Teoria degli insiemi minimale

Paolo Lipparini

24 dicembre 2020

Questi appunti sono stati scritti molto di fretta, potrebbero contenere molti errori! Cercherò di rivederli non appena possibile, nel frattempo faccio notare che è molto meritorio da parte degli studenti scoprire errori negli appunti dei docenti!

Questa è una versione incompleta, verrà aggiunto altro materiale.

1. Teoria degli insiemi minimale

Premessa. Lo scopo di questa sezione è quello di presentare nella maniera più breve e semplice possibile, evitando dettagli eccessivamente tecnici, alcune nozioni e idee di teoria degli insiemi che per uno studente, ad esempio di matematica, sarebbe opportuno conoscere. Le sezioni indicate con un asterisco e le note possono essere saltate in prima lettura.

1.1. Nozione intuitiva di insieme. Molte delle definizioni in questa sottosezione potrebbero essere già note al lettore. Preferiamo riepilogarle comunque per completezza e affinché non sussista alcun dubbio riguardo a terminologia e notazioni.

Intuitivamente, un *insieme* è una collezione, un aggregato, un raggruppamento di oggetti. Se x è un insieme, e l'oggetto A appartiene ad x, si scrive $A \in x$ e si dice che A è *un elemento di* x, che A *sta in* x, o altre simili espressioni. Per brevità, talvolta si scriverà $A, B \in x$ per intendere che contemporaneamente $A \in x$ e $B \in x$. Se A non appartiene ad x, si scrive $A \notin x$.

1.1.1. *Uguaglianza fra insiemi.* Due insiemi x e y si considerano *uguali*, cioè identici, e si scrive $x = y$, se x e y contengono *esattamente* gli stessi oggetti[1] [2].

[1] L'introduzione dell'uguaglianza come presentata sopra a prima vista potrebbe sembrare una semplice definizione, ma in realtà si tratta di un'assunzione forte. Si richiede che due insiemi uguali soddisfino esattamente le stesse proprietà; cioè, ad esempio, se $x = y$, allora, per ogni insieme z, deve valere $x \in z$ se e solo se $y \in z$.

[2] In generale, nel calcolo dei predicati, una *teoria con uguaglianza* ha un simbolo speciale di relazione binario $=$ tale che le seguenti formule sono assiomi (o comunque dimostrabili):
$x = x$,
$x = y \Rightarrow y = x$,
$x = y \wedge y = z \Rightarrow x = z$,
$x = y \Rightarrow t(z_0, z_1, \dots, z_{i-1}, x, z_{i+1}, \dots) = t(z_0, z_1, \dots, z_{i-1}, y, z_{i+1}, \dots)$, per ogni termine t,

La precedente affermazione è chiamata *Principio di estensionalità*. Ad esempio, gli insiemi descritti dalle seguenti clausole (a) - (c′) sono uguali:

(a) L'insieme $\{4, 6, 8\}$ che contiene esattamente i numeri 4, 6, 8.

(a′) L'insieme $\{6, 8, 4\}$.

(b) L'insieme $\{x \in \mathbb{N} \mid \text{x è un numero naturale pari e } 3 \leq x \leq 9\}$ costituito da tutti i numeri naturali pari compresi fra 3 e 9. Ricordiamo che i numeri naturali sono 0, 1, 2... e che l'insieme di tutti i numeri naturali[3] si indica con $\mathbb{N}$.

(c) L'insieme $\{2t \mid t \in \mathbb{N} \text{ e } 1 < t < 5\}$ di tutti i numeri che possono essere espressi nella forma $2t$ al variare di t fra i numeri naturali strettamente compresi fra 1 e 5.

(c′) L'insieme $\{n \in \mathbb{N} \mid \text{esiste un } t \in \mathbb{N} \text{ tale che } t = 2n \text{ e } 1 < t < 5\}$ (l'espressione fra graffe in (c) può essere considerata un'abbreviazione dell'espressione indicata qui in (c′)).

Quindi l'uguaglianza fra due insiemi dipende solo dagli elementi che essi contengono, ed è completamente indipendente dal modo in cui questi insiemi vengono definiti o descritti; in particolare, è indipendente dall'ordine in cui vengono eventualmente elencati i loro elementi. In altre parole, almeno in linea di principio, un insieme x risulta ben definito quando esiste una netta e precisa distinzione fra gli elementi che appartengono ad x e quelli che non vi appartengono, cioè quando è perfettamente chiaro[4] cosa appartiene e cosa non

---

$x = y \;\Rightarrow\; (\varphi(z_0, z_1, \dots, z_{i-1}, x, z_{i+1}, \dots) \;\Rightarrow\; \varphi(z_0, z_1, \dots, z_{i-1}, y, z_{i+1}, \dots))$,
per ogni formula φ.

Le condizioni si possono indebolire, ed esistono molte formulazioni equivalenti, vedi ad esempio la Sezione 8 nel Capitolo 2 del libro del Mendelson. Solitamente si assume che in un modello di una teoria con uguaglianza il simbolo $=$ venga effettivamente interpretato come la relazione di uguaglianza fra gli elementi del modello; i modelli per cui questo avviene si chiamano modelli *normali*.

[3] Alcuni autori non includono il numero 0 fra i numeri naturali (questo corrisponde all'origine storica dell'idea di numero naturale); altri autori includono il numero 0 e indicano con $\mathbb{N}^*$ oppure con $\mathbb{N}^+$ l'insieme dei numeri naturali escluso lo 0. Dovrebbe risultare chiaro che non si tratta di una questione sostanziale, ma esclusivamente di convenzioni di comodo. Non sempre esistono notazioni e convenzioni universalmente accettate in matematica. In questo e altri casi, quando si tratta di convenzioni e definizioni, è sempre opportuno consultare il testo che si sta leggendo, facendo riferimento con attenzione alle notazioni usate. Beninteso, può essere difficoltoso passare da un testo all'altro, specie se i testi fanno uso di notazioni e definizioni molto diverse.

[4] Esiste una teoria degli insiemi "sfumati", dove l'appartenenza di qualche oggetto ad un insieme è incerta o ha valori probabilistici. Qui ci limiteremo alla teoria classica.

È anche ovvio che espressioni del tipo "precisa distinzione", "chiaro" etc. sono altrettanto vaghe quanto "aggregato", "raggruppamento" etc. Questa osservazione non costituisce certo un problema, visto che in questa sottosezione ci limitiamo a presentare le nozioni intuitivamente. Va però fatto notare che, mentre la definizione (o meglio, presentazione) degli insiemi come collezioni non sembra poter dare adito a molti tipi diversi di interpretazione, invece parlare di "netta distinzione" può dar luogo a differenti interpretazioni. Esistono collezioni, dette *ricorsivamente enumerabili* per cui esiste una procedura effettiva che elenca tutti gli elementi di una tale collezione. Ma non sempre è detto che esista una procedura effettiva che elenca tutti gli elementi che *non* vi appartengono (qui supponiamo per semplicità di considerare solo collezioni di numeri naturali). Certamente qualcuno potrebbe interpretare

appartiene ad x.

Non solo, un dato elemento non può appartenere ad un insieme "più di una volta", in altre parole, nella nozione di appartenenza non si considerano "molteplicità". Gli insiemi $\{4, 6, 8\}$ e $\{4, 4, 6, 6, 8, 8, 8\}$ vanno considerati come lo stesso insieme[5].

D'ora in poi le lettere romane corsive minuscole $a, b, \ldots, x, y \ldots$ (e talvolta anche maiuscole $A, B, \ldots$) indicheranno sempre insiemi, anche senza che questo venga dichiarato esplicitamente.

1.1.2. *Sottoinsiemi.* Se tutti gli elementi di un certo insieme x appartengono ad un altro insieme y, si dice che x è un *sottoinsieme* di y, oppure che x è *contenuto* in y, o anche che y *contiene* x, e si scrive $x \subseteq y$. In altre parole, $x \subseteq y$ significa che, per ogni z, si ha che $z \in x$ implica $z \in y$.

Osserviamo che la nozione di appartenenza $\in$ e quella di essere sottoinsieme $\subseteq$ sono ben distinte fra di loro. Per esempio, per ogni insieme x, è vero che $x \subseteq x$. Invece non sempre[6] è vero che $x \in x$. Ad esempio, se $\emptyset$ indica l'insieme che non ha elementi, sicuramente $\emptyset \notin \emptyset$. È perciò curioso notare che la maggior parte degli autori che hanno usato la teoria degli insiemi all'inizio sembra confondessero (per lo meno a livello di notazione) i due concetti. La distinzione esplicita fra le due nozioni sembra dovuta a Giuseppe Peano.

Se $x \subseteq y$ e $x \neq y$, si dice che x è un *sottoinsieme proprio* di x, e si scrive $x \subset y$, oppure $x \subsetneq y$. Osserviamo che, per ragioni tipografiche, molti testi, specie in passato, usavano $x \subset y$ col significato che abbiamo attribuito qui a $x \subseteq y$. Ribadiamo che, per quanto riguarda convenzioni, notazioni e definizioni, è sempre opportuno fare riferimento al testo che si sta utilizzando, leggendo con attenzione le parti introduttive.

In particolare, $x = y$ vale se e solo se valgono sia $x \subseteq y$ e $y \subseteq x$.

---

come "non perfettamente chiara" la definizione di tale insieme, perchè non si è in grado di conoscere con esattezza quali numeri non vi appartengono (e, comunque, il problema si presenterebbe per il suo complementare). Questo è il motivo per cui abbiamo precisato "in linea di principio". Problemi di questo tipo non si presenteranno nella teoria assiomatica, dove si precisa in ogni dettaglio quali sono gli insiemi di cui si assume l'esistenza. Resta il fatto che nella teoria assiomatica usuale è richiesta l'esistenza di insiemi di natura molto astratta che qualcuno potrebbe non ritenere corrispondente alla nozione intuitiva appena descritta.

[5] Esiste la nozione di "multiinsieme", in cui si tiene conto di eventuali molteplicità. I multiinsiemi sono talvolta utili, particolarmente nella combinatoria finita. Sembra comunque più comodo definire i multiinsiemi in termini di insiemi, anziché viceversa. In questo senso, un multiinsieme può essere definito formalmente come una coppia (X, m) dove m è una funzione da X in $\mathbb{N}$, o eventualmente in un insieme di cardinali, se si ammettono molteplicità infinite.

[6] In effetti, solitamente si assume addirittura che $x \in x$ non valga mai. Esistono comunque teorie "alternative" degli insiemi in cui è ammessa la possibilità di insiemi che appartengono a se stessi.

1.1.3. *Variabili e costanti*.* È importante notare che le lettere x e t nelle condizioni (b) e (c) precedenti sono da considerare come *variabili*, nel senso che possono essere sostituite da altre lettere senza modificare la definizione[7].

Per esempio, la definizione data in (b) sarebbe completamente equivalente se scritta nella forma $\{y \in \mathbb{N} \mid y$ è un numero naturale pari e $3 \leq y \leq 9\}$. Concettualmente, questa osservazione non dovrebbe comportare particolari difficoltà. Per fare il paragone con una situazione più elementare, risolvere l'equazione $x^3 - 1$ (nella variabile x) equivale a risolvere l'equazione $y^3 - 1$ (nella variabile y). Del resto (come succede anche nel caso della risoluzione di equazioni quando compaiono parametri!) a volte solo dal contesto si è in grado di capire quali sono le variabili e quali sono le costanti. Ad esempio, si consideri la seguente frase:

Sia r un numero reale fissato e sia $X = \{nr \mid n \in \mathbb{N}\}$ ...

Nella definizione di X la variabile è n, e r va considerato come una costante, o un parametro. Una descrizione più concreta di X potrebbe essere $X = \{0, r, 2r, 3r, \dots\}$.

Secondo la convenzione più comune in matematica (ma talvolta vi sono eccezioni) si ammette che variabili distinte possano assumere lo stesso valore, per esempio $2 \in \{n^2 + m^2 \mid n, m \in \mathbb{N}\}$, perché posso considerare $m = n = 1$.

1.1.4. *Operazioni fra insiemi.* Possono essere definite in maniera naturale molte operazioni fra insiemi. Per esempio, l'*intersezione* $x \cap y$ di due insiemi x e y è l'insieme z che ha per elementi esattamente gli oggetti che sono elementi sia di x che di y. In altre parole, z è il più grande insieme contenuto sia in x che in y.

In maniera simile, l'*unione* $x \cup y$ di due insiemi x e y è l'insieme z che ha per elementi esattamente gli oggetti che sono elementi di almeno uno fra x che di y (è compreso il caso in cui un elemento stia contemporaneamente in x e y). Stavolta, z è il più piccolo insieme che contiene sia x che y.

Il *complemento di y in x* è l'insieme $x \setminus y = \{z \in x \mid z \notin y\}$. Come accennato in precedenza, è ammesso come insieme l'insieme che non ha elementi; esso viene chiamato *insieme vuoto* e indicato con $\emptyset$. Per il principio di estensionalità tutti gli insiemi senza elementi sono uguali o, più brevemente, l'insieme vuoto è unico. Questo giustifica l'uso dell'articolo determinativo quando diciamo *l'insieme* vuoto. Sempre per il principio di estensionalità, tutti gli insiemi che abbiamo introdotto poco sopra sono definiti univocamente, e questo giustifica l'introduzione della notazione che li indica. Notiamo che $x \setminus x = \emptyset$, per ogni insieme x.

---

[7] Avendo naturalmente l'accortezza di non utilizzare lettere già utilizzate in precedenza, cioè di non sovrapporre le notazioni. Ad esempio, posso sostituire n con m nella condizione (c′) precedente, ottenendo $\{m \in \mathbb{N} \mid$ esiste un $t \in \mathbb{N}$ tale che $t = 2m$ e $1 < t < 5\}$. Ma se invece sostituissi n con t, otterrei $\{t \in \mathbb{N} \mid$ esiste un $t \in \mathbb{N}$ tale che $t = 2t$ e $1 < t < 5\}$, definizione di dubbia comprensibilità, e che fornisce l'insieme che non ha nessun elemento, visto che non esiste nessun t tale che contemporaneamente $t = 2t$ e $1 < t < 5$. In alcune delle definizioni che seguono daremo per scontato che non si verificano situazioni come quella appena descritta. In senso strettamente formale, a volte andrebbe precisata una condizione in cui si dichiara che una certa variabile va scelta fra variabili non ancora utilizzate.

Gli insiemi possono contenere altri insiemi come oggetti. In effetti, tutti gli insiemi che considereremo avranno come loro elementi esclusivamente altri insiemi[8].

Per esempio, il *singoletto* $\{x\}$ è l'insieme che ha x come unico elemento. Cioè, per qualunque z, si ha $z \in \{x\}$ se e solo se $z = x$.

La *coppia (non ordinata)* $\{x, y\}$ è l'insieme che ha come unici elementi x e y. Osserviamo che, per il principio di estensionalità, $\{x, y\} = \{y, x\}$. Inoltre, $\{x, x\} = \{x\}$.

È spesso utile considerare una *coppia ordinata* (x, y) di due insiemi x e y. Si richiede che questa nozione di coppia ordinata soddisfi alla seguente proprietà:

(C) dati x, y, x_1, y_1 qualunque, si ha che $(x, y) = (x_1, y_1)$ vale se e solo se valgono contemporaneamente $x = x_1$ e $y = y_1$.

Naturalmente, si potrebbe pensare di introdurre una nuova nozione di "insieme ordinato". Questo non è però necessario: la nozione di coppia ordinata si può comunque introdurre senza "moltiplicare le entità"; una possibile definizione è $(x, y) = \{\{x\}, \{x, y\}\}$. Lasciamo al lettore il compito di verificare che la coppia ordinata definita come sopra[9] soddisfa effettivamente alla proprietà (C). Suggerimento: trattare separatamente i casi $x \neq y$ e $x = y$.

---

[8] Si può sviluppare tutta o praticamente tutta la matematica utilizzando solo gli insiemi, cioè codificando sotto forma di insiemi tutti gli oggetti matematici di cui si ha necessità. O, se si preferisce, costruendo una copia "isomorfa" all'interno della teoria degli insiemi di ciascuna struttura matematica di cui si ha necessità. Ad esempio, vedremo in seguito un metodo per introdurre i numeri naturali sotto forma di insiemi. Da un lato questo modo di trattare gli oggetti matematici può apparire artificioso; d'altro canto ha il vantaggio concettuale di "non moltiplicare le entità". In ogni caso, è stato fatto notare che è tipico della matematica studiare i propri oggetti indipendentemente dal modo in cui vengono presentati o costruiti, cioè basandosi solo sulle relazioni che si suppone valgano fra di loro. Quindi il problema di stabilire se gli (altri) oggetti matematici vadano effettivamente considerati insiemi oppure no è sicuramente un problema di scarso interesse matematico.

Questo aspetto non è comunque fondamentale per la teoria degli insiemi. Si possono dividere gli oggetti di cui si tratta in due categorie, gli insiemi veri e propri e gli altri "oggetti" che non sono insiemi (spesso chiamati "urelementi", dal tedesco). Solo gli insiemi possono avere elementi, e questi elementi possono essere sia altri insiemi sia "urelementi". Invece gli urelementi non possono avere elementi. Il principio di estensionalità si applica solo agli insiemi, e gli "urelementi" si distinguono fra di loro per aspetti che stanno al di fuori della teoria degli insiemi e si considerano noti in altro modo. Esistono pochi ambiti molto tecnici e specialistici in cui l'uso degli urelementi si rivela necessario. Noi non avremo la necessità di considerare urelementi.

[9] Naturalmente questa definizione di coppia ordinata può apparire artificiosa e poco naturale. Se, da un lato, si tratta comunque di una convenzione, è ovvio che invece lavorare con due nozioni distinte di insieme (non ordinato e ordinato) comporterebbe alla lunga complicazioni ben peggiori. L'unico fatto importante, comunque, è che la proprietà (C) è soddisfatta.

[**] In alcune situazioni particolari la definizione di coppia ordinata che abbiamo dato ha il difetto di utilizzare "troppe" parentesi graffe. Sapreste dire perchè la definizione alternativa $(x, y)^* = \{\{1\} \cup x, \{2\} \cup y\}$ non funziona? Comunque W. Quine è riuscito a modificare la definizione precedente $(x, y)^*$ in modo che la proprietà (C) sia effettivamente soddisfatta. Vedi Drake, Set Theory, Esercizio 10 in Capitolo 2, 3.11 oppure https://en.wikipedia.org/wiki/Ordered pair

Il *prodotto (cartesiano)* $A \times B$ di due insiemi A e B è l'insieme $\{(a, b) \mid a \in A, b \in B\}$ di tutte le coppie ordinate con primo elemento in A e secondo elemento in B. Una *relazione* R da A verso B è un sottoinsieme di $A \times B$. In questo modo si può definire la nozione di funzione e, in seguito, tutte[10] le nozioni usate in matematica, le cui definizioni (nei rari casi in cui avremo bisogno di usarle) supporremo generalmente note al lettore.

Un'altra costruzione fondamentale in matematica è quella dell'*insieme potenza*, o *insieme delle parti*. Se x è un insieme, il suo insieme potenza $\mathcal{P}(x)$ è l'insieme di tutti i sottoinsiemi di x. In altre parole, per un insieme qualunqe y, abbiamo $y \in \mathcal{P}(x)$ se e solo se $y \subseteq x$.

1.1.5. *Cardinalità.* Si dice che due insiemi X e Y hanno la stessa cardinalità, e si scrive $|X| = |Y|$, se esiste una funzione biiettiva da X su Y. Si dice che la cardinalità di X è minore o uguale alla cardinalità di Y, e si scrive $|X| \leq |Y|$, se esiste una funzione iniettiva da X in Y. La cardinalità di X è strettamente minore della cardinalità di Y, scritto $|X| < |Y|$ se esiste una funzione iniettiva da X in Y, ma non esiste una funzione biiettiva, cioè se $|X| \leq |Y|$ ma non $|X| = |Y|$.

Le notazioni precedenti sottintendono che si possa definire la nozione di cardinalità di un insieme. Nel caso degli insiemi finiti basta scegliere un insieme "tipico" con la cardinalità voluta, ad esempio, $n = \{0, 1, 2, \ldots, n-1\}$ per un insieme X con n elementi, e affermare che la cardinalità di X è n, scrivendo $|X| = n$. Nel caso degli insiemi infiniti, in una teoria formalizzata, scegliere un insieme rappresentativo per una data cardinalità può comportare problemi. Nella teoria intuitiva si può comunque assumere di poter effettuare una tale scelta e di usare il termine cardinalità e notazioni analoghe alle precedenti con questo significato. Altrimenti si può osservare che, in generale, la nozione di cardinalità compare quasi esclusivamente nel confrontare insiemi fra di loro. Quindi non c'è bisogno, a rigore, di assegnare ad un insieme una sua "cardinalità": basta semplicemente introdurre le nozioni di essere in corrispondenza biunivoca (equivalente ad "avere la stessa cardinalità", se è stata data una definizione di cardinalità), oppure essere in corrispondenza biunivoca con un sottoinsieme (equivalente ad "avere cardinalità minore o uguale").

Ad esempio, un classico teorema di Cantor viene frequentemente enunciato affermando che per ogni insieme x la sua potenza $\mathcal{P}(x)$ ha cardinalità strettamente maggiore di x, cioè $|x| < |\mathcal{P}(x)|$. Mentre l'enunciato precedente è sicuramente sintetico e intuitivamente chiaro, non c'è bisogo di utilizzare la nozione di cardinalità per enunciare il Teorema di Cantor nella forma seguente.

[10] o quasi, secondo l'opinione di alcuni. Rimandiamo il lettore interessato, ad esempio, all'interessante articolo (su sviluppi recenti del dibattito sui fondamenti della matematica) di P. Maddy, *Set-theoretic foundations* apparso in Andrés Eduardo Caicedo, James Cummings, Peter Koellner, Paul B. Larson (editors), *Foundations of Mathematics, Logic at Harvard, Essays in Honor of W. Hugh Woodin's 60th Birthday March 27–29, 2015, Harvard University, Cambridge, MA*, Contemporary Mathematics Volume 690, 2017. Può essere anche utile consultare gli ulteriori riferimenti bibliografici ivi indicati.

Teorema di Cantor. *Sia x un insieme qualunque. Allora non esiste una funzione iniettiva da $\mathcal{P}(x)$ ad x, mentre esiste una funzione iniettiva da x in $P(x)$.*

Dimostrazione. Fissiamo x. La funzione che manda a in $\{a\}$, per $a \in x$, è evidentemente iniettiva da x in $\mathcal{P}(x)$, dunque dimostra la seconda affermazione.

Per l'altra affermazione, dimostriamo prima che non esiste una funzione suriettiva da x in $\mathcal{P}(x)$. Se per assurdo esistesse una tale funzione, diciamo f, si consideri l'insieme $A = \{\, a \in x \mid a \notin f(a) \,\}$. Siccome f è suriettiva, esiste $a \in x$ tale che $f(a) = A$. Ma allora, per la definizione di A, abbiamo $a \in A$ se e solo se $a \notin f(a)$, cioè $a \notin A$, assurdo. [[NB: la somiglianza con il paradosso di Russell [...]]]

Per finire, se esistesse $g : \mathcal{P}(x) \to x$ iniettiva, possiamo ottenere $f : x \to \mathcal{P}(x)$ suriettiva ponendo

$$f(a) = \begin{cases} B & \text{se esiste } B \in \mathcal{P}(x) \text{ tale che } g(B) = a, \\ \emptyset & \text{altrimenti,} \end{cases}$$

una contraddizione, per il paragrafo precedente. Il B nella definizione precedente, se esiste, è unico poiché g si supponeva iniettiva, quindi f è effettivamente una funzione; e il vuoto nella seconda riga potrebbe essere sostituito da qualunque altro sottoinsieme di x. □

[[Teorema di Cantor Schröder-Bernstein [...]]]

1.1.6. *Uso degli insiemi come linguaggio e uso sostanziale*.* [...]

1.2. L'impostazione assiomatica. Le argomentazioni nella sottosezione precedente sono esclusivamente intuitive. Le argomentazioni matematiche, solitamente, richiedono invece una maggiore precisione, in particolare, si richiede di specificare esattamente tutte le ipotesi che vengono usate. Alcune assunzioni vengono prese come basi di partenza, e chiamate *assiomi*. A partire da queste assunzioni, mediante ragionamenti logici, si otterranno i teoremi e le altre conclusioni. I ragionamenti così effettuati dovrebbero risultare validi indipendentemente dalla concezione intuitiva degli oggetti trattati. Questo modo di procedere prende il nome di *metodo assiomatico*[11].

