Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Matematica

Prove di consistenza e indipendenza nella Teoria degli Insiemi

Tesi di Laurea in Logica Matematica

Relatore:
Chiar.mo Prof.
Piero Plazzi

Presentata da:
Lorenzo Venieri

Sessione 3
Anno Accademico 2020/2021

Indice

Introduzione

La matematica ordinaria moderna poggia i propri fondamenti sulla teoria assiomatica degli insiemi. Partendo dagli assiomi si cerca di ottenere una definizione implicita precisa di "insieme" e poi costruire un albero di deduzioni in grado di catturare tutto ciò che è vero in matematica.
Possono esserci però domande a cui il sistema non è in grado di rispondere. Domande di questo tipo sono dette indipendenti dal dato sistema di assiomi. Più precisamente, dato un insieme di enunciati Γ, diciamo che un enunciato ϕ è **indipendente** da Γ se né ϕ né $\neg\phi$ sono dimostrabili a partire da Γ. Equivalentemente: sia $\Gamma + \phi$ sia $\Gamma + \neg\phi$ sono consistenti.
Gli assiomi, così come tutte le regole di inferenza e tutti i teoremi dedotti non hanno alcuna valenza semantica, ma solo sintattica. Interpretandoli secondo l'interpretazione prevista si ottengono le proprietà degli insiemi come "intuitivamente" li immaginiamo, ma proprio il fatto che esistono altre interpretazioni possibili è la base per tutti i risultati di consistenza e indipendenza presentati in questa tesi.
Un'interpretazione del linguaggio della teoria degli insiemi è definita specificando un *dominio di individui* non vuoto, in cui variano le variabili, insieme ad una relazione binaria su quel dominio, che corrisponde all'interpretazione di $\in$.
Lo strumento chiave per dimostrare la consistenza (o coerenza) di un insieme di enunciati ci viene dato da un'implicazione del Teorema del Modello: un insieme Γ di enunciati è consistente se e solo se ha un modello $\mathcal{M}$. L'esistenza di un modello infatti garantisce la consistenza dell'insieme di enunciati. Se $\Gamma \vdash \phi$ allora ϕ deve essere vera in ogni interpretazione che rende veri tutti gli enunciati in Γ. Se fissiamo un'interpretazione in cui vale Γ, allora ogni enunciato falso in quella interpretazione non è dimostrabile da Γ. Poiché $\neg\phi$ e ϕ non possono essere entrambe vere nella stessa interpretazione, Γ non può dimostrare sia ϕ sia $\neg\phi$. Dunque, Γ è consistente.
Le prove di indipendenza sono in sostanza doppie prove di consistenza, di un enunciato (assioma) e della sua negazione.

0.1 Cenni storici[1]

La prima teoria formale degli insiemi venne delineata implicitamente da Cantor e poi formalizzata da Frege nel tentativo di dare una fondazione puramente logica all'intera matematica. La teoria intuitiva degli insiemi si reggeva su due principi, spesso impliciti:

- **Principio di Estensione:** Due insiemi coincidono se e solo se hanno gli stessi elementi.
- **Principio di Comprensione:** Data una proprietà P, esiste l'insieme A_P che ha per elementi tutti e soli gli oggetti che godono di quella proprietà.

Sfortunatamente, questi due principi generano una contraddizione, come evidenziato dal celebre Paradosso di Russell: non esiste un insieme che contenga tutti gli insiemi che *non* contengono se stessi come elemento[2].
Quando nel giugno del 1902 Russell comunicò questa contraddizione a Frege, era già in stampa il secondo volume dell'opera *Grundgesetze der Arithmetik* (Principi dell'aritmetica), in cui Frege credeva finalmente di essere riuscito a realizzare il proprio "programma logicista", come fu in seguito chiamato da Russell: definire i concetti aritmetici in termini puramente logici a partire da un ristretto numero di proposizioni primitive (gli assiomi) mediante regole di inferenza. Frege, mosso da grande integrità intellettuale[3], si precipitò subito ad aggiungere una nota al volume in stampa in cui spiegava il problema evidenziato da Russell, commentando: *"Qui non è in causa il mio metodo di fondazione in particolare, ma la possibilità di una fondazione logica dell'aritmetica in generale."*
Si aprì così la "crisi dei fondamenti", un periodo di grande incertezza per la comunità matematica. Si sentì il bisogno di trovare delle basi solide per la matematica e dei metodi per dimostrarne la consistenza, in modo tale da non incorrere nuovamente in paradossi come quello trovato da Russell. Furono messi a punto diversi sistemi per costruire i fondamenti della matematica. Tra questi, quello che ebbe più seguito negli anni, fu il sistema assiomatico sviluppato sulla base dell'opera di E. Zermelo e completato poi da A. Fraenkel, da cui il nome del sistema standard per la teoria assiomatica degli insiemi ZF, che analizzeremo in questa Tesi.
Nell'ultimo decennio dell' Ottocento già molti matematici si erano concentrati nel tentativo di assiomatizzare le branche più elementari della matematica come l'aritmetica e

[1] Le citazioni, indicate in corsivo, sono prese da [2]

[2] Osserviamo che questo paradosso è di natura puramente logica: infatti ha validità logica la formula ben formata

$$\neg\exists v_0 \forall v_1 \left(R\left(v_1, v_0\right) \Leftrightarrow \neg R\left(v_1, v_1\right)\right)$$

dal momento che essa risulta vera comunque si interpreti il predicato binario R

[3] Diversi anni dopo, lo stesso Russell commentò questo gesto: *"Fu una cosa quasi sovrumana, una dimostrazione significativa di ciò di cui sono capaci gli uomini se è al lavoro creativo e alla conoscenza che si dedicano, e non all'impresa, tanto più grossolana, di emergere e farsi conoscere".*

la geometria. Un primo esempio significativo fu l'opuscolo di Dedekind *Was sind und was sollen die Zahlen?* (Essenza e significato dei numeri, 1888) in cui per la prima volta tentò di elencare i postulati fondamentali dell'aritmetica.
Allo scritto di Dedekind faceva seguito l'anno seguente un opuscolo di Peano dal titolo *Arithmetices principia, nova metodo exposita.* In questo scritto Peano, dopo aver spiegato il significato dei simboli utilizzati, enunciava un gruppo di 9 assiomi, di cui 4 relativi al simbolo di uguaglianza mentre gli altri 5 sono i celebri "Assiomi di Peano". Due anni dopo Peano pubblicò l'articolo *Sul concetto di numero* in cui, riflettendo sul problema della scelta delle idee primitive, discuteva l'indipendenza dei suoi cinque assiomi per l'aritmetica. Subito dopo gli *Arithmetices principia* Peano pubblicò un altro opuscolo: *Principii di geometria logicamente esposti* in cui, esponendo il tutto in linguaggio simbolico, individuava tra le proposizioni quelle più elementari, gli assiomi, e introduceva senza definirli gli enti geometrici primitivi quali punto e retta limitata. A tal proposito osservava nella conclusione: *"Il lettore può intender col segno 1 (punto) una categoria qualunque di enti, e con* $c \in ab$ *una relazione qualunque fra enti di quella categoria".* Nell'opuscolo non è data alcuna prova di indipendenza degli assiomi, Peano si limitava a dichiarare che l'ordine delle proposizioni chiariva *"il valore degli assiomi"* e questo bastava per essere "moralmente certi della loro indipendenza". Sorprendentemente Peano non reputava importante una dimostrazione di coerenza degli assiomi:

> *Quanto alla coerenza degli assiomi, questa era secondo Peano una questione irrilevante: "La prova che i postulati dell'aritmetica o della geometria non involgano contraddizioni di sorta, non è a parer mio necessaria; posto che noi non li inventiamo ad arbitrio ma li scegliamo tra le proposizioni che contempla (sia pure implicitamente) ogni trattato d'aritmetica o di geometria" scriverà ancora oltre quindici anni dopo, nel mezzo delle polemiche sui fondamenti della matematica.*

Questo era dovuto al fatto che gli assiomi erano ancora visti come corrispondenti a fatti empirici. Un cambio di paradigma avvenne più avanti con i lavori del matematico italiano Mario Pieri, con cui iniziava a delinearsi la moderna concezione delle teorie matematiche. Agli enti primitivi non definiti si può attribuire qualsivoglia significato, purché sia in armonia con i postulati che saranno introdotti. Pieri considerava la geometria come un sistema puramente ipotetico deduttivo, liberato da ogni legame con l'intuizione empirica. Venendo meno ogni riferimento alla realtà fisica, ora è necessario discutere il problema dell'indipendenza e soprattutto della coerenza degli assiomi. Pieri ne era pienamente consapevole ma non se ne occupò personalmente, rimandando ai contemporanei lavori di Padoa. Questi affermava che per dimostrare la compatibilità occorre trovare una interpretazione dei simboli non definiti che verifica simultaneamente tutti i postulati, ossia trovare, come si dice oggi, un modello della teoria. Analogamente, l'indipendenza dei postulati si dimostrava trovando per ciascuno di essi un'interpretazione dei simboli non definiti che non verifichi il postulato considerato, ma verifichi simultaneamente tutti gli

