ELEMENTI DI TEORIA DEGLI INSIEMI
Dispensa 3

Mauro Di Nasso

Ultimo aggiornamento: October 21, 2024

La teoria di Zermelo-Fraenkel

A partire da questo capitolo, cambieremo la nostra impostazione che, come hanno mostrato la collezione di Russell $R = \{x \mid x \notin x\}$ e la collezione universale $V = \{x \mid x = x\}$, si è rivelata contraddittoria. Procederemo in modo più attento e rigoroso seguendo il moderno metodo *assiomatico*, ed introdurremo, a partire dagli assiomi dati, tutti i fondamentali oggetti e principi della matematica, tra cui i numeri naturali e l'induzione. Precisamente, presenteremo e svilupperemo la teoria degli insiemi ZFC di Zermelo-Fraenkel, che è ad oggi quella più largamente adottata come fondamento della matematica.[1] Tutte le varie nozioni insiemistiche – anche le più elementari – saranno definite in dettaglio, a partire da quelle già viste informalmente nelle lezioni precedenti. Come è caratteristica del metodo assiomatico, le uniche proprietà che potremo assumere saranno quelle espresse dagli assiomi ZFC. È onesto ammettere però che, nel definire la teoria, verranno implicitamente assunti alcuni principi fondamentali, che costituiscono la nostra "metateoria". Ad esempio, nella definizione di formula, il concetto di "stringa finita" e una qualche nozione intuitiva di numero naturale e di induzione, sono dati come noti.

1. Formule del linguaggio degli insiemi

Come abbiamo già anticipato nel primo capitolo, tutte le proprietà che considereremo, e in particolare gli assiomi, saranno espressi mediante formule nel linguaggio della teoria degli insiemi. Ricordiamo qua sotto quella nozione e – per maggiore precisione – specifichiamo anche con esattezza cosa debba intendersi per "formula".

Definizione 1.1. Chiamiamo *simboli logici* i seguenti simboli:

- *Connettivi*:
  negazione: $\neg$ ("non"); congiunzione: $\wedge$ ("e"); disgiunzione: $\vee$ ("o"); implicazione: $\to$ ("se ... allora"); equivalenza: $\leftrightarrow$ ("se e solo se").
- *Variabili*:
  $x, y, z, t, \ \ldots \ , x_1, x_2, x_3 \ldots$
- *Quantificatori*:
  esistenziale $\exists$ ("esiste"); universale $\forall$ ("per ogni").

Definizione 1.2. Le *formule del linguaggio della teoria degli insiemi*, in breve le *formule*, sono particolari sequenze finite di simboli nelle quali possono comparire, oltre ai simboli logici e alle parentesi "(" e ")", soltanto il simbolo di uguaglianza "=", e il simbolo di appartenenza "$\in$". Precisamente:

- Se x e y sono variabili, $x = y$ e $x \in y$ sono formule. Le variabili x e y si dicono *variabili libere* in quelle formule ;
- Se φ è una formula, anche $\neg(\varphi)$ è una formula che ha le stesse variabili libere di φ ;

[1] Più avanti nel corso, sarà talvolta conveniente adottare una teoria assiomatica più ampia, cioè la teoria NGB di von Neumann-Gödel-Bernays. In tale teoria, oltre agli insiemi, esiste un'altro tipo di oggetti, chiamati *classi proprie*, che si possono pensare come collezioni di insiemi "troppo grandi" per poter essere esse stesse insiemi.

- Se φ e ψ sono formule, allora anche $(\varphi \vee \psi)$, $(\varphi \wedge \psi)$, $(\varphi \to \psi)$, $(\varphi \leftrightarrow \psi)$ sono formule, le cui variabili libere sono quelle di φ più quelle di ψ ;
- Se x è una variabile libera della formula φ, allora anche $\forall x\,(\varphi)$ e $\exists x\,(\varphi)$ sono formule, le cui variabili libere sono quelle di φ *tranne* x. In questo caso x si dice variabile *legata* ;
- Ogni formula si ottiene applicando un numero finito di volte le procedure indicate sopra.

Si dice *enunciato* una formula senza variabili libere, cioè una formula dove tutte le variabili sono legate.

Vediamo subito qualche esempio.

(1) $\exists x$ e $\forall x$ *non* sono formule.
(2) $\exists x\,(x \in y)$ è una formula dove la variabile x è legata, e la variabile y è libera.
(3) $\forall x\,\exists y\,(x \in y)$ è un enunciato perché le sue due variabili x e y sono entrambe legate.

In algebra, quando scriviamo equazioni del tipo $E(x, y)$: "$x^2 = y^2 - 1$", pensiamo alle variabili libere x e y come a numeri non meglio precisati. Soltanto dopo aver specificato a quali numeri corrispondano x e y, avrà senso chiedersi se quell'equazione è valida o no.[2] Tuttavia, se leghiamo le variabili con quantificatori, allora si ottengono proprietà che sono o vere o false (in ogni specificato contesto). Ad esempio, nel contesto dei numeri reali, $\forall x \forall y E(x, y)$ e $\exists x \forall y E(x, y)$ sono proprietà false, mentre $\forall x \exists y E(x, y)$ e $\exists x \exists y E(x, y)$ sono vere.[3]

In modo del tutto analogo, le formule della teoria degli insiemi che contengono variabili libere non sono di per sé né vere né false, perché le variabili libere sono insiemi "generici", non precisati. Ma se ogni variabile è legata da un quantificatore, cioè se abbiamo un *enunciato*, allora viene espressa una proprietà dal significato definito, cui possiamo attribuire un valore di verità: vero o falso. Ad esempio, la formula (2) di sopra ha un significato ambiguo, che dipende da quale insieme assegnamo alla variabile libera y (se ad y assegnamo l'insieme vuoto otteniamo una proprietà falsa, altrimenti otteniamo una proprietà vera). Al contrario, la formula (3), che è un enunciato, esprime una proprietà matematica precisa relativa alle coppie di insiemi x e y considerati nella loro totalità. Risulta quindi chiaro perchè tutti gli assiomi che daremo, e tutti i teoremi che dimostreremo, saranno formulati mediante enunciati.

Per non appesantire la scrittura delle formule, spesso ometteremo alcune parentesi, se non sono strettamente necessarie ad una corretta comprensione.[4] Inoltre, seguendo l'uso comune, scriveremo:

- "$x \neq y$" per intendere "$\neg(x = y)$" ;
- "$x \notin y$" per intendere "$\neg(x \in y)$" ;

Seguiremo inoltre le usuali notazioni per le cosiddette *quantificazioni ristrette*:

[2] Nel linguaggio della logica, questo procedimento si chiama "assegnamento delle variabili libere".

[3] È consuetudine in algebra scrivere equazioni come "$x^2 = y^2 - 1$", sottintendendo la loro quantificazione universale, cioè "$\forall x\,\forall y\ (x^2 = y^2 - 1)$". Per evitare ambiguità, noi specificheremo sempre tutti i quantificatori coinvolti nelle nostre formule.

[4] Ad esempio, al punto (3) di sopra abbiamo scritto $\forall x\,\exists y\,(x \in y)$ anziché $\forall x\,(\exists y\,(x \in y))$, come avremmo dovuto fare per attenerci strettamente alla definizione di formula.

- "$\forall\, x \in y\ \varphi$" per intendere "$\forall x\,(x \in y \to \varphi)$" ;
- "$\exists\, x \in y\ \varphi$" per intendere "$\exists x\,(x \in y \wedge \varphi)$" ;

2. I primi assiomi

Iniziamo finalmente ad elencare gli assiomi della teoria ZFC di Zermelo-Fraenkel, la più comunemente usata in matematica.