[11] Nella concezione moderna, gli assiomi non sono interpretati come verità assolute imposte in maniera dogmatica. A volte li si intende come verità intuitivamente evidenti riguardanti certi oggetti particolari, altre volte semplicemente come ipotesi di lavoro che possono o meno essere valide. Secondo questo modo di vedere, l'attività del matematico non fornirebbe verità assolute, presenterebbe solo ragionamenti del tipo: *ammettendo queste e queste ipotesi si ottengono queste e queste conclusioni.* Va da sè che in molti casi queste deduzioni sono tutt'altro che ovvie, sono di una complessità notevole e talvolta vengono giudicate di estrema bellezza o profondità. Ci premeva soltanto sottolineare che decidere sulla validità o meno delle ipotesi non viene considerato solitamente un problema di tipo matematico; il problema viene demandato ad altri, ad esempio, ai fisici (o, qualora non sia necessaria una soluzione immediata, ai filosofi).

Quasi tutte le branche della matematica sono state trattate in maniera assiomatica, anche nel caso in cui le nozioni usate non comportassero nessuna problematicità. Illustri matematici hanno invece spesso messo in dubbio la liceità dell'uso degli insiemi in matematica. Questa constatazione, unita ai problemi e paradossi a cui accenneremo in seguito, suggerisce che in questo caso esiste l'effettiva necessità di una trattazione assiomatica. È importante notare che la trattazione assiomatica non è assolutamente un mezzo per liberarsi dalle controversie o per garantire un tipo di validità assoluta ai metodi che fanno uso degli insiemi. Tutto il contrario! Semplicemente, se si deve discutere su quali metodi possono essere considerati validi o meno, meglio specificare con precisione ciò su cui si sta discutendo.

Grossomodo e a volte con particolari precisazioni, gli assiomi che indicheremo riguardo agli insiemi sono accettati dalla comunità dei matematici[12]. Siccome il nostro scopo è di presentare gli argomenti evitando quanto più possibile i dettagli tecnici, trascureremo alcuni assiomi senza descriverli in dettaglio. Questi assiomi sarebbero necessari per realizzare certi obiettivi particolari. Facciamo riferimento ai testi che verranno indicati in seguito per una trattazione più completa e rigorosa. Ci sentiamo corroborati in questa nostra scelta di privilegiare la semplicità alla completezza dal fatto che alcuni dei dettagli tecnici che sarebbero necessari sfuggirono, a suo tempo, anche a grandi personalità matematiche.

Naturalmente, se si richiedesse un rigore assoluto, si dovrebbero specificare esattamente anche quali sono i metodi di ragionamento da considerare validi. Questo può essere fatto, ma esula dall'argomento della presente nota. Rimandiamo il lettore interessato ad un qualunque testo di logica matematica, ad esempio il testo di Mendelson che citeremo nella sezione sulle altre letture. Allo stesso modo di quanto osserveremo riguardo agli assiomi, dichiarare esplicitamente i metodi logici che vengono utilizzati non implica necessariamente la loro validità. D'altro canto, fra la maggior parte dei matematici, risulta esserci un consenso implicito su quali siano i ragionamenti corretti. Noi accetteremo questa pratica senza ulteriori precisazioni, rimandando di nuovo il lettore al libro citato o ad altri testi dedicati esplicitamente ai fondamenti della matematica.

[12] Molte parti della matematica tradizionale possono essere sviluppate facendo uso di sistemi di assiomi molto più deboli di quello che presenteremo. Il campo di ricerca che si occupa di trovare le ipotesi minimali necessarie per dimostrare teoremi classici va sotto il nome di *reverse mathematics* e ha ottenuto risultati di particolare interesse, ad esempio l'identificazione di un piccolo numero di sistemi di assiomi che "misurano" esattamente la complessità delle ipotesi necessarie in un gran numero di casi. Si veda S. G. Simpson, *Subsystems of Second Order Arithmetic*, Second edition, 2009. È modesto parere di chi scrive che questo campo di ricerca è ingiustamente trascurato e non sta ricevendo tutta l'attenzione che meriterebbe. In fondo, è caratteristico della matematica cercare di dimostrare teoremi utilizzando ipotesi minimali.

Come argomento collegato, ma da una prospettiva diametralmente opposta, alcuni problemi matematici complessi non sono risolvibili nella teoria standard degli insiemi, e hanno soluzione solo assumendo ulteriori assiomi. Le tecniche che si occupano di questi argomenti sono estremamente sofisticate e includono, fra gli altri, il cosiddetto *forcing*, i *modelli interni*, i *grandi cardinali*, l'*ipotesi di determinatezza*. Il lettore interessato può approfondire l'argomento dapprima studiando il libro di Jech e, in seguito, l'*Handbook of Set Theory*, entrambi citati nella sezione sulle ulteriori letture.

1.2.1. *Nozioni primitive.* Oltre agli assiomi, è necessario precisare anche le nozioni di cui si tratta. Altre nozioni e concetti potranno essere introdotti mediante definizioni, ma le nozioni di partenza non possono essere definite, a meno di non cadere in un circolo vizioso. In teoria degli insiemi gli unici concetti di base sono quelli di *insieme* e di *appartenenza*. Per comodità utilizzeremo anche la nozione di uguaglianza, supponendo che per essa valgano le proprietà intuitive.

1.2.2. *Principio di estensionalità.* Come precisato sopra, due insiemi si considerano uguali se e solo se hanno esattamente gli stessi elementi. Il nostro primo assioma sarà dunque il seguente[13].

(Principio di Estensionalità) Due insiemi sono uguali se e solo se hanno esattamente gli stessi elementi.

Intuitivamente il Principio di estensionalità fornisce una "definizione" di insieme, corrispondente alla nozione informale introdotta nella precedente sottosezione. Va comunque considerato come un assioma vero e proprio. Ovviamente, il Principio di estensionalità non può essere usato per dimostrare l'esistenza di insiemi. È quindi necessario introdurre ulteriori assiomi.

1.2.3. *Assiomi per la costruzione di insiemi.*

(Assioma della Coppia) Dati due insiemi qualunque x e y, esiste un insieme $\{x, y\}$ che ha per elementi esattamente[14] x e y.

L'assioma della coppia si può esprimere in linguaggio simbolico come

$\forall xy \exists z \forall w (w \in z \Leftrightarrow (w = x \vee w = y))$,

dove $\vee$ significa "oppure" (in senso inclusivo, ovvero nel senso che può verificarsi una o l'altra possibilità, e possono anche verificarsi entrambe contemporaneamente). Lasciamo per esercizio al lettore di verificare che tutti gli assiomi che enunceremo si possono scrivere in un linguaggio simbolico come sopra. Mentre cercheremo di essere il meno formali possibile, la necessità di un simile trattamento formale apparirà chiara quando enunceremo l'assioma di separazione più sotto.

Per il principio di estensionalità, data una qualunque coppia di insiemi x e y, l'insieme la cui esistenza è stabilita dall'assioma della coppia è unico, e quindi può essere effettivamente indicato[15] con $\{x, y\}$. D'ora in poi quando un

[13] ** (Le note a pie' di pagina contrassegnate da due asterischi non sono strettamente necessarie per la comprensione del testo e possono essere "saltate" da chi lo desidera, oppure in una prima lettura. Contengono osservazioni e precisazioni che ci sarebbe sembrato improprio omettere.)

Se, come stiamo facendo, si assume la nozione di uguaglianza come primitiva. In caso contrario, il principio, come stiamo per introdurlo, risulta una definizione. In tal caso è necessario richiedere poi un assioma che dice che due insiemi uguali, nel modo così definito, soddisfano alle stesse proprietà. Preciseremo in seguito cosa debba intendersi per "proprietà". Il lettore che risultasse perplesso da questo commento non si preoccupi: a volte anche studiosi esperti nel settore confondono i due approcci.

[14] ** Utilizzando l'assioma di separazione, che enunceremo in seguito, è sufficiente richiedere la seguente forma più debole dell'assioma della coppia: *Dati due insiemi qualunque x e y, esiste almeno un insieme u tale che $x \in u$ e $y \in u$.*

[15] La possibilità di introdurre nuovi simboli per oggetti di cui si dimostrano esistenza ed unicità può apparire lecita al di là di ogni possibile ombra di dubbio e non suscettibile

assioma implica l'esistenza di un insieme definito univocamente per estensionalità, daremo direttamente un nome a quest'insieme senza ulteriori precisazioni. Va comunque notato che è necessario fare uso dell'assioma di estensionalità, affinché ciò sia giustificato.

Nell'enunciato dell'assioma della coppia è possibile avere $x = y$; in questo caso si otterrà il singoletto $\{x\}$. In particolare, la coppia ordinata $(x, y) = \{\{x\}, \{x, y\}\}$ si può costruire iterando l'assioma della coppia.

Enunceremo adesso l'assioma dell'unione. Questo assioma ci permette di costruire l'unione $x \cup y$ due insiemi qualunque x e y. Come già precisato $x \cup y$ ha per elementi esattamente tutti gli insiemi che sono elementi di x oppure sono elementi di y (oppure di entrambi). Più in generale, data una famiglia di insiemi $\{A_i \mid i \in I\}$, l'assioma ci permette di costruire un insieme $\bigcup_{i\in I} A_i$ tale che, per ogni insieme z, si ha che $z \in \bigcup_{i\in I} A_i$ se e solo se esiste $i \in I$ tale che $z \in A_i$.

Qui l'espressione *famiglia* è sinonimo di insieme, ed è usata solo per evitare ripetizioni. La presentazione appena fornita dell'assioma dell'unione ci sembra intuitivamente chiara, ma dovremmo dare un significato preciso all'espressione $\{A_i \mid i \in I\}$. In seguito questo significato verrà reso esplicito, ma va notato che non sempre abbiamo la possibilità di dimostrare l'esistenza di "famiglie" del tipo $\{A_i \mid i \in I\}$, in base ai soli assiomi che abbiamo introdotto finora. In ogni caso, per enunciare la versione rigorosa e "ufficiale" dell'assioma dell'unione non c'è la necessità di considerare famiglie "indicizzate", quindi, formalmente, l'eventuale indicizzazione risulta una complicazione anziché una

---

di creare problemi logici. Effettivamente l'introduzione di nuovi simboli è lecita in questa situazione, ma ad un esame più approfondito la questione risulta parecchio delicata.

Una prima possibilità è quella di considerare i nuovi simboli introdotti come abbreviazioni. Ad esempio, tutte le volte che si usa l'espressione $\{x, y\}$ all'interno di un'altra espressione, si suppone che $\{x, y\}$ vada sostituita utilizzando la sua effettiva definizione. Ad esempio, la formula $\{x, y\} \in h$ può essere considerata come un'abbreviazione della formula più complessa $\exists z(\forall w(w \in z \Leftrightarrow (w = x \vee w = y)) \wedge z \in h)$. In questo modo non si introduce nessun nuovo assioma, e i nuovi simboli introdotti sono intesi semplicemente come abbreviazioni utili per migliorare la leggibilità delle formule.

Un approccio più complesso, ma in un certo senso più elegante è quello di introdurre un nuovo assioma per ogni oggetto di cui si dimostrano esistenza ed unicità. A titolo di esempio, l'assioma che descrive il significato che attribuiamo ad $\{x, y\}$ è $\forall w(w \in \{x, y\} \Leftrightarrow (w = x \vee w = y))$. Questo metodo moltiplica il numero dei concetti e degli assiomi usati. Ma la complessità aggiunta è solo apparente. Si può dimostrare che introdurre un nome per ogni oggetto di cui è dimostrabile l'esistenza e l'unicità, insieme ad assiomi che ne caratterizzano le proprietà, produce una *estensione conservativa* della teoria precedente all'introduzione di questi nuovi simboli ed assiomi. Ciò significa che se un enunciato utilizza *solo* il linguaggio della teoria precedente (quella senza i simboli e gli assiomi aggiuntivi), questo enunciato è dimostrabile nella teoria precedente se e solo se è dimostrabile nella teoria "nuova" (quella con i nuovi simboli e i nuovi assiomi). In altre parole, *se ci si limita agli enunciati che non fanno uso esplicito dei nuovi simboli*, in questo caso, ad esempio, del simbolo $\{x, y\}$, si ottengono esattamente gli stessi teoremi. In altri termini ancora, l'aggiunta di questi nuovi simboli ed assiomi può essere considerata inessenziale. Vedi ad esempio la Proposizione 2.29 nel libro di Mendelson.

In qualunque modo si consideri la questione, gli argomenti precedenti ci autorizzano ad introdurre nuovi simboli, cosa che faremo per semplificare la leggibilità

semplificazione. Tuttavia, forse, il seguente enunciato dell'assioma può apparire meno intuitivo. L'insieme $\mathcal{F}$ considerato nell'assioma seguente va comunque pensato come una famiglia di insiemi.

(Assioma dell'Unione) Dato un qualunque insieme $\mathcal{F}$, esiste l'insieme $\bigcup\mathcal{F} = \{z \mid \text{esiste } h \in \mathcal{F} \text{ tale che } z \in h\}$.

Cioè, per ogni z, $z \in \bigcup\mathcal{F}$ se e solo se esiste $h \in \mathcal{F}$ tale che $z \in h$.

Osserviamo che non è scontato che la forma finita dell'assioma dell'unione segue dalla forma generale. Dobbiamo usare l'assioma della coppia per costruire $\{x, y\}$. Dopodiché $x \cup y = \bigcup\{x, y\}$.

Usando gli assiomi della coppia e dell'unione[16] possiamo costruire terne $\{x, y, z\}$ come $\{x, y\}\cup\{z\}$, e così via. È invece curioso osservare che non abbiamo bisogno dell'assioma dell'unione per costruire le *terne ordinate*, mediante la definizione $(x, y, z) = ((x, y), z)$.

(Assioma dell'insieme Potenza (o delle Parti)) Dato un insieme qualunque x, esiste l'insieme $\mathcal{P}(x)$ che ha per elementi esattamente tutti i sottoinsiemi di x.

Usando gli assiomi introdotti finora, si può tentare di costruire il prodotto cartesiano $A \times B$ di due insiemi A e B. Se $a \in A$ e $b \in B$, per l'assioma della coppia esistono il singoletto $\{a\}$ e la coppia $\{a, b\}$. Applicando di nuovo l'assioma della coppia con $x = \{a\}$ e $y = \{a, b\}$, abbiamo la coppia ordinata $(a, b) = \{\{a\}, \{a, b\}\}$. Inoltre, siccome $a \in A$, abbiamo $\{a\} \subseteq A$ e, quindi, $\{a\} \in \mathcal{P}(A)$. Siccome $a, b \in A \cup B$, abbiamo anche $\{a, b\} \subseteq A \cup B$ e $\{a, b\} \in \mathcal{P}(A \cup B)$. Siccome $A \subseteq A \cup B$, abbiamo inoltre $\mathcal{P}(A) \subseteq \mathcal{P}(A \cup B)$ (perché ogni sottoinsieme di A è anche sottoinsieme di $A \cup B$). In conclusione, sia $\{a\}$ che $\{a, b\}$ appartengono a $\mathcal{P}(A \cup B)$, quindi $\{\{a\}, \{a, b\}\} \subseteq \mathcal{P}(A \cup B)$, da cui segue $(a, b) = \{\{a\}, \{a, b\}\} \in \mathcal{PP}(A\cup B)$. Quindi abbiamo che, se $A\times B$ esiste, $A \times B \subseteq \mathcal{PP}(A \cup B)$. Ma, naturalmente, $A \times B \neq \mathcal{PP}(A \cup B)$. Per poter costruire $A\times B$ abbiamo quindi bisogno di un assioma che, dato un insieme W, ci autorizzi a costruire il sottoinsieme di W costituito da tutti gli elementi di W che soddisfano ad una certa proprietà. Costruzioni di questo tipo vengono effettuate in continuazione in matematica, lo studente avrà ascoltato numerose volte frasi del tipo "Sia X l'insieme di tutti i numeri reali tali che ..." e simili, dove al posto dei puntini possono apparire svariate espressioni di vario tipo, a volte anche estremamente complesse. L'assioma che ci serve è dunque il seguente.

(Assioma di Separazione) Per ogni insieme W e ogni "proprietà" φ, esiste l'insieme[17] $\{x \in W \mid \varphi(x)\}$, cioè l'insieme costituito da tutti gli elementi di W per cui vale la proprietà φ.

---

16 ** Va comunque precisato che l'assioma della coppia e più in generale l'esistenza delle n-uple sono una conseguenza degli altri assiomi, quando si consideri la teoria completa.

17 Anche in questo caso, se tale insieme esiste, è unico per estensionalità, quindi siamo autoirizzati ad usare una scrittura simbolica per denotarlo.

Formalmente, l'assioma di separazione viene considerato non come un singolo assioma, ma come un'infinità di assiomi, uno per ogni "proprietà" φ. Questo si esprime solitamente dicendo che si tratta di uno *schema* di assiomi.

Più sostanziale è la richiesta di definire esattamente cosa si intenda per "proprietà". Sebbene esistano possibilità alternative, per *proprietà* si intende solitamente (una proprietà definita da) un'espressione simbolica[18] che può essere costruita in maniera naturale utilizzando i simboli[19] [20] $\in$ e $=$, i connettivi logici $\wedge$ (e), $\vee$ (o), $\neg$ (non), $\Rightarrow$ (implica), variabili $x_1, x_2, \ldots$ e i quantificatori $\forall$ (per ogni) e $\exists$ (esiste). Il lettore che fosse a conoscenza dei primi rudimenti di logica simbolica riconoscerà sicuramente che le "proprietà" appena introdotte corrispondono esattamente alle formule del calcolo dei predicati del primo ordine nel linguaggio con due relazioni binarie $\in$ e $=$.

Tornando all'esempio precedente, cioè al tentativo di costruire $A \times B$, gli assiomi della coppia, dell'unione e della potenza ci consentono di costruire $\mathcal{PP}(A \cup B)$. Esiste una formula φ che esprime l'affermazione "x è una coppia ordinata con primo elemento in A e secondo elemento in B". Dunque l'assioma di separazione ci consente di costruire l'insieme $\{x \in \mathcal{PP}(A \cup B) \mid$ x è una coppia ordinata con primo elemento in A e secondo elemento in B$\}$. Per quanto detto sopra, questo insieme è proprio $A \times B$.

---

[18] È abbastanza intuitivo capire quali sono le regole di costruzione per le possibili "formule" φ ammesse nello schema di assiomi di separazione. Per il lettore che richiedesse i dettagli formali, la definizione è data dalle seguenti clausole.

(1) Se x e y sono variabili, allora sia $x \in y$ che $x = y$ sono formule.

(2) Se φ e ψ sono formule e x è una variabile, allora tutte le seguenti sono formule: $\varphi \wedge \psi$, $\varphi \vee \psi$, $\neg\varphi$, $\varphi \Rightarrow \psi$, $\forall x\varphi$ e $\exists x\varphi$.

(3) Sono formule tutte e sole le espressioni simboliche che possono essere ottenute in un numero finito di passi applicando (1) e (2).

Alcune condizioni sono pleonastiche, nel senso che, ad esempio, alcuni connettivi o quantificatori possono essere definiti in termini di altri. A volte è necessario inserire opportune parentesi nella costruzione delle formule come sopra, affinché esse risultino di interpretazione non ambigua. I dettagli sono intuitivamente ovvi.

Inoltre si assume la possibilità che φ dipenda da altri parametri, non solo da x. L'assioma garantisce l'esistenza dell'insieme $\{x \in W \mid \varphi(x)\}$ per ogni valore che può assumere ogni eventuale parametro (facendo uso degli altri assiomi, ci si può comunque ridurre equivalentemente al caso di un solo parametro).

[19] Come precisato in precedenza, all'atto pratico si possono usare ulteriori simboli in φ, purchè le formule che contengono questi simboli siano interpretabili come un'abbreviazione di un'altra formula che non contiene i nuovi simboli.

Sarebbe anche molto importante osservare che qui stiamo identificando i simboli con la loro interpretazione. Le due nozioni sono in realtà ben distinte.

[20] Quando scriviamo $A \in x$ intendiamo che la relazione $\in$ vale realmente per certi insiemi A ed x. Invece, quando parliamo della *formula* $x \in y$, allora $\in$ va inteso come un simbolo grafico. Allo stesso modo, nella *formula* $x \in y$ le lettere x e y sono semplici simboli che si pensano possibilmente interpretabili come insiemi, ma, in questo caso, non vanno considerate *esse stesse* insiemi. Il lettore che decidesse di dedicarsi allo studio della logica matematica, in particolare della teoria dei modelli, sarebbe costretto molto presto a rendersi conto dell'importanza di questa distinzione, che a prima vista potrebbe apparire dovuta esclusivamente a pignoleria.

1.2.4. *Insiemi ereditariamente finiti.* Gli assiomi presentati finora ci garantiscono la possibilità di costruire certi insiemi a partire da uno o più insiemi dati, ma finora non abbiamo nulla che ci dimostri l'esistenza di almeno un insieme[21]. Se si assume l'esistenza di almeno un insieme W, l'assioma di separazione ci fornisce il vuoto, dato da $\{x \in W \mid x \neq x\}$. Usando poi l'assioma della coppia possiamo costruire altri insiemi come $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}\}$ ecc.

Gli insiemi che si possono costruire con gli assiomi presentati finora si dicono ereditariamente finiti. Vediamo più in dettaglio quali sono questi insiemi.

Per ogni numero naturale definiamo
$V_0 = \emptyset$,
$V_{n+1} = \mathcal{P}(V_n)$.

Questi insiemi esistono per l'assioma dell'insieme potenza, ma potrebbero essere costruiti anche come sopra usando ripetutamente gli assiomi della coppia e dell'unione. Ad esempio,
$V_1 = \mathcal{P}(V_0) = \mathcal{P}(\emptyset) = \{\emptyset\}$,
$V_2 = \mathcal{P}(V_1) = \{\emptyset, \{\emptyset\}\}$,
$V_3 = \mathcal{P}(V_2) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$,
...

Se potessimo costruire l'insieme $\mathcal{F} = \{V_0, V_1, V_2, \dots\}$, allora potremmo anche costruire $V_\omega = \bigcup \mathcal{F} = \bigcup_{n\in\mathbb{N}} V_n$ (sia chiaro che per ora non abbiamo ancora dato un significato preciso a quest'ultima espressione!). Assiomi che permettono di costruire V_ω verranno forniti in seguito, per ora cerchiamo di descriverlo intuitivamente.

Per induzione, ogni V_n ha un numero finito (in genere molto grande) di elementi, infatti $|V_{n+1}| = 2^{|\mathcal{P}(V_n)|}$, quindi le cardinalità sono 0, $2^0 = 1$, 2, 2^2, 2^{2^2}, $2^{2^{2^2}}$ ... In ogni caso, tutti i V_n sono finiti. Inoltre, un elemento x di V_{n+1} è un sottoinsieme di V_n, quindi x è finito. Ogni elemento di x è finito, e così via. Ogni elemento di V_ω sta in almeno un V_n, quindi gli elementi di V_ω sono finiti, ogni loro elemento è finito, ogni elemento di ogni loro elemento è finito, e così via. Gli insiemi di questo tipo vengono detti *ereditariamente finiti*. Più in dettaglio, e ancora abbastanza informalmente, un insieme x si dice ereditariamente finito se x è finito e inoltre, per ogni numero naturale $i > 0$, ogni volta che $x_1 \in x_2 \in x_3 \in \cdots \in x_i \in x$, allora x_1 è un insieme finito[22]. Viceversa, anche se per ora non lo possiamo giustificare rigorosamente, ogni insieme ereditariamente finito sta in almeno un V_n, quindi V_ω è l'insieme degli insiemi ereditariamente finiti.

Per chi conoscesse un minimo di teoria dei modelli, possiamo considerare V_ω come un modello, dove il simbolo di appartenenza viene interpretato dalla

---

[21] **Nella maggior parte dei sistemi logici, per esempio il calcolo dei predicati del primo ordine, nel quale implicitamente stiamo lavorando, è comunque un teorema l'esistenza di almeno un oggetto.

[22] Qui $x_1 \in x_2 \in x_3 \in \cdots \in x_i \in x$ è un'abbreviazione per $x_1 \in x_2$ e $x_2 \in x_3$ ... e $x_i \in x$. Naturalmente, siccome i è un naturale qualunque, se x è ereditariamente finito, allora anche x_2, x_3, ..., x_i sono finiti.

relazione stessa di appartenenza [23] in V_ω (questa interpretazione si usa molto spesso in teoria degli insiemi, e modelli di questo tipo vengono chiamati *modelli standard*.)