altri.
Nel 1899 Hilbert presentò le *Grundlagen der Geometrie* in cui oltre a esporre un sistema di assiomi riuscì a dimostrare che, se l'aritmetica è coerente, lo è anche il suo sistema di assiomi per la geometria. Ecco dunque nascere il Programma di Hilbert: dimostrare la coerenza dell'aritmetica. Fu questo ambizioso progetto a motivare le ricerche logiche di Hilbert e della sua scuola fino a quando Kurt Gödel comunicò al convegno di Königsberg del 1930 un risultato inaspettato destinato a sconvolgere gli studi sull'assiomatica: il suo Teorema di Incompletezza. Gödel aveva dimostrato che non esiste alcun sistema finito di assiomi che sia completo rispetto alle proposizioni aritmetiche, nell'ipotesi che tale sistema sia coerente. Da questo risultato discendeva che tutti i sistemi formali presentati negli ultimi anni e a cui avevano lavorato i più grandi matematici dell'epoca come per esempio i *Principia Mathematica* di Russell e Whitehead, oppure ZF, contengono proposizioni aritmetiche indecidibili. Ma Gödel non si fermò a questo risultato: grazie al metodo dell'aritmetizzazione da lui sviluppato per la dimostrazione del teorema, era possibile vedere la coerenza del sistema formale come una proprietà puramente combinatoria del sistema. Gödel a questo punto scoprì che per i sistemi formali per cui vale il teorema di incompletezza, una delle proposizioni indecidibili nel sistema è proprio quella affermante la coerenza di tale sistema. Questa conseguenza fu rovinosa per il programma di Hilbert: l'aritmetica non può provare la propria consistenza.
Per quanto riguarda invece i fondamenti della geometria, nel 1951, nell'articolo *"A decision method for elementary algebra and geometry"* il matematico polacco Alfred Tarski presentò un'assiomatizzazione della geometria euclidea "più debole" di quella di Hilbert, dimostrandone la coerenza, senza appoggiarsi all'ipotesi di coerenza dell'aritmetica, e la completezza. La geometria assiomatizzata da Tarski è in un certo senso "qualitativa": non è possibile associare misure ad angoli e segmenti, ma solo fare confronti tra essi. Se così non fosse anche questo sistema ricadrebbe nell'incompletezza di Gödel e sarebbe impossibile dimostrarne la coerenza.
Al fondamentale articolo del 1931 che conteneva il teorema di Gödel, il matematico austriaco fece seguire nel giro di pochi anni numerosi altri lavori importantissimi che hanno segnato una svolta nelle moderne ricerche di logica. In un opuscolo del 1940 (*The consistency of the continuum hypothesis*) Gödel dimostrava che l'assioma della scelta e l'ipotesi del continuo generalizzata sono coerenti con gli altri assiomi della teoria degli insiemi, sotto l'ipotesi che questi ultimi assiomi siano coerenti. Il problema di dimostrare o refutare l'assioma della scelta e l'ipotesi del continuo a partire degli altri assiomi restava però ancora aperto. Chiaramente, dopo la scoperta del teorema di incompletezza, tali proposizioni potevano anche essere indecidibili nella teoria assiomatica degli insiemi. Questo è proprio quello che J.P. Cohen riuscì a dimostrare nel 1963 sviluppando un nuovo metodo di dimostrazione, chiamato *forcing*. L'idea è quella di "forzare" in un senso tecnico ben preciso una determinata proposizione di ZF ad essere vera o falsa in un opportuno modello di ZF. Dopo quella di Cohen, sono state trovate altre dimostrazioni di indipendenza dell'assioma della scelta e dell'ipotesi del continuo facendo ricorso a metodi diversi.

Questa Tesi si propone di esporre i risultati di consistenza e indipendenza tra gli assiomi del sistema ZFC. Il sistema di assiomi adottato è quello di [1], che meglio si presta alle prove di indipendenza. Nel primo capitolo verranno presentati gli assiomi di estensione, della potenza, dell'unione e lo schema di sostituzione. Per le prove di coerenza e indipendenza verranno utilizzati modelli elementari con domini di interpretazione finiti o al massimo quello dei numeri naturali.
Nel secondo capitolo verranno presentati i restanti assiomi (dell'infinito, della scelta e di regolarità). Con l'aggiunta dell'assioma dell'infinito il sistema di assiomi cade sotto la scure del Teorema di Incompletezza di Gödel. È dunque impossibile fornire prove di coerenza assolute. Per questo motivo le prove di consistenza e indipendenza presentate saranno relative all'assunzione che il sistema formato dagli assiomi di estensione, della potenza, dell'unione, dell'infinito e dallo schema di sostituzione sia coerente.
Il terzo capitolo inizia con un'introduzione alla teoria dei numeri ordinali e cardinali necessaria per i risultati avanzati che seguono. Verrà dunque dimostrata la coerenza dell'assioma di regolarità con i restanti assiomi attraverso l'utilizzo del P-modello. Per finire, verranno presentati altri tre risultati di indipendenza per cui sono necessari i risultati della teoria degli ordinali e cardinali.
Non verranno discusse la coerenza e l'indipendenza dell'assioma della scelta, per cui si rimanda a [4].
Per concludere, una tabella riassuntiva riepiloga i risultati visti nell'elaborato.

Capitolo 1

I primi assiomi e prove di consistenza e indipendenza elementari

La teoria di Zermelo-Fraenkel è una teoria del primo ordine con uguaglianza $=$ e unico simbolo proprio $\in$ per predicato binario, usato infisso. In questo capitolo verranno presentati i primi assiomi di ZF e ne verrà discussa la consistenza e la mutua indipendenza. In questo primo capitolo utilizzeremo domini di interpretazione finiti o al massimo quello costituito dai numeri naturali.

1.1 L'Assioma di Estensione [E]

L'Assioma di Estensione riprende il Principio di Estensione della teoria intuitiva degli insiemi: due insiemi coincidono se hanno gli stessi elementi.

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y) \qquad ([\mathrm{E}])$$

Osservazione 1.1. *L'implicazione inversa vale per l'Assioma di Sostitutività dell'uguaglianza.*[1]

1.2 Lo Schema di Sostituzione [S]

[E] permette di riconoscere l'uguaglianza di insiemi già dati ma da solo non è in grado di garantirne l'esistenza. Per questo è necessario un altro assioma che permetta di costruire

[1] Per ogni fbf ϕ è un assioma

$$\forall^n \omega (\forall x \forall y (P(x,y) \rightarrow (\phi[u|x] \rightarrow \phi[u|y])))$$

(x e y sono variabili libere per u in ϕ)

insiemi. Prima di enunciarlo è necessario formalizzare la nozione di predicato binario funzionale in una data variabile.

Def 1.1. *Diciamo che un predicato binario $F(x, y)$ è **funzionale in x** se*

$$(\forall x)(\forall y)(\forall z)((F(x, y) \wedge F(x, z)) \rightarrow (y = z))$$

Def 1.2.

- *Sia $p(x, y)$ un predicato binario. Se in un modello $p(a, c)$ è vero, allora (in quel modello) chiamiamo l'insieme c un **associato** dell'insieme a rispetto a $p(x, y)$.*
- *Sia $f(x, y)$ un predicato binario funzionale in x in un dato modello. Indichiamo con $f(x)$ l'unico associato y di x: $y = f(x)$.*

Ora è possibile enunciare l'Assioma di Sostituzione, che è in realtà uno schema di assiomi, in quanto per ogni predicato abbiamo un assioma diverso.

Schema di Sostituzione: Per ogni insieme S e ogni predicato binario $F(x, y)$ funzionale in x, esiste l'insieme i cui elementi sono gli associati e solo gli associati di tutti gli elementi di S rispetto a $F(x, y)$.[2] Formalmente:

$$\begin{array}{l}(\forall s)((\forall x)(\forall y)(\forall z)(((x \in s) \wedge F(x, y) \wedge F(x, z))) \rightarrow (y = z)) \\ \rightarrow(\exists t)(\forall y)((y \in t) \leftrightarrow (\exists x)((x \in s) \wedge F(x, y))))\end{array} \qquad ([S])$$

Uno schema di predicati binari F(x,y) funzionale in x molto importante è dato da:

$$F(x, y) \equiv ((x = y) \wedge P(y)) \tag{1.1}$$

dove $P(y)$ è un qualunque predicato in cui y è l'unica variabile libera. Usando (1.1) in [S] si ottiene per modus ponens:

$$(\forall s)(\exists t)(\forall y)((y \in t) \leftrightarrow (\exists x)((x \in s) \wedge (x = y) \wedge P(y))) \tag{1.2}$$

Che è equivalente a:

$$(\forall s)(\exists t)(\forall y)((y \in t) \leftrightarrow ((y \in s) \wedge P(y))) \tag{1.3}$$

Che afferma che nella Teoria degli Insiemi se esiste un insieme s, esiste anche l'insieme t di tutti gli elementi di s che soddisfano un predicato unario $P(y)$.

Osservazione 1.2. *A volte (1.3) viene presentato come Assioma di Comprensione o Schema di Specificazione. Abbiamo visto come lo Schema di Sostituzione, formulato in questo modo, renda superfluo questo assioma. Anche l'Assioma della Coppia, che a volte viene presentato a sé stante, può essere dedotto da E, S e dall'Assioma della Potenza, che vedremo nella prossima sezione* [3].

[2] Lo schema di Sostituzione presentato è quello di Fraenkel, da cui è possibile derivare quelli che spesso vengono presentati come assioma della coppia e schema di specificazione, vedi Osservazione 1.2

[3] Vedi Corollario 1.1

Presupponendo l'esistenza di determinati insiemi, lo schema S permette di provare l'esistenza di una grande varietà di altri insiemi.

Esempio 1.1. *Se nella Teoria degli Insiemi esistono i seguenti insiemi:*

$$s = \{a, b, c\} \;\; e \;\; r = \{\{a, m\}, \{b, n\}, \{c, n\}\}$$

allora l'insieme $t = \{m, n\}$ *esiste.*
Per vederlo basta considerare il predicato:

$$(x \in s) \wedge (\{x, y\} \in r)$$

Questo predicato è funzionale in x e gli associati di a,b e c sono rispettivamente m,n e n. Dunque, per S, deve esistere l'insieme t i cui elementi sono gli associati di tutti gli elementi di $\{a, b, c\}$.

È importante osservare che (1.3) non asserisce l'esistenza di un insieme composto da tutti gli elementi che soddisfano il predicato P(x), come il Principio di Comprensione. (1.3) afferma solo l'esistenza dell'insieme di tutti gli elementi che soddisfano P(x) e *che sono elementi di un altro dato insieme.*
Un'applicazione importante di (1.3) è che grazie ad esso è possibile asserire l'esistenza di un insieme vuoto nella Teoria degli Insiemi. Per costruirlo basta usare in (1.3) come predicato unario $P(x)$: $x \neq x$. Si ottiene:

$$(\forall s)(\exists t)(\forall x)((x \in t) \leftrightarrow ((x \in s) \wedge (x \neq x))) \tag{1.4}$$

Ma $(\forall x)((x \in s) \wedge (x \neq x))$ non è soddisfacibile e quindi

$$(\exists t)(\forall x)(x \notin t) \tag{1.5}$$

è un teorema nella Teoria degli Insiemi. Questo teorema può essere interpretato nella nostra interpretazione prevista come l'esistenza di un insieme che non ha elementi, dunque come insieme vuoto.

Teorema 1.1. *Esiste un unico insieme vuoto.*

Dimostrazione. L'esistenza è provata dalla formula (1.5). Per provarne l'unicità supponiamo che esistano due insiemi vuoti a e b, per l'Assioma di Estensione si ha che $a = b$ □

Questo teorema giustifica l'introduzione del simbolo $\emptyset$ come **l'insieme vuoto** della Teoria degli Insiemi.