La teoria ZFC è guidata dal criterio intuitivo noto come "limitazione della grandezza" ("*limitation of size*"). Partendo dall'osservazione che le collezioni coinvolte nei paradossi sono "grandi", si è pensato di considerare come sicuro un assioma quando esso determina solo l'esistenza di insiemi aventi "grandezza limitata", a partire da insiemi già dati.[5]

Il primo assioma è la diretta formalizzazione del principio intuitivo di estensionalità, che abbiamo già visto e commentato nel primo capitolo.

Assioma 1: Estensionalità.

$$\forall A\, \forall B\, \big((\forall x\,(x \in A \leftrightarrow x \in B)) \leftrightarrow A = B\, \big).$$

Per non rendere banale la nostra teoria ed evitare che parli di niente, dobbiamo garantire l'esistenza di almeno un insieme. Può sembrare un po' strano, ma anche per questo occorre un assioma. Non dobbiamo infatti dimenticare che, procedendo col metodo assiomatico, *niente* può essere assunto se non quello che segue logicamente dagli assiomi.

Assioma 2: Insieme vuoto.

$$\exists x \text{ ``} x = \emptyset \text{''}.$$

I prossimi due assiomi ci forniscono due basilari principi per estendere l'universo degli insiemi.

Assioma 3: Coppia.

$$\forall a\, \forall b\, \exists X \text{ ``} X = \{a, b\} \text{''}.$$

Dunque, per ogni coppia assegnata, è possibile formare l'insieme che contiene esattamente di quei due elementi. Per l'assioma di estensionalità, tale insieme coppia è necessariamente unica.

Notiamo che se $a = b$, la coppia $X = \{a, a\}$ è uguale a $\{a\}$, che si chiama *singoletto* di a.

Con un uso ripetuto dell'assioma della coppia, si ottiene l'esistenza delle coppie ordinate di Kuratowski.

PROPOSIZIONE 2.1. *Per ogni a, b esiste ed unico insieme* $(a, b) = \{\{a\}, \{a, b\}\}$.

[5] Al di là della plausibilità filosofica di una tale assunzione, resta comunque il fatto oggettivo che esso ha prodotto la teoria ZFC, dalla quale non sono state mai derivate contraddizioni, anche dopo l'enorme lavoro di deduzioni operato dai migliori matematici in oltre un secolo (la prima incompleta formulazione di Zermelo risale al 1908).

Il prossimo assioma garantisce l'esistenza dell'unione di famiglie di insiemi.[6]

Assioma 4: Unione.

$$\forall \mathcal{F}\, \exists X \text{ ``}X = \bigcup_{F \in \mathcal{F}} F\text{''}.$$

Di nuovo per *estensionalità*, un tale insieme unione è necessariamente unico.

Come abbiamo già ricordato, nel linguaggio degli insiemi, è più comune scrivere $\bigcup \mathcal{F}$ anziché $\bigcup_{F \in \mathcal{F}} F$; in altre parole, con $\bigcup \mathcal{F}$ si denota l'insieme degli elementi di elementi di $\mathcal{F}$. In maniera simile, si scrive talvolta $\bigcap \mathcal{F}$ anziché $\bigcap_{F \in \mathcal{F}} F$.

Nelle formule di sopra abbiamo usato delle notazioni metalinguistiche che erano già state introdotte nel primo capitolo come convenienti abbreviazioni di formule. Precisamente:

- "$x = \emptyset$" indica la formula
$$\forall y\, (y \notin x).$$
- "$X = \{a, b\}$" indica la formula
$$\forall x\, \big((x \in X) \leftrightarrow (x = a \vee x = b)\big).$$
- "$X = \bigcup_{F \in \mathcal{F}} F$" denota la formula
$$\forall x\, \big((x \in X) \leftrightarrow \exists F\, (F \in \mathcal{F} \wedge x \in F)\big).$$

Combinando gli assiomi della *coppia* e dell'*unione*, otteniamo l'esistenza dell'unione di due insiemi.

Proposizione 2.2. *Per ogni A e B esiste l'insieme*

$$A \cup B = \{x \mid (x \in A) \vee (x \in B)\}.$$

Dim. Per l'assioma della coppia esiste $\{A, B\}$, e per l'assioma dell'unione esiste $\bigcup\{A, B\} = \{x \mid \exists X \in \{A, B\}\ x \in X\} = \{x \mid (x \in A) \vee (x \in B)\}$. $\square$

Notiamo che, dall'equivalenza logica $(x \in A \vee x \in B) \leftrightarrow (x \in B \vee x \in A)$, segue banalmente che $A \cup B = B \cup A$.

Con gli assiomi dati fin qui, non è ancora possibile dimostrare l'esistenza dell'insieme intersezione $A \cap B$ nè, più in generale, l'esistenza di sottoinsiemi di un dato insieme A. A questo rimedierà il prossimo assioma di *separazione*, che permetterà di formare l'insieme di tutti e soli gli elementi che godono di una fissata proprietà, ma solo a patto che tali elementi siano presi dentro un insieme già dato. La *separazione* è quindi una versione più debole del principio di *comprensione* (che era contraddittorio!), che fornisce l'esistenza di opportuni sottoinsiemi di insiemi già assegnati, in pieno accordo con il criterio della "limitazione della grandezza".

Assioma 5: Separazione.
Sia $\varphi(x, x_1, \ldots, x_n)$ una formula dove $x, x_1, \ldots, x_n$ sono tutte e sole le variabili libere. Allora il seguente è un assioma:

$$\forall A_1 \ldots \forall A_n\, \forall X\, \exists B \text{ ``}B = \{x \in X \mid \varphi(x, A_1, \ldots, A_n)\}\text{''}.$$

[6] Parliamo qui di "famiglie di insiemi" per seguire l'uso comune. Come abbiamo già osservato nel primo capitolo, in realtà nella teoria assiomatica degli insiemi, ogni insieme è una famiglia di insiemi.

Seguendo l'uso comune, scriviamo "$B = \{x \in X \mid \varphi(x, A_1, \dots, A_n)\}$" per denotare quell'insieme i cui elementi sono tutti e soli gli $x \in X$ che soddisfano la proprietà $\varphi(x, A_1, \dots, A_n)$ relativa ad insiemi assegnati $A_1, \dots, A_n$. Ci riferiremo a proprietà di questo genere come a *proprietà con parametri* $A_1, \dots, A_n$.

Attenzione! La *separazione* non è in realtà un singolo assioma, ma piuttosto di uno *schema di assiomi*, uno per ogni formula.

Prime immediate conseguenze della *separazione* sono le seguenti.

Proposizione 2.3. *Per ogni A e B, esistono gli insiemi:*
(1) $A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$;
(2) $A \setminus B = \{x \mid (x \in A) \wedge (x \notin B)\}$.

Dim. Basta usare l'assioma di *separazione* dove si considerano rispettivamente le formule $\varphi_1(x, B) :=$ "$x \in B$" e $\varphi_2(x, B) :=$ "$x \notin B$". Infatti $A \cap B = \{x \in A \mid x \in B\}$ e $A \setminus B = \{x \in A \mid x \notin B\}$. □

Esercizio 2.4. Per ogni A_1, A_2, A_3, esistono gli insiemi:
(1) $A_1 \cap A_2 \cap A_3 = \{x \mid (x \in A_1) \wedge (x \in A_2) \wedge (x \in A_3)\}$;
(2) $A_1 \cup A_2 \cup A_3 = \{x \mid (x \in A_1) \vee (x \in A_2) \vee (x \in A_3)\}$.

Attenzione! Possiamo anche dimostrare le proprietà di sopra per 4 insiemi, per 5 insiemi, e così via. In altre parole, per ogni n fissato, possiamo dimostrare che l'unione di n insiemi e l'intersezione di n insiemi sono insiemi. Tuttavia *non* possiamo per il momento formalizzare all'interno della teoria la quantificazione "per ogni n", perché non abbiamo ancora definito formalmente cosa sono i numeri naturali.