Non è difficile vedere che con questa interpretazione V_ω è un modello di tutti gli assiomi introdotti finora. Innanzitutto, osserviamo per induzione che, per ogni n, se $x \in V_n$, allora $x \subseteq V_n$. Questo è ovvio per $n = 0$. Se è stato dimostrato per n e $x \in V_{n+1}$, allora $x \subseteq V_n$, per la definizione di V_{n+1}, quindi, per l'ipotesi induttiva, ogni elemento di x è sottoinsieme di V_n, quindi ogni elemento di x appartiene a V_{n+1} ma allora $x \subseteq V_{n+1}$.

In particolare, otteniamo $V_n \subseteq V_{n+1}$, per ogni n, quindi anche $V_n \subseteq V_m$, se $n \leq m$.

Dimostriamo adesso che l'assioma della coppia vale in V_ω pensato come modello. Se $x, y \in V_\omega$, allora per qualche n abbiamo $x, y \in V_n$, siccome i V_n sono contenuti uno nell'altro, ma allora $\{x, y\} \subseteq V_n$, cioè $\{x, y\} \in V_{n+1}$, quindi $\{x, y\} \in V_\omega$.

Vediamo adesso l'assioma dell'insieme potenza. Sia $x \in V_n$. Vogliamo dimostrare che $\mathcal{P}(x) \in V_{n+1}$. Questo è banale se $n = 0$. Se $n > 0$, allora $x \subseteq V_{n-1}$, cioè $\mathcal{P}(x) \subseteq \mathcal{P}(V_{n-1}) = V_n$. Quindi $\mathcal{P}(x) \in V_{n+1}$.

Gli altri assiomi si dimostrano in maniera simile.

Siccome V_ω è modello di tutti gli assiomi introdotti finora e V_ω non contiene insiemi infiniti, abbiamo che l'esistenza di un insieme infinito (in qualunque modo venga formalizzata) non segue dagli assiomi precedenti. [24] [25]

---

[23] O, meglio, dalla sua restrixione. Naturalmente, stiamo facendo ora un discorso relativamente informale. Si può pensare di lavorare in una metateoria sufficientemente potente e tale che si possa esprimere la nozione di modello. Oppure si può introdurre una nozione di soddisfacibilità parziale all'interno della teoria degli insiemi stessa (la nostra teoria oggetto). Questo è tecnicamente abbastanza complesso. Una nozione di soddisfacibilità totale non si può introdurre per il Teorama di Tarski, vedi 3.1.

Quello che è importante è osservare che le notazioni che abbiamo introdotto giustificano l'introduzione di nomi per certi oggetti, ad esempio, l'insieme vuoto $\emptyset$, le coppie non ordinate, etc., ma questi nomi non necessariamente vengono "interpretati" allo stesso modo in tutti i modelli.

Per semplificare, facciamo un esempio in una teoria più semplice rispetto alla teoria degli insiemi. Sia T la teoria di un ordine totale con minimo. Siccome in ogni modello di T un minimo esiste ed è unico, possiamo indicarlo, ad esempio, con m. Per esempio, nell'intervallo $[0, 2]$ di numeri reali, il minimo è 0, cio è possiamo scrivere $m = 0$. Ma $[1, 2]$ è anch'esso un insieme ordinato con minimo, e la relazione di ordine in $[1, 2]$ è proprio la restrizione della relazione d'ordine in $[0, 2]$. Ma, nel modello $[1, 2]$, il minimo è 1, non 0, cio è abbiamo $m = 1$. Allo stesso modo, in teoria degli insiemi, alcuni nomi potrebbero essere interpretati in maniera diversa in alcuni sottomodelli. Vedi anche la nota successiva. [...]

[24] per ora, questo è un argomento intuitivo, non del tutto rigoroso! [...] In particolare, ad esempio, (dati due nomi x e y) l'espressione $\{x, y\}$ è il nome di un oggetto in un certo modello. Ma, quando si confrontano due o più modelli, non è a priori scontato che $\{x, y\}$ venga interpretato esattamente dallo stesso oggetto in tutti i modelli. Nel caso che abbiamo considerato l'intuizione combacia con quello che si può dimostrare rigorosamente. In altri casi l'intuizione potrebbe suggerire risultati errati.

[25] L'insieme V_ω è numerabile e W. Ackermann, tramite un'opportuna biiezione, ha codificato la relazione di appartenenza in V_ω all'interno dell'insieme dei numeri naturali. In altre parole, se si volessero considerare solo gli insiemi ereditariamente finiti, a prescindere

1.2.5. *L'assioma dell'infinito.* Come precisato sopra, è necessario richiedere l'esistenza di almeno un insieme. Anziché richiedere l'esistenza di un insieme qualunque, richiederemo l'esistenza di un insieme che soddisfi ad una particolare proprietà.

(Assioma dell'Infinito) (versione informale) Esiste un insieme infinito.

Forse la definizione di "infinito" può sembrare ovvia. In realtà non è affatto così; addirittura, esistono diverse definizioni di "infinito" che non sono equivalenti, se non sotto certe assunzioni, anche se ciascuna cattura alcune proprietà che intuitivamente caratterizzano le collezioni infinite.

Per esprimere con precisione l'assioma dell'infinito, chiederemo l'esistenza di un insieme che contiene tutti i numeri naturali. Detto in questo modo si tratta di un circolo vizioso, poiché, insiemisticamente, un numero naturale è esattamente un elemento di $\mathbb{N}$. Ma è proprio $\mathbb{N}$ che vogliamo definire! All'inconveniente si può ovviare nel modo che stiamo per spiegare, ma prima descriviamo informalmente i numeri naturali. I primi numeri naturali si definiscono (o si interpretano, se si preferisce) nel seguente modo:

$0 = \emptyset$,
$1 = 0 \cup \{0\} = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\}$,
$2 = 1 \cup \{1\} = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$,
$3 = 2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{0, 1, 2\}$, e così via.

Potremmo pensare di iterare queste definizioni al seguente modo:

$$\begin{aligned} 0 &= \emptyset, \\ s(n) = n + 1 &= n \cup \{n\}, \quad \text{per ogni naturale } n, \end{aligned} \tag{*}$$

ma questa definizione "ricorsiva" è lecita solo se ammettiamo già di conoscere i numeri naturali[26]. La conoscenza dei numeri naturali non è affatto una richiesta forte, ma preferiamo comunque che la teoria che presentiamo sia completamente autosufficiente[27]. Osserviamo che, in base alle definizioni precedenti, abbiamo (intuitivamente) che un numero naturale è l'insieme di tutti i suoi predecessori, e che il numero n ha esattamente n elementi.

---

da problemi di convenzioni, notazioni e, a volte, di complessità di calcolo, non ci sarebbe nessuna differenza rispetto allo studio dei numeri naturali.

[26] ** L'uso della struttura di tutti i numeri naturali è implicito nell'espressione "e così via". Beninteso, possiamo iterare le definizioni date in precedenza un numero finito di volte, cioè possiamo definire un qualunque numero naturale, grande quanto si vuole. Quello che non possiamo ancora fare è considerare la definizione precedente come una definizione che comprende contemporaneamente *tutti* i numeri naturali.

[27] In effetti, anche la definizione di formula, in una nota precedente relativa all'assioma di separazione, è implicitamente data per induzione, quindi comporta la conoscenza di alcune proprietà dei numeri naturali. Il punto sostanziale è che si tratta di due livelli differenti, la nozione di formula è *metamatematica*, ed è praticamente impossibile sviluppare la metamatematica in maniera significativa senza dare per note alcune nozioni e proprietà riguardanti l'aritmetica elementare (o, per lo meno, questa è l'opinione largamente diffusa. Per opinioni diverse, che vengono talvolta classificate sotto il nome *ultrafinitismo*, si veda [...]). Invece, a livello della teoria formale che stiamo sviluppando, tutte le nuove nozioni devono essere definite, inclusa quella di numero naturale. Per maggiori dettagli sulla distinzione fra matematica e metamatematica facciamo riferimento al libro di Mendelson, o a libri più specificatamente dedicati ai fondamenti della matematica.

Il trucco per "definire l'infinito senza fare uso dell'infinito", essenzialmente dovuto a Dedekind (e formalizzato in questa maniera probabilmente da von Neumann), è il seguente. Diciamo che un insieme I è *induttivo* se $\emptyset \in I$ e, ogni volta che un insieme x appartiene ad I, allora anche il suo *successore* $s(x) = x \cup \{x\}$ appartiene ad I. Così, ricordando le definizioni precedenti, un insieme induttivo contiene $0 = \emptyset$. Ma allora contiene anche $1 = 0 \cup \{0\}$, $2 = 1 \cup \{1\}$ ...

Quindi l'enunciato formale dell'assioma dell'infinito è il seguente.

(Assioma dell'Infinito) Esiste un insieme induttivo I.

Come abbiamo detto, intuitivamente un insieme induttivo contiene tutti i numeri naturali. La definizione di $\mathbb{N}$ sarà dunque la seguente: $\mathbb{N}$ è l'insieme che contiene tutti gli elementi che appartengono a tutti gli insiemi induttivi. La definizione è giustificata in base all'assioma di separazione e siccome, in base all'assioma dell'infinito, esiste almeno un insieme induttivo I. Formalmente,

$\mathbb{N} = \{n \in I \mid n$ appartiene ad ogni insieme induttivo$\}$,

dove è facile costruire una formula che esprime la frase in parole contenuta nell'espressione precedente. Dunque $\mathbb{N}$ esiste, per l'assioma di separazione, ed è facile vedere che la definizione di $\mathbb{N}$ non dipende dalla particolare scelta di un insieme induttivo I. Inoltre è facile controllare che $\mathbb{N}$ stesso è induttivo, quindi contiene 0, 1, ...

Si può vedere che $\mathbb{N}$ con l'operazione di successore soddisfa agli assiomi di Peano-Dedekind[28], che se $n \neq m \in \mathbb{N}$, allora non esiste una biiezione fra m ed n, e che se $n \in \mathbb{N}$, allora non esiste una biiezione fra n ed $\mathbb{N}$. Si possono dunque finalmente dare le seguenti definizioni. Un insieme x si dice *finito* se esistono un $n \in \mathbb{N}$ ed una biiezione fra x ed n. Un insieme x si dice *infinito* se non è finito; così, per quanto affermato sopra, abbiamo che $\mathbb{N}$ è infinito. Un insieme si dice *numerabile*[29] [30] se può essere messo in corrispondenza biunivoca con $\mathbb{N}$.

1.2.6. *Costruzioni ulteriori.* Una volta "costruito" l'insieme $\mathbb{N}$ dei numeri naturali, lo si può dotare delle consuete operazioni[31]. Infatti, disponendo dei

---

[28] ** L'operazione di successore $s : \mathbb{N} \to \mathbb{N}$ data da $s(n) = n \cup \{n\}$ è effettivamente definita, poichè, pensandola come un insieme di coppie ordinate, è $s = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid y = x \cup \{x\}\}$, e l'esistenza di questo insieme segue dagli assiomi.

[29] Alcuni autori usano "numerabile" nel senso di "finito oppure numerabile". In lingua inglese, solitamente *denumerable* significa "numerabile" secondo la nostra definizione, mentre *countable* significa "finito oppure numerabile".

[30] ** Per quanto le convenzioni non abbiano particolare importanza, purché esplicitamente dichiarate, e per quanto, limitatamente alla matematica o alla scienza in generale, la praticità d'uso abbia sicuramente la preminenza su questioni di purismo linguistico, l'uso italiano del termine "contabile" (che significa "ragioniere, computista") al posto di "finito oppure numerabile" ci apparirebbe una violenza non giustificata alla nostra lingua.

[31] ** mediante le definizioni "ricorsive"
$n + 0 = n$,
$n + s(m) = s(n + m)$,
$n \cdot 0 = 0$,
$n \cdot s(m) = n \cdot m + n$.
Mentre è intuitivamente chiaro che le precedenti condizioni definiscono effettivamente due operazioni su $\mathbb{N}$, una giustificazione rigorosa richiederebbe alcuni dettagli per i quali rimandiamo ad un qualunque testo di teoria degli insiemi.[...]

prodotti cartesiani, un'operazione binaria su $\mathbb{N}$ è (o si può pensare) come un sottoinsieme di $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$. Una volta costruito $\mathbb{N}$, si può costruire l'insieme $\mathbb{Z}$ dei numeri *interi* (positivi e negativi), per esempio pensandolo come opportuno quoziente di $\mathbb{N} \times \mathbb{N}$. In questo modo, come è ben noto, risulta facile estendere le operazioni da $\mathbb{N}$ a $\mathbb{Z}$. La struttura $\mathbb{Q}$ dei numeri razionali può poi essere introdotta facendo uso di un quoziente di $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Supponiamo che queste costruzioni siano note al lettore. In base agli esempi dati, appare evidente come gli assiomi che abbiamo presentato giustifichino queste costruzioni.

La struttura dei numeri reali $\mathbb{R}$ può poi essere introdotta facendo uso delle sezioni di Dedekind, o (di certe classi di equivalenza) delle successioni di Cauchy di numeri razionali, secondo costruzioni che (anche queste!) dovrebbero essere ben note al lettore.

È importante osservare che, mentre i passaggi da $\mathbb{N}$ a $\mathbb{Z}$ e da $\mathbb{Z}$ a $\mathbb{Q}$ non fanno uso sostanziale della teoria degli insiemi (ad esempio, si può sempre considerare un numero razionale come una coppia di interi ridotta ai minimi termini; anzi, è ciò che si fa abitualmente quando i numeri razionali si scrivono sotto forma di "frazioni"), d'altro canto l'introduzione dei numeri reali fa effettivamente uso essenziale degli insiemi. Per esempio, le sezioni di Dedekind sono coppie di *sottoinsiemi* di $\mathbb{Q}$. Qualunque opinione si abbia sulla teoria degli insiemi, ammettere la possibilità di lavorare con numeri reali arbitrari (non definibili da particolari regole od espressioni, come è invece possibile per $\sqrt{2}$ o π, ad esempio), significa comunque ammettere la validità di una teoria equivalente ad un frammento non insignificante della teoria degli insiemi che qui abbiamo presentato. La stessa presentazione assiomatica dei numeri reali, come campo ordinato, archimedeo e completo, dà per nota la conoscenza dei sottoinsiemi di numeri reali (nella definizione di completezza).

1.2.7. *I paradossi.*

Il paradosso di Russell. Nell'enunciare l'assioma di separazione abbiamo fatto riferimento ad un insieme W e ad una proprietà φ, richiedendo l'esistenza dell'insieme $\{x \in W \mid \varphi(x)\}$. Senza far riferimento a qualche insieme W di cui si conosca già l'esistenza, l'assioma relativo porta ad una contraddizione. Il paradosso viene generalmente attribuito a Russell, ma l'argomento era già probabilmente noto anche a Zermelo, e, almeno in forma simile, allo stesso Cantor. Il termine "assioma" viene usato esclusivamente per motivi storici; l'assioma seguente **non** fa parte degli assiomi della teoria che stiamo prendendo in considerazione[32].

[32]Va comunque precisato che l'assioma non porta necessariamente a contraddizioni nelle teorie in cui si fa la distinzione fra insiemi e classi. Vedi la sottosezione *Insiemi e classi*. Un altro modo per conservare l'assioma di comprensione e non ottenere palesi contraddizioni è quello di porre limitazioni alle formule che definiscono le "proprietà" che si prendono in considerazione. Teorie basate su questa possibilità sono state proposte da W. Quine.

("Assioma" di Comprensione (contraddittorio!)) Per ogni proprietà φ, esiste l'insieme $\{x \mid \varphi(x)\}$, cioè l'insieme costituito da tutti gli insiemi per cui vale la proprietà φ.

Vediamo ora che l'assioma di comprensione porta ad una contraddizione. Consideriamo la proprietà $\varphi(x)$ determinata dalla formula $x \notin x$. In questo caso, l'assioma ci fornirebbe l'esistenza dell'insieme $\{x \mid x \notin x\}$, cioè l'insieme di tutti gli insiemi che non appartengono a se stessi. Supponiamo per assurdo che tale insieme esista e chiamiamolo Z. Allora, per ogni insieme x, si ha

$$x \in Z \text{ se e solo se } x \notin x.$$

Siccome l'assioma di comprensione ci garantisce (o, meglio, garantirebbe) che Z sia un insieme, e siccome la formula precedente deve valere per qualunque insieme x, possiamo sostituire Z ad x ottenendo

$$Z \in Z \text{ se e solo se } Z \notin Z,$$

una contraddizione. [...]

1.2.8. *Insiemi e classi.* Intuitivamente si può pensare ad una classe propria come ad una collezione "troppo grande" per appartenere ad un altro insieme. Nella teoria degli insiemi che stiamo presentando le classi proprie si introducono come abbreviazioni.

Ad esempio, se φ è una "proprietà" si può considerare la classe $K = \{\, x \mid \varphi(x) \,\}$ (come abbiamo appena visto, in generale, le classi definite in questo modo non possono essere considerate insiemi, se non vogliamo ottenere contraddizioni). Allora, $x \in K$ va considerata semplicemente come un'abbreviazione dell'enunciato $\varphi(x)$. Se H è un'altra classe, allora $H \in K$ è un'abbreviazione di: *esiste un x tale che $x = H$ e $\varphi(x)$* (osserviamo che qui le variabili $x, z, \ldots$ si intendono variare fra insiemi, non classi e che enunciare il principio di estensionalità anche per le classi non comporta particolari problemi).

Esistono teorie (sotto certi aspetti più eleganti, ma meno usate) in cui l'unica nozione primitiva è quella di classe (oltre ovviamente a quella di appartenenza); in queste teorie un insieme è, per definizione, una classe che appartiene ad almeno una classe. Una classe che non appartiene a nessun insieme viene detta *classe propria*.

In questo senso, il paradosso di Russell viene inteso semplicemente come una dimostrazione che la classe di tutti gli insiemi è una classe propria. Perchè se invece fosse un insieme, potremmo utilizzare l'assioma di separazione e ottenere l'*insieme* Z che conduce al paradosso.

1.2.9. *L'assioma di scelta.* L'assioma di scelta è probabilmente l'assioma più controverso fra gli assiomi che usualmente si assumono nella teoria assiomatica degli insiemi. Nonostante ciò (e nonostante alcuni aspetti della matematica che non ne fa uso siano molto interessanti), al giorno d'oggi è comunemente accettato dalla maggior parte dei matematici. È stato dimostrato da Gödel che, se la teoria costituita dai restanti assiomi è non contraddittoria, allora

assumere anche l'assioma di scelta non porta a contraddizioni. Successivamente Paul Cohen ha dimostrato che, sotto le stesse ipotesi, non si ottengono contraddizioni nemmeno assumendo la negazione dell'assioma di scelta[33]. In un certo senso, quindi, accettare o meno questo assioma è una questione di gusto personale. Attualmente, nella comune pratica matematica, l'assioma è implicitamente accettato e, qualora si intenda non farne uso, questo viene di solito dichiarato esplicitamente, mentre il contrario non sempre avviene.

L'assioma è stato usato da molti matematici senza rendersene conto, o comunque senza enunciarlo esplicitamente, talvolta anche molto prima della sua esplicita formulazione. Anche matematici che si sono schierati dichiaratamente contro l'assioma, l'hanno a volte usato, quasi certamente a loro insaputa[34]. Enunciamo adesso l'assioma in una forma leggermente semplificata.

(Assioma di Scelta) Se $\mathcal{F}$ è una famiglia di insiemi non vuoti e a due a due disgiunti, allora esiste un insieme S tale che $|A \cap S| = 1$, per ogni $A \in \mathcal{F}$.

Quindi l'assioma di scelta ci permette di "scegliere" esattamente un elemento da ciascun insieme appartenente ad una famiglia, purché gli insiemi della famiglia siano a due a due disgiunti.

Precisiamo che ci sono casi in cui la scelta può essere effettuata senza necessità di un assioma aggiuntivo. Si considera generalmente ammissibile la scelta di un numero finito di elementi. Ma questo non è l'unico caso in cui non è necessario l'assioma di scelta. Per esempio, se $\mathcal{F}$ è una famiglia di sottoinsiemi chiusi e limitati inferiormente di $\mathbb{R}$ (naturalmente, a due a due disgiunti), allora $S = \{\, x \in \mathbb{R} \mid \text{esiste } A \in \mathcal{F} \text{ tale che } x = \min A \,\}$ è un insieme che soddisfa la conclusione dell'assioma di scelta. In questo caso particolare non abbiamo bisogno dell'assioma di scelta per ottenere S: l'esistenza di S segue immediatamente dall'assioma di separazione!

Intuitivamente, tutte le volte che può essere stabilita una regola per scegliere un elemento ben preciso da ciascun A di $\mathcal{F}$, allora l'assioma di scelta non è necessario. Volendo essere più formali, quello che serve è una formula φ tale che per ogni $A \in \mathcal{F}$ esiste esattamente un elemento $a \in A$ tale che valga $\varphi(a)$. In questo caso l'assioma di separazione ci fornisce un "insieme di scelta" S dato da $\{\, x \in \bigcup \mathcal{F} \mid \varphi(x) \,\}$.

Al di là di questioni "filosofiche"[35] e di metodo, l'asioma della scelta presenta una significativa differenza rispetto agli assiomi introdotti finora. A parte

[33]Queste sono dimostrazioni di non contraddittorietà *relativa*, cioè si dimostra che se una certa teoria T è non contraddittoria, allora un'altra teoria T' è non contraddittoria. Una dimostrazione (non relativa) della non contraddittorietà di una teoria degli insiemi sufficientemente forte è impossibile a causa dei teoremi di incompletezza di Gödel.

[34]A riguardo va comunque precisato che esistono varie versioni più deboli dell'assioma di scelta e alcuni di questi matematici, pur dichiarandosi contrari alla versione "completa" dell'assioma di scelta, hanno esplicitamente ammesso la possibilità di usare alcune di queste versioni più deboli. Questo fatto ha a volte portato a fraintendimenti del reale pensiero di questi matematici

[35]Le dimostrazioni che usano l'assioma della scelta non sono "costruttive" cioè non forniscono un esempio esplicito degli oggetti di cui si dimostra l'esistenza.

l'assioma di estensionaità, che caratterizza la natura degli insiemi, tutti gli altri assiomi ci forniscono insiemi definiti univocamente (sempre per estensionalità), mentre l'insieme fornito dall'assioma di scelta è in generale tutt'altro che unico.

Nella prossima sottosezione presentiamo una forma equivalente (particolarmente utile e intuitiva) dell'assioma di scelta.

1.2.10. *Prodotti infiniti.* Una *successione generalizzata (ad indici su un insieme I) e (ad elementi in un insieme $\mathcal{F}$)*, per brevità, una *sequenza* è una funzione $A : I \to \mathcal{F}$.

Spesso si scriverà A_i al posto di $A(i)$, e la stessa funzione A verrà indicata come[36] $(A_i)_{i\in I}$. Osserviamo che questa notazione combacia con quella usuale per indicare le successioni (ad indici in $\mathbb{N}$). Formalmente, una successione è una funzione s da $\mathbb{N}$ verso un certo insieme; ma solitamente le successioni vengono indicate con $(s_n)_{n\in\mathbb{N}}$ ed s_n indica l'elemento $s(n)$ della successione.

Se $(A_i)_{i\in I}$ è una sequenza di insiemi, il *prodotto (cartesiano* o *diretto)* $\prod_{i\in I} A_i$ della sequenza $(A_i)_{i\in I}$ è definito da

$$\prod_{i\in I} A_i = \{a \mid a \text{ è una funzione da } I \text{ a } \bigcup_{i\in I} A_i \text{ tale che } a(i) \in A_i, \text{ per ogni } i \in I\}$$

In parole, $\prod_{i\in I} A_i$ è l'insieme delle sequenze $(a_i)_{i\in I}$ tali che $a_i \in A_i$, per ogni $i \in I$ (come precisato sopra, $a(i)$ ed a_i sono due modi per indicare lo stesso elemento della sequenza).

Se tutti gli A_i sono uguali ad A, si scriverà A^I al posto di $\prod_{i\in I} A_i$, e si parlerà di *potenza* di A o più precisamente *potenza alla* I. In questo caso A^I è l'insieme di tutte le funzioni da I ad A.

Non è difficile dimostrare che l'assioma di scelta è equivalente al seguente principio.

(Assioma Moltiplicativo) Se $(A_i)_{i\in I}$ è una sequenza di insiemi non vuoti, allora il prodotto $\prod_{i\in I} A_i$ è non vuoto.