1.2.1 Consistenza di E + S

Per dimostrare la consistenza di $E+S$ è sufficiente esibire un modello in cui siano verificati entrambi gli assiomi. Chiamiamo modello $\mathcal{A}$ il modello composto dal solo insieme z, e la cui tavola è data da

$z \in z$	**F**

È ovvio che E è vero in $\mathcal{A}$, in quanto in $\mathcal{A}$ non ci sono due insiemi distinti. Inoltre, ogni insieme la cui esistenza è asserita attraverso S sarà necessariamente vuoto. Quindi anche S è vero in $\mathcal{A}$.
Il fatto che $\mathcal{A}$ sia un modello per E ed S dimostra che questi due soli assiomi non sono in grado di dimostrare l'esistenza di alcun altro insieme.

1.2.2 Mutua indipendenza di E e S

L'Assioma di Estensione e lo Schema di Sostituzione sono indipendenti. Abbiamo già visto in 1.2.1 che esiste un modello per E + S. Per dimostrare che E ed S sono indipendenti non ci resta che esibire un modello per E + ¬S e un modello per ¬E + S.

Un modello per E + ¬S

Si consideri il modello $\mathcal{B}$ in cui il dominio di individui consiste dell'insieme z e la cui tavola è data da

$z \in z$	**V**

Questo modello ha uno e un solo elemento, dunque in esso vale E. D'altra parte, dato che nel modello $\mathcal{B}$ non è presente un insieme vuoto e dato che (come visto nel Teorema 1.1) S implica l'esistenza di un insieme vuoto, ne segue che S non è valido nel modello dato.

Un modello per ¬E + S

Si consideri il modello $\mathcal{C}$ il cui dominio di individui consiste degli insiemi 0, 1, 2, 3, 4, ... e dove

$$m \in n \textit{ se e solo se } m \textit{ é } n-2 \textit{ con } n > 2 \tag{1.6}$$

Così, $2 = \{0\}$, $3 = \{1\}$, $4 = \{2\}$, ...
In questo modello si ha che $(\forall x)(x \notin 0)$ e $(\forall x)(x \notin 1)$. Dunque in $\mathcal{C}$ sia 0 sia 1 sono un insieme vuoto. Ma, per (1.6), $0 \in 2$ e $1 \notin 2$. Di conseguenza 0 e 1 non possono essere uguali (non rispetterebbero l'assioma di sostitutività dell'uguaglianza), dunque E non è valido in questo modello. D'altra parte, ogni insieme del modello $\mathcal{C}$ o non ha nessun elemento o ne ha uno solo, dunque S è necessariamente valido nel modello dato.

1.3 L'Assioma della Potenza [P]

Come abbiamo già visto in 1.2.1, gli assiomi di Estensione e Specificazione non possono dimostrare l'esistenza di insiemi diversi dall'insieme vuoto. Per sviluppare una teoria degli insiemi sufficientemente espressiva abbiamo dunque bisogno di altri assiomi che permettano di costruire altri insiemi. Il primo di questi assiomi è l'Assioma della Potenza.
Assioma della Potenza: Per ogni insieme S, esiste l'insieme i cui elementi sono tutti e soli i sottoinsiemi di S (cioè l' *insieme potenza* di S). Formalmente:

$$(\forall s)(\exists t)(\forall x)((x \in t) \leftrightarrow (x \subseteq s)) \qquad ([\mathrm{P}])$$

Se vale l'Assioma di Estensione l'insieme potenza di un insieme s è unico e si denota con: $\mathscr{P}(s)$

1.3.1 Consistenza di E + S + P

Costruiamo un modello per il sistema di assiomi $E + S + P$.
Osserviamo preliminarmente che ogni numero naturale positivo n ammette una unica *rappresentazione binaria* data da:

$$n = 2^{e_1} + 2^{e_2} + \ldots + 2^{e_n} \text{ con } e_1 > e_2 > ... > e_n \geq 0$$

Basandoci su questa considerazione, consideriamo il
Modello 1:[4] Il dominio di individui consiste di 0, 1, 2, 3, ... dove

$(x \in y)$ se e solo se
(x appare come esponente nell'unica rappresentazione binaria di y, se $y > 0$, e
0 è l'insieme vuoto)

Conseguentemente, nel modello si ha $1 = \{0\}$, $2 = \{1\}$, $11 = \{0, 1, 3\}$, $0 \in 1$, $0 \in 11$, $1 \in 2$, $3 \in 11$, $1 \in 11$, ...
Si osservi che ogni insieme del modello ha un numero finito di elementi.
Vediamo ora come questo sia un modello per $E + S + P$.
Dato che numeri naturali distinti hanno rappresentazioni binarie distinte, ne consegue che numeri naturali distinti sono insiemi distinti e quindi nel Modello 1 vale l'assioma di Estensione.
Ora sia $P(x, y)$ un qualunque predicato binario funzionale in x nel Modello 1 e sia: $s = \{s_1, s_2, ..., s_n\}$ un insieme nel Modello 1.
Gli associati degli elementi di s rispetto a $P(x, y)$ siano dati da $m_1, ..., m_n$ dove $P(s_i, m_i)$ è vera. Sia $e_1, ..., e_k$ la lista degli associati distinti tra gli $m_1, ..., m_n$. Allora $2^{e_1} + \ldots + 2^{e_k}$

[4]Per uniformità di notazione con il testo di riferimento [1], indicheremo con dei numeri progressivi i modelli che nel testo sono numerati. Indicheremo invece con delle lettere maiuscole calligrafiche i modelli più semplici, che nel testo non sono numerati.

è l'insieme di tutti e soli gli associati di s rispetto a $P(x, y)$. Dunque nel Modello 1 è valido l'Assioma di Sostituzione.
Vediamo un esempio per fissare le idee:
sia $P(x, y)$ il predicato binario funzionale in x:

$$x + 1 = y$$

dove + indica l'ordinaria addizione tra numeri naturali. Consideriamo l'insieme

$$s = 290 = 2^8 + 2^5 + 2^1 = \{8, 5, 1\}$$

$P(x, y)$ è vera per le coppie (s_i, m_i):

$$(8, 9),\ (5, 6),\ (1, 2)$$

Gli associati agli elementi di s rispetto a $P(x, y)$ sono dunque $9, 6$ e 2. In questo caso gli m_i sono tutti distinti quindi coincidono con gli e_i. Consideriamo allora l'insieme

$$\{9, 6, 2\} = 2^9 + 2^6 + 2^2 = 580$$

580 è ovviamente un insieme del Modello 1 ed ha per elementi tutti e soli gli associati di s rispetto al predicato $P(x, y)$.
Per concludere la dimostrazione, siano $h_1, ..., h_u$ sottoinsiemi distinti di s. Si ha che $2^{h_1} + \ldots + 2^{h_u}$ è l'insieme potenza di s. Dunque l'Assioma della Potenza è valido nel Modello 1.

1.3.2 Mutua indipendenza di E, S e P

Un modello per E + S + ¬P

L'Assioma della Potenza è indipendente dagli assiomi di Estensione e di Sostituzione, infatti abbiamo già visto in 1.2.1 che nel modello $\mathcal{A}$ composto dal solo insieme z, e la cui tavola è data da

$z \in z$	**F**

valgono E e S. Osserviamo che nel modello $\mathcal{A}$ non esiste $\mathscr{P}(z)$ dato che non c'è alcun insieme in $\mathcal{A}$ il cui solo elemento è z. Dunque, nel modello $\mathcal{A}$ l'Assioma della Potenza non è valido.

Un modello per E + ¬S + P

Un modello in cui valgono E e P ma non S è il modello $\mathcal{B}$ che abbiamo già usato in 1.2.2 per dimostrare l'indipendenza di S da E. Abbiamo già visto che in tale modello non vale S. P invece è facilmente verificato osservando che $\mathscr{P}(z) = z$, che è un insieme del modello.

Un modello per ¬E + S + P

Cerchiamo ora un modello in cui siano validi S e P ma non E:
Modello 2: Il dominio di individui consiste di 0, 1, 2, 3, ... dove

$(x \in y)$ se e solo se (x appare come esponente nell'unica rappresentazione binaria di $y-1$, se $y > 1$, e 0 e 1 sono ciascuno un insieme vuoto)

Ma $0 \in 2$ mentre $1 \notin 2$, e quindi $0 \neq 1$.
Dal momento che abbiamo due insiemi con gli stessi elementi che non sono uguali (perché appartengono a insiemi differenti), E non è valido nel Modello 2. D'altra parte, con un ragionamento analogo a quello fatto per il Modello 1, si verifica che S e P sono validi nel Modello 2.

1.4 L'Assioma dell'Unione [U]

Se in un modello valgono E, S e P, valgono i seguenti teoremi:

Teorema 1.2. *Dato comunque un n, con $n = 0, 1, 2, \ldots$, esiste un insieme che possiede esattamente n elementi.*

Dimostrazione. Se $n = 0$, allora l'insieme nullo $\emptyset$ è un insieme che ha 0 elementi. Sia ora n un qualunque numero naturale non nullo, ossia $n = 1, 2, 3, \ldots$. Si consideri l'insieme p ottenuto formando per n volte consecutive l'insieme potenza, cominciando da $\emptyset$, ossia

$$p = \mathscr{P}(\ldots \mathscr{P}(\mathscr{P}(\emptyset)) \ldots)$$

In virtù dell'assioma delle potenze un tale insieme p esiste. È ovvio che p possiede i seguenti n elementi distinti:

$$\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \ldots, \{\ldots \{\emptyset\} \ldots\}$$

Si consideri ora l'insieme

$$q = \{x \mid (x \in p) \wedge ((x = \emptyset) \vee (x = \{\emptyset\}) \vee \ldots \vee \{x = \{\ldots \{\emptyset\} \ldots\}))\}$$

che esiste grazie a allo schema di specificazione (1.3) e all'esistenza di p. L'insieme q ha precisamente n elementi distinti, essendo

$$q = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \ldots, \{\ldots \{\emptyset\} \ldots\}\}$$

□

Teorema 1.3. *Dati comunque n insiemi a_1, a_2, ..., a_n con $n = 1, 2, 3, \ldots$, esiste l'insieme $t = \{a_1, a_2, \ldots, a_n\}$*