Esercizio 2.5. Per ogni famiglia non vuota di insiemi $\mathcal{F}$, esiste l'insieme

$$\bigcap \mathcal{F} = \{x \mid \forall F \in \mathcal{F}\ x \in F\}.$$

Per ogni fissato insieme A, l'assioma di *separazione* garantisce l'esistenza di tutti i suoi sottoinsiemi che possono essere "descritti" usando una formula. Non possiamo però ancora dimostrare l'esistenza di un insieme che contenga *tutti* i sottoinsiemi di A.

Assioma 6: Potenza.

$$\forall A\, \exists X \text{ "} X = \mathcal{P}(A) \text{"}.$$

Ricordiamo che "$X = \mathcal{P}(A)$" indica la formula

$$\forall x \ \big((x \in X) \leftrightarrow \text{"}(x \subseteq A)\text{"} \big)$$

dove, a sua volta, "$x \subseteq A$" è una abbreviazione di

$$\forall y \big((y \in x) \to (y \in A) \big).$$

Attenzione! Per ogni insieme A, l'*assioma delle parti* garantisce l'esistenza di un insieme $\mathcal{P}(A)$ che contiene tutti e soli quegli insiemi a che soddisfano la proprietà "$a \subseteq A$"; non sappiamo però quali collezioni di elementi di A esistono effettivamente come insiemi, cioè come oggetti della nostra teoria. In altre parole, anche quando sia possibile "descrivere" una collezione a di elementi di A, *non* siamo autorizzati a concludere che un tale a sia un insieme, a meno che ciò non sia dimostrabile a partire dagli assiomi. Per questo, è del tutto sbagliato pensare che l'assioma di *separazione* sia una conseguenza dell'assioma delle *parti*.

Osserviamo che, mentre gli assiomi dell'*insieme vuoto*, della *coppia*, dell'*unione*, e lo schema di *separazione*, sono in linea col principio della limitazione della grandezza, l'assioma della *potenza* ha una posizione più critica, visto che postula l'esistenza di una collezione più "grande" dell'insieme di partenza (nel senso preciso della cardinalità, come abbiamo visto nel primo capitolo).

Esercizio 2.6. Dimostrare che se $\mathcal{P}(A) \in \mathcal{P}(B)$ allora $A \in B$. Vale l'implicazione inversa?

Esercizio 2.7. Dimostrare che le seguenti proprietà valgono per ogni X:

(1) $X = \bigcup \mathcal{P}(X)$.
(2) $X \in \mathcal{P}(\mathcal{P}(\bigcup X))$.
(3) $\bigcup\bigcup \mathcal{P}(X) \in \mathcal{P}(\bigcup X)$.
(4) Se $x \in X$ allora $\mathcal{P}(x) \in \mathcal{P}(\mathcal{P}(\bigcup X))$.

Abbiamo già visto che per ogni a, b, esiste la coppia ordinata (a, b). Tuttavia, dati due insiemi A e B, questo non garantisce l'esistenza del prodotto cartesiano $A \times B$, cioè dell'insieme di tutte le coppie ordinate (a, b) dove $a \in A$ e $b \in B$. A questo scopo è fondamentale l'uso dell'assioma delle *parti*.

Proposizione 2.8. *Per ogni A e per ogni B, esiste il prodotto cartesiano*

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

Dim. Siano $a \in A$ e $b \in B$. Sia $\{a\}$ che $\{a, b\}$ sono sottoinsiemi di $A \cup B$, e quindi sono elementi di $\mathcal{P}(A \cup B)$. Dunque la coppia ordinata $(a, b) = \{\{a\}, \{a, b\}\}$ è un sottoinsieme di $\mathcal{P}(A \cup B)$, e quindi $(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B))$. Si osservi che l'esistenza di quest'ultimo insieme è garantita dall'esistenza dell'unione $A \cup B$ (Proposizione 2.3), e da una doppia applicazione dell'assioma delle *parti*. L'esistenza del prodotto cartesiano segue allora dall'assioma di *separazione*, visto che

$$A \times B = \{x \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid \varphi(x, A, B)\},$$

dove $\varphi(x, A, B)$ è la formula: $\exists a \exists b\, ((a \in A) \wedge (b \in B) \wedge \text{“}x = (a, b)\text{”})$.[7] $\square$

Sono adesso pienamente giustificate le definizioni di *relazione binaria* e di *funzione* che avevamo dato nel primo capitolo.

Esercizio 2.9.

(1) Se R è una relazione binaria, allora esistono:
- L'insieme *dominio* $\mathrm{dom}(R) = \{a \mid \exists\, b\ (a, b) \in R\}$
- L'insieme *immagine* $\mathrm{imm}(R) = \{b \mid \exists\, a\ (a, b) \in R\}$.

(2) Per ogni relazione di equivalenza $\approx$ su un insieme A, esiste l'*insieme quoziente*, $A/\!\approx\, = \{[a] \mid a \in A\}$ i cui elementi sono tutte e sole le classi di equivalenza $[a] = \{a' \in A \mid a' \approx a\}$.

(3) Per ogni A e B, esiste l'insieme $B^A = \mathrm{Fun}(A, B) = \{f \mid f : A \to B\}$.

[7] Ricordiamo che "$x = (a, b)$" è un'abbreviazione della formula:

$$\exists s\, \exists t\ (s = \{a\} \wedge t = \{a, b\} \wedge x = \{s, t\}),$$

dove, a loro a volta, le scritture "$s = \{a\}$", "$t = \{a, b\}$" e "$x = \{s, t\}$" abbreviano altre formule.

(4) Per ogni sequenza di insiemi $(A_i \mid i \in I)$, esiste l'*insieme prodotto*

$$\prod_{i \in I} A_i = \{f \mid f \text{ è una } I\text{-sequenza } \wedge \ \forall i \in I \ f(i) \in A_i\}.$$

Usando gli assiomi visti fin qui, con gli stessi argomenti usati nella prima parte di teoria "intuitiva" degli insiemi, possiamo dimostrare in modo formale le seguenti proprietà:

PROPOSIZIONE 2.10.
(1) *Non esistono insiemi R tali che $R = \{x \mid x \notin x\}$.*
(2) *Non esistono insiemi V tali che $V = \{x \mid x = x\}$.*

ESERCIZIO 2.11. Usando gli assiomi visti fin qui, dimostrare che per ogni insieme $A \neq \emptyset$, non esiste l'insieme classe di equipotenza $[A] := \{B \mid |B| = |A|\}$.

Gli assiomi dati fin qui garantiscono l'esistenza dei prodotti $\prod_{i \in I} A_i$, ma *non* garantiscono che tali prodotti siano non vuoti quando tutti gli A_i sono non vuoti. Come abbiamo anticipato nel primo capitolo, nel caso di prodotti infiniti questa proprietà viene postulata in un apposito assioma, cioè l'assioma di scelta. Visto che, per il momento, non abbiamo ancora definito la nozione di "finito" e "infinito", adottiamo la seguente formulazione che postula l'esistenza di una funzione di scelta f per ogni famiglia $\mathcal{F}$ di insiemi:

Assioma 7: Scelta.

$$\forall \mathcal{F} \, \exists f \ (f \text{ funzione } \wedge \ \forall F \in \mathcal{F} \ (F \neq \emptyset \to f(F) \in F)).$$

3. L'assioma dell'infinito

Osserviamo che i primi 7 assiomi che abbiamo presentato non permettono di dimostrare l'esistenza di insiemi infiniti; infatti, supponendo di vivere in un universo dove tutti gli insiemi sono finiti, tutte le proprietà postulate dagli assiomi introdotti fin qua sono verificate. Occorre quindi introdurre un nuovo assioma, perché in matematica l'esistenza di insiemi infiniti è di centrale importanza.