Dunque l'assioma di scelta è equivalente alla richiesta che il prodotto di ogni sequenza di insiemi non vuoti sia esso stesso non vuoto[37].

Come ulteriore esempio (molto semplice!) di un caso in cui non c'è bisogno di particolari assiomi, supponiamo che $A_i = A$, per ogni $i \in I$. Allora, se A è non vuoto, anche A^I è non vuoto. Basta scegliere un qualunque $a \in A$. L'esistenza della funzione costante $\hat{a} : I \to A$ tale che $\hat{a}(i) = a$ per ogni $i \in I$ segue dagli altri assiomi.

---

[36] **In senso strettamente formale una sequenza, nel senso appena introdotto, è una nozione differente da quella di una famiglia (indicizzata) di insiemi. Se $A = (A_i)_{i\in I}$ è una sequenza, allora possiamo sicuramente considerare l'insieme (famiglia indicizzata) $\{ A_i \mid i \in I \}$, cioè l'immagine della funzione A. D'altro canto, le due nozioni sono formalmente distinte, per esempio, se tutti gli A_i sono uguali ad A, allora $\{ A_i \mid i \in I \} = \{A\}$. In altre parole, in una sequenza la molteplicità con cui compaiono gli elementi (ed eventualmente il loro ordine, nel caso in cui I sia ordinato) sono elementi rilevanti; non così in una famiglia di insiemi. Nella maggior parte delle situazioni non crea problemi identificare sequenze e famiglie indicizzate, ma va precisato che si tratta di due nozioni distinte.

[37] Equivalentemente, basta supporre che il prodotto di ogni sequenza di insiemi non vuoti della stessa cardinalità sia non vuoto, vedi la Forma AC7 nel libro di H. Rubin J.E. Rubin, Equivalents of the Axiom of Choice, II.

Accenniamo alla dimostrazione che l'assioma della scelta è equivalente all'assioma moltiplicativo. Se vale l'assioma moltiplicativo e $\mathcal{F}$ è come nelle ipotesi dell'assioma di scelta, allora si può considerare il prodotto $\prod_{A\in\mathcal{F}} A$ (in altre parole, stiamo prendendo come successione generalizzata la funzione identica da $\mathcal{F}$ ad $\mathcal{F}$, cioè $\mathcal{F}$ indicizza se stessa). Per l'assioma moltiplicativo esiste $f \in \prod_{A\in\mathcal{F}} A$, e se prendo come S l'immagine di f ho un insieme di scelta per $\mathcal{F}$.

Il viceversa è ovvio quando gli insiemi della sequenza $(A_i)_{i\in I}$ sono a due a due disgiunti: considero $f(i) = S \cap A_i$, dove S è dato dall'assioma di scelta. Ma posso sempre ricondurmi al caso precedente se al posto di A_i considero l'insieme $A_i^* = \{i\} \times A_i = \{\, (i, a) \mid a \in A_i \,\}$.

1.2.11. *Conseguenze dell'assioma di scelta.* [da riorganizzare!]

Altre formulazioni equivalenti L'assioma di scelta è equivalente ad un altro principio importante in teoria degli insiemi, un principio introdotto da Cantor molto prima della formulazione esplicita dell'assioma di scelta. In effetti, Zermelo ha introdotto l'assioma di scelta proprio per tentare di dimostrare il principio introdotto da Cantor.

Principio del buon ordinamento. Ogni insieme può essere bene ordinato[38].

Come vedremo, l'assioma della scelta, nella forma del principio del buon ordinamento, ci permetterà di dare una definizione esplicita di cardinaltà di un insieme. Ogni classe di insiemi bene ordinati ha uno speciale "rappresentante", l'ordinale associato, e si può definire la cardinalità di un insieme X come l'ordinale più piccolo (che esiste) associato ad un possibile buon ordinamento di X.

L'assioma della scelta è chiaramente equivalente al seguente principio:

(I) se $f : A \to B$ è una funzione suriettiva, allora esiste una funzione $g : B \to A$ tale che $g \circ f$ sia la funzione identità su B (in particolare, f risulta iniettiva).

Infatti, se $f : A \to B$, la relazione definita da $a \sim a'$ se $f(a) = f(a')$ induce una partizione di A alla quale si può applicare l'assioma di scelta. Viceversa, se $\mathcal{F}$ è come nell'enunciato dell'assioma di scelta, basta applicare (I) alla funzione $f : \bigcup \mathcal{F} \to A$ definita da $f(a) = A$, dove A è l'unico elemento di $\mathcal{F}$ tale che $a \in A$ (A è unico perchè gli elementi di $\mathcal{F}$ sono a due a due disgiunti).

Si può indebolire (I) chiedendo solo

(I′) se $f : A \to B$ è una funzione suriettiva, allora esiste una funzione iniettiva $g : B \to A$

Ovviamente (I) $\Rightarrow$ (I′), ma sembra essere un problema ancora aperto se vale il viceversa, oppure se (I′) è strettamente più debole di (I). Questo problema è stato indicato come il più antico problema non ancora risolto in teoria degli insiemi.

https://karagila.org/2014/on-the-partition-principle/

- Senza assumere l'assioma di scelta:

[38] La definizione di buon ordine viene data in seguito.

unione di una famiglia numerabile di insiemi numerabili non necessariamente numerabile (anzi, addirittura $\mathbb{R}$ potrebbe essere unione di una famiglia numerabile di insiemi numerabili!) [ma $\mathbb{N} \times \mathbb{N}$ è sempre numerabile! Il problema non è costruire la biiezione fra $\bigcup_{i \in I} X_i$ ed $\mathbb{N}$, il problema è che non è scontato che si possano *scegliere* contemporaneamente biiezioni fra X_i ed $\mathbb{N}$.]

possono esistere insiemi che non sono finiti, ma che sono finiti nel senso di Dedekind. Può esistere un insieme X che non è finito, ma tale che non esiste una funzione iniettiva da $\mathbb{N}$ in X.

- Con l'assioma di scelta (conseguenze paradossali):
- sottoinsiemi di $\mathbb{R}$ non misurabili
- paradosso di Banach Tarski
- esiste un gioco infinito senza che nessuno dei due giocatori abbia una strategia vincente (gioco= deterministico, senza fattori casuali, a due persone; risultato solo vittoria o sconfitta; nel caso finito uno dei due ha sempre una strategia vincente: basta analizzare tutte le possibilità, esempio: tris)

(L'ipotesi che per tutti i giochi numerabili almeno un giocatore abbia una strategia vincente viene chiamato assioma di determinatezza (AD) - per quanto detto contraddice l'assioma di scelta - e ha trovato moltissime applicazioni, anche a problemi di analisi su numeri reali. Soprattutto, è stato utile per analizzare le conseguenze di certe proprietà *anche sotto l'ipotesi dell'assioma della scelta*: usando AD si possono costruire modelli con proprietà particolari, che poi possono essere modificati ottenendo modelli della teoria con l'assioma di scelta, e viceversa.)

1.2.12. *Cenni ad ulteriori assiomi*.* Come abbiamo accennato all'inizio, l'elenco degli assiomi che abbiamo presentato non è del tutto completo.

L'assioma di rimpiazzamento. Per ottenere alcuni risultati è necessario considerare una forma più forte dell'assioma di separazione che, detto in maniera molto approssimativa, ci consenta di costruire certe famiglie $\{A_i \mid i \in I\}$ di insiemi la cui esistenza non seguirebbe dagli altri assiomi. Come già detto, la questione è talmente delicata che ha tratto in inganno illustri matematici.

Più in dettaglio, l'assioma di rimpiazzamento richiede che, se $\varphi(x, y)$ è una formula che rappresenta una funzione parziale (cioè φ è tale che per ogni insieme x esiste al massimo un y tale che $\varphi(x, y)$), allora, ogni qualvolta A è un insieme, è un insieme anche $B = \{\, y \mid \varphi(a, y), \text{ per qualche } a \in A \,\}$. Come per l'assioma di separazione, anche in questo caso non si tratta di un singolo assioma, ma di uno schema di assiomi, uno per ogni formula. Ma, mentre l'assioma di separazione si applica a qualunque formula, in questo caso l'assioma si può applicare solo per formule che soddisfano alla suddetta condizione di funzionalità[39]

[39]Questo è ovvio; se per esempio $\varphi(x, y)$ dicesse "esiste una funzione iniettiva da x ad y" allora prendendo $A = \{\emptyset\}$ otterrei l'insieme di tutti gli insiemi, e abbiamo visto che questo porta ad una contraddizione.

L'assioma è giustificato dal principio (intuitivo) implicito nelle idee di Cantor del *limitare la grandezza* ("limitation of size"). Secondo Cantor, infatti, i paradossi hanno origine semplicemente dal considerare collezioni "non completate", insiemi eccessivamente grandi (come l'insieme di tutti gli insiemi). Mentre considerare queste "collezioni" come insiemi porta a contraddizioni, le contraddizioni non dovrebbero sorgere se ci si limita a considerare insiemi relativamente "piccoli". Nel caso precedente la restrizione di φ ad A fornisce una funzione biiettiva da un sottoinsieme di A a B, quindi sicuramente B è da considerare "più piccolo (o al massimo altrettanto grande)" di A, quindi se A esiste come insieme, è sensato supporre che anche B sia un insieme. Torneremo sull'argomento accennando alle elaborazioni di von Nemann sul tema.

Al lettore potrebbe sorgere il dubbio che l'assioma di rimpiazzamento non sia necessario poiché, avendo l'insieme B e usando le tecniche presentate in precedenza, posso costruire una funzione f che è un insieme (non semplicemente una relazione determinata da una formula) e che mi rappresenta la restrizione di φ ad A. Ma questo posso farlo solo se so già che B è un insieme: f è un sottoinsieme di $\mathcal{P}(\mathcal{P}(A \times B))$, quindi in generale non posso costruire f se prima non ho B.

Ad esempio, l'assioma di rimpiazzamento ci consente di costruire l'insieme V_ω presentato nella sottosezione 1.2.4. Si può scrivere, anche se non è completamente banale, una formula[40] φ tale che $\varphi(x, y)$ vale se e solo se $x \in \mathbb{N}$ e $y = V_n$. Quindi prendendo $A = \mathbb{N}$ e usando l'assioma di rimpiazzamento, otteniamo l'insieme $\mathcal{F} = \{V_0, V_1, V_2, \dots\}$, che ci serviva per costruire $V_\omega = \bigcup \mathcal{F}$.

È abbastanza facile vedere che l'assioma di rimpiazzamento vale in V_ω, pensato come modello (cf. 1.2.4) quindi ci si potrebbe chiedere se per caso l'assioma di rimpiazzamento non sia una conseguenza degli altri assiomi. Costruiamo un altro modello per far vedere che in effetti si tratta di un assioma che non segue dagli altri.

---

[40] Sia $\psi(z)$ la formula che afferma:

z è un insieme di coppie ordinate e $(\emptyset, \emptyset) \in z$; inoltre
ogni volta che $(u, v) \in z$ allora $u \in \mathbb{N}$ e se $(u, v') \in z$, allora $v = v'$ e, per finire,
per ogni u, se $(u, v) \in z$ e $u = n + 1$, allora esiste w tale che $(n, w) \in z$ e $v = \mathcal{P}(w)$.

Quindi, se z è un insieme tale che vale $\psi(z)$, allora z è del tipo $\{(0, V_0), (1, V_1), (2, V_2) \dots\}$, dove z può essere finito ma, a priori, potrebbe essere anche infinito. Però posso dimostrare, in base agli assiomi, che, per ogni n, esiste uno z tale che $\psi(z)$ e z contiene n coppie, mentre invece, senza l'assioma di rimpiazzamento non posso dimostrare l'esistenza di un tale z infinito.

Sia allora $\varphi(x, y)$ la formula che esprime *esiste un z tale che $\psi(z)$ e la coppia $(x, y) \in z$*.

In altre parole, riassumendo, posso costruire *come insieme*, per n arbitrariamente grande, un funzione definita su $\{0, 1, \dots, n\}$ e tale che $f(m) = V_m$, per m nel dominio. Questo mi dà la possibilità di scrivere *una formula* che implicitamente mi definisce una funzione con dominio tutto $\mathbb{N}$. L'assioma di rimpiazzamento mi garantisce poi l'esistenza di un insieme che rappresenta effettivamente questa funzione (l'assioma di rimpiazzamento mi garantisce l'esistenza dell'immagine di questa funzione, ma una volta che si sa che l'immagine è un'insieme, la funzione si può costruire al solito modo come insieme di coppie ordinate.).

La forma generale di questo argomento giustifica le definizione ricorsive (o per induzione). Naturalmente, qui abbiamo presentato l'argomento in un caso particolare.

Continuiamo ad iterare la costruzione dei V_i. Poniamo
$V_{\omega+1} = \mathcal{P}(V_\omega)$,
$V_{\omega+2} = \mathcal{P}(V_{\omega+1})$,
$V_{\omega+3} = \mathcal{P}(V_{\omega+2}) \dots$,
in generale,
$V_{\omega+(n+1)} = \mathcal{P}(V_{\omega+n})$.
(Non ci si preoccupi per ora del significato degli indici del tipo $\omega + n$. Se la notazione creasse difficoltà, si scriva semplicemente W_n al posto di $V_{\omega+n}$ o, ancor meglio, $V_{1,n}$ al posto di $V_{\omega+n}$ e, magari, si pensi a V_n come a $V_{0,n}$)

L'assioma di rimpiazzamento, con un po' di elaborazioni tecniche necessarie per scrivere una formula opportuna, ci consente di costruire l'insieme $\mathcal{G} = \{V_\omega, V_{\omega+1}, V_{\omega+2}, \dots\}$ e chiamiamo $V_{\omega+\omega}$ l'insieme $\bigcup \mathcal{G} = \bigcup_{n\in\mathbb{N}} V_{\omega+n}$.

Allo stesso modo che nella sottosezione 1.2.4, si vede che $V_{\omega+n} \subseteq V_{\omega+m}$, se $n \leq m$ e allo stesso modo si vede che $V_{\omega+\omega}$ soddisfa a tutti gli assiomi introdotti fino alla sezione 1.2.3 inclusa. Anche qui consideriamo $V_{\omega+\omega}$ come modello con la relazione di appartenenza che interpreta il simbolo stesso di appartenenza. Ma $V_{\omega+\omega}$ contiene anche $\mathbb{N}$; addirittura $\mathbb{N}$ sta già in $V_{\omega+1}$. Infatti, per ogni $n \in \mathbb{N}$, abbiamo $n \in V_{n+1}$ (per induzione), quindi $\mathbb{N} \subseteq V_\omega$ cioè $\mathbb{N} \in V_{\omega+1} \subseteq V_{\omega+\omega}$.

In conclusione, $V_{\omega+\omega}$ è modello di tutti gli assiomi introdotti finora. Ma si può verificare che $V_{\omega+\omega}$ non è modello dell'assioma di rimpiazzamento, Anche se questo è intuitivo, una giustificazione rigorosa della nostra affermazione comporta dettagli delicati [...]

- su $V_{\omega+\omega}$ si può svolgere gran parte della matematica, per lo meno della matematica classica.

Ad esempio, abbiamo visto che $\mathbb{N} \in V_{\omega+1}$, quindi, seguendo le costruzioni precedenti, $\mathbb{N} \times \mathbb{N} \in \mathcal{P}(\mathcal{P}(V_{\omega+1})) = V_{\omega+3}$, quindi, se si costruisce $\mathbb{Z}$ come insieme di classi di equivalenza di $\mathbb{N} \times \mathbb{N}$, allora $\mathbb{Z} \in V_{\omega+5}$, e così via per $\mathbb{Q}$ ed $\mathbb{R}$, ma anche per l'insieme di tutte le funzioni da $\mathbb{R}$ in $\mathbb{R}$ etc. Naturalmente. è possibile codificare questi insiemi (costruire una copia isomorfa) in un $V_{\omega+m}$ con m molto più piccolo. Questo è utile ma generalmente laborioso, per cui non entriamo in dettagli. L'importante è osservare che tutto quello a cui abbiamo appena accennato può essere svolto senza "uscire" da $V_{\omega+\omega}$.

La teoria degli insiemi ha ottenuto comunque risultati interessanti che riguardano insiemi molto più complessi di quelli che stanno in $V_{\omega+\omega}$. Tra l'altro, questi risultati che riguardano insiemi "relativamente grandi" hanno una diretta influenza su alcune proprietà, ad esempio, dei sottoinsiemi dei numeri reali.

- è difficile sostenere che potenza, unione, rimpiazzamento tutti insieme rispettino il principio del "limitare la grandezza". Infatti V_ω è numerabile ma, per il Teorema di Cantor (Sez. 1.1.5), $V_{\omega+1}$ ha cardinalità strettamente maggiore (in effetti, la sua cardinalità è la stessa dell'insieme dei numerni reali), e così via, ciascun $V_{\omega+n+1}$ ha cardinalità strettamente maggiore di $V_{\omega+n}$. Alla fine, $V_{\omega+\omega}$ deve avere cardinalità ancora maggiore di ciascun $V_{\omega+n}$.

Il Teorema di Cantor (vedi 1.1.5) ha spinto alcuni a sollevare dubbi sull'ammissibilità dell'assioma della potenza, a maggior ragione visto che, coi risultati di forcing, si può dimostrare che la cardinalità dell'insieme potenza di un insieme infinito può essere arbitrariamente alta (nel senso che non è possibile dimostrare che esistono dei limiti superiori). Ma, anche accettando l'applicazione indiscriminata dell'assioma della potenza, l'esempio di $V_{\omega+\omega}$ mostra che l'uso congiunto degli assiomi dell'unione e di rimpiazzamento porta ad ottenere insiemi di cardinalità molto più alta di quella degli insiemi di partenza. Chiamando $\beth_\omega$ la cardinalità di $V_{\omega+\omega}$, abbiamo che $|V_{\omega+n}| < \beth_\omega$, per ogni $n \in \mathbb{N}$, ma $\beth_\omega$ si può ottenere come unione numerabile di cardinalità strettamente minori[41].

L'assioma di fondazione (o regolarità). [da ricontrollare] Come abbiamo detto, gran parte della matematica si può svolgere in $V_{\omega+\omega}$, quindi non avremmo bisogno dell'assioma di rimpiazzamento (è vero che l'assioma di rimpiazzamento è necessario per costruire V_ω, ma anche senza rimpiazzamento si può codificare una struttura che "rappresenti" V_ω. In ogni caso, per costruire V_ω è necessaria solo una singola applicazione specifica del rimpiazzamento, non l'intero schema.)

Vi sono comunque alcuni teoremi di matematica classica che richiedono il rimpiazzamento; e comunque l'assioma di rimpiazzamento rende la teoria molto più elegante e semplice.

Invece l'assioma di fondazione, che stiamo per introdurre, ha un numero minimo di applicazioni matematiche "pure", ed è utilizzato generalmente per motivi tecnici interni alla teoria degli insiemi. Ha comunque una forte motivazione di cui parleremo in seguito. Enunciamo l'assioma in una forma equivalente, quella che garantisce la posibilità di una "induzione insiemistica".

Assioma di fondazione, o di regolarità (formulazione equivalente, assumendo gli altri assiomi: induzione insiemistica). Se $\varphi(x)$ è una formula e $\forall y\ ((\forall x \in y\ \varphi(x)) \Rightarrow \varphi(y))$, allora[42] $\forall y\ \varphi(y)$.

Come esempio di applicazione dell'induzione insiemistica, vediamo che l'assioma di fondazione ci permette di dimostrare che nessun insieme appartiene a se stesso. Sia $\varphi(x)$ la formula $x \notin x$. Se y è tale che

$\forall x \in y\ \varphi(x)$,

allora non può essere $y \in y$ perchè, potremmo prendere y al posto di x nella formula precedente, ottenendo $\varphi(y)$, cioè $y \notin y$, una contraddizione. Quindi, per questa φ, abbiamo dimostrato che

$\forall y\ ((\forall x \in y\ \varphi(x)) \Rightarrow \varphi(y))$.

---

[41] Al contrario, ad esempio, una unione finita di insiemi finiti è ancora finita, una unione numerabile di insiemi numerabili è ancora numerabile. Invece $\beth_\omega$ si può ottenere come unione di una famiglia di cardinaità $< \beth_\omega$ e tale che ciascun insieme della famiglia abbia cardinaità $< \beth_\omega$. Un cardinale di questo tipo si dice *singolare*.

[42] Abbiamo espresso l'assioma parzialmente a parole per renderlo più intuitivo. Formalmente, lo schema di assiomi è costituito da tutte le formule $(\forall y\ ((\forall x \in y\ \varphi(x)) \Rightarrow \varphi(y))) \Rightarrow \forall y\ \varphi(y)$, al variare della formula φ.

Per l'assioma di fondazione, nella forma in cui l'abbiamo enunciato, vale $\forall y\ \varphi(y)$, cioè nessun insieme appartiene a se stesso.

La teoria con tutti gli assiomi considerati finora viene detta teoria di Zermelo-Fraenkel con l'assioma di scelta, abbreviata in ZFC (solo ZF, se non si assume l'assioma di scelta).

Altre letture. Un libro molto utile, apparentemente elementare ma in realtà decisamente denso, dove (a dispetto del titolo) si presenta la teoria degli insiemi in maniera assiomatica anche se non formalizzata è Paul Halmos, *Naive Set Theory*, varie edizioni, trad. it., *Teoria elementare degli insiemi*, varie ristampe.

Utile materiale in lingua italiana si può trovare ai seguenti indirizzi:

(Alessandro Andretta)
http://www.logicatorino.altervista.org/materiale/Elementi.pdf

(Mauro Di Nasso) http://www.dm.unipi.it/cluster-pages/dinasso/eti-2014.html

(Piero Plazzi) http://campus.unibo.it/74334/1/Insiemi.pdf

Un'introduzione interessante e molto dettagliata dal punto di vista storico si trova in

https://www.treccani.it/enciclopedia/la-seconda-rivoluzione-scientifica-matematica-e-logica-la-teoria-degli-insiemi_(Storia-della-Scienza)/

Il manuale ormai classico riguardante la teoria degli insiemi è Thomas Jech, *Set Theory. The Third Millennium Edition, revised and expanded*, 2002, successive ristampe con correzioni.

Un manuale aggiornato agli sviluppi più recenti è Matthew Foreman, Akihiro Kanamori (Editors), *Handbook of Set Theory*, 2010, tre volumi.

Sull'assioma di scelta e sue forme equivalenti, si può consultare Herman Rubin, Jean E. Rubin, *Equivalents of the axiom of choice.* 1985

Inoltre Howard, Paul; Rubin, Jean E. *Consequences of the axiom of choice, 1998* presenta un elenco di enunciati che seguono dall'assioma di scelta (cioè che non seguono dagli assiomi senza usare l'assioma di scelta) ma che, generalmente, sono più deboli (cioè non implicano la forma "completa" dell'assioma di scelta).

Come testo di base riguardante la logica matematica consigliamo, fra le tante possibilità, il libro di Elliot Mendelson, *Introduction to Mathematical Logic*, varie edizioni, trad. it. *Introduzione alla Logica Matematica*.

Di sicuro interesse per lo studente che voglia approfondire le questioni fondazionali è il libro di Gabriele Lolli, *Filosofia della matematica*, 2002. Sono molto utili anche le pagine della Stanford Encyclopedia of Philosophy, giusto per fare un esempio:

https://plato.stanford.edu/entries/set-theory/

2. Insiemi bene ordinati

In questa sezione studiamo le relazioni di buon ordine, che hanno fatto parte della teoria degli insiemi fino dagli inizi, e che hanno trovato applicazioni di tipo molto vario. Prima di dare la definizione di insieme bene ordinato, presentiamo alcuni esempi (fra i tanti possibili) che forniscono motivazioni per lo studio della nozione generale.

2.1. Iterazioni transfinite. In matematica abbondano procedimenti che possono essere iterati un numero finito ma arbitrariamente alto di volte. Abbiamo visto sopra le definizioni ricorsive[43] di successore, e della somma e del prodotto fra naturali. Un altro esempio tipico è la definizione di fattoriale di un numero naturale, data da $0! = 1$ e $(n+1)! = n!(n+1)$.

In alcuni casi è possibile considerare un passo "all'infinito", per esempio, se $(a_n)_{n\in\mathbb{N}}$ è una successione di numeri reali, si possono considerare le somme finite (parziali) degli elementi a_n definite ovviamente da

$S_0 = 0$,

$S_{m+1} = S_m + a_m$,

cioè, $S_m = \sum_{n<m} a_n = a_0 + a_1 + \cdots + a_{m-1}$. Allora, come ben noto, la serie $\sum_{n\in\mathbb{N}} a_n$ è definita come $\lim_{m\in\mathbb{N}} S_m$, naturalmente supponendo che il limite esista.