Dimostrazione. Per il teorema 1.2, per ogni $n = 1, 2, 3, \ldots$ esiste l'insieme q dato da

$$q = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \ldots, \{\ldots\{\emptyset\}\ldots\}\}$$

che possiede n elementi distinti. Si consideri ora il predicato funzionale in x su q

$$\begin{aligned} f(x,y) \equiv & ((x = \emptyset) \wedge (y = a_1)) \vee ((x = \{\emptyset\}) \wedge (y = a_2)) \\ & \vee \ldots \\ & \vee ((x = \{\ldots\{\emptyset\}\ldots\}) \wedge (y = a_n)) \end{aligned} \tag{1.7}$$

Per l'assioma di Sostituzione S, l'insieme

$$t = \{y \mid ((\exists x)(x \in q) \wedge f(x,y))\}$$

esiste e ovviamente

$$t = \{a_1, a_2, \ldots, a_n\}$$

□

Corollario 1.1. *(**Assioma della coppia**) Dati comunque due insiemi a e b, esiste l'insieme $c = \{a, b\}$.*

Osservazione 1.3. *L'assioma della coppia ci permette di definire in maniera rigorosa il concetto di coppia ordinata:*

$$(x, y) = \{\{x\}, \{x, y\}\}$$

Si può poi definire il concetto di prodotto cartesiano di due insiemi, di relazione e di funzione.[5]

Grazie al teorema 1.3 che abbiamo appena enunciato, è possibile affermare che se esiste un insieme s con un numero finito di elementi

$$s = \{a_1, a_2, a_3\}$$

in cui ciascun elemento di s abbia a sua volta un numero finito di elementi, siano

$$a_1 = \{a, b, c\},\ a_2 = \{m, n\},\ a_3 = \{p, q\}$$

Allora nel modello esiste l'insieme

$$t = \{a, b, c, m, n, p, q\}$$

L'insieme t è l'insieme di tutti e soli gli elementi di tutti gli elementi di s.
Tuttavia, se s avesse avuto un numero illimitato di elementi, o se uno dei suoi elementi

[5]Queste nozioni non sono centrali in questa tesi, per vederle nel dettaglio rimandiamo a [1] cap.III

avesse avuto un numero illimitato di elementi, non si sarebbe potuta dedurre sulla base di E, S e P l'esistenza dell'insieme t nel modello considerato.
Per garantire l'esistenza dell'insieme di tutti elementi di tutti gli elementi di un dato insieme è necessario introdurre un nuovo assioma:

Assioma dell' Unione:

$$(\forall s)(\exists t)(\forall x)((x \in t) \leftrightarrow (\exists z)((z \in s) \wedge (x \in z))) \qquad ([\mathrm{U}])$$

L'insieme la cui esistenza è asserita dall'Assioma dell'Unione è detto *insieme unione* degli elementi di s, o *insieme somma* di s.
La sua unicità è garantita dall'Assioma di Estensione. Dunque quando vale E, l'unico insieme unione degli elementi di s si indica con $\bigcup s$ ed è possibile scriverlo come

$$\bigcup s = \{x \mid (\exists z)((z \in s) \wedge (x \in z))\} \tag{1.8}$$

Supponendo che nella teoria degli insiemi esistano due insiemi a e b, il teorema 1.3 garantisce l'esistenza dell'insieme $\{a, b\}$. Per l'assioma dell'unione esiste l'insieme $\bigcup\{a, b\}$. Per (1.8) si ha:

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

In corrispondenza dunque a ogni insieme u e a ogni insieme v esiste l'insieme t i cui elementi sono tutti e soli gli elementi di u o di v. Questo insieme prende il nome di *unione* di u e v e si denota con $u \cup v$. Dunque

$$u \cup v = \bigcup\{u, v\} = \{x \mid (x \in u) \vee (x \in v)\}$$

Entrambi i simboli $\bigcup$ e $\cup$ che compaiono, per esempio, in $\bigcup s$ e $u \cup v$ rispettivamente, si chiamano *operatore di unione*. Nel primo caso, $\bigcup$ opera sull'insieme s unendo gli elementi degli elementi di s nell'insieme $\bigcup s$. Nel secondo caso, $\cup$ opera su u e v unendo i loro elementi nell'insieme $u \cup v$. Così, nel primo caso, $\bigcup$ è un operatore unario e nel secondo caso è un operatore binario.

1.4.1 Consistenza di E + S + P + U

Per quanto già visto sulla consistenza di E + S + P (sezione 1.3.1), per dimostrare la consistenza di E + S + P + U è sufficiente mostrare che l'assioma U è valido nel Modello 1, in cui valgono gli altri tre assiomi. Ogni insieme s del Modello 1 ha un numero finito di elementi, quindi ci sono in tutto un numero finito di insiemi distinti $e_1, e_2, ..., e_n$ che sono gli elementi di tutti gli elementi di s. Consideriamo allora

$$h = 2^{e_1} + 2^{e_2} + \ldots + 2^{e_n}$$

h è un insieme del Modello 1 e inoltre $h = \bigcup s$. Dunque, ogni insieme del Modello 1 ha un insieme somma in quel modello, quindi vale U.

1.4.2 Mutua indipendenza di E, S, P e U

Per dimostrare che E, S, P e U formano un sistema indipendente di assiomi mostriamo che per ogni assioma esiste un modello per gli altri tre assiomi in cui esso non è valido.

Un modello per $\neg$E + S + P + U

Abbiamo già visto in 1.3.2 che nel Modello 2 valgono S e P ma non E. Come per il Modello 1, l'Assioma dell'Unione è valido nel Modello 2.

Un modello per E + $\neg$S + P + U

Consideriamo il modello $\mathcal{B}$ che abbiamo usato in 1.2.2 per dimostrare l'indipendenza di S da E. Il dominio di individui è costituito dal solo insieme z e la cui tavola è data da

$z \in z$	**V**

Abbiamo già visto che in questo modello E è valido mentre S non lo è. Osserviamo che $\mathscr{P}(z) = \bigcup z = z$ quindi P e U sono validi.

Un modello per E + S + $\neg$P + U

Nel modello $\mathcal{A}$ composto dal solo insieme z, e la cui tavola è data da

$z \in z$	**F**

che abbiamo già considerato per provare la consistenza di E + S, si ha che $\bigcup z = z$. Dunque in $\mathcal{A}$ è valido U. Tuttavia P non è valido in $\mathcal{A}$ dal momento che in questo modello non esiste l'insieme $\mathscr{P}(z) = \{z\}$.

Un modello per E + S + $\neg$U

Consideriamo il
Modello 3: Il dominio di individui consiste di 0, 1, 2, 3, ... dove

$$(x \in y) \textit{ se e solo se } \begin{cases} \exists z \leqslant x \text{ tale che } & y = \frac{1}{2}(x+1)(x+2) - z \\ \textit{oppure} & \\ \exists z \geqslant x \text{ tale che } & y = \frac{1}{2}(z+1)(z+2) - x \end{cases} \tag{1.9}$$

Osserviamo che nel Modello 3:

1. l'unico insieme vuoto è 0 ($\frac{1}{2}(x+1)(x+2) > x$)

2. un insieme ha al più due elementi distinti. Per dimostrarlo consideriamo la funzione $f(x) = \frac{1}{2}x(x+1)$, che è monotona strettamente crescente (la derivata $x+\frac{1}{2}$ è sempre positiva per $x > 0$, quale è il nostro caso). Fissato allora $y > 0$ esiste un unico $x \geq 0$ tale che $\frac{1}{2}x(x+1) < y \leq \frac{1}{2}(x+1)(x+2)$. Osserviamo ora che nell'intervallo dato dalla disuguaglianza precedente cadono $\frac{1}{2}(x+1)(x+2) - \frac{1}{2}x(x+1) = \frac{1}{2}(x+1)(x+2-x) = x+1$ numeri naturali, tra cui l'y fissato. Dunque, poiché la differenza tra $\frac{1}{2}(x+1)(x+2)$ e y è minore di $x+1$, esiste, ed è unico, uno $z \leq x$ che verifica l'uguaglianza $y = \frac{1}{2}(x+1)(x+2) - z$. Scambiando x e z si trova una coppia che verifica la seconda uguaglianza e di conseguenza l'altro elemento dell'insieme y. Nel caso in cui x e z siano uguali, le due soluzioni coincidono e y ha un solo elemento. Dunque:

3. per ogni coppia di numeri naturali m e n con $m \leq n$, l'insieme

$$\frac{1}{2}(n+1)(n+2) - m$$

   è l'unico insieme i i cui elementi sono m e n

4. gli elementi di un insieme s sono gli unici numeri naturali m e n con $m \leq n$ tali che

$$s = \frac{1}{2}(n+1)(n+2) - m$$

L'Assioma di Estensione è valido nel Modello 3, infatti se si considerano due numeri naturali distinti s_1 e s_2 allora (per il punto 4 dell'osservazione precedente) essi sono insiemi distinti.
Ogni insieme del modello ha al più due elementi distinti e per il punto 3 dell'osservazione precedente, dati due numeri naturali m e n esiste un insieme nel modello i cui soli elementi sono m e n. Dunque nel Modello 3 è valido l'Assioma di Sostituzione.
L'Assioma dell'Unione invece non vale. Si consideri ad esempio l'insieme 12.

$$12 = \{4, 3\},\ 4 = \{2\},\ 3 = \{1, 0\}$$

Non esiste nel Modello 3 alcun insieme i cui elementi sono 0, 1 e 2, dunque 12 non ha alcun insieme somma nel modello.

1.5 Intersezione di insiemi

Si supponga che nella teoria degli insiemi (con gli assiomi introdotti finora: E, S, P, U) esista un insieme b tale che

$$b = \{a_1, a_2, a_3\}$$

con

$$a_1 = \{m, n, p\}, \quad a_2 = \{m, n, q\}, \quad a_3 = \{m, n, p, q\}$$

dove m, n, p e q sono insiemi distinti. Allora in virtà dei nostri assiomi esiste l'insieme

$$\bigcup b = \{m, n, p, q\}$$

Di conseguenza, per S (in particolare per (1.3)) esiste anche l'insieme

$$\{m, n\} = \left\{x \mid (x \in \bigcup b) \wedge (x \in a_1) \wedge (x \in a_2) \wedge (x \in a_3)\right\}$$

$\{m, n\}$ è l'insieme di tutti e soli gli elementi comuni a tutti gli elementi di b. Si è soliti chiamare $\{m, n\}$ l' *insieme intersezione* dell'insieme b e indicarlo con $\bigcap b$.
Anche per un qualunque insieme s i nostri assiomi garantiscono l'esistenza dell'insieme intersezione $\bigcap s$:

$$\bigcap s = \{x \mid (x \in \bigcup s) \wedge (\forall z)((z \in s) \rightarrow (x \in z))\} \tag{1.10}$$

Analogamente a quanto visto per gli operatori di unione, anche per l'intersezione esiste un operatore binario. Supponendo che esistano due insiemi a e b nella teoria degli insiemi, allora esiste l'insieme

$$\bigcap\{a, b\} = \{x \mid (x \in a) \wedge (x \in b)\}$$

Definiamo dunque $a \cap b$ come $\bigcap\{a, b\} = \{x \mid (x \in a) \wedge (x \in b)\}$.