Vedremo in questo capitolo come si possono introdurre i numeri naturali, forse l'esempio più importanti in matematica di insieme infinito. Poiché stiamo lavorando nel quadro di una teoria *pura* degli insiemi, anch'essi saranno definiti come opportuni insiemi. L'*euristica*, cioè l'intuizione informale, che seguiremo per costruirli è la seguente. Definiamo $0 = \emptyset$ come l'insieme vuoto; poi $1 = \{0\}$ come l'insieme che contiene 0 come suo unico elemento; poi $2 = \{0, 1\}$ come l'insieme contenente i due elementi precedenti, cioè 0 e 1; poi $3 = \{0, 1, 2\}$; poi $4 = \{0, 1, 2, 3\}$, e così via. Dunque:

- $0 = \emptyset$
- $1 = \{\emptyset\} = \{0\}$
- $2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$
- $3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}$
- $4 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} = \{0, 1, 2, 3\}$
- ...

Infine raccogliamo tutti questi numeri in un insieme, che sarà l'insieme dei numeri naturali. Il problema è riuscire a formalizzare questo procedimento intuitivo in modo preciso e rigoroso all'interno della nostra teoria.

Notiamo che, a partire dagli assiomi introdotti fin qui, è in effetti possibile dimostrare l'esistenza di ciascuno degli insiemi finiti di sopra. L'esistenza di 0 è garantita dall'assioma dell'*insieme vuoto*. Applicando l'assioma della *coppia* si ottiene l'esistenza di $\{0,0\} = \{0\} = 1$. Di nuovo per l'assioma della *coppia* si ottiene $2 = \{0,1\} = 1 \cup \{1\}$. Per l'esistenza di $3 = \{0,1,2\} = 2 \cup \{2\}$ è necessario anche l'assioma dell'*unione*. Analogamente per $4 = \{0,1,2,3\} = 3 \cup \{3\}$, e così via.

È importante tenere presente che questo procedimento dimostra l'esistenza dei singoli numeri $0,1,2,3,4,\dots$ uno alla volta, ma *non* dimostra l'esistenza di un insieme che li contenga tutti.

Può venire la tentazione di postulare un nuovo assioma che dica: "Esiste un insieme $\mathbb{N}$ tale che $1 \in \mathbb{N}$ e $2 \in \mathbb{N}$ e $3 \in \mathbb{N}$ e $4 \in \mathbb{N}$ *etc.*". Notiamo però che una tale proprietà *non* è formalizzabile nel nostro linguaggio: infatti per noi una formula è comunque una espressione *finita*, e quindi non possiamo congiungere tutte le infinite proprietà "$n \in \mathbb{N}$".

Riusciremo ad aggirare queste difficoltà con la nozione di "insieme induttivo", che permetterà di formalizzare all'interno della teoria degli insiemi la nostra intuizione dei numeri naturali e del processo induttivo. Nella costruzione informale vista sopra, una volta definito un numero n, si definiva il numero successivo aggiungendo n stesso come nuovo elemento, cioè si considerava l'unione $n \cup \{n\}$. Come abbiamo già osservato, questo tipo di costruzione è giustificato dagli assiomi della *coppia* e dell'*unione*.

Notazione 3.1. Per ogni x, denotiamo $\widehat{x} = x \cup \{x\}$.

La prossima definizione è suggerita dal procedimento *euristico* che abbiamo usato sopra per "generare" i numeri naturali.

Definizione 3.2. Un insieme X si dice *induttivo* se soddisfa le proprietà:

(1) $\emptyset \in X$;
(2) $\forall x\,(x \in X \to \widehat{x} \in X)$.

Notiamo che la proprietà "X è induttivo" è in effetti esprimibile da una formula. L'intuizione ci suggerisce che un insieme induttivo è necessariamente infinito, perché $0 \in X$ per definizione, inoltre da $0 \in X$ segue che $\widehat{0} = 1 \in X$, e quindi anche $2 = \widehat{1} \in X$, e così via. Per garantire l'esistenza di tali insiemi, occorre un apposito assioma, l'ottavo della nostra lista.

Assioma 8: Infinito.

$$\exists X \text{ “}X \text{ induttivo”}.$$

Osserviamo che l'assioma dell'insieme *vuoto* è adesso ridondante perché segue dall'assioma dell'infinito più lo schema di *separazione*; infatti, preso un qualunque insieme induttivo X, si ha $\emptyset = \{x \in X \mid x \neq x\}$.

Come abbiamo visto, dentro un fissato insieme induttivo X troviamo gli elementi 0, 1, 2, 3, *etc.*, ma in generale dobbiamo aspettarci di trovare anche altri elementi. Questa *euristica* suggerisce la seguente

DEFINIZIONE 3.3. n si dice *numero naturale* se appartiene a tutti gli insiemi induttivi X.

I nostri assiomi garantiscono che i numeri naturali formano un insieme.

PROPOSIZIONE 3.4. Esiste ed unico un insieme ω i cui elementi sono tutti e soli i numeri naturali:

$$\omega = \{n \mid \text{"}n \text{ è un numero naturale"}\}.$$

Inoltre un tale insieme ω è esso stesso induttivo, e dunque è il "più piccolo" insieme induttivo.

DIM. Si prenda un qualunque insieme induttivo X, che esiste per l'assioma dell'*infinito*. Per *separazione*, esiste l'insieme

$$\omega = \{x \in X \mid \text{"}x \text{ è un numero naturale"}\}.$$

Per definizione, ogni numero naturale appartiene necessariamente ad X che è induttivo, e quindi ω contiene tutti e soli i numeri naturali. Per *estensionalità*, un tale ω è necessariamente unico.

Vediamo ora che ω stesso è un insieme induttivo. Questo segue direttamente dalle definizioni. Infatti $0 = \emptyset$ è un numero naturale (cioè appartiene ad ogni induttivo), dunque $0 \in \omega$. Inoltre, se $x \in \omega$, cioè se $x \in X$ per ogni insieme induttivo X, allora si avrà anche $\widehat{x} \in X$ per ogni insieme induttivo X, e quindi $\widehat{x} \in \omega$. $\square$

Nella nostra definizione di numero naturale ci siamo uniformati alla consuetudine in teoria degli insiemi di includere anche 0 (mentre fin qui avevamo convenuto che $0 \notin \mathbb{N}$); non ci sarà comunque ambiguità perché useremo due scritture diverse.

NOTAZIONE 3.5.

- ω denota l'insieme dei numeri naturali garantito dalla proposizione di sopra (dove $0 \in \omega$).
- $\mathbb{N} = \omega \setminus \{0\} = \{1, 2, \ldots\}$ denota l'insieme dei naturali diversi da zero.

Qui di seguito, vedremo un po' alla volta che ω soddisfa le familiari proprietà che l'intuizione e la pratica matematica attribuiscono all'insieme dei numeri naturali. Questo giustificherà la nostra "strana" definizione di numero naturale, un po' come la proprietà fondamentale $(a, b) = (a', b') \leftrightarrow (a = a' \wedge b = b')$ aveva giustificato la nostra "strana" definizione di coppia ordinata $(a, b) = \{\{a\}, \{a, b\}\}$.[8]

La proprietà qua sotto, che è diretta conseguenza della minimalità di ω, riveste un ruolo fondamentale.

[8] Uno dei criteri per valutare la validità fondazionale di una teoria degli insiemi è la possibilità di definire al suo interno opportuni insiemi che "codificano" in modo soddisfacente i principali oggetti della matematica, cioè che ne soddisfano le proprietà caratterizzanti come mostrate dalla pratica matematica.

Teorema 3.6 (Principio di induzione).
Sia $P(x, y_1, \ldots, y_k)$ una formula, dove $x, y_1, \ldots, y_k$ sono tutte e sole le sue variabili libere. Siano $A_1, \ldots, A_k$ insiemi fissati (parametri), e supponiamo che valgano le due condizioni:

- *Base induttiva: $P(0, A_1, \ldots, A_k)$;*
- *Passo induttivo: Per ogni $n \in \omega$, $P(n, A_1, \ldots, A_k) \Rightarrow P(\widehat{n}, A_1, \ldots, A_k)$.*

Allora $P(n, A_1, \ldots, A_k)$ vale per ogni $n \in \omega$.