In alcuni casi è addirittura possibile procedere ancora oltre, come stiamo per vedere[44].

2.1.1. *Gruppi risolubili generalizzati.* [Questa sottosezione non fa parte del programma del corso di Logica, AA 20-21] Ricordiamo che se H e K sono sottogruppi di un gruppo G, il loro commutatore $[H, K]$ è il sottogruppo di G generato da $\{hkh^{-1}k^{-1} \mid h \in H, k \in K\}$. Non è necessario conoscere approfonditamente la teoria dei gruppi per seguire questo esempio, basta sapere che $[H, K]$ è un sottogruppo contenuto sia in H che in K, in particolare, $G^{(1)} = [G, G]$ è un sottogruppo di G, $G^{(2)} = [G^{(1)}, G^{(1)}]$ è un sottogruppo di $G^{(1)}$ (quindi anche un sottogruppo di G), e così via. In dettaglio, se definiamo

$G^{(0)} = G$, e

$G^{(n+1)} = [G^{(n)}, G^{(n)}]$, per $n \in \mathbb{N}$,

otteniamo una successione decrescente[45] $(G^{(n)})_{n\in\mathbb{N}}$ di sottogruppi di G.

---

[43] In questo senso, ricorsivo è sinonimo di induttivo.

[44] ** In realtà anche la somma si può iterare "oltre l'infinito". Se $(b_n)_{n\in\mathbb{N}}$ è un'altra successione di numeri reali, possiamo definire $S_\omega = \sum_{n\in\mathbb{N}} a_n$, poi $S_{\omega+1} = S_\omega + b_0$, e $S_{\omega+2} = S_\omega + b_0 + b_1$ e, in generale, $S_{\omega+m} = S_\omega + \sum_{n<m} b_n$ e prendere ancora il limite, sempre supponendo che esista, $S_{\omega+\omega} = \lim_{m\in\mathbb{N}} (S_\omega + \sum_{n<m} b_n)$. Non sembrano esserci però molte applicazioni di questa iterazione transfinita della somma (vedi comunque per argomenti correlati il Capitolo IV di Udo Hebisch, Hanns Joachim Weinert, *Semirings: Algebraic Theory and Applications in Computer Science*, 1998). Invece le definizioni che presentiamo nelle prossime sottosezioni hanno molte applicazioni interessanti.

[45] decrescente rispetto alla relazione di inclusione; qui con *decrescente* si intende decrescente in senso non necessariamente stretto.

Un gruppo si dice *risolubile* se esiste $n \in \mathbb{N}$ tale che $G^{(n)} = \{e\}$, il sottogruppo minimo. Ricordiamo che un gruppo G è *abeliano* se $hk = kh$, per tutti gli $h, k \in G$. Siccome un gruppo è abeliano se e solo se $G^{(1)} = [G, G] = \{e\}$, la nozione di gruppo risolubile estende quella di gruppo abeliano. Intuitivamente un gruppo è risolubile se e solo se può essere costruito usando "blocchi" abeliani. Esistono definizioni equivalenti di gruppo risolubile che rendono più precisa questa intuizione. In particolare, se $G^{(1)} = [G, G] = G$, allora G è invece "il meno abeliano possibile".

Ovviamente, se $G^{(\bar{n}+1)} = G^{(\bar{n})}$, per qualche $\bar{n}$, allora la successione si stabilizza, cioè $G^{(\bar{n}+2)} = [G^{(\bar{n}+1)}, G^{(\bar{n}+1)}] = [G^{(\bar{n})}, G^{(\bar{n})}] = G^{(\bar{n}+1)} = G^{(\bar{n})}$, dove abbiamo usato a turno la definizione di $G^{(n+2)}$ o di $G^{(n+1)}$ e l'ipotesi $G^{(\bar{n}+1)} = G^{(\bar{n})}$. Continuando allo stesso modo, se $G^{(\bar{n}+1)} = G^{(\bar{n})}$, allora $G^{(m)} = G^{(\bar{n})}$, per ogni $m \geq \bar{n}$.

Se G è un gruppo finito, la successione $(G^{(n)})_{n\in\mathbb{N}}$ si stabilizza da un certo punto in poi, e sono possibili entrambi i casi estremi $G^{(1)} = G$, e quindi $G^{(n)} = G$, per ogni $n \in \mathbb{N}$, oppure $G^{(\bar{n})} = \{e\}$, per qualche $\bar{n}$, e quindi $G^{(m)} = \{e\}$ per ogni $m \geq \bar{n}$.

Se invece G è infinito, è possibile che la successione $(G^{(n)})_{n\in\mathbb{N}}$ sia strettamente decrescente. In questo caso il sottogruppo $G^{(\omega)} = \bigcap_{n\in\mathbb{N}} G^{(n)}$ è un gruppo strettamente contenuto in ciascuno dei $G^{(n)}$. Si ha quindi una generalizzazione della nozione di gruppo risolubile, quella di gruppo risolubile di indice ω, cioè un G tale che $G^{(\omega)} = \{e\}$.

Fino a qui il nostro esempio non ha nulla di sostanzialmente diverso dal caso delle serie discusso in precedenza. Ma in questo caso possiamo continuare oltre. Avendo definito

$G^{(\omega)} = \bigcap_{n\in\mathbb{N}} G^{(n)}$,

possiamo porre

$G^{(\omega+1)} = [G^{(\omega)}, G^{(\omega)}]$,

$G^{(\omega+2)} = [G^{(\omega+1)}, G^{(\omega+1)}]$, ...

(qui, almeno per ora, gli esponenti ω, $\omega+1$, $\omega+2$ non hanno un significato particolare, li stiamo semplicemente usando come indici con significato intuitivo. Il simbolo ω rappresenta l'infinito, anzi, *un* infinito, visto che poi consideriamo subito dopo "infiniti ancor più grandi". Tutto il discorso verrà reso rigoroso fra qualche sezione). In generale, poniamo

$G^{(\omega+n+1)} = [G^{(\omega+n)}, G^{(\omega+n)}]$, per $n \in \mathbb{N}$,

e così abbiamo definito $G^{(\omega+n)}$, per ogni $n \in \mathbb{N}$. Ormai che abbiamo iniziato, sarebbe limitativo fermarsi qui! Poniamo

$G^{(\omega+\omega)} = \bigcap_{n\in\mathbb{N}} G^{(\omega+n)}$,

e, ancora,

$G^{(\omega+\omega+n+1)} = [G^{(\omega+\omega+n)}, G^{(\omega+\omega+n)}]$, per $n \in \mathbb{N}$,

$G^{(\omega+\omega+\omega)} = \bigcap_{n\in\mathbb{N}} G^{(\omega+\omega+n)}$.

È convenzione (dovuta a motivi storici e di notazione che sarebbero lunghi da spiegare) scrivere $\omega 2$ (anziché 2ω) per $\omega+\omega$, scrivere $\omega 3$ per $\omega+\omega+\omega$ e così

via. Procedendo come sopra, possiamo definire $G^{(\omega m+n)}$, per ogni $m, n \in \mathbb{N}$. Ma possiamo andare ancora oltre. Sia

$G^{(\omega^2)} = \bigcap_{m\in\mathbb{N}} G^{(\omega m)}$.

Il lettore si potrebbe chiedere perchè non abbiamo invece definito

$G^{(\omega^2)} = \bigcap_{m,n\in\mathbb{N}} G^{(\omega m+n)}$.

È chiaro che queste definizioni di $G^{(\omega^2)}$ risultano equivalenti; basta controllare che $G^{(\omega(m+1))} \subseteq G^{(\omega m+n)} \subseteq G^{(\omega m)}$, per ogni $m, n \in \mathbb{N}$.

Quanto a lungo si può continuare con costruzioni di questo tipo? Il problema è semplicemente quello di stabilire un opportuno insieme di indici (ma questo compito è tutt'altro che banale!). Per questo appropriato insieme di indici, diciamo, $\alpha \in A$, deve essere ben definito $G^{(\alpha+1)}$ ogni qual volta è definito $G^{(\alpha)}$, e inoltre, se α non ha nessun immediato predecessore (come, ad esempio, ω oppure $\omega + \omega$ nella costruzione precedente), $G^{(\alpha)}$ deve essere definito in funzione solo dei $G^{(\beta)}$, con β che varia fra tutti gli elementi che "precedono" α. Questo "sistema di indici" deve essere congegnato in modo che questo tipo di definizioni garantiscano davvero che $G^{(\alpha)}$ è definito *per ogni* $\alpha \in A$.

Stabiliremo in seguito un sistema di indici che soddisfa alle proprietà desiderate; supponiamo di averlo definito e lo chiameremo On. Avvertiamo da subito che On risulterà una classe propria, non un insieme. Ovviamente, in ogni singolo caso pratico, sarà sempre possibile considerare come sistema di indici un *insieme* A contenuto in On.

Sotto queste ipotesi, possiamo definire:

$G^{(0)} = G$,

$G^{(\alpha+1)} = [G^{(\alpha)}, G^{(\alpha)}]$, e

$G^{(\alpha)} = \bigcap_{\beta<\alpha} G^{(\beta)}$, se α è *limite*, cioè se non ha un immediato predecessore, cioè ancora se non è della forma $\alpha = \beta + 1$, per qualche β.

Nella definizione precedente, $\beta < \alpha$ significa che β è un indice che è stato costruito, o considerato, prima di α; tutto questo verrà reso rigoroso in seguito.

Un gruppo *risolubile generalizzato* è un gruppo G tale che $G^{(\alpha)} = \{e\}$, per qualche $\alpha \in On$. I gruppi risolubili generalizzati costituiscono un'estensione molto ampia della classe dei gruppi risolubili. Un'introduzione all'argomento si può trovare nel libro di Robinson *Generalized solvable groups.*

Costruzioni analoghe alla precedente possono svolgersi in un ambito molto ampio: basta disporre di un oggetto iniziale X_0, avere una regola che definisce $X_{\alpha+1}$ ogni volta che si conosce X_α, e infine poter costruire X_α quando α non ha predecessori immediati; quest'ultima costruzione deve dipendere solo dagli X_β precedenti; solitamente, in questo "caso limite" X_α è l'intersezione (oppure l'unione) di tutti gli X_β precedenti[46].

---

[46] ** In realtà, le condizioni precedenti si possono sia unificare che generalizzare richiedendo che, per ogni α, X_α sia definito in funzione di tutti gli X_β, con β che precede α. Grossomodo, la differenza è simile alla differenza fra l'induzione "semplice" e l'induzione forte, cosiddetta "sul decorso dei valori". Rimandiamo a qualunque libro di teoria degli insiemi per i dettagli tecnici. In realtà questi dettagli, a nostro parere, illuminano l'idea principale, ma non sembrano comunque adatti per chi si stia avvicinando all'argomento.

Nell'esempio intuitivo precedente, quando ci siamo fermati a $G^{(\omega^2)}$, abbiamo considerato un insieme numerabile di indici. La costruzione può essere prolungata con insiemi di indici non numerabili, anzi, di qualunque cardinalità (assumendo l'assioma di scelta).

È invece molto significativo che la costruzione che presentiamo nella sottosezione seguente si stabilizza sempre dopo un numero finito oppure un'infinità numerabile di passi, anche se, sempre restando nel numerabile, la costruzione può risultare lunga a piacere.

2.1.2. *Il derivato di uno spazio topologico e cenni al teorema di Cantor-Bendixson.* [...] [Questa sottosezione non fa parte del programma del corso di Logica, AA 20-21] Per ora chi fosse interessato può guardare i Teoremi 4.5 e 4.6 del libro di Jech.

Storicamente questa costruzione sembra essere stata la prima in cui si fa uso di insiemi bene ordinati, anzi, sembra essere stata la motivazione principale di Cantor per introdurre la nozione di buon ordine.

2.1.3. *La gerarchia V_α di von Neumann.* Ricordiamo che abbiamo definito
$V_0 = \emptyset$,
$V_{n+1} = \mathcal{P}(V_n)$.
In questo modo abbiamo ottenuto una successione crescente (rispetto all'inclusione) di insiemi $(V_n)_{n\in\mathbb{N}}$. È quindi stato naturale definire
$V_\omega = \bigcup_{n\in\mathbb{N}} V_n$, e[47], iterando come sopra,
$V_{\omega+1} = \mathcal{P}(V_\omega) \dots$,
$V_{\omega+(n+1)} = \mathcal{P}(V_{\omega+n})$.
Abbiamo poi definito
$V_{\omega+\omega} = \bigcup_{n\in\mathbb{N}} V_{n+\omega}$.
Scriviamo per brevità $V_{\omega 2}$ al posto[48] di $V_{\omega+\omega}$. Possiamo continuare l'iterazione con
$V_{\omega 2+1} = \mathcal{P}(V_{\omega 2})$,
$V_{\omega 2+2} = \mathcal{P}(V_{\omega 2+1})$,
$V_{\omega 2+3} = \mathcal{P}(V_{\omega 2+2}) \dots$,
in generale,
$V_{\omega 2+(n+1)} = \mathcal{P}(V_{\omega 2+n})$.
Continuando, sia
$V_{\omega 3} = \bigcup_{n\in\mathbb{N}} V_{\omega 2+n}$ e, così via,
$V_{\omega m+n+1} = \mathcal{P}(V_{\omega m+n})$,
$V_{\omega(m+1)} = \bigcup_{n\in\mathbb{N}} V_{\omega m+n}$.
Ovviamente non siamo costretti a fermarci qui!
Possiamo definire
$V_{\omega^2} = \bigcup_{m\in\mathbb{N}} V_{\omega m}$,
e poi ancora

[47] ricordiamo che per costruire V_ω abbiamo avuto bisogno dell'assioma di rimpiazzamento.

[48] È convenzione (dovuta a motivi storici e di notazione che sarebbero lunghi da spiegare) scrivere $\omega 2$ (anziché 2ω) per $\omega + \omega$ etc.

$V_{\omega^2+1} = \mathcal{P}(V_{\omega^2})$, più in generale,
$V_{\omega^2+n+1} = \mathcal{P}(V_{\omega^2+n})$,
$V_{\omega^2+\omega} = \bigcup_{n\in\mathbb{N}} V_{\omega^2+n}$
e, così via, definire $V_{\omega^2+\omega m}$, $V_{\omega^2+\omega^2}$, che scriveremo $V_{\omega^2 2}$, e poi andando oltre, arriviamo a $V_{\omega^2 3}$, $V_{\omega^2 m}$, e $V_{\omega^3} = \bigcup_{m\in\mathbb{N}} V_{\omega^2 m}$ ...

Quanto a lungo possiamo iterare costruzioni di questo tipo? Dovrebbe essere abbastanza chiaro che l'unico problema è quello di trovare un appropriato insieme (ordinato) di indici (ma questo compito è tutt'altro che banale!). Per questo appropriato insieme di indici, diciamo, $\alpha \in A$, deve essere ben definito $V_{\alpha+1}$ ogni qual volta è definito V_α. Questo siginifca che l'ordine deve essere tale che, per ogni $\alpha \in A$, esiste il più piccolo elemento di A strettamente maggiore di α. Vista la somiglianza con la procedura classica di induzione su $n \in \mathbb{N}$, abbiamo chiamato questo elemento $\alpha + 1$.

Inoltre, dato un insieme $B \subseteq A$ di questi indici, se B non ha un massimo, deve esistere il più piccolo elemento α di A maggiore di tutti gli elementi di B. Quindi in questo caso α non ha nessun immediato predecessore (come, ad esempio, ω oppure $\omega+\omega$ nella costruzione precedente) e devo poter definire V_α in funzione solo dei V_β, con β che varia fra tutti gli elementi che "precedono" α.

Nell'esempio che stiamo trattando, in questo passo "limite" stiamo prendendo l'unione insiemistica, in altri casi si prende l'intersezione; in generale, si deve utilizzare qualche tipo di "limite".

Questo "sistema di indici" deve essere congegnato in modo che questo tipo di definizioni garantiscano davvero che V_α è definito *per ogni* $\alpha \in A$ e che la definizione di V_α non sia ambigua.

Stabiliremo in seguito un sistema di indici che soddisfa alle proprietà desiderate; supponiamo di averlo definito e lo chiameremo On. Avvertiamo da subito che On risulterà una classe propria, non un insieme. Gli elementi di On si chiamano ordinali. In altre parole, ammettendo la non contraddittorietà della nostra teoria degli insiemi, possiamo procedere con induzioni "transfinite" di questo tipo fino a che continuiamo ad avere insiemi e non classi proprie.

In generale, supponiamo di stare costruendo in questo modo una successione trasfinita di oggetti X_α. Può succedere, come nelle sezioni precedenti, che $X_{\alpha+1} = X_\alpha$, per qualche α, nel qual caso, a partire da α in poi la successione si stabilizza[49]. Se la successione non si stabilizza, come in questo caso (infatti se $\alpha < \beta$ allora V_α ha cardinalità strettemente minore di V_β, per il teorema di Cantor) allora l'oggetto "limite" finale diventa generalmente una classe propria.

[49]Naturalmente, qui stiamo supponendo che le nostre definizioni per induzione transfinita procedano in maniera sufficientemente "uniforme", per esempio che la condizione che ci porta da X_α ad $X_{\alpha+1}$ sia sempre la stessa, indipendentemente dal valore di α. Ad esempio, anche solo nel caso numerabile, potrebbe darsi che X_{n+1} sia definito in maniera diversa a seconda che n sia pari o dispari. In tal caso, potrebbe benissimo darsi che $X_n = X_{n+1}$ ma $X_{n+1} \neq X_{n+2}$. Inoltre, supponiamo che i nostri "limiti" non modifichino il valore di successioni costanti da un certo punto in poi.

Ovviamente, in ogni singolo caso pratico, sarà sempre possibile limitarsi a considerare come sistema di indici un *insieme* A contenuto in On.

Nel nostro caso, sempre supponendo di essere già riusciti ad introdurre un opportuno sistema di indici, possiamo definire:

$V_0 = \emptyset$,

$V_{\alpha+1} = \mathcal{P}(V_\alpha)$,

$V_\alpha = \bigcup_{\beta<\alpha} V_\beta$, se α è limite, cioè se non ha un immediato predecessore[50].

- si chiama gerarchia di von Neumann; [impredicativa...]

- l'assioma di fondazione è equivalente a dire che ogni insieme sta almeno in un V_α Simbolicamente, si scrive $V = \bigcup_{\alpha\in On} V_\alpha$, dove V è la classe di tutti gli insiemi e l'unione ha un significato simbolico, poiché $\{ V_\alpha \mid \alpha \in On \}$ è una classe propria, non un insieme.

Abbiamo visto che, usando l'assioma di fondazione nella forma dell'induzione insiemistica, nessun insieme appartiene a se stesso.

Anche senza bisogno dell'assioma di fondazione, si può dimostrare che nessun $x \in V$ è tale che $x \in x$. Supponiamo che esista $x \in V$ tale che $x \in x$, quindi $x \in V_\alpha$, per qualche ordinale α. Come vedremo, ogni sottoclasse non vuota della classe degli ordinali ha un minimo. Sia α il minimo ordinale tale che $x \in V_\alpha$ (questo ordinale si chiama il *rango* di x e la sua introduzione è molto utile). Per costruzione, α ha un immediato predecessore, diciamo, $\alpha = \beta + 1$, quindi $V_\alpha = \mathcal{P}(V_\beta)$. Da $x \in V_\alpha$ otteniamo $x \subseteq V_\beta$, ma se $x \in x$, allora $x \in V_\beta$. Questo contraddice l'ipotesi che α sia il minimo ordinale tale che $x \in V_\alpha$.

Grandi cardinali Abbiamo visto che V_ω e $V_{\omega+\omega}$ sono modelli per molti degli assiomi che stiamo considerando, ma non di tutti. Ricordiamo che la teoria che stiamo considerando è indicata con ZFC.

Ci si potrebbe chiedere se qualche V_α può essere un modello di tutta ZFC. Per il teorema di incompletezza di Gödel non si potrà mai dimostrare (in ZFC) l'esistenza di un tale α, perchè altrimenti ZFC dimostrerebbe la sua stessa non contraddittorietà.

Però, a priori, non si può escludere l'esistenza di un siffatto α. I cardinali α per cui V_α è un modello di ZFC sono (grossomodo) quelli che vengono chiamati *grandi cardinali*. Anche in questo caso, anche se introdotti per motivi astratti e puramente teorici, i grandi cardinali (se esistono) hanno influenze su proprietà dei livelli iniziali della gerarchia dei V_α, per esempio, hanno influenze su proprietà dei sottoinsiemi dei numeri reali.

2.1.4. *Iterare l'operazione di successore.* Ricordiamo che avevamo definito il successore $s(x)$ di un insieme x come $s(x) = x \cup \{x\}$. In particolare, abbiamo costruito i numeri naturali definendo $0 = \emptyset$ e $n+1 = s(n) = n \cup \{n\}$. Ricordiamo che questa definizione è delicata e le abbiamo potuto dare un senso preciso solo dopo l'introduzione dell'assioma dell'infinito. Con questa definizione ogni

[50] Ad essere precisi, per verificare che alcune delle definizioni precedenti sono equivalenti a quest'ultima va controllato che la sequenza dei V_α è crescente rispetto all'inclusione.

numero naturale n ha cardinalità n ed è l'insieme di tutti i numeri naturali più piccoli.

Possiamo iterare l'operazione di successore come negli esempi precedenti, utilizzando l'operazione di unione nel caso "limite" (intuitivamente questo è giustificato poiché vogliamo che qualunque insieme costruito in questo modo sia l'insieme di tutti gli oggetti "minori").

Quindi la definizione di successore generalizzato sarebbe la seguente:

$s_0 = \emptyset$,

$s_{\alpha+1} = s_\alpha \cup \{s_\alpha\}$,

$s_\alpha = \bigcup_{\beta<\alpha} s_\beta$, se α è limite.

Intuitivamente, un *ordinale* è un insieme che si può ottenere nel modo precedente iterando al transfinito l'operazione di successore. Per ogni ordinale, la relazione $\in$ è una relazione di ordine totale; infatti, ogni ordinale, come definito sopra, è l'insieme di tutti gli ordinali costruiti "in precedenza". In realtà, la classe degli ordinali sarà esattamente la classe degli indici appropriata per le iterazioni transfinite di cui abbiamo dato esempi in questa e nelle sottosezioni precedenti. Quindi sarebbe circolare dare la definizione di ordinale nel modo appena presentato. Può forse comunque essere intuitivamente utile.

In ogni caso possiamo dare esplicitamente la definizione dei primi ordinali. Gli ordinali finiti sono esattamente i numeri naturali, come definiti nella Sezione 1.2.5. Gli ordinali infiniti si indicano generalmente con lettere greche. L'insieme $\mathbb{N}$ dei numeri naturali è effettivamente un ordinale; per mantenere la notazione uniforme, nella teoria degli ordinali lo si indica con ω. Quindi ω ed $\mathbb{N}$, nelle nostre notazioni, sono lo stesso insieme.

Quindi, il primo ordinale infinito è $\omega = \mathbb{N}$, poi

$\omega + 1 = s(\omega) = \omega \cup \{\omega + 1\}$.

Come insieme ordinato $\omega+1$ è ottenuto da ω, cioè $\mathbb{N}$, aggiungendo un nuovo elemento maggiore di tutti i numeri naturali. Più in generale,

$\omega + (n + 1) = (\omega + n) + 1 = s(\omega + n) = (\omega + n) \cup \{\omega + n\}$, al variare di $n \in \mathbb{N}$:

in questo caso, ad $\mathbb{N}$ aggiungiamo $n + 1$ elementi tutti maggiori di ogni numero naturale. Continuando,

$\omega + \omega = \omega 2 = \bigcup_{n\in\mathbb{N}}(\omega + n)$,

come inieme ordinato è ottenuto prendendo due copie di $\mathbb{N}$ e considerando tutti gli elementi della seconda copia come maggiori di ogni elemento della prima copia. Proseguendo,

$\omega 2 + (n + 1) = (\omega 2 + n) + 1 = s(\omega 2 + n) = (\omega 2 + n) \cup \{\omega 2 + n\}$, per ogni $n \in \mathbb{N}$,

in generale, per $m > 1$,

$\omega m + (n + 1) = (\omega m + n) + 1 = s(\omega m + n) = (\omega m + n) \cup \{\omega m + n\}$, per ogni $n \in \mathbb{N}$.

$\omega(m + 1) = \bigcup_{n\in\mathbb{N}}(\omega m + n)$, per ogni $n \in \mathbb{N}$.

