione $\omega \longrightarrow \mathcal{P}(B) \times \mathcal{P}(A) : i \longmapsto (B_i, A_i)$, con:

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

Definiamo quindi:

$$B_* = \bigcup_{i\in\omega} B_i \overset{\text{def}}{=} \bigcup\{B_i | i \in \omega\} \qquad A_* = \bigcup_{i\in\omega} A_i$$

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

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

Ci basta dimostrare che h e k sono ben definita, $k \circ h = id_A$ e $h \circ k = id_B$.

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

(2) $k \circ h = id_A$: 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 $k(h(y)) = k(g^{-1}(x)) = k(y) = g(y) = x$. Per il caso $x \notin A_*$, osserviamo, intanto, che $x \notin A_* \to f(x) \notin B_*$. Infatti, se $f(x) \in B_i$, con $i \in \omega$, allora $i \neq 0$,

[28] Perché la controimmagine di ogni elemento ha sempre un solo elemento, essendo f e g per ipotesi iniettive.

perché $B_0 = B \setminus \mathrm{Im}(f)$, quindi possiamo scrivere $i = s(j)$, e $f(x) \in B_{s(j)} = f[A_j]$. Per l'iniettività di f, abbiamo allora $x \in A_j$ ↯.
Di conseguenza, se $x \notin A_*$, $k(h(x)) = k(f(x)) = f^{-1}f(x) = x$.

(3) $\underline{h \circ k = id_B}$: Se $y \in B_*$, allora $y \in B_i$, per qualche $i \in \omega$, quindi $g(y) \in A$. 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 $f^{-1}(y) \in A_i \to y = f(f^{-1}(y)) \in A_{s(i)}$. Quindi $h(k(y)) = h(f^{-1}(y)) = f(f^{-1}(y)) = y$.

□