Dim. Per ogni $A_1, \ldots, A_k$, l'insieme $A = \{n \in \omega \mid P(n, A_1, \ldots, A_k)\} \subseteq \omega$ esiste per *separazione*. Le ipotesi ci dicono che A è un insieme induttivo. Visto che ω è il più piccolo degli insiemi induttivi, deve necessariamente essere $A = \omega$, e questo dimostra la tesi. $\square$

Anche se la formulazione in termini di insiemi $\widehat{x}$ potrebbe lasciare perplessi, tra poco risulterà chiaro che questo principio corrisponde esattamente al principio di induzione sui numeri naturali cui siamo abituati. Intanto cominciamo ad usarlo per dimostrare un paio di semplici proprietà che ci risulteranno utili nel seguito.

Proposizione 3.7.

(1) *Se $x \neq 0$ è un numero naturale, allora $0 \in x$.*
(2) *Siano $x, y \in \omega$ numeri naturali. Se $x \in y$ allora $\widehat{x} \in \widehat{y}$.*

Dim. (1). Dimostriamo per induzione che per ogni $x \in \omega$, vale la proprietà $P(x)$: $(x \neq 0) \to (0 \in x)$. $P(0)$ è banalmente vera, perchè l'ipotesi "$0 \neq 0$" non vale. Assumiamo ora $P(x)$ e dimostriamo $P(\widehat{x})$. Se $x = 0$, allora $0 \in \{0\} = \widehat{x}$. Se $x \neq 0$, per ipotesi induttiva $0 \in x$, e dunque anche $0 \in \widehat{x}$.

(2). Procedendo per induzione, dimostriamo che per ogni $y \in \omega$ vale la proprietà $P(y)$: $\forall x \in \omega\ (x \in y) \to (\widehat{x} \in \widehat{y})$. Se $y = 0$ la proprietà è vera a vuoto perché l'ipotesi $x \in y$ non è mai realizzata. Al passo induttivo, assumiamo $P(y)$ e dimostriamo $P(\widehat{y})$. Supponiamo che $x \in \omega$ sia tale che $x \in \widehat{y} = y \cup \{y\}$; dobbiamo mostrare che allora $\widehat{x} \in \widehat{\widehat{y}}$. Si hanno due casi: se $x \in y$, per ipotesi induttiva $\widehat{x} \in \widehat{y}$, e quindi $\widehat{x} \in \widehat{\widehat{y}}$; se invece $x = y$, allora $\widehat{x} = \widehat{y} \in \widehat{\widehat{y}}$. $\square$

Esercizio 3.8. Dimostrare che $a = \{\{\emptyset\}\}$ e $b = \{\emptyset, \{\{\emptyset\}\}\}$ *non* sono numeri naturali.

Possiamo finalmente dimostrare una proprietà fondamentale dei numeri naturali.

Teorema 3.9.
La relazione di appartenenza $\in$ è una relazione di ordine lineare stretto su ω. Infatti valgono le seguenti proprietà:

(1) Antiriflessività*: $\forall x \in \omega\ (x \notin x)$;*
(2) Transitività*: $\forall x, y, z \in \omega\ (x \in y \wedge y \in z) \to x \in z$;*
(3) Tricotomia*: $\forall x, y \in \omega$, vale una ed una sola delle proprietà seguenti: $x \in y$, $x = y$, $y \in x$.*

Dim. (2). Procediamo per induzione su z, e consideriamo la seguente proprietà (con parametro ω):

$$P(z): \quad \forall x, y \in \omega\ (x \in y \wedge y \in z) \to x \in z.$$

Notiamo che $P(0)$ è banalmente vera. Infatti l'ipotesi $(x \in y \wedge y \in z)$ non è mai verificata (non esistono y tali che $y \in 0\,!$). Supponiamo ora vera la proprietà $P(z)$. Vogliamo dimostrare che vale

$$P(\widehat{z}): \quad \forall x, y \in \omega\ (x \in y \wedge y \in \widehat{z}) \rightarrow x \in \widehat{z}.$$

Assumiamo dunque $x \in y$ e $y \in \widehat{z}$. Dimostreremo che $x \in z$, e quindi $x \in \widehat{z}$. Da $y \in \widehat{z} = z \cup \{z\}$, segue che $y \in z$ o $y = z$. Nel primo caso, abbiamo $(x \in y \wedge y \in z)$ e quindi, per ipotesi induttiva, $x \in z$. Nel secondo caso, $x \in y$ equivale a $x \in z$, cioè quanto voluto.

(1). Per induzione su x. Banalmente $0 \notin 0$. Vediamo adesso il passo induttivo $(x \notin x) \rightarrow (\widehat{x} \notin \widehat{x})$ o, equivalentemente, $(\widehat{x} \in \widehat{x}) \rightarrow (x \in x)$. Se $\widehat{x} \in \widehat{x} = x \cup \{x\}$, allora $\widehat{x} \in x$ o $\widehat{x} = x$. Nel primo caso, visto che $x \in \widehat{x}$, per la proprietà transitiva (2) appena dimostrata, possiamo concludere che $x \in x$; e anche nel secondo caso vale $x \in x$ perché $x \in \widehat{x} = x$.

(3). Osserviamo intanto che può verificarsi al più una di quelle tre possibilità. Infatti se $x \in y$ e $x = y$, allora $x \in x$ contro la (1). Analogamente se $y \in x$ e $x = y$. Inoltre, se $x \in y$ e $y \in x$, per la (2) avremmo che $x \in x$, di nuovo contro la (1).

Resta da vedere che almeno una di quelle tre eventualità si verifica sempre. Diciamo che $y \in \omega$ è *confrontabile* (con ogni $x \in \omega$) se vale la seguente proprietà:

$$P(y): \quad \forall x \in \omega\ (x \in y \vee x = y \vee y \in x).$$

Vogliamo dimostrare che tutti i numeri naturali sono confrontabili. Procediamo per induzione su y. La base induttiva $P(0)$ è la proprietà:

$$\forall x \in \omega\ (x \in 0 \vee x = 0 \vee 0 \in x).$$

Visto che $x \in 0$ non è mai verificata, $P(0)$ equivale al punto (1) della Proposizione precedente. Consideriamo ora il passo induttivo. Supponiamo dunque che y sia confrontabile, e dimostriamo che anche $\widehat{y}$ lo è. Sia $x \in \omega$ qualunque. Per ipotesi induttiva:

$$(x \in y \vee x = y \vee y \in x).$$

Sia nel primo caso $x \in y$ che nel secondo caso $x = y$, banalmente $x \in \widehat{y}$, e quindi $\widehat{y}$ è confrontabile con x. Nel terzo caso, per la (2) della Proposizione precedente, da $y \in x$ segue che $\widehat{y} \in \widehat{x}$. Ma allora $\widehat{y} \in x$ o $\widehat{y} = x$, e anche in questo caso $\widehat{y}$ è confrontabile con x. $\square$

Proposizione 3.10. $\widehat{n}$ è il *successore* di $n \in \omega$ nell'insieme ordinato $(\omega, \in)$, cioè $\widehat{n}$ è il più piccolo dei numeri naturali maggiori di n.