Come insieme ordinato, ωm è costituito da m copie di $\mathbb{N}$ ordinate "una dopo l'altra".

Come nella sezione precedente, possiamo definire ω^2 ($\mathbb{N}$ copie di $\mathbb{N}$ una dopo l'altra, vedremo in seguito che si pu ò considerare il prodotto di $\mathbb{N}$ per se stesso), ω^3 ($\mathbb{N}$ copie di ω^2 una dopo l'altra), e così via; in generale, possiamo definire l'ordinale $p(\omega)$, dove p è un "polinomio" a coefficienti in $\mathbb{N}$ (per convenzione, la moltiplicazione viene scritta in ordine inverso). Se $p(x) = x^i n_i + \cdots + x n_1 + n_0$, e $q = p + 1$, definiamo

$q(\omega) = s(p(\omega)) = p(\omega) \cup \{p(\omega)\}$;

Se $q(x) = x^i n_i + \cdots + x^j n_j$, con $j, n_j > 0$, allora

$q(\omega) = \bigcup_{m \in \mathbb{N}} (\omega^i n_i + \cdots + \omega^j (n_j - 1) + \omega^{j-1} m)$.

Fino ad ora non abbiamo costruito nulla per cui non si possa dare una trattazione elementare: gli ordinali costruiti finora si possono identificare con l'insieme dei polinomi in una variabile x e a coefficienti in $\mathbb{N}$, ordinati in modo tale che x viene considerato maggiore di qualunque numero (se si pensano i polinomi p e q come funzioni reali, $p > q$ in questo senso significa che $\lim_{x \to \infty}(p(x) - q(x)) = \infty$).

Ma, considerando gli ordinali, possiamo andare oltre: definiamo

$\omega^\omega = \bigcup_p p(\omega)$,

dove p varia fra tutti i polinomi come sopra. Per andare oltre sarebbe più conveniente definire delle operazioni di somma, prodotto ed esponente fra ordinali. Converrà farlo nel caso generale quando si considererà la classe di tutti gli ordinali. Comunque, esattamente come sopra, si possono definire $\omega^\omega + p(\omega)$, $\omega^\omega + \omega^\omega = \omega^\omega 2$, $\omega^\omega n$, $\omega^{\omega+1}$, eccetera, fino a ordinali che vengono indicati con ω^{ω^ω}, $\omega^{\omega^{\omega^\omega}}$, $\omega^{\omega^{\omega^{\omega^\omega}}}$, ... L'unione di tutti questi ordinali è il primo ordinale che non si può ottenere iterando le operazioni di somma, prodotto ed esponente, e viene indicato come ε_0.

Vedremo che ogni insieme non vuoto di ordinali ha un minimo (per come li abbiamo costruiti - per ora sempre a livelli intuitivo - dati due ordinali, uno dei due è contenuto nell'altro, quindi gli ordinali formano un ordine totale). Dato un ordinale α, la sua cardinalità $\beta = |\alpha|$ è il minimo fra gli ordinali β che possono essere messi in corrispondenza biunivoca con α (almeno un tale β esiste: ad esempio, α stesso). Mentre, per le proprietà di $\mathbb{N}$ che abbiamo enunciato, secondo questa definizione ogni $n \in \mathbb{N}$ è un cardinale, non tutti gli ordinali sono cardinali. Ad esempio, $\omega + 1 = \omega \cup \{\omega\}$ può essere messo in corrispondenza biunivoca con ω, quindi $|\omega + 1| = \omega$. In effetti, tutti gli ordinali costruiti finora sono numerabili, quindi, anche limitandoci al caso degli ordinali numerabili, esistono ordinali "relativamente grandi".

Assumendo l'assioma di scelta, che è equivalente al principio del buon ordinamento, ogni insieme può essere bene ordinato. Vedremo che ogni buon ordine è isomorfo ad un ordinale. Quindi, assumendo l'assioma di scelta, ad ogni insieme X può essere associato l'ordinale che rappresenta la sua cardinalità: l'ordinale α più piccolo tale che esiste un buon ordine su X isomorfo ad α.

2.2. Metodi per controllare che un programma termini dopo un numero finito di passi. [Questa sezione non fa parte del programma del corso di Logica, AA 20-21] Quando si lavora con numeri naturali, spesso si usa il fatto che non esistono successioni infinite strettamente decrescenti di numeri naturali.

Ad esempio, se si calcola il massimo comun divisore di due numeri naturali m ed n utilizzando l'algoritmo delle divisioni successive, si ottiene una successione[51] decrescente di resti. Questa successione dunque termina dopo un numero finito di passi, per quanto detto sopra, e ciò significa che prima o poi si ottiene un resto nullo (se il resto non fosse nullo il procedimento potrebbe continuare). L'algoritmo, che supponiamo noto al lettore, ci dice che l'ultimo resto non nullo è il massimo comun divisore dei due numeri dati[52].

Considereremo adesso dei programmi in cui, in alcuni passi, può essere richiesto all'utilizzatore di inserire numeri naturali arbitrari. Ogni passo del programma, generalmente, viene effettuato scegliendo una fra due o più opzioni. La modalità in cui viene effettuata questa scelta non ci interessa, può essere effettuata dall'utilizzatore, o dipendere da un qualche stato interno della macchina, o anche semplicemente essere effettuata in base ad una scelta casuale. Vogliamo però che il programma termini *sempre* dopo un numero finito (anche se arbitrario, cioè non prefissato in partenza) di passi, qualunque siano i numeri inseriti dall'utilizzatore, e in qualunque modo venga effettuata la scelta fra le eventuali opzioni ad ogni passo.

Un esempio è il seguente:

(a) All'inizio il programma chiede all'utilizzatore di inserire due numeri naturali a e b.

(b) Ad ogni passo successivo il programma esegue una delle seguenti due operazioni[53]:

$a \mapsto a + 1$ e $b \mapsto b - 2$, oppure

$a \mapsto a - 2$ e $b \mapsto b + 1$.

(c) Il programma termina se almeno uno fra a e b assume un valore strettamente negativo. Altrimenti una delle operazioni in (b) viene eseguita nuovamente.

Questo programma prima o poi termina, poiché la funzione $\rho(a, b) = a + b$ assume sempre valori naturali e decresce strettamente ad ogni passo (a rigore

---

[51] Per comodità in questa sezione *successione* può significare sia successione numerabile nel senso usuale in matematica, sia una successione finita, cioè una n-upla ordinata di oggetti, per qualche $n \in \mathbb{N}$.

[52] Ci sembra importante osservare che la divisione con resto è possibile per numeri reali arbitrari t ed s. Dati tali t ed $s \neq 0$ reali esistono e sono unici $q \in \mathbb{Z}$ ed $r \in \mathbb{R}$ tali che $t = qs + r$ e $0 \leq r < |s|$. Ma, nel caso di numeri reali, l'algoritmo delle divisioni successive non sempre termina. Il lettore saprebbe precisare quali sono i casi in cui termina?

[53] Qui quando scriviamo, ad esempio, $a \mapsto a + 1$, intendiamo che il programma *assegna* alla variabile a il valore precedente aumentato di 1. Siccome questo è un lavoro rivolto anche ai matematici, si creerebbero troppe ambiguità usando a questo scopo invece il simbolo $=$, come avviene in molti linguaggi di programmazione.

$\rho(a, b)$ potrebbe assumere valori interi negativi, ma allora almeno uno fra a e b è negativo, e questo implica che il programma termina). Che un programma del tipo precedente prima o poi termini non è affatto scontato, in generale. Se avessimo invece considerato la seguente condizione (b*) al posto di (b):

(b*) Ad ogni passo successivo il programma esegue una delle seguenti due operazioni:
$a \mapsto a + 1$ e $b \mapsto b - 1$
oppure
$a \mapsto a - 1$ e $b \mapsto b + 1$

allora vi sono situazioni in cui il programma può continuare all'infinito senza fermarsi. Ad esempio, basta scegliere $a > 0$ e $b > 0$ ed eseguire alternativamente le due opzioni.

Altro esempio:

(b**) Ad ogni passo il programma esegue una delle seguenti operazioni:
$a \mapsto a + 1$ e $b \mapsto b - 2$
oppure
$a \mapsto a - 1$ e $b \mapsto b + 1$

Questo programma termina sempre, poiché $\rho(a, b) = 3a + 2b$ è strettamente decrescente ad ogni passo. Osserviamo che in questo caso la funzione $\rho(a, b) = a + b$ non sarebbe servita, poiché non *strettamente* devrescente.

Esistono però situazioni in cui la dimostrazione che il programma termina è più complessa. Consideriamo il seguente esempio (le condizioni (a) e (c) restano sempre invariate).

(b***) Ad ogni passo il programma esegue una delle seguenti operazioni:
$a \mapsto a - 1$ e b viene sostituito da un numero positivo qualunque,
oppure
a resta invariato e $b \mapsto b - 1$.

È intuitivo che questo programma prima o poi termina, poiché a non può mai crescere, e prima o poi deve calare, perché nel caso in cui a resti invariato è b che decresce. Ma in questo caso si può dimostrare che non esiste una funzione $\rho(a, b)$ strettamente decrescente ad ogni passo e *a valori in* $\mathbb{N}$.

Per dimostrare che questo programma prima o poi termina conviene considerare le coppie di numeri naturali col seguente *ordine lessicografico*:

$$(a, b) < (a', b') \text{ se e solo se } \begin{cases} a = a' \text{ e } b < b', \text{ oppure} \\ a < a'. \end{cases}$$

Si può verificare (e lo faremo nella prossima sottosezione) che, con quest'ordine, non esistono successioni infinite strettamente decrescenti di coppie in $\mathbb{N} \times \mathbb{N}$. In questo caso la funzione ρ che serve per dimostrare che il programma termina è la funzione identica su $\mathbb{N} \times \mathbb{N}$.

Concludiamo con un esempio più sofisticato.

(a′) Lo stato del programma è dato da una lista finita F di coppie di numeri naturali. All'inizio la lista F è vuota. Intuitivamente F rappresenta una lista di coppie "vietate"; inoltre, se (c, d) è una coppia vietata, allora anche tutte le coppie (a, b) con $a \geq c$ e $b \geq d$ sono "vietate". NB: il $\geq$ deve valere per *entrambe* le componenti.

(b′) Ad ogni passo il programma chiede all'utilizzatore di inserire una coppia (a, b) di numeri naturali.

(c′) Il programma confronta la coppia (a, b) inserita dall'utilizzatore con le coppie già presenti in F. Se esiste una coppia (c, d) nella lista F tale che $a \geq c$ e $b \geq d$, il programma termina. Altrimenti il programma aggiunge la coppia (a, b) ad F e si ripete il passo (b').

Questo programma termina sempre in qualunque modo l'operatore inserisca i dati? Se sì, in che modo lo si può verificare?

Chi desiderasse più informazioni sul problema della verificabilità dei programmi, può consultare Z. Manna, *Mathematical Theory of Computation*, 1974, trad. it. *Teoria matematica della computazione*, 1978.

2.3. Insiemi bene ordinati.

Definizione 2.1. Si dice che un insieme totalmente ordinato $\langle W, < \rangle$ è un *buon ordine*, o che W è *bene ordinato (da $<$)* se ogni sottoinsieme non vuoto di W ha un minimo (secondo l'ordine $<$). Come d'uso, se non vi è possibilità di equivoci, scriveremo W al posto di $\langle W, < \rangle$.

Osservazione 2.2. I buoni ordini sono gli insiemi appropriati per eseguire le induzioni trasfinite di cui abbiamo dato esempi nella sezione precedente. Verifichiamolo in maniera informale.

Ad esempio, avevamo annunciato che la seguente è una possibile definizione della gerarchia di von Neumann:

$V_0 = \emptyset$,

$V_{\alpha+1} = \mathcal{P}(V_\alpha)$,

$V_\alpha = \bigcup_{\beta<\alpha} V_\beta$, se α è limite, cioè se non ha un immediato predecessore.

Facciamo variare α su un insieme bene ordinato non vuoto A, dove 0 è il minimo di A (il minimo esiste perchè A è un sottoinsieme non vuoto di A e A stesso è bene ordinato). Inoltre, se $\alpha \in A$ e α non è il massimo di A, l'insieme $\{\, \beta \in A \mid \alpha < \beta \,\}$ è non vuoto, quindi ha un minimo, che è l'immediato successore di α, chiamiamo questo minimo $\alpha + 1$.

La definizione precedente ci fornisce davvero un insieme V_α, per ogni $\alpha \in A$. Supponiamo per assurdo che questo non sia vero, quindi esiste $\beta \in A$ tale che V_β non è definito. Siccome A è bene ordinato, esistera il minimo fra tali β. Ma questo β non può essere 0, perchè la prima riga nella definizione precedente ci definisce V_0. Se β ha un immediato predecessore α, allora V_α è definito, per la scelta di β. Ma allora, secondo le nostre convenzioni, $\beta = \alpha + 1$ e la seconda riga ci fornisce la definizione di V_β. Resta il caso in cui β è diverso da 0 e non ha un immediato predecessore. Ma in questo caso la terza riga

(con α e β scambiati) ci definisce V_β. In ciascun caso abbiamo ottenuto una contraddizione, quindi V_α è effettivamente definito, per ogni $\alpha \in A$.

Allo stesso modo si "dimostra" che la definizione è ben posta, cioè che la successione $(V_\alpha)_{\alpha\in A}$ è unica. Infatti, se ce ne fosse un'altra diversa $(U_\alpha)_{\alpha\in A}$ che soddisfa alla stessa definizione, consideriamo il più piccolo $\alpha \in A$ tale che $V_\alpha \neq U_\alpha$. Ragionando per casi come nel paragrafo precedente otteniamo un assurdo.

Naturalmente, il ragionamento che abbiamo fatto è abbastanza informale. Per renderlo pienamente rigoroso bisognerebbe giustificare la possibilità della ricorsione transfinita in un modo simile a quello accennato nella nota 40 (e usando di nuovo l'assioma di rimpiazzamento).

Se W è bene ordinato $w \in W$, definiamo l'insieme $w^\downarrow$ come $w^\downarrow = \{v \in W \mid v < w\}$. L'insieme $w^\downarrow$ è dotato di una struttura di ordine totale indotta da W, ed è immediato vedere che anche $w^\downarrow$ è un buon ordine. I sottoinsiemi di W della forma $w^\downarrow$ si dicono *segmenti iniziali (propri)* di W.[54]

NB: nella precedente definizione ammettiamo la possibilità che W oppure $w^\downarrow$ siano l'insieme vuoto. Del resto, se W è bene ordinato e $W \neq \emptyset$, essendo W sottoinsieme di se stesso, lo stesso W ha un minimo w. Ma allora in questo caso $w^\downarrow$ è l'insieme vuoto.

Ogni insieme finito (e totalmente ordinato) è ovviamente bene ordinato[55]. Vediamo adesso che esistono buoni ordini infiniti.

Proposizione 2.3. *N (con l'ordine usuale) è bene ordinato.*

Dimostrazione. Sia $X \subseteq \mathbb{N}$ e $X \neq \emptyset$. Quindi $n \in X$ per qualche $n \in \mathbb{N}$. Allora $\{0, 1, \ldots, n-1, n\} \cap X$ è finito e non vuoto, quindi ha un minimo, che è anche il minimo di X, poiché $n \in X$. □

Proposizione 2.4. *Se W è bene ordinato, allora non esiste una successione infinita (ad indici in $\mathbb{N}$) strettamente decrescente di elementi di W.*[56]

Dimostrazione. Supponiamo per assurdo che esista una tale successione $(w_n)_{n\in\mathbb{N}}$. L'insieme $X = \{w_n \mid n \in \mathbb{N}\}$ è un sottoinsieme non vuoto di W, quindi ha un minimo, visto che W è bene ordinato. Sia w_n il minimo di X. Dall'ipotesi che $(w_n)_{n\in\mathbb{N}}$ è strettamente decrescente, otteniamo $w_{n+1} < w_n$; ma $w_{n+1} \in X$, e questo contraddice l'assunzione che w_n sia il minimo di X. □

---

[54] ** Alcuni testi considerano W stesso come segmento iniziale (improprio) di W. In questa nota *segmento iniziale* avrà sempre il significato di segmento iniziale *proprio*.

[55] Ad essere pignoli, si deve dimostrare che se W è totalmente ordinato e un sottoinsieme X non vuoto è finito, allora X ha un minimo. Il minimo fra due elementi di W esiste perchè W è totalmente ordinato. Se X è finito, allora per definizione X è in corrispondenza biunivoca con qualche $n \in \mathbb{N}$. L'affermazione desiderata si ottiene per induzione su $n \geq 1$.

[56] ** In realtà la proposizione fornisce una condizione equivalente, ma l'altra implicazione utilizza una forma dell'assioma di scelta. Supponiamo che W non sia bene ordinato, quindi esiste un sottoinsieme X non vuoto senza un minimo. Siccome X è non vuoto, esiste $x_1 \in X$. Per ipotesi x_1 non è il minimo di X, quindi esiste $x_2 \in X$ tale che $x_2 < x_1$. Ma neanche x_2 può essere il minimo di X, quindi iterando la costruzione si ottiene una successione strettamente decrescente di elementi di X, quindi anche di W.

$\mathbb{N}$ non è l'unico insieme infinito bene ordinato. Supponiamo che W sia bene ordinato, consideriamo un "nuovo" elemento $u \notin W$, e ordiniamo $W \cup \{u\}$ in modo che u sia maggiore di tutti gli elementi di W. Con questo ordine, $W \cup \{u\}$ è bene ordinato (perchè?). Faremo presto vedere che W e $W \cup \{u\}$ non sono mai isomorfi (che W e $W \cup \{u\}$ non siano isomorfi è intuitivamente ovvio nel caso in cui W è finito).

Osserviamo che non è affatto scontato che W e $W \cup \{u\}$ non siano isomorfi. Infatti possiamo compiere una costruzione simile quando W è un ordine totale qualunque, non necessariamente bene ordinato. Se $W = \mathbb{Z}^-$, l'insieme dei numeri interi negativi (o anche N con l'ordine inverso), allora $W \cup \{u\}$ è isomorfo a W.

2.3.1. *Confrontabilità di buoni ordini.*

Proposizione 2.5. *Se W è bene ordinato e $w^\downarrow$ è un suo segmento iniziale, allora W e $w^\downarrow$ non sono isomorfi.*

Dimostrazione. Supponiamo per assurdo che $f : W \to w^\downarrow$ sia un isomorfismo. Siccome $w \in W$, il valore $f(w)$ è definito, e inoltre $f(w) \in w^\downarrow$, cioè $f(w) < w$. Quindi $X = \{v \in W \mid f(v) < v\}$ è non vuoto. Siccome W è bene ordinato, X ha un minimo v. Siccome $v \in X$, abbiamo $f(v) < v$. Siccome f è un isomorfismo, abbiamo anche $f(f(v)) < f(v)$. Ma allora $z = f(v)$ è tale che $f(z) < z$ e inoltre $z < v$. Questo contraddice l'assunzione che v è il minimo di X, e abbiamo ottenuto l'assurdo desiderato. □

Teorema 2.6. *Se W e V sono insiemi bene ordinati, allora si verifica una (ed una sola) delle seguenti condizioni.*

(1) W e V sono isomorfi;
(2) W è isomorfo ad un segmento iniziale di V;
(3) V è isomorfo ad un segmento iniziale di W.

Dimostrazione. Le condizioni sono incompatibili fra di loro. Ad esempio, supponiamo che valgano sia (2) che (3). Sia W isomorfo ad un segmento iniziale $v^\downarrow$ di V, come dato da (2), e sia f un isomorfismo da V ad un segmento iniziale di W, come dato da (3), e sia $w = f(v)$. L'isomorfismo f chiaramente induce un isomorfismo f' da $v^\downarrow$ a $w^\downarrow$. Componendo l'isomorfismo dato da (2) con f' otterremmo un isomorfismo fra W e $w^\downarrow$, assurdo per la Proposizione 2.5.

Le incompatibilità fra (1) e (2) e fra (1) e (3) si dimostrano in maniera simile e più semplice.

Dimostriamo adesso che almeno una delle condizioni si presenta. Si consideri la seguente relazione $R \subseteq W \times V$:

$$R = \{(w, v) \in W \times V \mid w^\downarrow \text{ e } v^\downarrow \text{ sono isomorfi } \},$$

che esiste (come insieme) per l'assioma di rimpiazzamento. Abbiamo che l'inversa di R è univoca, cioè che se $(w, v) \in R$ e $(w_1, v) \in R$, allora $w = w_1$. Infatti, se fosse $w \neq w_1$, avremmo che $w > w_1$ oppure $w_1 > w$, siccome W è

totalmente ordinato. Se, ad esempio, $w > w_1$, allora, componendo l'isomorfismo dato da $(w, v) \in R$ con l'inverso dell'isomorfismo dato da $(w_1, v) \in R$, avremmo che $w^{\downarrow}$ sarebbe isomorfo a $w_1^{\downarrow}$, un suo segmento iniziale, e questo è impossibile per la Proposizione 2.5..

In maniera simmetrica abbiamo che R è univoca, cioè che se $(w, v) \in R$ e $(w, v_1) \in R$, allora $v = v_1$.

Inoltre, se $(w, v) \in R$ e $w_1 < w$, esiste $v_1 \in V$ tale che $(w_1, v_1) \in R$ e $v_1 < v$. Infatti, se f è l'isomorfismo dato da $(w, v) \in R$ e $v_1 = f(w_1)$, allora f induce un isomorfismo da $w_1^{\downarrow}$ a $v_1^{\downarrow}$.

Dalle considerazioni precedenti segue che, se $D = \{w \in W \mid$ esiste un $v \in V$ tale che $(w, v) \in R\}$ è il dominio di R e $C = \{v \in V \mid$ esiste un $w \in W$ tale che $(w, v) \in R\}$ è il codominio di R, allora

(*) R definisce un isomorfismo da D a C.

Dimostriamo adesso che almeno una delle seguenti due condizioni si verifica: o D è tutto W, oppure C è tutto V.

Infatti, se nessuna delle due condizioni si verifica, allora $W \setminus D$ e $V \setminus C$ sono entrambi non vuoti. Siccome W e V sono buoni ordini, esistono un minimo s di $W \setminus D$ ed un minimo t di $V \setminus C$. Quindi $D = s^{\downarrow}$ e $C = t^{\downarrow}$, perchè abbiamo dimostrato che se $w \in D$, allora $w^{\downarrow} \subseteq D$, e la condizione simmetrica vale per C. Ma allora, per (*), $(s, t) \in R$, ma questo contraddice $s \in W \setminus D$.

Quindi $D = W$, oppure $C = V$, oppure entrambi. Se si verificano entrambe le condizioni, R è un isomorfismo da W su V. Altrimenti, nel primo caso R è un isomorfismo da W su un segmento iniziale di V e nel secondo caso R è un isomorfismo da un segmento iniziale di W su V. □

2.3.2. *Somme e prodotti di buoni ordini.* Se $(W, <_W)$ e $(V, <_V)$ sono buoni ordini e W e V sono disgiunti, allora $Z = W \cup V$ diventa un buon ordine rispetto alla relazione $<_Z$ definita da

$$s <_Z t \text{ se e solo se } \begin{cases} s <_W t \text{ e } s, t \in W, \text{ oppure} \\ s <_V t \text{ e } s, t \in V, \text{ oppure} \\ s \in W \text{ e } t \in V. \end{cases}$$

Intuitivamente, tutti gli elementi di V vengono "messi in cima", cioè considerati maggiori di qualunque elemento di W. Lasciamo per esercizio al lettore di dimostrare che, se W e V sono buoni ordini disgiunti, allora anche $W \cup V$ è un buon ordine. Nel caso W e V non fossero disgiunti, la costruzione precedente si può sempre effettuare (a meno di isomorfismo) considerando al posto di V un buon ordine V' isomorfo a V.

Prendendo V non vuoto otteniamo dal Teorema 2.6 che per ogni buon ordine W esiste un buon ordine strettamente maggiore, fatto a cui avevamo già accennato in precedenza, sostanzialmente considerando la stessa costruzione nel caso in cui V aveva un solo elemento.

