Assiomi per la teoria degli insiemi di Zermelo-Fraenkel

Stefano Baratella
Versione LaTeX a cura di Tullio Garbari e Luca Tasin

0 Introduzione

La teoria degli insiemi costituisce il fondamento della matematica. Tutti i concetti matematici sono definiti a partire dalle nozioni *primitive* (cioè non definite) di *insieme* e di *appartenenza*.

Nella teoria assiomatica degli insiemi si formulano alcuni semplici assiomi a proposito di queste due nozioni primitive nel tentativo di catturare tutti i principi di base "ovviamente veri" che riguardano gli insiemi.

La presentazione della teoria è assiomatica e gli assiomi devono essere dati in un linguaggio formale, per evitare "paradossi" (ad esempio la frase "il più piccolo numero non definibile con meno di venti parole della lingua italiana" definisce quel più piccolo numero con meno di venti parole: il problema qui è che non è stata data una definizione rigorosa di definibilità).

Un'altra ragione per introdurre un linguaggio formale è che quando si fanno affermazioni del tipo "l'asserzione x è derivabile dall'insieme di assiomi y" si vuole una definizione rigorosa di derivabilità (o, se vogliamo, di dimostrabilità).

Non introdurremo in dettaglio il linguaggio formale della teoria degli insiemi. Abbiamo soltanto che, assieme agli usuali simboli per connettivi, quantificatori e uguaglianza, c'è un simbolo di predicato binario $\in$ per l'appartenenza (successivi esempi chiariranno quanto appena detto).

Adottare un metodo assiomatico significa, come già detto, esprimere proprietà di oggetti di cui *non* si dà una definizione (nello stesso modo in cui punto e retta sono enti primitivi della geometria euclidea piana). *Non* definiremo quindi cos'è un insieme ("Un insieme è una collezione di oggetti" *non* è una definizione matematicamente accettabile) e nemmeno definiremo la relazione $\in$.

Quali insiemi descriviamo? In accordo con il fatto che la teoria degli insiemi è la base della matematica, dovremmo essere in grado di catturare tutta la matematica parlando di insiemi e non di cani o di polli: le nostre variabili non dovrebbero correre su queste due categorie. Così, se C è un cane, $\{C\}$ è un insieme, ma *non* un legittimo oggetto matematico.

In altre parole, descriviamo gli insiemi che sono *ereditariamente tali*, quelli cioè i cui elementi e gli elementi dei cui elementi... e così via sono insiemi.

1 Gli assiomi

Diamo una lista degli assiomi della teoria più diffusa: ZFC, cioè la teoria di Zermelo-Fraenkel (ZF) potenziata con l'Assioma di Scelta (AC).

Per gli assiomi daremo anche una formulazione nel linguaggio formale, anche se questo aspetto può essere tralasciato.

Assioma 0. *Esistenza di un insieme*

La presenza di questo assioma non deve stupire: garantiamo anzitutto che il mondo che vogliamo descrivere sia abitato.

Ecco una formalizzazione dell'assioma (d'ora in poi, le variabili variano su insiemi):

$$\exists x\ (x = x)$$

[“esiste un insieme che è uguale a se stesso” è come dire “esiste un insieme” perché la relazione di uguaglianza è riflessiva].

Assioma 1. *Estensionalità: comunque dati due insiemi, se essi hanno gli stessi elementi, allora sono uguali.*

Formalmente:

$$\forall x\ \forall y\ (\forall z\ (z \in x \to z \in y) \to x = y)$$

Osservazione Due insiemi uguali hanno gli stessi elementi (per una delle proprietà dell'uguaglianza), quindi si potrebbe sostituire “$\to$” in $A1$ con “$\leftrightarrow$”.

Il senso dell'assioma di estensionalità è che un insieme è determinato dagli elementi che lo abitano, e non da come esso è stato pensato (atteggiamento *estensionale*.

Esempio di atteggiamento *intensionale* (non estensionale): i due insiemi

$$A = \{x \in \mathbb{N} : x^2 - x = 0\} \text{ e } B = \{x \in \mathbb{N} : 0 \leqslant x \leqslant 1\}$$

sono

- intensionalmente diversi (le proprietà che li definiscono sono diverse),

ma

- estensionalmente uguali

Assioma 2 (Schema di Separazione). *Sia $\phi(x)$ una proprietà esprimibile nel linguaggio formale di ZF e sia A un insieme. Allora la collezione*

$$\{x \in A : \phi(x)\}$$

è un insieme.