Dim. Supponiamo per assurdo che esista $m \in \omega$ tale che $n \in m \in \widehat{n}$; quindi $m \in n$ oppure $m = n$. Nel primo caso avremmo $n \in m \in n$, da cui $n \in n$ per transitività, ma questo contraddice l'antiriflessività; nel secondo caso avremmo direttamente $n \in n$, di nuovo contraddicendo l'antiriflessività. $\square$

Anche se non abbiamo ancora definito la somma tra numeri naturali, per seguire l'uso comune da qui in avanti useremo la seguente

Notazione 3.11. *Se $n \in \omega$ è un numero naturale, denotiamo $\widehat{n} = n + 1$.*

Proposizione 3.12. *La funzione "successore" $S : n \mapsto n + 1$ è una bigezione tra ω e $\omega \setminus \{0\}$.*

Dim. Notiamo anzitutto che l'esistenza della funzione S è garantita dall'assioma di *separazione*:

$$S = \{(n, m) \in \omega \times \omega \mid m = n + 1\}.$$

Chiaramente S è una relazione univoca. Per vedere l'iniettività, supponiamo $n+1 = m + 1$. Da $n \in n + 1 = m + 1$ segue che $n \in m$ o $n = m$; analogamente, da $m \in m + 1 = n + 1$ segue che $m \in n$ o $m = n$. Se per assurdo fosse $n \neq m$, avremmo allora sia $n \in m$ che $m \in n$, contro la proprietà di tricotomia di $(\omega, \in)$. La suriettività è immediata, perché afferma che ogni numero naturale diverso da 0 è un successore, e questo fa parte del principio di induzione. Formalmente, si dimostra banalmente per induzione che la seguente proprietà vale per ogni $n \in \omega$:

$$P(n) : \quad n \neq 0 \to (\exists m \in n \;\; m + 1 = n).$$

$\square$

Esercizio 3.13. Dimostrare per induzione le seguenti proprietà relative a numeri naturali n, m:

(1) $n \in m$ se e solo se $n \subsetneq m$;
(2) L'intersezione di due numeri naturali è un numero naturale, e precisamente $n \cap m = \min\{n, m\}$;
(3) L'unione di due numeri naturali è un numero naturale, e precisamente $n \cup m = \max\{n, m\}$.
(4) Ogni elemento di un numero naturale è un numero naturale, cioè $(x \in n \in \omega) \to (x \in \omega)$;
(5) Se $\widehat{x} \in \omega$ allora $x \in \omega$;

Il prossimo teorema riguarda forme equivalenti del principio di induzione, cioè la cosiddetta "induzione forte" e il principio del "buon ordinamento", una nozione centrale della teoria degli insiemi che indagheremo a fondo più avanti.

Teorema 3.14.
Sia $(N, <)$ un insieme totalmente ordinato avente un elemento minimo 0. *Allora le due proprietà seguenti sono equivalenti:*

(1) Buon Ordinamento: *Ogni sottoinsieme non vuoto $X \subseteq N$ ha minimo ;*
(2) Induzione Forte: *Sia $P(x)$ una proprietà.*[9] *Supponiamo:*
  (I) *$P(0)$;*
  (II) *Per ogni $x \neq 0$ in N, vale l'implicazione $(\forall y < x \;\, P(y)) \to P(x)$.*[10]
  Allora $\forall x \in N \;\, P(x)$.

Se inoltre ogni elemento $x \in N$ ha un successore $x + 1$ e tutti gli $x \neq 0$ sono successori[11]*, vale anche l'equivalenza con:*

(3) Induzione: *Sia $P(x)$ una proprietà. Supponiamo:*
  (I)$'$ *$P(0)$;*
  (II)$'$ *Per ogni $x \in N$, vale l'implicazione $P(x) \to P(x + 1)$.*

[9] Qui per "proprietà" va intesa nel senso più generale, e non soltanto nel senso di proprietà formalizzabile in una fissato linguaggio del primo ordine. In altre parole, assumiamo che ad ogni sottoinsieme $A \subseteq N$ corrisponda una proprietà $P(x)$ tale che $\{x \in N \mid P(x)\} = A$.

[10] Seguendo l'uso comune, con abuso di notazione abbiamo scritto "$\forall y < x \; P(y)$" per intendere "$\forall y \, (y < x \to P(y)\,)$".

[11] In un insieme ordinato $(A, <)$, un elemento a' si dice *successore* di a se $a < a'$ e non esistono elementi x tali che $a < x < a'$.

Allora $\forall x \in N \ P(x)$.

Visto che $(\omega, \in)$ soddisfa tutte le ipotesi richieste in (3), in particolare dal principio di induzione segue che in ω valgono anche il principio di *induzione forte* e la proprietà di *buon ordinamento.*

DIM. (1) $\Rightarrow$ (2). Per assurdo supponiamo che esista una proprietà $P(x)$ che soddisfa le condizioni (I) e (II) ma tale che non valga $\forall x \in N \ P(x)$. Dunque l'insieme $X = \{x \in N \mid \neg P(x)\}$ è non vuoto e quindi, per il buon ordinamento, ammetterà un elemento minimo ξ. Chiaramente $\xi \neq 0$ perché vale $P(0)$. Per definizione di minimo, tutti gli elementi $y < \xi$ *non* appartengono ad X, cioè vale la proprietà $\forall y < \xi \ P(y)$. Per la (II) avremmo allora $P(\xi)$, contro il fatto che $\xi \in X$.

(2) $\Rightarrow$ (1). Per assurdo sia $X \subseteq N$ un sottoinsieme non vuoto senza minimo, e consideriamo la proprietà $P(x) : \ x \notin X$. Certamente vale $P(0)$, altrimenti $0 \in X$ sarebbe il minimo. Supponiamo ora $\forall y < x \ P(y)$, cioè che ogni y minore di x *non* appartenga ad X. Ma allora anche $x \notin X$, cioè vale $P(x)$, altrimenti avremmo che $x = \min X$. Abbiamo così verificato (I) e (II). Per Induzione Forte seguirebbe allora $P(x)$ per ogni $x \in X$, cioè $X = \emptyset$, contro l'ipotesi.

Non appena sappiamo che ogni elemento x ha successore $x + 1$, l'implicazione (2) $\Rightarrow$ (3) vale banalmente (per questo la (2) è chiamata *induzione forte*). Infatti fissiamo una proprietà $P(x)$. Se le condizioni $(\mathrm{I})'$ e $(\mathrm{II})'$ sono soddisfatte, a maggior ragione sono soddisfatte le corrispondenti condizioni (I) e (II) della induzione forte. Dunque, applicando (2) si può concludere $\forall x \in N \ P(x)$, come voluto.

L'implicazione (3) $\Rightarrow$ (1) si dimostra esattamente come (2) $\Rightarrow$ (1), considerando la proprietà: $P'(x) : \ \forall y \leq x \ y \notin X$, ed usando l'ipotesi che ogni $x \neq 0$ è successore $x = y + 1$ di qualche $y \in N$. $\square$

Nel passo induttivo di alcune dimostrazioni, per giungere a dimostrare la proprietà $P(n + 1)$ è talvolta utile assumere come ipotesi induttiva non soltanto la proprietà $P(n)$, ma *tutte* le proprietà "precedenti" $P(1), P(2), \ldots, P(n)$. In questo caso, è "più facile" dimostrare il passo induttivo. È infatti evidente che assumere un maggior numero di ipotesi, cioè $P(1), P(2), \ldots, P(n)$ anziché soltanto $P(n)$, rende "più facile" verificare $P(n + 1)$. Di conseguenza, con questa forma di induzione, è "più facile" dimostrare la tesi $\forall n \ P(n)$, il che significa che abbiamo uno strumento dimostrativo più potente. Per questo si parla di induzione *forte.*

4. Il teorema di ricorsione numerabile

Le definizioni per ricorrenza sui numeri naturali sono uno strumento molto usato in matematica. Il prossimo teorema ne dà una piena giustificazione a partire dagli assiomi già dati della teoria degli insiemi.

TEOREMA 4.1 (Ricorsione Numerabile). *Siano dati un insieme A, un elemento $a \in A$, ed una funzione $g : \omega \times A \to A$. Allora esiste ed unica successione $f : \omega \to A$ tale che*

$$\begin{cases} f(0) = a \\ f(n+1) = g(n, f(n)). \end{cases}$$

Naturalmente, l'analogo risultato vale se consideriamo, al posto di ω, l'insieme $\mathbb{N} = \omega \setminus \{0\}$ dei naturali diversi da zero.