Capitolo 2

Prove di consistenza e indipendenza relative

2.1 Relativizzazione

Informalmente, dato un modello M, una *classe* nel modello è un sottoinsieme del dominio di individui. Una *classe propria* è un sottoinsieme che non è anche elemento del dominio di individui. Formalmente, una classe non è altro che una formula. Per esempio se consideriamo la classe propria

$$\mathbf{V} = \{x | x = x\}$$

quando scriviamo $y \in V$ stiamo in realtà scrivendo la formula $y = y$.
Per spiegare formalmente cosa si intende quando diciamo che "un enunciato è vero in una classe" introduciamo la nozione di relativizzazione, di cui faremo uso in modo implicito nello sviluppo della trattazione.
In realtà per i risultati elementari presentati in questa tesi non è necessario utilizzare la nozione di relativizzazione che risulta invece indispensabile qualora si volessero trattare le dimostrazioni di consistenza e indipendenza dal punto di vista sintattico.[1] I risultati presentati qui saranno invece esposti utilizzando un approccio meno formale, introducendo esplicitamente i modelli di cui faremo uso e lavorando su di essi.

Def 2.1. *Sia* $\boldsymbol{M}$ *una classe qualsiasi. Per ogni formula* ϕ *definiamo* $\phi^{\boldsymbol{M}}$*, la relativizzazione di* ϕ *a* $\boldsymbol{M}$*, per induzione su* ϕ*:*

1. $(x = y)^{\boldsymbol{M}}$ *è* $x = y$
2. $(x \in y)^{\boldsymbol{M}}$ *è* $x \in y$
3. $(\phi \wedge \psi)^{\boldsymbol{M}}$ *è* $\phi^{\boldsymbol{M}} \wedge \psi^{\boldsymbol{M}}$

[1] Vedi [4]

4. $(\neg\phi)^{\boldsymbol{M}}$ *è* $\neg(\phi^{\boldsymbol{M}})$

5. $(\exists x\ \phi)^{\boldsymbol{M}}$ *è* $\exists x(x \in \boldsymbol{M} \wedge \phi^{\boldsymbol{M}})$

Osservazione 2.1. *Più formalmente,* $\boldsymbol{M}$ *è in realtà una formula* $\boldsymbol{M}(v)$*,* ϕ *è un'altra formula, e stiamo definendo, nella metateoria, una terza formula* $\phi^{\boldsymbol{M}}$*. La formula* $(\exists x\ \phi)^{\boldsymbol{M}}$ *dovrebbe essere in realtà* $\exists x(\boldsymbol{M}(x) \wedge \phi^{\boldsymbol{M}})$*.*

Osservazione 2.2. *Intuitivamente, sia* $\phi(x_1, ..., x_n)$ *una formula con* $x_1, ..., x_n$ *variabili libere, allora per* $x_1, ..., x_n \in \boldsymbol{M}$*,* $\phi^{\boldsymbol{M}}(x_1, ..., x_n)$ *"afferma" che* $\phi^{\boldsymbol{M}}(x_1, ..., x_n)$ *è vera con la restrizione che le variabili vincolate di* $\boldsymbol{M}$ *varino su* $\boldsymbol{M}$*.*
Per $x_1, ..., x_n$ *non in* $\boldsymbol{M}$*, l'interpretazione intuitiva di* $\phi^{\boldsymbol{M}}(x_1, ..., x_n)$ *non è chiara, ma questo risulta irrilevante per lo sviluppo della teoria.*[2]

Osservazione 2.3. *Abbiamo definito* $\phi^{\boldsymbol{M}}$ *solo per le formule non abbreviate in cui compaiono solo i simboli primitivi del linguaggio. Per le abbreviazioni logiche questo non crea alcun problema: si può verificare che mantengono il loro significato previsto. Per esempio,* $(\phi \vee \psi)^{\boldsymbol{M}}$ *è in realtà* $\neg(\neg\phi \wedge \neg\psi)^{\boldsymbol{M}}$*, che per la definizione di relativizzazione diventa* $\neg(\neg(\phi^{\boldsymbol{M}}) \wedge \neg(\psi^{\boldsymbol{M}})$*, cioè* $\phi^{\boldsymbol{M}} \vee \psi^{\boldsymbol{M}}$*. La situazione per le abbreviazioni di relazioni e operazioni definite nella teoria degli insiemi, come* $\subseteq$ *o* $\mathscr{P}$*, è più delicata. In ogni caso, nel seguito di questo elaborato, queste nozioni verranno trattate informalmente.*

Def 2.2. *Sia* $\boldsymbol{M}$ *una classe qualsiasi.*

1. *Per un enunciato* ϕ*, "*ϕ *è vero in* $\boldsymbol{M}$*" significa* $\phi^{\boldsymbol{M}}$

2. *Per un insieme di enunciati* S*, "*S *è vero in* $\boldsymbol{M}$*" o "*$\boldsymbol{M}$ *è un modello per* S*" significa che ogni enunciato in* S *è vero in* M*.*

Il risultato fondamentale che useremo, implicitamente, per le dimostrazioni di consistenza relative è il seguente.

Lemma 2.1. *Siano* S *e* T *due insiemi di enunciati nel linguaggio della teoria degli insiemi. Supponiamo che per una certa classe* $\boldsymbol{M}$ *possiamo dimostrare da* T *che* $\boldsymbol{M} \neq 0$ *e che* $\boldsymbol{M}$ *sia un modello per* S*. Allora se* T *è consistente anche* S *lo è.*[3]

Dimostrazione. Se S fosse inconsistente, si potrebbe provare $\chi \wedge \neg\chi$ da S per un certo (o qualunque) enunciato χ. Dimostrando da T che S è vero in $\mathbf{M}$ si avrebbe $\chi^M \wedge \neg\chi^M$, che sarebbe una contraddizione. Dunque T sarebbe inconsistente. □

[2][4] cap. IV §2

[3]Una trattazione più formale di questo risultato si può trovare in [4] cap. IV §8

2.2 L'Assioma dell'Infinito [I]

Gli assiomi visti finora non garantiscono l'esistenza di un insieme con un numero illimitato di elementi. Per uno sviluppo soddisfacente della teoria degli insiemi, si ritiene necessaria l'esistenza di un insieme con un numero illimitato di elementi. Per questo viene introdotto l'Assioma dell'Infinito.

Assioma dell'Infinito: Esiste un insieme W tale che:

$$\emptyset \in W \tag{2.1}$$

e

$$\text{se } x \in W, \text{ allora } (x \cup \{x\}) \in W \tag{2.2}$$

Formalmente:

$$(\exists W)((\emptyset \in W) \wedge (\forall x)((x \in W) \rightarrow ((x \cup \{x\}) \in W))) \tag{[I]}$$

Introduciamo una notazione e una definizione che saranno utili in seguito.

Def 2.3. $x^+ = x \cup \{x\}$ *è il successivo immediato di* x

Grazie all'introduzione della nozione di *successivo immediato* possiamo enunciare l'assioma dell'Infinito come segue:
[I]: Esiste un insieme W tale che l'insieme vuoto è un elemento di W e tale che, se x è un elemento di W, lo è anche il suo successivo immediato x^+.

Con gli assiomi fin qui introdotti è possibile dimostrare che

Teorema 2.1. *Esiste un unico insieme* ω *che soddisfa le condizioni (2.1) e (2.2) e che è l'insieme minimale soddisfacente queste condizioni, nel senso che per qualunque altro insieme* V *che soddisfa (2.1) e (2.2), si ha che* $\omega \subseteq V$.

Dimostrazione. Sia W un insieme che soddisfa le condizioni (2.1) e (2.2) e che, grazie all'assioma di infinità, esiste. W è dunque un insieme tale che $\emptyset \in W$, e tale che, se $x \in W$ allora anche $x^+ \in W$. Si consideri l'insieme potenza $\mathscr{P}(W)$, e sia H l'insieme di tutti quei sottoinsiemi h di W soddisfacenti ciascuno le condizioni (2.1) e (2.2): ogni elemento h di H è un insieme tale che $\emptyset \in h$ e tale che, se $x \in h$ allora anche $x^+ \in h$. Ovviamente, H è un sottoinsieme di $\mathscr{P}(W)$ che esiste, in virtù dello schema di sostituzione (in particolare per 1.3).
Si consideri ora

$$\omega = \cap H$$

che esiste, in base a quanto visto sull'intersezione di insiemi (1.10).
Facciamo ora vedere che ω soddisfa le condizioni (2.1) e (2.2). Dato che $\emptyset \in h$ per ogni $h \in H$, si vede che $\emptyset \in \bigcap H$. Così, effettivamente $\emptyset \in \omega$. Dunque, ω soddisfa la condizione (2.1). Si supponga ora $x \in \omega$, ossia $x \in h$ per ogni $h \in H$. Dato che ogni h soddisfa la condizione (2.2) e dato che abbiamo supposto che $x \in h$ per ogni $h \in H$, vediamo che $x \cup \{x\} = x^+$ appartiene anch'esso a ogni h. Di conseguenza, $x^+ \in \bigcap H = \omega$. Dunque, $x^+ \in \omega$ e ω soddisfa la condizione (2.2).
Per dimostrare la minimalità di ω si osservi che, se V è un qualunque insieme soddisfacente le condizioni (2.1) e (2.2), allora, con una dimostrazione analoga a quella appena data si mostra che $\omega \cap V$ è anch'esso un insieme soddisfacente le condizioni (2.1) e (2.2). Tuttavia, $\omega \cap V \subseteq \omega \subseteq W$ e quindi $\omega \cap V$ è uno degli h sopra descritti. Dunque, $\omega \subseteq \omega \cap V$ il che implica $\omega \subseteq V$ come si voleva.
Per dimostrare l'unicità di ω, sia v un altro insieme che gode delle stesse proprietà di ω. Applicando quanto provato sulla minimalità a ω e a v, otteniamo rispettivamente

$$\omega \subseteq v \quad e \quad v \subseteq \omega$$

Di conseguenza $\omega = v$ e quindi ω è unico □

Chiamiamo questo insieme ω *l'insieme di tutti i numeri naturali.*

Def 2.4. *Un numero naturale è un elemento dell'insieme ω.*

Osservazione 2.4. *Ogni numero naturale è un insieme.*

2.2.1 Consistenza di E + S + P + U + I

È possibile dimostrare che in ogni modello in cui valgono tutti gli assiomi elencati finora sono validi gli assiomi di PA. Per il Secondo Teorema di Incompletezza di Gödel dunque sappiamo che è impossibile dimostrare all'interno della teoria sviluppata finora la consistenza del sistema di assiomi su cui si basa.
Le successive dimostrazioni di consistenza saranno dunque dimostrazioni di consistenza relative all'assunzione che E + S + P + U + I sia un sistema di assiomi consistente e che dunque esista un modello in cui siano tutti validi.