Intuitivamente, Separazione afferma che, dato un insieme, la collezione degli elementi di quell'insieme che soddisfano una fissata proprietà costituisce a loro volta un insieme.

Formalmente:

$$\forall x \ \exists y \ \forall z \ (z \in y \leftrightarrow z \in x \wedge \phi(x))$$

[si richiede che la variabile y non compaia in $\phi(x)$]

Nota Nella formulazione dello Schema di Separazione *non* si può essere liberali al punto da richiedere che ogni proprietà definisca un insieme.

Se si assume che, per ogni proprietà $\phi(x)$, la collezione $\{x : \phi(x)\}$ sia un insieme, si ha, in particolare, che la collezione

$$U = \{x : x = x\}$$

di tutti gli insiemi è un insieme e si ottiene quindi immediatamente il Paradosso di Russell, separando su U mediante la proprietà $x \notin x$ (verificarlo formalmente).

Osserviamo dunque che esistono collezioni che non sono insiemi (come U). Tecnicamente tali collezioni si chiamano *classi proprie.*

Intuitivamente una classe propria è una collezione "grossa". Delle classi proprie la teoria degli insiemi non può trattare formalmente, però le classi proprie si riescono in qualche modo a recuperare "sintatticamente". Infatti classe è sinonimo di proprietàesprimibile nel linguaggio formale di ZF.

Esercizio Esistenza e unicità dell'insieme vuoto. Sia x un insieme (esiste per $A0$). Separiamo su x mediante la formula $y \neq y$: la collezione

$$\{y \in x : y \neq y\}$$

è quindi un insieme privo di elementi. Quindi esiste (almeno) un insieme vuoto. Per Estensionalità due insiemi emtrambi privi di elementi sono uguali, da cui l'unicità.

Assioma 3 (Coppia). *Comunque dati due insiemi ne esiste uno a cui entrambi appartengono*

$$\forall x \ \forall y \ \exists z \ (x \in z \wedge y \in z)$$

Abbiamo formulato l'assioma di coppia per ottenere la coppia $\{x, y\}$ di due insiemi x e y come insieme. Per come è stato formulato, Coppia assicura l'esistenza di un insieme z a cui x e y appartengono entrambi. Basta applicare Separazione (come?) per ottenere un insieme che contiene esattamente x e y.

Nota Il vantaggio di formulare l'assioma di Coppia (e gli altri assiomi che seguiranno) in forma debole è legato alla maggiore facilità nel verificare la verità di un assioma debole, quando si considerano modelli della teoria degli insiemi.

Esercizio Coppia ordinata. Definire la coppia ordinata di x e y (notazione: $< x, y >$) così:

$$< x, y > := \{\{x\}, \{x, y\}\}.$$

Provare che

1. $< x, y >$ è un insieme;
2. se $< x, y > = < z, w >$, allora $x = z$ e $y = w$.

Assioma 4 (Unione). *Comunque data una famiglia di insiemi, esiste un insieme che è sovrainsieme di tutti gli elementi della famiglia.*

$$\forall x\ \exists y\ \forall z\ (\exists u \in x(z \in u) \to z \in y)$$

Osservare che anche Unione è data in forma "debole": basta applicare Separazione per ottenere esattamente l'unione della famiglia.

Esercizio Dedurre dall'assioma di Unione e dagli altri assiomi finora introdotti che se A, B sono insiemi, allora $A \cup B$ è un insieme.

Esercizio Preannunciamo che non ci sarà un assioma per l'intersezione su una famiglia di insiemi. In particolare non ci sarà un assioma che garantisca che, se A e B sono insiemi, allora $A \cap B$ è un insieme. Un tale assioma è superfluo. Spiegare perché. [Usare Separazione]

Assioma 5 (Potenza). *Per ogni insieme x ne esiste un altro cui appartengono tutte le sottocollezioni di x che sono insiemi.*

$$\forall x\ \exists y\ \forall z\ (z \subseteq y \to z \in x)$$

(dove $z \subseteq y$ abbrevia $\forall w\ (w \in x \to w \in y)$).