Un esempio molto familiare di definizione per ricorsione è il seguente.

Esempio 4.2. L'esistenza ed unicità della funzione *fattoriale* $f(n) = n!$ segue dal teorema di ricorsione (assumiamo qui di conoscere già la definizione di prodotto tra numeri naturali, che vedremo più avanti). Infatti, considerando come insieme $A = \mathbb{N}$, come elemento $a = 1 \in \mathbb{N}$, e come $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ la funzione $g : (n, m) \mapsto (n+1) \cdot m$, otteniamo l'esistenza ed unicità di una funzione $f : \mathbb{N} \to \mathbb{N}$ tale che:

$$(\star) \qquad \begin{cases} f(1) = 1 \\ f(n+1) = (n+1) \cdot f(n) = g(n, f(n)). \end{cases}$$

Prima di dimostrare il teorema di ricorsione numerabile, ci è utile chiarire alcuni aspetti che riguardano l'unione di funzioni. Intanto, l'unione di un insieme di relazioni binarie è ancora una relazione binaria, in quanto è un insieme di coppie ordinate. La stessa proprietà non vale però in generale per le funzioni. Ad esempio, se $f(a) = b$ e $g(a) = b'$ dove $b \neq b'$, allora l'unione di coppie ordinate $f \cup g$ *non* è una funzione, cioè non è una relazione univoca. Tuttavia l'unione di una famiglia di funzioni è una funzione nel caso in cui valga un'opportuna ipotesi di compatibilità.

Definizione 4.3. Due funzioni φ e ψ sono *compatibili* se assumono gli stessi valori sull'intersezione dei rispettivi domini:

$$\forall \varphi, \psi \in \mathcal{F} \;\; \forall x \in \mathrm{dom}(\varphi) \cap \mathrm{dom}(\psi) \;\; \varphi(x) = \psi(x).$$

Equivalentemente, in termini puramente insiemistici, le funzioni φ e ψ sono compatibili se $\varphi \cap \psi$ è una funzione.

Esercizio 4.4. Sia $\mathcal{F}$ un insieme di funzioni. Allora l'unione $\Phi = \bigcup_{\varphi \in \mathcal{F}} \varphi$ è una funzione se e solo se le funzioni in $\mathcal{F}$ sono a due a due compatibili. In questo caso, $\mathrm{dom}(\Phi) = \bigcup_{\varphi \in \mathcal{F}} \mathrm{dom}(\varphi)$.

Occupiamoci finalmente della dimostrazione del teorema di ricorsione numerabile.

Dim. Diciamo che φ è una *approssimazione finita* (in breve AF) se $\varphi : k \to A$ è una funzione che ha come dominio un numero naturale positivo k, ed è tale che $\varphi(0) = a$ e $\varphi(n+1) = g(n, \varphi(n))$ per ogni naturale $n + 1 < k$. Ad esempio, la funzione $\varphi : 1 = \{0\} \to A$ dove $\varphi(0) = a$, è banalmente una AF. Notiamo ogni AF è un sottoinsieme di $\omega \times A$. Per *separazione* possiamo allora considerare l'insieme di *tutte* le AF:

$$\mathcal{F} = \{\varphi \in \mathcal{P}(\omega \times A) \mid \varphi \text{ è una AF}\}.$$

Il nostro scopo è adesso quello di "rincollare" le varie AF per formare una funzione $f : \omega \to A$ che soddisfi la $(\star)$. Vogliamo dimostrare che valgono le proprietà:

(1) Le funzioni di $\mathcal{F}$ sono a due a due compatibili, cioè:

$$\forall \varphi, \psi \in \mathcal{F} \;\; \forall x \in \mathrm{dom}(\varphi) \cap \mathrm{dom}(\psi) \;\; \varphi(x) = \psi(x).$$

(2) Per ogni $n \in \omega$, esiste $\varphi \in \mathcal{F}$ tale che $\mathrm{dom}(\varphi) = n + 1 = \{0, \ldots, n\}$.

Una volta verificate le due proprietà di sopra, l'esistenza della funzione cercata si ottiene prendendo $f = \bigcup_{\varphi \in \mathcal{F}} \varphi$. Infatti, per l'Esercizio 4.4 di sopra, f è una funzione con $\mathrm{dom}(f) = \bigcup_{\varphi \in \mathcal{F}} \mathrm{dom}(\varphi) = \omega$. Inoltre, per ogni $\varphi \in \mathcal{F}$ e per ogni $n \in \mathrm{dom}(\varphi)$, si ha $f(n) = \varphi(n)$, e le proprietà $(\star)$ seguono direttamente dal fatto che tutte le funzioni $\varphi \in \mathcal{F}$ sono AF.

Per dimostrare la (1), procediamo per induzione considerando la proprietà

$$P(n) : \quad \forall \varphi, \psi \in \mathcal{F} \ \ (n \in \mathrm{dom}(\varphi) \cap \mathrm{dom}(\psi)) \to \varphi(n) = \psi(n).$$

Quando $n = 0$ la cosa è banale, perchè tutte le AF assumono il valore a per $n = 0$. Per il passo induttivo, supponiamo che un successore $n + 1 \in \mathrm{dom}(\varphi) \cap \mathrm{dom}(\psi)$ appartenga al dominio di due AF; notiamo che allora anche $n \in \mathrm{dom}(\varphi) \cap \mathrm{dom}(\psi)$. Usando l'ipotesi induttiva $\varphi(n) = \psi(n)$, dalle proprietà di AF si ottengono le uguaglianze:

$$\varphi(n + 1) = g(n, \varphi(n)) = g(n, \psi(n)) = \psi(n + 1).$$

Anche per dimostrare la (2) procediamo per induzione. Per $n = 0$ basta considerare $\varphi = \{(0, a)\}$, che è banalmente una AF con $\mathrm{dom}(\varphi) = \{0\} = 1$. Inoltre, se $\varphi \in \mathcal{F}$ e $\mathrm{dom}(\varphi) = n + 1 = \{0, 1, \ldots, n\}$, anche $\psi = \varphi \cup \{(n + 1, b)\}$ dove $b = g(n, \varphi(n))$ è una AF con $\mathrm{dom}(\psi) = \{0, 1, \ldots, n, n + 1\} = n + 2$.

Occupiamoci infine della questione dell'*unicità*, e supponiamo che f_1 che f_2 entrambe soddisfino le proprietà $(\star)$. Per induzione su n, mostriamo che $f_1(n) = f_2(n)$. Per $n = 0$ questo è immediato perché $f_1(0) = a = f_2(0)$. Nel passo induttivo, basta notare che dall'ipotesi $f_1(n) = f_2(n)$ segue che $f_1(n + 1) = g(n, f_1(n)) = g(n, f_2(n)) = f_2(n + 1)$. $\square$

In alcune definizioni per ricorsione, il valore al passo successore $n + 1$ è determinato non solo dal valore nel predecessore n, ma anche da valori precedenti. Ad esempio, la *successione di Fibonacci* è definita per ricorsione ponendo: $a_1 = a_2 = 1$, e $a_{n+1} = a_n + a_{n-1}$ per $n \geq 2$. Per giustificare questo tipo di definizioni, occorre una forma più forte del teorema di ricorsione. Precisamente:

Teorema 4.5 (Ricorsione Numerabile II).
Per ogni insieme A, per ogni $a \in A$, e per ogni funzione $g : \omega \times FSeq(A) \to A$,[12] *esiste ed unica funzione $f : \omega \to A$ tale che:*

$$(\star) \qquad \begin{cases} f(0) & = \ a \\ f(n + 1) & = \ g(n, f|_{n+1}). \end{cases}$$

Ovviamente anche questa versione del teorema di ricorsione vale se sostituiamo $\mathbb{N}$ al posto di ω.