Assunzione di consistenza: Il sistema di assiomi E + S + P + U + I è consistente, dunque esiste un modello nel quale sono tutti validi.

2.2.2 Mutua indipendenza di E, S, P, U e I

Un modello per E + S + P + U + ¬I

Consideriamo il Modello 1 che abbiamo già usato più volte. In esso abbiamo già visto che valgono E, S, P e U.

Facciamo ora vedere che I non vale nel Modello 1. Si supponga per assurdo che l'Assioma dell'Infinito valga nel modello. Ma allora deve esistere un insieme W tale che

$$0 \in W,$$
$$0^+ = 0 \cup \{0\} = 0 + 2^0 = 1 \in W,$$
$$1^+ = 1 \cup \{1\} = 1 + 2^1 = 3 \in W,$$
$$3^+ = 3 \cup \{3\} = 3 + 2^3 = 11 \in W,$$
$$11^+ = 11 \cup \{11\} = 11 + 2^{11} = 2059 \in W, \ldots$$

La successione dei successivi immediati è strettamente crescente, proviamolo per induzione:
Abbiamo già visto che $0^+ = 1$ e $1 > 0$, dunque il passo base è verificato.
Assumiamo come ipotesi induttiva $n^+ > n$ e proviamo che $(n^+)^+ > n^+$:
$(n^+)^+ = n^+ \cup \{n^+\} = n^+ + 2^{n^+}$ che per ipotesi induttiva è maggiore di $n + 2^n = n \cup \{n\} = n^+$. W quindi deve essere necessariamente infinito, ma ogni insieme del Modello 1 possiede un numero finito di elementi, dunque W non può essere un insieme del Modello 1. Abbiamo così provato che I è indipendente dagli altri quattro assiomi.

Un modello per $\neg$E + S + P + U + I

Modello 4: Sia K un modello per E + S + P + U + I, supponiamo esista per l'assunzione di consistenza. Sia K' il modello il cui dominio di individui è quello di K con l'eccezione dell'insieme vuoto $\emptyset$ di K. Denotati con $\in$ e $\in'$ rispettivamente i simboli di predicato di appartenenza di K e K', poniamo

$$(x \in' y) \text{ se e solo se } (x \in y \text{ e } x \neq \emptyset)$$

Si ha dunque, ad esempio,

$$\text{il solo insieme vuoto del modello } K' \text{ è l'insieme } \{\emptyset\}$$

dato che in K' nessun insieme è un elemento di $\{\emptyset\}$.
In $(K', \in')$ risulta che $\{\{\emptyset\}\}$ e $\{\emptyset, \{\emptyset\}\}$ hanno gli stessi elementi. Tuttavia,

$$\{\{\emptyset\}\} \in' \{\{\{\emptyset\}\}\} \text{ mentre } \{\emptyset, \{\emptyset\}\} \notin' \{\{\{\emptyset\}\}\}$$

Dunque in $(K', \in')$ insiemi con gli stessi elementi non sono elementi dei medesimi insiemi, quindi non è rispettato l'assioma di sostitutività dell'uguaglianza e per questo i due insiemi non possono essere uguali. Quindi l'Assioma di Estensione non vale nel Modello K'. Gli altri assiomi sono validi nel Modello 4.[4]

[4]Lo vedremo esplicitamente nella sezione 2.5.1

Un modello per E + S + P + U + ¬I

Abbiamo già visto un modello per il sistema di assiomi E + S + P + U + ¬I (il Modello 1). In questa sezione vedremo un altro modello per questo sistema di assiomi che ci sarà utile, assieme alla teoria sviluppata per costruirlo, per trovare un modello per E + ¬S + P + U + I, che osserveremo nella prossima sezione.

Def 2.5. *Sia $\mathscr{P}(u)$ l'insieme potenza di u, definiamo:*

1. $\mathscr{P}_0(u) = u$
2. $\mathscr{P}_{x^+}(u) = \mathscr{P}(\mathscr{P}_x(u))$, *per ogni numero naturale x.*

Si consideri il predicato binario, funzionale in x sull'insieme ω di tutti i numeri naturali

$$y = \mathscr{P}_x(\emptyset) \tag{2.3}$$

Per l'Assioma di Sostituzione, l'insieme S di tutti gli associati degli elementi di ω rispetto al predicato (2.3) esiste e

$$S = \{\emptyset, \mathscr{P}(\emptyset), \mathscr{P}(\mathscr{P}(\emptyset)), \ldots\} \tag{2.4}$$

Per l'Assioma dell'Unione allora esiste l'insieme somma A dell'insieme S:

$$A = \bigcup\{\emptyset, \mathscr{P}(\emptyset), \mathscr{P}(\mathscr{P}(\emptyset)), \ldots\} \tag{2.5}$$

Per studiare le proprietà dell'insieme A enunciamo una serie di risultati utili.

Osserviamo preliminarmente che valgono:

$$x \in \mathscr{P}(y) \leftrightarrow (x \subseteq y) \leftrightarrow \mathscr{P}(x) \subseteq \mathscr{P}(y) \tag{2.6}$$

$$(\mathscr{P}(x) \in \mathscr{P}(y)) \leftrightarrow (\mathscr{P}(\mathscr{P}(x)) \in \mathscr{P}(\mathscr{P}(y))) \rightarrow (x \in y) \tag{2.7}$$

Lemma 2.2. *Dati comunque due numeri naturali m e n, si ha*

1. *$m < n$ se e solo se $\mathscr{P}_m(\emptyset) \in \mathscr{P}_n(\emptyset)$*
2. *$m \leq n$ se e solo se $\mathscr{P}_m(\emptyset) \subseteq \mathscr{P}_n(\emptyset)$*

Dimostrazione. Dato che $\mathscr{P}_0(\emptyset) = \emptyset$ e $\emptyset \in \mathscr{P}_n(\emptyset)$ per ogni numero naturale non nullo n, si vede chiaramente che

$$0 < n \text{ se e solo se } \mathscr{P}_0(\emptyset) \in \mathscr{P}_n(\emptyset)$$

Si supponga ora che $m < n$ se e solo se $\mathscr{P}_m(\emptyset) \in \mathscr{P}_n(\emptyset)$ valga per m e dimostriamo che vale per m^+. Ma

$$\left(m^+ < n^+\right) \leftrightarrow (m < n) \leftrightarrow (\mathscr{P}_m(\emptyset) \in \mathscr{P}_n(\emptyset))$$

e quindi dalla (2.7) segue che

$$m^+ < n^+ \text{se e solo se } \mathscr{P}_{m^+}(\emptyset) \in \mathscr{P}_{n^+}(\emptyset)$$

Dunque abbiamo mostrato per induzione finita che il punto 1 è vero.
Per dimostrare il punto 2 è sufficiente osservare che

$$(m \leqslant n) \leftrightarrow \left(m < n^+\right) \leftrightarrow \mathscr{P}_m(\emptyset) \in \mathscr{P}_{n^+}(\emptyset) \leftrightarrow \mathscr{P}_m(\emptyset) \subseteq \mathscr{P}_n(\emptyset)$$

□

Lemma 2.3. *Per ogni numero naturale m*

$$x \in \mathscr{P}_m(\emptyset) \text{ implica } x \subseteq \mathscr{P}_m(\emptyset)$$

Dimostrazione. Ovviamente, $x \in \mathscr{P}_0(\emptyset) = \emptyset$ implica $x \subseteq \mathscr{P}_0(\emptyset$.
Supponiamo ora che $x \in \mathscr{P}_m(\emptyset)$ con $m > 0$. Ma allora $x \subseteq \mathscr{P}_{m^-}(\emptyset)$ e per il lemma 2.2 si vede che $x \subseteq \mathscr{P}_m(\emptyset)$, come si voleva. □

Per come è stato definito l'insieme A, il lemma 2.3 implica i seguenti corollari.

Corollario 2.1. *Se $x \in A$ allora $x \subseteq \mathscr{P}_n(A)$ per qualche numero naturale n.*

Corollario 2.2. *Se $x \in A$, allora $x \subseteq A$*

Def 2.6. *Un insieme s si dice transitivo se e solo se per ogni x: $x \in s$ implica $x \subseteq s$.*

Il lemma 2.3 e il corollario 2.2 stabiliscono rispettivamente che $\mathscr{P}_m(\emptyset)$ per ogni $m \in \omega$, e A, sono insiemi transitivi.