Osserviamo che l'assioma è dato in forma debole. Valgono le condizioni precedenti, così da ottenere che, se x è un insieme, anche $\mathcal{P}(x)$ è un insieme.

Nota Potenza *non* dice che tutte le sottocollezioni di un insieme x sono insiemi, ma semplicemente assicura la possibilità di poter collezionare in un insieme tutte le sottocollezioni di x che sono a loro volta insiemi.

L'assioma di Potenza consente di ottenere insiemi di cardinalità arbitrariamente grande (si pensi al Teorema di Cantor che afferma $x \not\approx \mathcal{P}(x)$ per ogni insieme x).

Assioma 6 (Infinito). *Esiste un insieme che contiene $\varnothing$ e ogni volta che un insieme y vi appartiene, anche $y \cup \{y\}$ vi appartiene.*

$$\exists x \ (\varnothing \in x \land \forall y \ (y \in x \to y \cup \{y\} \in x)$$

Un insieme la cui esistenza è garantita dall'assioma di Infinito è detto *insieme induttivo.*

L'assioma di Infinito assicura che la collezione dei numeri naturali (pensati come gli ordinali finiti) è un insieme.

Osservazione Supponiamo ZFC consistente, cioè libero da contraddizioni. Definiamo ricorsivamente

$$R_0 = \varnothing; \ R_{n+1} = \mathcal{P}(R_n)$$

e poniamo $R_\omega = \bigcup_{n \in \mathbb{N}} R_n$.

Non è difficile far vedere che gli Assiomi da 0 a 5 sono veri in $< R_\omega, \in >$, e che l'Assioma di Infinito è falso in $< R_\omega, \in >$. Anche tutti gli assiomi che introdurremo in seguito dono veri in $< R_\omega, \in >$: questo dice che l'Assioma di Infinito è indipendente dagli altri assiomi di ZFC.

Assioma 7 (Schema di Rimpiazzamento). *(Formulazione semplificata) Sia $\phi(x, y)$ una proprietà esprimibile nel linguaggio di ZF e sia z un insieme tale che per ogni $x \in z$ esiste ed è unico y tale che $\phi(x, y)$.*

Allora esiste un insieme u a cui appartengono tutti gli y per cui esiste $x \in z$ che soddisfa $\phi(x, y)$.

$$\forall z \ (\forall x \in z \ \exists! y \ \phi(x, y) \to \exists u \ \forall y \ (\exists x \in z \ \phi(x, y) \to y \in u))$$

Certamente lo Schema di Rimpiazzamento non è di immediata comprensione, ma una sua interpretazione intuitiva aiuta a capirlo: sia z come nella formulazione dell'assioma: possiamo allora pensare a ϕ come ad una funzione di dominio z ("per ogni $x \in z$ esiste ed è unico y tale che $\phi(x, y)$"). L'assioma garantisce che c'è un insieme che contiene l'immagine della funzione associata a ϕ.

Impropriamente si dice che lo Schema di Rimpiazzamento garantisce che l'immagine di un insieme (pensato come collezione "non troppo grossa") mediante una funzione è un insieme (cioè una collezione "non troppo grossa"). Conviene ricordare lo Schema di Rimpiazzamento in questa forma intuitiva.

Rimpiazzamento non ha un grosso ruolo nella pratica matematica, ma è essenziale – ad esempio – per dimostrare che gli ordinali classificano i buoni ordini (cioè che ogni insieme bene ordinato è isomorfo ad un unico ordinale).

Assioma 8 (Fondazione). *Tutti gli insiemi sono costruiti a partire dall'insieme vuoto iterando l'applicazione dell'assioma di Potenza.*

$$\forall x \ (x \neq \varnothing \to \exists y \ (y \in x \wedge y \cap x = \varnothing))$$