Se W e V sono buoni ordini, si può definire l'*ordine lessicografico*[57] su $W \times V$ nel seguente modo:

$$(w, v) < (w', v') \text{ se e solo se } \begin{cases} w < w', \text{ oppure} \\ w = w' \text{ e } v < v'. \end{cases}$$

Proposizione 2.7. *Se W e V sono buoni ordini, allora $W \times V$, dotato dell'ordine lessicografico, è un buon ordine.*

Dimostrazione. Lasciamo per esercizio al lettore di verificare che $W \times V$ è un ordine totale. Sia $X \subseteq W \times V$ e X non vuoto. Allora $A = \{w \in W \mid \text{ esiste } v \in V \text{ tale che } (w, v) \in X\}$ è un sottoinsieme non vuoto di W, dunque A ha un minimo a. Anche $\{v \in V \mid (a, v) \in X\}$ è non vuoto, dunque ha un minimo b.

Dalla definizione dell'ordine lessicografico segue che (a, b) è il minimo di X. □

Queste definizioni di somma e prodotto di buoni ordini giustificano le notazioni che abbiamo usato nella sezione 2.1.4. Ad esempio, l'ordinale $\omega + \omega$ è isomorfo alla somma di due ordinali isomorfi ciasuno ad $\omega = \mathbb{N}$. Nel caso del prodotto, per problemi di convenzioni e notazioni, l'ordine dei fattori va invertito. Ad esempio, $\omega 2 = \omega + \omega$ è isomorfo al prodotto lessicografico di $2 = \{0, 1\}$ per ω. Gli elementi di questo prodotto sono, infatti, in ordine,

$(0,0), (0,1), (0,2), (0,3), \ldots (0,n), \ldots \quad (1,0), (1,1), (1,2), (1,3), \ldots (1,n), \ldots$

Al contrario, gli elementi del prodotto lessicografico di ω per $2 = \{0, 1\}$ sono

$(0,0), (0,1), (1,0), (1,1), (2,0), (2,1), \ldots$

che è quindi isomorfo ad $\mathbb{N} = \omega$. Qundi il prodotto di buoni ordini non è commutativo (nemmeno a meno di isomorfismi). Neppure la somma è commutativa, ad esempio, $1 + \omega \cong \omega \ncong \omega + 1$.

2.3.3. *Cenni agli ordinali.* Un insieme A si dice *transitivo* se $x \in y \in A$ implica $x \in A$. Equivalentemente, A è transitivo se ogni elemento di A è un sottoinsieme di A. Un *ordinale* è un insieme transitivo e bene ordinato dalla relazione di appartenenza. Intuitivamente, gli ordinali si costruiscono iterando l'operazione di successore e prendendo unioni nel caso limite, come abbiamo accennato in 2.1.4, ma usare quella costruzione per definire gli ordinali necessiterebbe di parecchi dettagli aggiuntivi e comunque non è l'approccio usuale.

Si può dimostrare, ma la dimostrazione è delicata, che ogni buon ordine è isomorfo ad un ordinale, quindi gli ordinali possono essere presi come rappresentanti delle classi di equivalenza dei buoni ordini rispetto alla relazione di isomorfismo.[58]

Si dimostra abbastanza facilmente che l'unione di un insieme di ordinali è ancora un ordinale, e che ogni ordinale è l'insieme degli ordinali precedenti (gli

[57] Essenzialmente, l'ordine "alfabetico" che si usa in un vocabolario.

[58] In questo caso sarebbe stato problematico costruire il quoziente, poiché le classi di equivalenza non sono insiemi, ma classi proprie.

ordinali sono confrontabili fra di loro per il Teorema 2.6). Quindi ogni classe non vuota X di ordinali ha un minimo (se $\alpha \in X$ e α non è il minimo di X, $\alpha \cap X$ è un sottoinsieme non vuoto di α, dunque ha un minimo, che è anche il minimo di X). Quindi intuitivamente la *classe* di tutti i buoni ordini è bene ordinata, ma non può essere considerata un insieme, perchè abbiamo visto che per ogni insieme bene ordinato ne esiste uno strettamente maggiore. Questo è il paradosso di Burali-Forti[59]. Nella teoria degli insiemi moderna questo non è più un paradosso, semplicemente dimostra che non esiste un insieme che contiene tutti gli ordinali (così come il contenuto del paradosso di Russell diventa che non esiste un insieme che contiene tutti gli insiemi).

Gli ordinali diversi da zero si dividono in due tipi: quelli che hanno un immediato predecessore, e quelli che sono unione di ordinali strettamente più piccoli (questi ultimi si chiamano *ordinali limite*.) In quanto insiemi bene ordinati, gli ordinali successore corrispondono a insiemi ordinati con un massimo, gli ordinali limite ad insiemi ordinati senza massimo. Ad esempio, tutti gli ordinali finiti diversi da zero sono successori, ω è limite, gli $\omega + n$ con $n > 0$ sono successori, $\omega + \omega$ è limite, e così via.

2.3.4. *Alcuni cardinali.* Si può dimostrare che l'assioma di scelta è equivalente all'assunzione che ogni insieme è bene ordinabile. Quindi, se si accetta l'assioma di scelta, si può definire la *cardinalità* di un insieme Y come il più piccolo ordinale α che può essere posto in biiezione con Y, e si scrive $|Y| = \alpha$. Gli ordinali ottenibili in questo modo si chiamano *cardinali* e sono solo una piccola parte di tutti gli ordinali (perchè? Considerate ad esempio il caso degli ordinali numerabili...)

Avendo identificato i numeri cardinali con una sottoclasse dei numeri ordinali, possiamo enumerare, di nuovo per ricorsione, i cardinali infiniti. Poniamo:

$\aleph_0 = \omega$;

$\aleph_{\alpha+1}$ = il più piccolo cardinale strettamente maggiore di $\aleph_\alpha$ = il più piccolo ordinale β tale che non esiste una funzione iniettiva da $\aleph_\alpha$ in β;

$\aleph_\alpha = \sup_{\beta<\alpha} \aleph_\beta$, se α è un ordinale limite (qui stiamo usando sup al posto di $\bigcup$; questo è giustificato dal fatto che gli ordinali formano una classe totalmente ordinata e l'unione in senso insiemistico corrisponde a prendere il sup nel senso dela teoria degli insiemi ordinati).

dove almeno un β come nella seconda riga esiste (per esempio, un qualunque ordinale che possa essere messo in biiezione con $\mathcal{P}(\aleph_\alpha)$; naturalmente, stiamo assumendo l'assioma di scelta[60]).

Un'altra funzione che genera cardinali infiniti è ottenuta definendo

[59] Che comunque non si era reso conto delle conseguenze paradossali del suo argomento.

[60] Hartogs ha comunque dimostrato, senza bisogno dell'assioma della scelta, che, per ogni insieme X, esiste il più piccolo ordinale γ tale che non c'è una funzione iniettiva da γ ad X. Questo giustifica la definizione di $\aleph_\alpha$ nella seconda riga. Quindi la classe degli $\aleph_\alpha$ può essere definita anche senza l'uso dell'assioma di scelta. Senza scelta, però, esistono cardinali che non sono degli $\aleph_\alpha$ o, meglio, la nozione di cardinalità va definita in altro modo.

$\beth_0 = \omega$;
$\beth_{\alpha+1} = |\mathcal{P}(\beth_\alpha)|$,
$\beth_\alpha = \sup_{\beta<\alpha} \beth_\beta$, se α è un ordinale limite.

L'ipotesi che $\aleph_\alpha = \beth_\alpha$, per ogni ordinale α è detta *ipotesi generalizzata del continuo*. Afferma[61] che non c'è nessuna cardinalità strettamente intermedia fra $\aleph_\alpha$ e $|\mathcal{P}(\aleph_\alpha)|$.

Anche senza assumere l'assioma della scelta si può enunciare l'ipotesi generalizzata del continuo: per ogni insieme infinito X e ogni insieme $Y \subseteq \mathcal{P}(X)$, esiste una biiezione fra Y e $\mathcal{P}(X)$, oppure una funzione iniettiva da Y a X (variazioni dell'enunciato sono possibili). In particolare, l'ipotesi del continuo dice che ogni sottoinsieme di $\mathbb{R}$ è finito, numerabile, oppure ha la stessa cardinalità di $\mathbb{R}$.

Come hanno dimostrato Gödel e Cohen, gli assiomi di Zermelo-Fraenkel (se non contraddittori) sono compatibili sia con l'ipotesi (generalizzata) del continuo, che con la sua negazione. Si dice spesso che l'ipotesi del continuo (allo stesso modo dell'assioma di scelta) è indecidibile, ma questa espressione ha un significato nettamente diverso dall'indecidibilità data dai teoremi di incompletezza di Gödel-Rosser. Nel secondo caso si tratta di una forma di indecidibilità irrimediabile: qualunque teoria, sotto le ipotesi del teorema di incompletezza, ha un'enunciato indecidibile; possiamo aggiungere questo enunciato alla teoria, ma otterremo un nuovo enunciato indecidibile. Nel caso invece dell'ipotesi del continuo o dell'assioma di scelta, spetta semplicemente a chi utilizza la teoria di decidere se accettare o meno l'ipotesi. A riguardo, Gödel ha proposto di cercare assiomi "naturali", "evidenti", "intuitivamente validi" o quanto meno "intuitivamente accettabili" e che possano decidere l'ipotesi del continuo. Questa proposta informale, che va sotto al nome di "Programma di Gödel", ha portato allo studio di molte proprietà interessanti, anche se non c'è consenso unanime sulla realizzabilità o meno di questo programma.

Tornando agli aleph $\aleph_\alpha$, si vede che non tutti i cardinali si comportano allo stesso modo. Per esempio, $\aleph_\omega$ è una unione numerabile di cardinali strettamente minori. Un cardinale infinito $\aleph_\alpha$ si dice *singolare* se è una unione di una famiglia di cardinalità $< \aleph_\alpha$ composta di insiemi tutti di cardinalità $< \aleph_\alpha$. Quindi $\aleph_\omega$ è un cardinale singolare. Usando l'assioma di scelta si dimostra che, al contrario, ogni cardinale "successore"[62] del tipo $\aleph_{\alpha+1}$ è sempre regolare, cioè non singolare. Un cardinale si dice limite se è del tipo $\aleph_\alpha$ con α ordinale limite oppure 0.

---

[61] Se $\aleph_\alpha = \beth_\alpha$, per ogni ordinale α, allora non ci sono mai cardinalità intermedi fra $\aleph_\alpha$ e $|\mathcal{P}(\aleph_\alpha)|$. Viceversa, se per nessun α ci sono cardinalità intermedie fra $\aleph_\alpha$ e $|\mathcal{P}(\aleph_\alpha)|$, supponiamo per assurdo che esista un α tale che $\aleph_\alpha \neq \beth_\alpha$. Siccome la classe degli ordinali è bene ordinata, possiamo scegliere il più piccolo α tale che $\aleph_\alpha \neq \beth_\alpha$. Se α è limite otteniamo subito una contraddizione dalle definizioni di $\aleph_\alpha$ e $\beth_\alpha$. Se α è successore, diciamo, $\alpha = \beta+1$, l'ipotesi che non ci sono cardinalità intermedi fra $\aleph_\beta$ e $|\mathcal{P}(\aleph_\beta)|$ implica $\aleph_\alpha = \beth_\alpha$, di nuovo una contraddizione.

[62] Osserviamo che, invece, in quanto ordinali, tutti i cardinali infiniti sono ordinali limiti.

2.3.5. *Cardinali inaccessibili.* [Da questo punto in poi tutti gli argomenti sono facoltativi, in riferimento al corso di Logica dell'AA 2020-21] Può esistere un cardinale limite regolare $> \aleph_0$? Questi cardinali si chiamano (debolmente) inaccessibili. Questa possibilità era già stata considerata da Hausdorff e altri fin dagli albori della teoria degli insiemi. Se esiste un tale cardinale, allora è possibile costruire un modello[63] di ZF, quindi, per il teorema di incompletezza di Gödel, non potrà mai essere dimostrata l'esistenza di un cardinale di questo tipo.

Vediamo che un cardinale inaccessibile deve essere "molto grande". Il primo cardinale limite non numerabile è $\aleph_\omega$, che non è inaccessibile. Ma $\aleph_\omega$ è anche un ordinale, quindi possiamo considerare il cardinale $\aleph_{\aleph_\omega}$, che è unione di un famiglia di cardinalità $\aleph_\omega$ di cardinali minori (quindi $\aleph_{\aleph_\omega}$ non è inaccessibile). Nessun cardinale limite $< \aleph_{\aleph_\omega}$ è inaccessibile, perchè comunque unione di meno di $\aleph_\omega$ cardinali minori. Così via, il primo cardinale inaccessibile, se esiste, deve essere maggiore di $\aleph_{\aleph_\omega}$, di $\aleph_{\aleph_{\aleph_\omega}}$, di $\aleph_{\aleph_{\aleph_{\aleph_\omega}}}$ ... Sia θ_0 l'unione di tutti i cardinali precedenti. Allora θ_0 è il primo cardinale tale che $\alpha = \aleph_\alpha$.

Continuando allo stesso modo, esiste θ_1, il secondo cardinale tale che $\alpha = \aleph_\alpha$, e θ_1 è minore del primo inaccessibile, se esiste. Al solito modo, possiamo definire una successione trasfinita di cardinali θ_α. Considerando la successione θ_α, θ_{θ_α}, $\theta_{\theta_{\theta_\alpha}}$ ... otteniamo un cardinale tale che $\alpha = \theta_\alpha$ e nemmeno questo è inaccessibile (è addirittura unione numerabile di cardinali precedenti). Questo argomento, prolungabile a piacere[64], dimostra che un cardinale inaccessibile, se esiste, è molto più grande di tutti i cardinali precedenti (e merita dunque l'appellativo di "grande cardinale"!) Ma vedremo fra poco cardinali ancor più "grandi"!

2.3.6. *Il modello di Solovay.* I cardinali inaccessibili sono coinvolti in un risultato stupefacente di Solovay e Shelah.

È un risultato classico attribuito a Vitali che esistono sottoinsiemi di $\mathbb{R}$ non misurabili secondo Lebesgue. La teoria di Lebesgue estende la teoria di Riemann (per integrazione, misura, etc.) e dal punto di vista matematico è molto più soddisfacente. È facile dare l'esempio di una funzione (diciamo, limitata su un intervallo reale limitato) che non sia integrabile secondo Riemann, mentre non è del tutto scontato trovare una funzione non integrabile secondo Lebesgue. Questo è il succo del teorema di Vitali.

Il risultato di Vitali necessita però dell'assioma di scelta. Nel 1970 Solovay ha dimostrato che, se ZFC più l'esistenza di un cardinale inaccessibile è non contraddittoria, allora è non contraddittoria anche la teoria ZF più l'assunzione che ogni sottoinsieme di $\mathbb{R}$ è misurabile secondo Lebesgue. Succesivamente

[63]Un cardinale κ si dice *fortemente limite* se $\lambda < \kappa$ implica $|\mathcal{P}(\lambda)| < \kappa$. Se κ è inaccessibile e fortemente linite, allor V_κ è un modello di ZF. Altrimenti, per chi conosce la gerarchia di Gödel degli insiemi costruibili, senza l'ipoesi fortemente limite si può considerare L_κ.

[64]Mentre, come abbiamo visto, potrebbe darsi che non esistano cardinali inaccessibili, segue dagli assiomi, in particolare, rimpiazzamento ed unione, che esistono sempre cardinali tali che $\alpha = \aleph_\alpha$, $\alpha = \theta_\alpha$ etc.

S. Shelah ha dimostrato che l'ipotesi della non contraddittorietà di un cardinale inaccessibile è neessaria per costruire il modello di Solovay. Quindi assumere che ogni sottoinsieme di $\mathbb{R}$ sia misurabile secondo Lebesgue implica la non contraddittorietà di un cardinale inaccessibile, e, a livello di non contraddittorietà relativa, le due cose sono equivalenti.

Il risultato è inaspettato sotto molti punti di vista. L'idea dei cardinali inaccessibili è stata sviluppata sostanzialmente per motivi di teoria degli insiemi (o al massimo di topologia) e all'apparenza non sembrerebbe collegata con problemi di analisi reale. Lo stesso Solovay aveva ventilato la possibilità che l'ipotesi di un inaccessibile fosse dovuta semplicemente a qualche debolezza della sua dimostrazione, e magari non fosse necessaria. Inoltre, appare strano che un'ipotesi di analisi reale implichi la non contraddittorietà di una teoria più forte della teoria classica degli insiemi.

Dal punto di vista opposto, altre proprietà che riguardavano la misurabilità di *alcuni* sottoinsiemi di $\mathbb{R}$ (anche assumendo l'assioma della scelta) erano state studiate in precedenza, e coinvolgevano cardinali ancor più "grandi" dei cardinali inaccessibili (vedi oltre). Dal punto di vista storico il risultato di Solovay e Shelah è stato inaspettato perchè coinvolge un tipo di cardinali relativamente "piccolo" rispetto ad altri cardinali che erano stati studiati fino ad allora, e la cui esistenza si era dimostrata equivalente ad altre proprietà formulabili nell'ambito della matematica "classica". Nelle sezioni successive accenniamo brevemente ad alcuni tipi di questi cardinali.

Come abbiamo accennato, limitandoci a considerare solo sottoinsiemi di $\mathbb{R}$ di alcuni tipi particolari, esistono variazioni del risultato di Solovay che coinvolgono anche altri tipi di cardinali. Alcuni di questi risultati erano stati ottenuti in precedenza, ulteriori risultati sono stati ottenuti in seguito. Come usuale nelle trattazioni dei grandi cardinali, anziché un approccio cronologico, abbiamo scelto un tipo di presentazione che parte dai cardinali più "piccoli" e va a quelli più grandi. Esistono anche molti altri tipi di grandi cardinali intermedi, che qui non possiamo trattare per mancanza di spazio.

Per finire questa sezione, accenniamo anche al fatto che i numeri reali nel modello di Solovay soddisfano ad ulteriori proprietà: ogni sottoinsieme di $\mathbb{R}$ ha la proprietà di Baire e ogni sottoinsieme non numerabile possiede un sottospazio perfetto (= chiuso e senza punti isolati) non vuoto. Molto grossolanamente, i sottoinsiemi di $\mathbb{R}$ nel modello di Solovay non sono mai "troppo" complicati. Nel modello di Solovay non vale l'assioma di scelta ma valgono alcune sue conseguenze che spesso lo possono rimpiazzare: l'assioma delle scelte dipendenti e l'assioma numerabile di scelta.

2.3.7. *Cardinali debolmente compatti.* Abbiamo visto un teorema che riguarda i cardinali inaccessibili ma che non riguarda *direttamente* alcune proprietà matematiche, ma solo la loro non contraddittorietà relativa. In molti casi l'esistenza di cardinali "grandi" si è rivelata importante in questo senso, come strumento per misurare la "forza" data dall'ipotesi che una certa teoria sia

non contraddittoria. Ma esistono anche implicazioni (ed equivalenze) dirette, cioè che asseriscono che una certa proprietà è proprio equivalente all'esistenza di cardinali di un certo tipo.

Vediamo adesso alcuni casi di queste equivalenze. Ci premeva solo sottolineare la differenza sostanziale fra i due tipi di risultati.

Per poter dare la definizione di un cardinale debolmente compatto e delle sue formulazioni equivalenti dobbiamo dare prima alcune definizioni.

D'ora in poi supponiamo che κ sia un cardinale infinito strettamente maggiore di ω e in questa sezione supponiamo inoltre che κ sia *fortemente limite* cioè che se $\lambda < \kappa$ è un altro cardinale, allora $|\mathcal{P}(\lambda)| < \kappa$[65]

Il *linguaggio infinitario* $\mathcal{L}_{\kappa,\omega}$ è definito come il calcolo dei predicati del primo ordine, salvo che vengono ammesse congiunzioni e disgiunzioni di un numero infinito, ma $< \kappa$, di formule del linguaggio. La sua semantica è definita in maniera naturale. Il linguaggio $\mathcal{L}_{\kappa,\omega}$ si dice *debolmente* κ*-compatto* se ogni insieme di enunciati di cardinalità κ ha un modello, sotto le ipotesi che ogni suo sottoinsieme di cardinalità $< \kappa$ abbia un modello. (Ad esempio, se si ammette la possibilità $\kappa = \omega$, $\mathcal{L}_{\omega,\omega}$ è esattamente il calcolo dei predicati del primo ordine, ed è debolmente κ-compatto, perchè ogni insieme numerabile di enunciati ha un modello, se ogni suo sottoinsieme finito ha un modello. Naturalmente sappiamo che il teorema di compattezza per $\mathcal{L}_{\omega,\omega}$ vale anche per insiemi più che numerabili, forme analoghe di compattezza verranno considerate in seguito).

Uno spazio topologico si dice κ*-compatto* se ogni ricoprimento aperto ha un sottoricoprimento di cardinalità $< \kappa$. La compattezza in senso classico è quindi la ω-compattezza.

Un campo di insiemi su X è una famiglia di sottoinsiemi di X chiusa per intersezioni, unioni e complementi (in X). I campi di insiemi sono gli esempi tipici di algebre di Boole, in effetti, ogni algebra di Boole è isomorfa ad un campo di insiemi. Un ideale in un campo di insiemi è una sottofamiglia chiusa per sottoinsiemi e per unioni finite.

Intuitivamente, definire un ideale significa definire una famiglia di sottoinsiemi che si considerano "piccoli". Ad esempio, dato un qualunque X, la famiglia dei sottoinsiemi di X che sono finiti oppure cofiniti è un campo di insiemi, e i sottoinsiemi finiti formano un'ideale.

Un campo di insiemi si dice κ-completo se è chiuso anche per intersezioni ed unioni di famiglie di $< \kappa$ membri. Un ideale si dice κ-completo se è anche chiuso per unioni di famiglie di $< \kappa$ membri.

---

[65] quest'ultima disuguaglianza si scrive spesso $2^\lambda < \kappa$, perchè c'è una biiezione naturale fra $\mathcal{P}(\lambda)$ e 2^λ, l'insieme di tutte le funzioni da λ a $\{0,1\}$. L'assunzione che κ sia fortemente limite semplifica gli enunciati, ma anche senza questa ipotesi si possono ottenere altri risultati interessanti. L'ipotesi non sar à necessaria per i cardinali che considereremo in seguito; generalmente sarà una conseguenza delle definiizioni.

Le condizioni seguenti su un cardinale κ sono equivalenti, e se valgono si dice che κ è debolmente compatto (quasi tutte le equivalenze valgono anche per $\kappa = \omega$.)

- $\mathcal{L}_{\kappa,\omega}$ è *debolmente κ-compatto* (vale anche per altri tipi di linguaggi infinitari, più in generale, per altri tipi di "logiche")

- ogni prodotto di spazi topologici κ-compatti è ancora κ-compatto, sotto le ipotesi che i fattori siano in numero $\leq \kappa$ e gli spazi abbiano cardinalità $< ch\kappa$ (vi sono molte altre equivalenze che riguardano spazi topologici, in alcuni casi è difficile trovarle elencate nei libri)

- Ogni insieme totalmente ordinato di cardinalità κ ha un sottoinsieme isomorfo a κ come ordinale, oppure a κ ordinato all'incontrario. Un cardinale con questa proprietà viene spesso chiamato cardinale di Hausdorff[66]

- ogni ideale κ-completo in un campo di insiemi κ-completo e di cardinalità κ può essere esteso ad un ideale κ-completo massimale.

Altre condizioni equivalenti a "κ è debolmente compatto" riguardano

- altri problemi di combinatoria infinita (definizione originale), in particolare, alberi infiniti (diagrammi che partono da un punto).

- anelli, gruppi abeliani, moduli, proprietà equivalenti a certe condizioni sui sottoinsiemi di κ [67]

- algebre di Boole

- problemi di descrivibilità, caratterizzabilità mediante formule

- caratterizzazioni in teoria dei modelli

Se κ è debolmente compatto, allora κ è inaccessibile ma un cardinale debolmente compatto è molto più grande del primo cardinale inaccessibile.

Supponendo che esista un cardinale debolmente compatto κ, enumeriamo i cardinali inaccessibili, diciamo

$I_0 =$ il più piccolo cardinale inaccessibile,

$I_{\alpha+1} =$ il più piccolo cardinale inaccessibile $> I_\alpha$,

$I_\alpha =$ il più piccolo cardinale inaccessibile maggiore di tutti gli I_β, con $\beta < \alpha$, se α è limite.