Lemma 2.4. *Per ogni numero naturale m:*

1. *$x \in \mathscr{P}_{m+2}(\emptyset)$ implica $\bigcup x \in \mathscr{P}_{m+1}(\emptyset)$*
2. *$x \in \mathscr{P}_1(\emptyset)$ implica $\bigcup x \in \mathscr{P}_1(\emptyset)$*

Dimostrazione. L'ipotesi del punto 1 implica $x \subseteq \mathscr{P}_{m+1}(\emptyset)$. Quindi, se $y \in x$, allora $y \in \mathscr{P}_m(\emptyset)$ che a sua volta implica $y \subseteq \mathscr{P}_m(\emptyset)$. Così, se $z \in y$, allora $z \in \mathscr{P}_m(\emptyset)$. Di conseguenza, $z \in \bigcup x$ implica $z \in \mathscr{P}_m(\emptyset)$. Ma allora $\bigcup x \subseteq \mathscr{P}_m(\emptyset)$ e $\bigcup x \in \mathscr{P}_{m+1}(\emptyset)$, come si voleva.
Per dimostrare il punto 2 basta osservare che $\emptyset \in \mathscr{P}_1(\emptyset)$ □

Corollario 2.3. *Se $x \in A$, allora $\bigcup x \in A$.*

Lemma 2.5. *Per ogni numero naturale m*

$$x \in \mathscr{P}_m(\emptyset) \text{ implica } \mathscr{P}(x) \in \mathscr{P}_{m+1}(\emptyset)$$

Dimostrazione. $x \in \mathscr{P}_m(\emptyset)$ per la (2.6) implica $\mathscr{P}(x) \subseteq \mathscr{P}_m(\emptyset)$ e quindi $\mathscr{P}(x) \subseteq \mathscr{P}_{m+1}(\emptyset)$, come si voleva. □

Corollario 2.4. *Se $x \in A$, allora $\mathscr{P}(x) \in A$*

Def 2.7. *Un numero naturale $r(x)$ si chiama rango di un elemento x di A se e solo se:*

$$x \in \mathscr{P}_{r(x)}(\emptyset) \text{ e } x \notin \mathscr{P}_{r(x)-1}(\emptyset)$$

Cioè $r(x)$ è l'indice del primo intervento di x come elemento di qualche $\mathscr{P}_m(\emptyset)$

Lemma 2.6. *Dati comunque due elementi x e y di A*

1. *$y \in x$ implica $r(y) < r(x)$*
2. *$y \subseteq x$ implica $r(y) \leq r(x)$*

Dimostrazione. Dato che $x \in \mathscr{P}_{r(x)}(\emptyset)$ si ha $x \subseteq \mathscr{P}_{r(x)-1}(\emptyset)$. Ora, se $y \in x$, allora $y \in \mathscr{P}_{r(x)-1}(\emptyset)$ il che implica che $r(y) < r(x)$. D'altra parte, se $y \subseteq x$ allora $y \subseteq \mathscr{P}_{r(x)-1}(\emptyset)$ e quindi $y \in \mathscr{P}_{r(x)}(\emptyset)$, il che implica che $r(y) \leq r(x)$, che è quanto volevamo. □

Corollario 2.5. *Se $x \in A$ allora $x \notin x$.*

Dimostrazione. Se avessimo $x \in x$, allora avremmo $r(x) < r(x)$, che è impossibile. □

Corollario 2.6. *Ogni elemento non vuoto x di A ha un elemento y tale che x e y non hanno elementi in comune.*

Dimostrazione. Per assurdo si supponga che ogni elemento non vuoto x_i di x abbia un elemento in comune con x. Allora si possono presentare due casi:

$$x_1 \in x,\ x_2 \in x_1,\ x_3 \in x_2,\ \ldots,\ x_{n+1} \in x_n,\ \ldots$$

continua indefinitamente, oppure

$$x_1 \in x,\ x_2 \in x_1,\ \ldots,\ x_k \in x_n$$

per qualche $k \leq n$.
Ma dato che ogni elemento di A ha un rango, il primo caso è impossibile perché sappiamo che $y \in x$ implica $r(y) < r(x)$ e non esiste una successione infinita strettamente decrescente di numeri naturali. Il secondo caso è anch'esso impossibile: identifichiamo x con x_0 e consideriamo la successione degli indici degli insiemi

$$x_k \in x_n \in \ldots \in x_2 \in x_1 \in x_0$$

La successione è strettamente decrescente e si dovrebbe avere quindi $k > n$, che porta all'assurdo. □

Lemma 2.7. *Per ogni numero naturale m,*

$$m \in \mathscr{P}_{m+1}(\emptyset) \text{ e } r(m) = m + 1$$

dove $r(m)$ è il rango di m.

Dimostrazione. Chiaramente, $0 \in \mathscr{P}_1(\emptyset)$. Sia $m \in \mathscr{P}_{m+1}(\emptyset)$; dimostriamo che $m^+ \in \mathscr{P}_{m+2}(\emptyset)$: dato che $m \in \mathscr{P}_{m+1}(\emptyset)$, per il lemma 2.3 si ha che $m \subseteq \mathscr{P}_{m+1}(\emptyset)$. Ne segue che $(m \cup \{m\}) \in \mathscr{P}_{m+2}(\emptyset)$. Ma $(m \cup \{m\}) = m^+$ e dunque $m^+ \in \mathscr{P}_{m+2}(\emptyset)$.
Il fatto che $r(m) = m + 1$ si stabilisce in modo simile. □

Corollario 2.7. *L'insieme ω di tutti i numeri naturali non è un elemento di A*

Dimostrazione. Supponiamo per assurdo che $\omega \in A$. Allora, per la definizione di A, deve esistere un numero naturale m tale che $\omega \in \mathscr{P}_m(\emptyset)$. Ma, dato che $m \in \omega$, per il lemma 2.3, si deve avere che $m \in \mathscr{P}_m(\emptyset)$, il che contraddice il lemma 2.7. Dunque la nostra supposizione deve essere falsa. □

Sia $(K, \in)$ un modello per E + S + P + U + I che supponiamo esista per l'assunzione di consistenza. Allora, dato che gli assiomi in questione implicano l'esistenza di A, A è un insieme di $(K, \in)$.
Introduciamo il seguente modello:
Modello 5: Il dominio di individui consiste degli elementi dell'insieme A, e

$$x \in y \text{ se e solo se } x \in y \text{ in } (K, \in)$$

Mostriamo che l'Assioma di Estensione è valido nel Modello 5. Per farlo, dimostriamo preliminarmente un utile lemma:

Lemma 2.8. *Se M è un insieme transitivo, l'Assioma di Estensione è vero in M.*

Dimostrazione. E relativizzato a M diventa

$$\forall x, y \in M(\forall z \in M(z \in x \leftrightarrow z \in y) \rightarrow x = y) \tag{2.8}$$

Se M è transitivo,

$$\forall x(x \in M \rightarrow x \subseteq M)$$

cioè, per definizione di $\subseteq$:

$$\forall x(x \in M \rightarrow \forall z(z \in x \rightarrow z \in M))$$

Ma allora:

$$\{z \in M : z \in x\} = x$$

Da cui si ottiene (2.8), quindi E vale in M. □

Il corollario 2.2 afferma che A è transitivo, dunque per il lemma 2.8 sappiamo che in A vale E.
In virtù dei corollari 2.3 e 2.4, sono validi rispettivamente U e P. Per il corollario 2.7 si ha che nel Modello 5 cade l'Assioma dell'Infinito.

Un modello per E + ¬S + P + U + I

Consideriamo ora l'insieme Q dato da

$$Q = \{A, \mathscr{P}(A), \mathscr{P}(\mathscr{P}(A)), \ldots\}$$

la cui esistenza in $(K, \in)$ è garantita dagli assiomi finora introdotti.
Per l'Assioma dell'Unione allora l'insieme somma B dell'insieme Q esiste e

$$B = \bigcup \{A, \mathscr{P}(A), \mathscr{P}(\mathscr{P}(A)), \ldots\}$$

Osserviamo che i lemmi e i corollari visti per A restano validi (tutti tranne il corollario 2.7) se in essi $\emptyset$ si sostituisce con A e A si sostituisce con B.
Dunque A e B hanno proprietà molto simili, tranne il fatto che mentre $\omega \notin A$, si ha che $\omega \in B$. Infatti dal lemma 2.7 e dalla definizione di A, si vede che $\omega \subseteq A$. Dalla definizione di B sappiamo che $A \subseteq B$ e dato che $A \in \mathscr{P}(A)$, sappiamo che $A \in B$. Dunque:

$$\omega \subseteq A \subseteq B \text{ e } \omega \in B$$

B è un insieme del modello $(K, \in)$, introduciamo il:
Modello 6: Il dominio di individui consiste degli elementi di B e

$$x \in y \text{ se e solo se } x \in y \text{ in } (K, \in)$$

Per il corollario 2.2 esteso a B sappiamo che B è un insieme transitivo, dunque in B vale E. Gli assiomi U e P valgono in virtù dei corollari 2.3 e 2.4 estesi all'insieme B.
Inoltre abbiamo visto che $\omega \in B$, quindi I è valido nel Modello 6.
Tuttavia, S nel Modello 6 non vale: supponiamo per assurdo che S sia valido nel Modello 6 e consideriamo il predicato

$$y = \mathscr{P}_x(A) \tag{2.9}$$

che è funzionale in x sull'insieme ω. Dato che $\omega \in B$, l'insieme M di tutti gli associati degli elementi di ω rispetto al predicato binario (2.9) deve essere un insieme del Modello 6, ossia un elemento di B.
Si ha allora che

$$M = \{A, \mathscr{P}(A), \mathscr{P}(\mathscr{P}(A)), \ldots\} \tag{2.10}$$

Tuttavia, $M \in B$ implica che per qualche $m \in \omega$ $M \subseteq \mathscr{P}_m(A)$. Ma questo contraddice il lemma 2.6:
Definiamo *rango di un elemento x di B* come un numero naturale $r(x)$ tale che

$$x \in \mathscr{P}_{r(x)}(A) \text{ e } x \notin \mathscr{P}_{r(x)-1}(A)$$

Allora si può dimostrare il lemma 2.6 esteso a B: Dati comunque due elementi x e y di B

1. $y \in x$ implica $r(y) < r(x)$

2. $y \subseteq x$ implica $r(y) \leq r(x)$

Ma allora, da $M \subseteq \mathscr{P}_m(A)$ otteniamo $r(M) \leq m$. Ma da (2.10) possiamo vedere che il rango di M deve essere maggiore di ogni $m \in \omega$. Abbiamo così una contraddizione, dunque la supposizione che S sia valido nel Modello 6 è falsa.

2.3 L'Assioma della Scelta [C]

Prima di enunciare l'assioma è necessario introdurre alcune definizioni e risultati preliminari.

Def 2.8. *Due insiemi si dicono disgiunti se non hanno elementi in comune.*

Osservazione 2.5. *Ovviamente, se $x \cap y = \emptyset$ allora x e y sono disgiunti. Tuttavia può accadere che in un modello x e y siano disgiunti senza che esistano né $x \cap y$ né $\emptyset$ nel modello.*
Vediamo un esempio di questa evenienza. Si consideri il modello il cui dominio di individui è costituito da soli due insiemi y e z e la cui tavola è data da

$y \in y$	**V**
$z \in z$	**V**
$y \in z$	**F**
$z \in y$	**F**

Nel modello considerato non esiste un insieme $y \cap z$, così come non esiste un insieme vuoto. Tuttavia y e z sono disgiunti, perché non hanno elementi in comune.
Ovviamente nel modello considerato non vale S, infatti E è valido perché non ci sono insiemi con nomi diversi che hanno gli stessi elementi e dal teorema 1.1 sappiamo che se valgono E e S allora nel modello esiste necessariamente un insieme vuoto.
Osserviamo inoltre che nel modello vale P:

$$\mathscr{P}(z) = \{\{z\}\} = \{z\} = z$$

dato che $z = \{z\}$, e lo stesso vale per y.
Non vale invece U: non esiste un insieme che ha per elementi y e z.
Ovviamente I non vale dato che nel dominio di individui sono presenti solo due insiemi.
Nella prossima sezione verrà presentato l'assioma di regolarità, anche esso non vale nel modello considerato.