La dimostrazione di questa forma di ricorsione numerabile è una semplice modifica della dimostrazione precedente, ed è lasciata per esercizio.

Siamo finalmente pronti a dimostrare un importante risultato sull'equipotenza che già abbiamo usato ripetutamente.

Teorema 4.6 (Cantor-Bernstein).
Se $|X| \leq |Y|$ e $|Y| \leq |X|$ allora $|X| = |Y|$.

[12] Ricordiamo che con $\mathrm{FSeq}(A) = \{\sigma \mid \exists n \in \mathbb{N} \ \sigma : \{1, \ldots, n\} \to A\}$ si denotava l'insieme delle *sequenze finite* di elementi di A.

Vista la particolare importanza di questo teorema, ne diamo due dimostrazioni.

Dim. 1. Prendiamo $f : X \to Y$ e $g : Y \to X$ funzioni iniettive. Chiaramente f determina una bigezione tra X e l'insieme immagine $f(X)$; e g determina una bigezione tra Y e $g(Y)$, e una bigezione tra $f(X)$ e $g(f(X))$. Abbiamo dunque $g(f(X)) \subseteq g(Y) \subseteq X$ dove $|g(f(X))| = |f(X)| = |X|$ e $|g(Y)| = |Y|$. La tesi segue allora dal lemma seguente, prendendo $A = X$, $B = g(Y)$, e $C = g(f(X))$. $\square$

Lemma 4.7. *Siano $A \supseteq B \supseteq C$ dove $|A| = |C|$. Allora $|A| = |B| = |C|$.*

Dim. Fissiamo una bigezione $\varphi : A \to C$. Sia $D = A \setminus B$, e definiamo una successione di sottoinsiemi di C come segue:

$$\begin{cases} E_1 & = \varphi(D) \\ E_{n+1} & = \varphi(E_n) \end{cases}$$

Osserviamo che l'esistenza della successione $(E_n \mid n \in \mathbb{N})$ è garantita dal Teorema di ricorsione numerabile.[13] Sia $E = \bigcup_{n\in\mathbb{N}} E_n$ l'unione di tutti questi insiemi, e definiamo la funzione $\psi : A \to B$ ponendo $\psi = \varphi|_{D\cup E} \cup \mathrm{id}_{B\setminus E}$, cioè:

$$\psi(a) = \begin{cases} \varphi(a) & \text{se } a \in D \cup E \\ a & \text{altrimenti, cioè se } a \in B \setminus E. \end{cases}$$

Verifichiamo che ψ è la bigezione cercata. Vediamo prima la suriettività. Dalla definizione, segue direttamente che $\mathrm{imm}(\psi) = \mathrm{imm}(\varphi|_{D\cup E}) \cup \mathrm{imm}(\mathrm{id}_{B\setminus E})$. Visto che banalmente $\mathrm{imm}(\mathrm{id}_{B\setminus E}) = B \setminus E$, basta vedere che $E \subseteq \mathrm{imm}(\varphi|_{D\cup E})$ (in realtà vale l'uguaglianza). Se $b \in E_0$, allora $b = \varphi(a) = \psi(a)$ con $a \in D$. Se invece $b \in E_{n+1}$ per qualche n, allora $b = \varphi(a) = \psi(a)$ per un $a \in E_n$. Per l'iniettività, notiamo che le restrizioni $\psi|_{D\cup E}$ e $\psi|_{B\setminus E}$ sono entrambe iniettive, perché uguali rispettivamente a $\varphi|_{D\cup E}$ e alla funzione identità $\mathrm{id}_{B\setminus E}$. Per concludere che ψ è iniettiva basta allora osservare che $\varphi|_{D\cup E}$ e $\mathrm{id}_{B\setminus E}$ hanno immagini disgiunte, e questo è immediato perché $\mathrm{imm}(\varphi|_{D\cup E}) = E$. $\square$

Dim. 2. Definiamo per ricorsione numerabile:

$$X_0 = X\,;\ Y_0 = Y\,;\ X_{n+1} = g(Y_n)\,;\ Y_{n+1} = f(X_n).$$

Formalmente, stiamo definendo la successione $a_n = (X_n, Y_n)$ ponendo $a_0 = (X, Y)$ e $a_{n+1} = F(a_n)$, dove $F : \mathcal{P}(X) \times \mathcal{P}(Y) \to \mathcal{P}(X) \times \mathcal{P}(Y)$ è la funzione tale che $F(Z, W) = (g(W), f(Z))$.

Notiamo anzitutto che le sequenze di insiemi $(X_n \mid n \in \omega)$ e $(Y_n \mid n \in \omega)$ sono debolmente descrescenti:

- Per ogni n, $X_{n+1} \subseteq X_n$ e $Y_{n+1} \subseteq Y_n$.

Questo si verifica facilmente per induzione. Se $n = 0$, $X_1 = g(Y) \subseteq X = X_0$ e $Y_1 = f(X) \subseteq Y = Y_0$. Consideriamo ora il passo induttivo $k + 1$. Per ipotesi induttiva $X_{k+1} \subseteq X_k$ e dunque $Y_{k+2} = f(X_{k+1}) \subseteq f(X_k) = Y_{k+1}$. Analogamente, dall'ipotesi $Y_{k+1} \subseteq Y_k$ segue che $X_{k+2} \subseteq X_{k+1}$.

[13] Precisamente, si applica il Teorema di ricorsione numerabile considerando l'insieme $\mathcal{P}(C)$, l'elemento $\varphi(D) \in \mathcal{P}(C)$, e la funzione $g : \omega \times \mathcal{P}(C) \to \mathcal{P}(C)$ dove $g(n, X) = \varphi(X)$.

Partizioniamo gli insiemi X e Y considerando rispettivamente le "fette"

$$X_0 \setminus X_1; X_1 \setminus X_2;\; X_2 \setminus X_3;\; \ldots\; ; \widetilde{X} = \bigcap_{n\in\mathbb{N}} X_n.$$

$$Y_0 \setminus Y_1; Y_1 \setminus Y_2;\; Y_2 \setminus Y_3;\; \ldots\; ; \widetilde{Y} = \bigcap_{n\in\mathbb{N}} Y_n.$$

Visto che f è iniettiva, $f(\widetilde{X}) = f(\bigcap_{n\in\omega} X_n) = \bigcap_{n\in\omega} f(X_n) = \bigcap_{n\in\omega} Y_{n+1} = \widetilde{Y}$. Inoltre, usando l'iniettività di f e di g, si hanno le uguaglianze

$$f(X_n \setminus X_{n+1}) = f(X_n) \setminus f(X_{n+1}) = Y_{n+1} \setminus Y_{n+2}.$$

$$g(Y_n \setminus Y_{n+1}) = g(Y_n) \setminus g(Y_{n+1}) = X_{n+1} \setminus X_{n+2}.$$

Ne segue che per ogni n abbiamo le bigezioni:

$$f_n = f|_{X_n \setminus X_{n+1}} : X_n \setminus X_{n+1} \to Y_{n+1} \setminus Y_{n+2}$$

$$g_n = g|_{Y_n \setminus Y_{n+1}} : Y_n \setminus Y_{n+1} \to X_{n+1} \setminus X_{n+2}.$$

La bigezione cercata $\varphi : X \to Y$ si ottiene "rincollando" tutte le f_n con n pari e tutte le inverse g_n^{-1} con n dispari con la restrizione $f|_{\widetilde{X}}$. Precisamente, poniamo:

$$\varphi(x) = \begin{cases} f_n(x) & \text{se } x \in X_n \setminus X_{n+1} \text{ con } n \text{ pari} \\ g_{n-1}^{-1}(x) & \text{se } x \in X_n \setminus X_{n+1} \text{ con } n \text{ dispari} \\ f(x) & \text{se } x \in \widetilde{X}. \end{cases}$$

La verifica in dettaglio che la funzione φ definita sopra è effettivamente una bigezione tra X e Y è lasciata per esercizio. □