Naturalmente, non è detto che I_α sia definita per ogni ordinale α (questo può succedere solo se esiste una classe propria di cardinali inaccessibili). Se non esiste nessun cardinale inaccessibile, nemmeno I_0 è definita! Però abbiamo che se esiste un cardinale debolmente compatto κ, allora I_α è definita per tutti gli ordinali $\alpha \leq \kappa$ e $I_\kappa = \kappa$. In parole, κ è il κ-esimo inaccessibile e κ contiene un insieme di cardinali inaccessibili di cardinalità κ. Quindi κ è molto più

[66]La proprietà non è banale, ad esempio $\mathbb{R}$ non è numerabile, ma tutti i suoi sottoinsiemi bene ordinati (con l'ordine originale di $\mathbb{R}$) sono numerabili (infatti se $a < b \in \mathbb{R}$, allora l'intervallo (a, b) contiene almeno un numero razionale, ma l'insieme dei numeri razionali è numerabile, quindi non può esistere un buon ordine più che numerabile). In effetti, ogni buon ordine numerabile può essere realizzato come sottoinsieme di $\mathbb{R}$. Ad esempio, $\{0, \frac{1}{2}, \frac{3}{4}, \frac{7}{8}, \dots\} \cup \{1\}$ è isomorfo ad $\omega + 1$, inoltre $\{0, \frac{1}{2}, \frac{3}{4}, \frac{7}{8}, \dots\} \cup \{1, \frac{5}{4}, \frac{11}{8}, \frac{23}{16}, \dots\} \cup \{\frac{3}{2}\}$ è isomorfo a $\omega + \omega + 1$, e così via.

[67]Vedi Eklof, Mekler, Almost Free Modules Set-theoretic Methods Revised Edition, ad esempio Sezione IV, 3

grande di quaunque inaccessibile $\lambda < \kappa$. E questa affermazione è molto più debole di quanto si potrebbe affermare dando alcune altre definizioni! Esiste una gerarchia di grandi cardinali che soddisfano a proprietà intermedie fra inaccessibilità e debole compattezza e, nella maggior parte dei casi, ciascuno di questi cardinali μ è il μ-esimo cardinale fra quelli che soddisfano a proprietà più deboli.

Questi argomenti funzionano anche a livello di non contraddittorietà relativa. Ad esempio, se κ è il più piccolo cardinale inaccessibile, allora L_κ è un modello non solo di ZFC, ma anche di "ZFC + non esistono cardinali inaccessibili". Se κ è il secondo cardinale inaccessibile, allora L_κ è un modello di "ZFC + esiste esattamente un cardinale inaccessibile". Se κ è debolmente compatto, allora V_κ è un modello di "ZFC + per ogni cardinale λ esiste un cardinale inaccessibile $> \lambda$".

2.3.8. *Cardinali misurabili.* I cardinali misurabili possono essere definiti mediante proprietà leggermente più forti di quelle che abbiamo presentato e che caratterizzano i cardinali debolmente compatti.

Nonostante questo, come sopra, se μ è un cardinale misurabile, allora μ è il μ-esimo cardinale debolmente compatto, e anche in questo caso è possibile definire nozioni intermedie ciascuna "molto più" forte delle precedenti nello stesso senso.

Alcune proprietà con immediato significato matematico dei cardinali misurabili:

- Esiste un cardinale misurabile se e solo se c' è un gruppo che non può essere rappresentato come gruppo fondamentale di uno spazio topologico compatto di Hausdorff. [...]

Le precedenti sono equivalenze logiche dirette. Come abbiamo visto, spesso i grandi cardinali sono coinvolti in equivalenze che riguardano la non contraddittorietà relativa di teorie (equicoerenza).

Ad esempio, la teoria ZFC + "esiste un cardinale misurabile" è equicoerente a "la misura di Lebesgue su $\mathbb{R}$ può essere estesa ad una misura completa (cioè ogni sottoinsieme di $\mathbb{R}$ ha una misura) e numerabilmente addittiva". Questo è un risultato molto diverso dal risultato di Solovay che coinvolge i cardinali inaccessibili. Qui stiamo usando l'assioma di scelta, quindi esiste sicuramente un sottoinsieme di $\mathbb{R}$ che non è misurabile secondo Lebesgue. Il problema che ci si pone (Ulam, 1930) è vedere se questa misura può essere estesa conservando l'addittività numerabile (il ragionamento classico di Vitali dimostra che una simile misura non può essere invariante per traslazioni, quindi si tratterebbe comunque di una misura con proprietà controintuitive).

Dal punto di vista strettamente logico i cardinali misurabili sono coinvolti in costruzioni che rendono esplicito il collegamento tra teoria degli insiemi e teoria dei modelli. Gli ultraprodotti sono un modo particolare di prendere in considerazione il quoziente di un prodotto di modelli. Nel caso tutti i fattori

del prodotto siano uguali, si parla di ultrapotenza. Le ultrapotenze conservano tutte le proprietà al primo ordine dei modelli (Teorema di Łoś).

Se esiste un cardinale misurabile, allora (usando un po' di dettagli tecnici sofisticati) è possibile prendere l'ultrapotenza di V, la classe di tutti gli insiemi, ed ottenere un modello che estende V, ma che è anche isomorfo ad un modello interno W, sottomodello *proprio* di V. Siccome le ultrapotenze conservano tutte le proprietà al primo ordine, e $V = L$ [...] può essere espressa al primo ordine, abbiamo che, se valesse $V = L$ in V, allora dovrebbe valere anche in W, ma L è il più piccolo modello interno, quindi $W = V$, contraddizione.

Quindi l'esistenza di un cardinale misurabile contraddice l'assioma di costruibilità di Gödel! (Questa è un'implicazione diretta, se esiste un cardinale misurabile, allora $V \neq L$) Questo teorema, dovuto a Scott, in origine ha suscitato una certa diffidenza nei confronti dei cardinali misurabili. Ma tutti i tentativi di dimostrare che l'assunzione che esiste un cardinale misurabile è contraddittoria non sono riusciti; al contrario, hanno portato ad una teoria relativamente completa e coerente, con teoremi di struttura particolarmente dettagliati. Inoltre, nemmeno molte assunzioni decisamente più forti della misurabilità hanno finora portato a contraddizioni, per cui allo stato attuale c'è una discreta fiducia nell'assunzione che i cardinali misurabili non siano contraddittori. E si suppone anche che, qualora lo fossero, qualunque argomento che ne dimostri la contraddittorietà sarebbe modificabile per ottenere la contraddittorietà di ipotesi molto più deboli (naturalmente queste sono solo argomentazioni informali che difficilmente potranno mai essere espresse in forma rigorosa).

Inoltre, modificando la costruzione di L si possono ottenere "modelli interni canonici" per un cardinale misurabile, e anche per cardinali più grandi. Questi modelli canonici conservano gran parte della struttura dettagliata di L; il problema di stabilire fino a quali grandi cardinali si può effettuare una costruzione di modelli "tipo-L" è uno dei probemi più importanti e difficili della teoria degli insiemi contemporanea, e va sotto il nome di "problema del modello interno".

2.3.9. *Cardinali fortemente compatti.* I cardinali fortemente compatti sono definiti mediante proprietà simili (di solito leggermente più semplici) ma più forti rispetto alle proprietà che caratterizzano i cardinali debolmente compatti.

Il linguaggio $\mathcal{L}_{\kappa,\omega}$ si dice *(fortemente) κ-compatto* se ogni insieme di enunciati (di qualunque cardinalità) ha un modello, sotto le ipotesi che ogni suo sottoinsieme di cardinalità $< \kappa$ abbia un modello (la differenza con la compattezza debole è che in quel caso ci eravamo limitati a insiemi di enunciati di cardinalità κ, qui invece la cardinalità dell'insieme di partenza è arbitraria).

Le condizioni seguenti su un cardinale κ sono equivalenti, e se valgono si dice che κ è fortemente compatto (quasi tutte le equivalenze valgono anche per $\kappa = \omega$.)

- $\mathcal{L}_{\kappa,\omega}$ è κ-*compatto* (vale anche per altre varianti, più in generale, per altri tipi di "logiche")

- ogni prodotto di spazi topologici κ-compatti è ancora κ-compatto (nel caso $\kappa = \omega$ questo è il cosiddetto Teorema di Tychonoff).

- ogni ideale κ-completo in un campo di insiemi κ-completo può essere esteso ad un ideale κ-completo massimale.

Come al solito, ci sono altre condizioni equivalenti che qui non elenchiamo.

Invece è significativo che la relazione fra i cardinali misurabili e i cardinali fortemente compatti sia un caso davvero eccezionale nell'ambito della teoria dei grandi cardinali. Abbiamo visto che, in generale, ciacuna proprietà che descrive un grande cardinale è più forte di altre proprietà nel senso che ogni cardinale κ con la proprietà forte contiene moltisimi cardinali con la proprietà più debole, di solito, ne contiene addirittura proprio κ.

Invece, mentre da un lato si può dimostrare che ogni cardinale fortemente compatto è misurabile, d'altro canto (se è non contraddittoria l'esistenza di un fortemente compatto, allora) è non contraddittorio assumere che il più piccolo cardinale fortemente compatto sia il più piccolo cardinale misurabile. Ma quest'ultima affermazione non è dimostrabile, e in qualche modello succede invece che il primo κ fortemente compatto contiene un numero di misurabili pari a κ (casi intermedi sono possibili). A livello di non contraddittorietà, l'assunzione che esiste un fortemente compatto è però sempre più forte dell'esistenza di un misurabile.

Per questi motivi, in teoria degli insiemi ora si usa più frequentemente una nozione più forte, quella di cardinale supercompatto.

Il primo fortemente compatto (sempre supponendo che tutti questi cardinali esistano) può essere uguale al primo misurabile, ma anche uguale al primo supercompatto. Dal punto di vista della teoria degli insiemi i cardinali supercompatti hanno una proprietà aggiuntiva molto utile e importante. D'altro canto, è difficile dare una caratterizzazione dei supercompatti che coinvolga nozioni di natura spiccatamente matematica, dello stesso tipo delle equivalenze che abbiamo presentato per i misurabili e per i debolmente e fortemente compatti.

Ogni cardinale supercompatto è fortemente compatto ed è molto più grande (sempre nel solito senso) del primo misurabile. Sembra però un problema ancora aperto se, assumendo la non contraddittorietà di un fortemente compatto, si ottenga la non contraddittorietà di un supercompatto.

Sui grandi cardinali si possono consultare

A. Kanamori, M. Magidor: The evolution of large cardinal axioms in set theory, in: Higher set theory (Proc. Conf., Math. Forschungsinst., Oberwolfach, 1977), Lecture Notes in Mathematics, 669, Springer, 99–275.

http://math.bu.edu/people/aki/e.pdf

Drake, F. R. (1974). Set Theory: An Introduction to Large Cardinals (Studies in Logic and the Foundations of Mathematics; V. 76). Elsevier

A. Kanamori: The Higher Infinite. Large Cardinals in Set Theory from their Beginnings., Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1994.

e inoltre il libro di Jech e l'Handbook of Set Theory già citati.

3. Appendice

Questa sezione contiene altro materiale (parecchio disparato!) per il corso di Logica 1, A.A. 2018–2019. **Non** fa invece parte del programma per il corso dell'A.A. 2020–2021, ad esclusione della prossima sezione sul Teorema di Tarski, che fa parte **anche** del programma per l'A.A. 2020–2021,

3.1. Il Teorema di Tarski. Supponiamo di lavorare in un'estensione non contraddittoria T dell'Aritmetica di Peano PA e di avere una gödelizzazione che ad ogni formula φ associa il numero $g(\varphi)$ con associato numerale $\ulcorner\varphi\urcorner = g(\bar{\varphi})$ (ricordiamo che, se $n \in \mathbb{N}$, il *numerale* $\bar{n}$ è il termine $0''''''^{\cdots}$ con n apici; intuitivamente, $\bar{n}$ è il nome di n nel linguaggio di PA).

Teorema 3.1. *(Tarski) Non esiste nessuna formula $\sigma(x, y)$ dipendente solo dalle variabili x e y e tale che, per ogni formula $\varphi(x)$ dipendente al massimo dalla variabile x ed ogni naturale $n \in \mathbb{N}$, il seguente enunciato sia un teorema di T*

$$\sigma(\ulcorner\varphi(x)\urcorner, \bar{n}) \Leftrightarrow \varphi(\bar{n}). \tag{3.1}$$

Dimostrazione. Supponiamo per assurdo che esista una siffatta σ. Sia $\varphi(x)$ la formula $\neg\sigma(x, x)$ e sia $\bar{n} = \ulcorner\varphi(x)\urcorner$. Quindi $\varphi(\bar{n})$ è $\neg\sigma(\bar{n}, \bar{n})$, cioè $\neg\sigma(\ulcorner\varphi(x)\urcorner, \bar{n})$. Sostituendo in (3.1) abbiamo

$$\sigma(\ulcorner\varphi(x)\urcorner, \bar{n}) \Leftrightarrow \neg\sigma(\ulcorner\varphi(x)\urcorner, \bar{n})$$

cioè una contraddizione. □

In particolare, se T è la teoria che contiene come assiomi tutti gli enunciati veri in (cioè soddisfatti da) $\mathbb{N}$, abbiamo[68] che non esiste nessuna formula che "esprime" la verità[69] in $\mathbb{N}$.

---

[68] Qui per $\mathbb{N}$ intendiamo $(\mathbb{N}, 0, ', +, \cdot, =)$, eventualmente a cui sono aggiunte ulteriori operazioni o relazioni. T è non contraddittoria perchè per costruzione ha un modello. Naturalmente, l'esistenza di questo modello, pur intuitiva, è un'assunzione metamatematica forte.

[69] ** Per semplicità abbiamo sottinteso nell'affermazione precedente che sia sempre possibile esprimere il gödeliano di una formula ottenuta sostituendo una variabile con un termine, conoscendo il gödeliano della formula di partenza. Se non si vogliono mescolare i due aspetti, ci si deve chiedere se esiste una formula τ tale che

$$\tau(\ulcorner\psi\urcorner) \Leftrightarrow \psi \tag{3.2}$$

sia un teorema, per ogni enunciato ψ.

Supponiamo di avere una formula α che esprime il risultato di una sostituzione, cioè tale che $\alpha(u, v, w)$ *esprime* (nel senso del Capitolo III, Sezione 2 del libro del Mendelson) la relazione $R(\bar{m}, \bar{n}, \bar{p})$ definita da " $\bar{m} = \ulcorner\varphi(x)\urcorner$, per qualche formula $\varphi(x)$, e $\bar{p} = \ulcorner\varphi(\bar{n})\urcorner$ ". Allora da una τ che soddisfa (3.2), otteniamo una σ che soddisfa (3.1) definendo $\sigma(u, v)$ come $\exists w(\tau(w) \wedge \alpha(u, v, w))$. Quindi sotto l'ipotesi dell'esistenza di α, (3.1) e (3.2) sono equivalenti.

3.2. Congruenze in semigruppi. Un *semigruppo* $\mathbf{S} = (S, \cdot)$ è un insieme S dotato di un'operazione binaria associativa $\cdot$ che in seguito indicheremo mediante giustapposizione, se questo non genererà confusione, cioè scriveremo st al posto di $s \cdot t$.

Se $\mathbf{S} = (S, \cdot)$ e $\mathbf{S}_1 = (S_1, \cdot)$ sono due semigruppi, una funzione $\varphi : S \to S_1$ si dice *morfismo* se $\varphi(st) = \varphi(s)\varphi(t)$ o, in notazione non abbreviata,

$\varphi(s \cdot t) = \varphi(s) \cdot \varphi(t)$, per ogni coppia di elementi $s, t \in S$.

Nella formula precedente, l'operazione a sinistra è quella in $\mathbf{S}$ e l'operazione a destra è quella in $\mathbf{S}_1$.

Se $\varphi : A \to B$ è una funzione, φ induce una relazione di equivalenza su A, se si considerano "identificati" due elementi di A se e solo se hanno la stessa immagine secondo φ. Sarebbe naturale chiamare questa relazione di equivalenza "nucleo" di φ, ma, per evitare conflitti di terminologia, per esempio, col nucleo di un morfismo di gruppi, modificheremo leggermente la terminologia.

Definizione 3.2. Se $\varphi : A \to B$ è una funzione, il *nucleo di φ nel senso di relazione di equivalenza* di φ è la seguente relazione su A

$KerEq(\varphi) = \{(a, b) \in A \times A \mid \varphi(a) = \varphi(b)\}$.

È ovvio verificare che, sotto le ipotesi nella definizione, $KerEq(\varphi)$ è effettivamente una relazione di equivalenza su A. Finora le operazioni di semigruppo e la nozione di morfismo non sono intervenute.

3.2.1. Se però $A = S$ e $B = S_1$ sono semigruppi, e φ è un morfismo da $\mathbf{S}$ ad $\mathbf{S}_1$, allora $\alpha = KerEq(\varphi)$ soddisfa all'ulteriore proprietà

(*) Per tutti gli elementi $s, s', t, t' \in S$, se $s \; \alpha \; s'$ e $t \; \alpha \; t'$, allora $st \; \alpha \; s't'$,

dove abbiamo scritto $s \; \alpha \; s' \; \ldots$ al posto di $(s, s') \in \alpha \; \ldots$

Infatti, da $s \; \alpha \; s'$ e $t \; \alpha \; t'$ otteniamo, per definizione di $\alpha = KerEq(\varphi)$, che $\varphi(s) = \varphi(s')$ e $\varphi(t) = \varphi(t')$. Se poi φ è un morfismo, applicando due volte la proprietà di essere un morfismo, abbiamo $\varphi(st) = \varphi(s)\varphi(t) = \varphi(s')\varphi(t') = \varphi(s't')$, cioè $\varphi(st) = \varphi(s't')$ e quindi $st \; \alpha \; s't'$. Dunque (*) vale se φ è un morfismo di semigruppi e $\alpha = KerEq(\varphi)$.

Inoltre osserviamo che il Teorema 3.1 vale in realtà sotto ipotesi estremamente generali. È sufficiente avere un sistema formale con:

- due simboli di variabile,
- un insieme di espressioni che chiamiamo *termini*, che contengono le variabili,
- una nozione di *sostituzione (di una variabile x con un termine t)* che ad ogni formula φ associa un'altra formula $\varphi(x|t)$, per ogni variabile x ed ogni termine t. Si richiede che questa operazione di sostituzione soddisfi ad alcune proprietà naturali, la cui enunciazione esplicita lasciamo al lettore,
- un operatore di *negazione* che ad ogni formula φ associa un'altra formula $\neg\varphi$. Questo operatore di negazione deve commutare con l'operazione di sostituzione,
- una nozione di equivalenza e la richiesta che φ e $\neg\varphi$ non siano mai equivalenti.

Una funzione gödeliana in questo ambito è semplicemente una funzione (a livello metamatematico, e non necessariamente iniettiva) dall'insieme delle formule all'insieme dei termini. In realtà non è nemmeno necessario assumere che variabili e termini siano espressioni del linguaggio, l'unico aspetto importante è l'esistenza dell'operazione di sostituzione con le opportune proprietà. Anche la nozione di equivalenza non deve necessariamente essere espressa da un simbolo del sistema formale, per esempio, si possono considerare φ e ψ equivalenti se $\varphi \vdash \psi$ e $\psi \vdash \varphi$.

Osserviamo che la struttura di $\mathbf{S}_1$ non compare in (*), cioè (*) riguarda esclusivamente $\mathbf{S}$ ed α; il morfismo φ ed $\mathbf{S}_1$ non compaiono in (*). In realtà, almeno in parte, le proprietà di φ seguono da (*), come vedremo.

Se $\mathbf{S}$ è un semigruppo, una relazione d'equivalenza su S che soddisfa ad (*) si dice una *congruenza su* $\mathbf{S}$.

3.2.2. Se α è un congruenza, indichiamo con s/α la classe di equivalenza di un elemento $s \in S$ e con S/α l'insieme delle classi di equivalenza. Su S/α definiamo la seguente operazione binaria

(**) $s/\alpha \cdot t/\alpha = (s \cdot t)/\alpha$, per $s/\alpha \in S/\alpha$ e $t/\alpha \in S/\alpha$.

Naturalmente va verificato che la definizione è indipendente dal rappresentante scelto per ogni classe, cioè che $s/\alpha = s'/\alpha$ e $t/\alpha = t'/\alpha$ implicano $(s \cdot t)/\alpha = (s' \cdot t')/\alpha$. Ma $s/\alpha = s'/\alpha$ se e solo se $s \ \alpha \ s'$, e così via, quindi la proprietà (*) garantisce che l'operazione introdotta su S/α è ben definita. È facile verificare che se S è un semigruppo, allora anche S/α è un semigruppo, con l'operazione appena introdotta.

Abbiamo quasi dimostrato la seguente proposizione.

Proposizione 3.3. *Se* $\mathbf{S}$ *è un semigruppo, allora una relazione binaria* α *su* S *è una congruenza se e solo se* α *è il nucleo* $\alpha = KerEq(\varphi)$ *di qualche morfismo* φ *da* $\mathbf{S}$ *ad* $\mathbf{S}_1$*, per qualche semigruppo* $\mathbf{S}_1$*.*

Dimostrazione. Se α è il nucleo $KerEq(\varphi)$ di un morfismo $\varphi : \mathbf{S} \to \mathbf{S}_1$, allora α è una congruenza per 3.2.1.

Viceversa, se α è una congruenza, sia $S_1 = S/\alpha$; abbiamo che S_1 diventa un semigruppo, se dotato dell'operazione introdotta in 3.2.2. Inoltre, la definizione stessa (**) di questa operazione implica che la proiezione π che ad ogni elemento $s \in S$ associa la sua classe $\pi(s) = s/\alpha$ è un morfismo di semigruppi, e $\alpha = KerEq(\pi)$ per costruzione. □

Le costruzioni effettuate nella dimostrazione precedente sono, in un certo senso, una l'inversa dell'altra. Se $\varphi : \mathbf{S} \to \mathbf{S}_1$ è un morfismo di semigruppi, l'*immagine* di φ è $\varphi(S) = \{u \in S_1 \mid \text{ esiste } s \in S \text{ tale che } \varphi(s) = u\}$. L'insieme $\varphi(S)$ diventa naturalmente un semigruppo con la (restrizione della) stessa operazione di S_1. Un morfismo di semigruppi si dice *isomorfismo* se, in quanto funzione, è biiettiva. Due semigruppi si dicono *isomorfi* se esiste un isomorfismo dall'uno all'altro.

Proposizione 3.4. *Se* $\varphi : \mathbf{S} \to \mathbf{S}_1$ *è un morfismo di semigruppi e* $\alpha = KerEq(\varphi)$*, allora* $\mathbf{S}/\alpha$ *è isomorfo all'immagine* $\varphi(\mathbf{S})$ *di* φ*.*

In particolare, se φ *è suriettivo, allora* $\mathbf{S}/\alpha$ *e* $\mathbf{S}_1$ *sono isomorfi.*

Dimostrazione. La funzione ψ che ad s/α associa $\varphi(s)$ è un isomorfismo da $\mathbf{S}/\alpha$ verso $\varphi(\mathbf{S})$.

Cosa ci assicura che ψ sia un morfismo?

Cosa ci assicura che ψ sia suriettiva?

C'è da effettuare un'altra verifica? □

In altre parole, la seconda parte della Proposizione 3.4 ci fornisce un modo "interno ad **S**" per descrivere (a meno di isomorfismo) tutte le "immagini omomorfe" di **S**.

Lo studente familiare con la teoria dei gruppi può confrontare le costruzioni precedenti con costruzioni simili effettuate per i gruppi. Se **S** è un gruppo, cos'è una congruenza, nella terminologia usata in teoria dei gruppi?

Lo studente saprebbe controllare che l'insieme delle congruenze di un semigruppo è un reticolo, rispetto alla relazione di inclusione?

Quali degli argomenti precedenti sono validi se si suppone che **S** sia dotato semplicemente di un'operazione binaria, senza l'ipotesi che l'operazione sia associativa (quindi senza nessuna ipotesi ulteriore sull'operazione)?

Quali dei ragionamenti precedenti sono validi nel caso in cui considerino al posto dei semigruppi *strutture algebriche* qualunque, cioè insiemi con un certo numero di operazioni, eventualmente anche dipendenti da più di due argomenti?

3.2.3. *Ulteriori letture.* Un'introduzione al cosiddetto "problema della parola" per gruppi e semigruppi si può trovare in Rotman, *An Introduction to the Theory of Groups*, Capitolo 12. Altro materiale, che riguarda anche parole di lunghezza infinita, nei capitoli IV e V del libro citato di Hebisch e Weinert, *Semirings: Algebraic Theory and Applications in Computer Science* e in D. Perrin, J.-E. Pin, *Infinite Words: Automata, Semigroups, Logic and Games*, 2004.

Paolo Lipparini

Dipartimento di Matematica, Viale della Ricerca Insiemistica, Università di Roma "Tor Vergata", I-00133 ROME ITALY