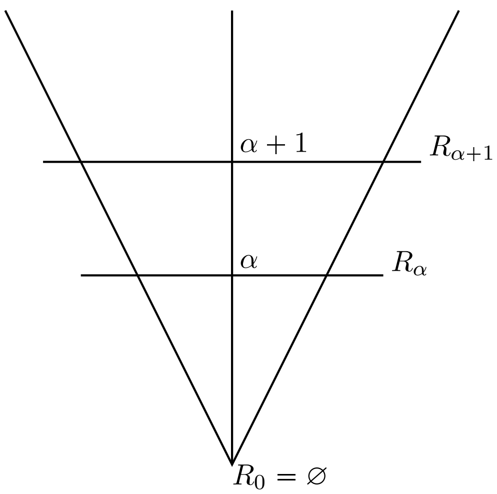
La formulazione dell'assioma di Fondazione non esprime immediatamente la descrizione intuitiva del significato dell'assioma: c'è del lavoro da fare per provare quanto segue: definiamo ricorsivamente nella classe On degli ordinali

$$R_0 = \varnothing; \ R_{\alpha+1}; \ R_\alpha = \bigcup_{\beta<\alpha} R_\beta (\text{se } \alpha \text{ è un ordinale limite})$$

e sia $R = \bigcup_{\alpha \in On} R_\alpha$.

Allora l'assioma di Fondazione è equivalente a "ogni insieme vive in R", o, anche, a $\forall x \ \exists \alpha \ (x \subseteq R_\alpha)$.

Ecco la gerarchia degli R_α (è crescente rispetto a $\subseteq$):



Il significato di Fondazione è che ogni insieme viene costruito a qualche livello (ordinale) della gerarchia.

Inoltre, ogni insieme viene costruito "dopo" (cioè compare ad un livello superiore della gerarchia rispetto a) i suoi elementi: ciò in particolare vieta che qualche insieme possa appartenere a se stesso: $x \in x$ è vietato, per ogni insieme x, dall'assioma di Fondazione.

L'assioma di Fondazione è irrilevante per la pratica matematica (di ogni oggetto non ben fondato esiste una coppia "isomorfa" ben fondata), però ci dice che l'universo degli insieme è costruito a partire da ingredienti "minimi" (l'insieme vuoto) e che al suo interno non ci sono "patologie" legate alla relazione $\in$.

Fondazione semplifica di molto la vita dei teorici degli insiemi.

Assioma 9 (Assioma di Scelta). *Su ogni famiglia di insiemi non vuoti esiste una funzione di scelta.*

$$\forall x \; ((\forall y \; \in x \; y \neq \varnothing) \rightarrow \exists f \; ((\mathrm{Fun}(f) \wedge \mathrm{dom}(f) = x \wedge \forall y \in x \; (f(y) \in y))$$

(dove $\mathrm{Fun}(f)$ *è la formula che esprime la proprietà "f è una funzione")*

Le conseguenze e gli equivalenti di AC sono tanti e tali che esso merita una trattazione a parte.

2 Consistenza

Come per ogni teoria (non solo in ambito matematico) è da porsi il problema se ZF sia una teoria libera da contraddizioni (o consistente).

A questo riguardo ricordiamo che, come conseguenza del 2° Teorema di Incompletezza di Gödel, se ZF è consistente, allora non esiste nessuna dimostrazione di consistenza di ZF che sia formalizzabile in ZF.

Cosa significa questo? Se identifichiamo ZF con la matematica, abbiamo che, se la matematica è consistente, non esiste nessuna dimostrazione di consistenza della matematica che faccia uso soltanto di principi matematici! Allora, una presunta dimostrazione di consistenza della matematica che validità ha? D'altra parte, avere una dimostrazione di consistenza della matematica all'interno della matematica ci farebbe dormire sonni tranquilli?

No! Perché se la matematica è inconsistente, allora è in grado di provare qualunque asserzione, inclusa la propria consistenza!

E se la matematica fosse davvero inconsistente? Anzitutto, allo stato attuale non si vede il modo di provare una contraddizione all'interno della matematica. Se ce n'è una, potremmo pensare che coinvolga principi così lontani dalle nostre conoscenze attuali da farci dormire sonni tranquilli per molte generazioni ancora.

Per le ragioni sopra esposte i risultati di consistenza che si ottengono in teoria degli insiemi sono sempre risultati di consistenza relativa, ad esempio:

$$\begin{aligned} ZF \text{ consistente} &\;\Rightarrow\; ZFC \text{ consistente} \\ ZF \text{ consistente} &\;\Rightarrow\; ZF + (\neg AC) \text{ consistente} \end{aligned}$$

Entrambe le implicazioni precedenti possono essere provate e, insieme, dicono che AC è indipendente da ZF. Anche l'Ipotesi del Continuo (CH) e l'Ipotesi Generalizzata del Continuo (GCH) sono indipendenti da ZF.