Def 2.9. *Un insieme si dice disgiunto se i suoi elementi distinti sono a due a due disgiunti.*

Def 2.10. *Un insieme t si dice un insieme di scelta di un insieme s se t ha uno e un solo elemento in comune con ogni elemento di s.*
Formalmente:

$$(\forall z)((z \in s) \to (\exists w)(\forall x)(((x \in t) \wedge (x \in z)) \leftrightarrow (x = w))) \tag{2.11}$$

Lemma 2.9. *Ogni insieme è un insieme di scelta dell'insieme vuoto $\emptyset$. Inoltre, s non ha insieme di scelta se $\emptyset \in s$.*

Dimostrazione. Chiaramente, se nella (2.11) sostituiamo s con $\emptyset$ allora l'ipotesi della implicazione nella (2.11) è falsa, e quindi l'intera implicazione è vera per ogni insieme t. Inoltre, se nella (2.11) avviene che $\emptyset \in s$, allora ovviamente

$$(\exists w)(\forall x)(((x \in t) \wedge (x \in \emptyset) \leftrightarrow (x = w)))$$

è impossibile per un qualunque insieme t. Dunque, se $\emptyset \in s$, allora s non ha nessun insieme di scelta, come volevamo. □

Dagli assiomi E, S, P e U è possibile dedurre l'esistenza dell'insieme di tutti gli insiemi di scelta di un insieme non vuoto:

Teorema 2.2. *Se s è un insieme non vuoto, allora esiste l'insieme S di tutti gli insiemi di scelta di s.*

Dimostrazione. Per l'assioma di somma, esiste l'insieme $\bigcup s$. Allora, in virtù dell'assioma delle potenze, esiste l'insieme $\mathscr{P}(\bigcup s)$. Ora, utilizzando lo schema di sostituzione (in particolare (1.3)) con

$$P(x) \equiv (\forall y)((y \in s) \to (\exists w)((y \cap x) = \{w\}))$$

si deduce l'insieme S dato da:

$$S = \{x \mid (x \in \mathscr{P}(\bigcup s)) \wedge ((\forall y)((y \in s) \to (\exists w)((y \cap x) = \{w\})))\}$$

che è il desiderato insieme S di tutti gli insiemi di scelta di s. □

Osservazione 2.6. *Il teorema non implica l'esistenza di un insieme di scelta di un insieme s con $\emptyset \notin s$, dato che l'insieme S di tutti gli insiemi di scelta di s potrebbe essere vuoto.*

Corollario 2.8. *Sia s un insieme. Se $\emptyset \in s$, allora l'insieme di tutti gli insiemi scelta di s è l'insieme vuoto $\emptyset$.*

Osservazione 2.7. *Ogni insieme è un insieme di scelta dell'insieme vuoto $\emptyset$, nella teoria degli insiemi dunque non esiste l'insieme di tutti gli insiemi di scelta di $\emptyset$ (l'insieme di tutti gli insiemi è una classe propria). Per questo si conviene di restringere gli insiemi di scelta di $\emptyset$ al solo insieme vuoto $\emptyset$. Dunque l'insieme di tutti gli insiemi di scelta di $\emptyset$ è l'insieme $\emptyset$.*

Per uno sviluppo soddisfacente della teoria degli insiemi, si ritiene necessaria l'esistenza di un insieme di scelta di un insieme disgiunto s con $\emptyset \notin s$. Introduciamo quindi l'Assioma della scelta:
Assioma della scelta: Per ogni insieme disgiunto $s \neq \emptyset$ tale che $\emptyset \notin s$, esiste un insieme di scelta t di s.
Formalmente:

$$\begin{aligned}(\forall s)((\forall z)(\forall y)(((z \in s) \wedge (y \in s) \wedge (z \neq y)) \rightarrow \\ \rightarrow (\exists u)((u \in z) \wedge (\forall v)((v \in z) \vee (v \notin y)))) \rightarrow \\ \rightarrow (\exists t)(\forall z)((z \in s) \rightarrow (\exists w)(\forall x)(((x \in t) \wedge (x \in z)) \leftrightarrow (x = w))))\end{aligned} \tag{[C]}$$

Una volta introdotto C vale anche l'inverso del corollario 2.8. Si può dunque asserire:

Corollario 2.9. *Sia s un insieme disgiunto. L'insieme di tutti gli insiemi di scelta di s è l'insieme vuoto $\emptyset$ se e solo se $\emptyset \in s$.*

Osservazione 2.8. *L'assioma della scelta è equivalente al corollario 2.9.*

Sono molti gli enunciati che sono stati provati essere equivalenti all'assioma della scelta, nei più svariati campi della matematica. Il primo tra questi fu il teorema di Zermelo del buon ordinamento.
Prima di enunciarlo diamo una definizione di *buon ordine*:

Def 2.11. *Un buon ordine è una coppia ordinata (A, R) dove A è un insieme e R è una relazione tale che:*

- *R è irriflessiva su A: $\forall x \in A(\neg(xRx))$.*
- *R è transitiva su A: $\forall x, y, z \in A(xRy \wedge yRz \rightarrow xRz)$.*

Inoltre ogni sottoinsieme di A non vuoto contiene un elemento m che è minimo per la relazione R: Per ogni $\emptyset \neq X \subseteq A$ $(\exists m \in X)(\forall y \in X)(\neg yRm)$.

Possiamo ora enunciare il

Teorema 2.3. ***(di Zermelo, del buon ordinamento)*** *Ogni insieme è bene ordinabile.*[5]

[5]La dimostrazione di questo teorema esula dallo scopo di questa tesi, è possibile trovarne una in [1] (cap.IV, §6, teorema 41).

2.3.1 Consistenza e indipendenza di C

È stato mostrato che C è consistente (Gödel) e indipendente dagli (Cohen) assiomi E, S, P, U e I. La dimostrazione di queste affermazioni richiede risultati avanzati che non vedremo in questa tesi[6]. È possibile però mostrare attraverso modelli finiti molto semplici che E, U, P e C formano un sistema di assiomi consistente e indipendente.
La consistenza è assicurata dal fatto che nel modello $\mathcal{B}$ che abbiamo introdotto in 1.2.2 ciascuno dei quattro assiomi sopra nominati è valido: abbiamo già visto in 1.4.2 che E, P e U valgono in $\mathcal{B}$, inoltre z è disgiunto ed è un insieme di scelta di z, quindi vale C.
Costruiamo ora il modello $\mathcal{D}$ il cui dominio di individui consiste degli insiemi $a_1, a_2, a_3, \ldots$ e che è descritto dalla seguente:

$$\begin{aligned}
&a_1 = \{a_1\}\\
&a_2 = \{a_1\}\\
&a_3 = \{a_1, a_2\}\\
&a_4 = \{a_1, a_2, a_3\}\\
&\ldots\ldots\ldots\ldots\\
&a_n = \{a_1, a_2, a_3, \ldots, a_{n-1}\}, \quad \text{per } n > 1\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned} \tag{2.12}$$

Si vede che nella precedente:

1. $a_1 = a_2$ e $a_1 \in a_1$, però $a_2 \notin a_1$. Dunque, nella (2.12) E non è valido.
2. $\bigcup a_1 = \bigcup a_2 = \bigcup a_3 = a_1$ e $\bigcup a_n = a_{n-1}$, per $n > 3$. Dunque U vale nel modello $\mathcal{D}$
3. $\mathscr{P}(a_1) = a_3$ e $\mathscr{P}(a_n) = a_{n+1}$, per $n > 1$. Dunque nel modello $\mathcal{D}$ vale P.
4. Nel modello $\mathcal{D}$ l'insieme a_1 è un insieme di scelta di a_1 e a_2 che sono gli unici insiemi disgiunti del modello. Nel modello $\mathcal{D}$ dunque vale C.

Costruiamo ora il modello $\mathcal{E}$ per dimostrare che l'assioma della somma è indipendente dai rimanenti tre assiomi: il dominio di individui consiste degli insiemi $a_1, b_1, a_2, b_2, a_3, b_3, \ldots$ e che è descritto dalla seguente:

$$\begin{aligned}
&a_1 = \{a_1\} && b_1 = \{a_1, a_2\}\\
&a_2 = \{a_1, b_1, b_2\} && b_2 = \{a_1, b_1\}\\
&a_3 = \{a_1, a_2, b_2, b_3\} && b_3 = \{a_1, b_2\}\\
&a_4 = \{a_1, a_3, b_1, b_3, b_4\} && \ldots\ldots\ldots\\
&a_5 = \{a_1, a_4, b_2, b_4, b_5\} && b_n = \{a_1, b_{n-1}\}, \text{ per } n > 1\\
&\ldots\ldots\ldots\ldots\ldots\\
&a_n = \{a_1, a_{n-1}, b_{n-3}, b_{n-1}, b_n\}, \text{ per } n > 3\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned} \tag{2.13}$$

Ora, vediamo che nel modello $\mathcal{E}$

[6] rimandiamo a [4]

1. Due insiemi indicati con lettere diverse hanno elementi diversi. Dunque nel modello $\mathcal{E}$ vale E.

2. Non c'è alcun insieme i cui elementi sono a_1, a_2, e b_1. Allora non esiste nessun insieme unione dell'insieme a_2. Nel modello $\mathcal{E}$ perciò non vale U.

3. $\mathscr{P}(a_1) = a_1$ e $\mathscr{P}(a_n) = a_{n+1}$, per $n > 1$. Inoltre, $\mathscr{P}(b_n) = b_{n+1}$, per $n \geq 1$. Nel modello $\mathcal{E}$ dunque P è valido.

4. Nel modello $\mathcal{E}$ l'insieme a_1 è un insieme di scelta di a_1, che è l'unico insieme disgiunto del modello. Quindi nel modello $\mathcal{E}$ vale C.

Consideriamo ancora il modello $\mathcal{A}$ che abbiamo già visto in 1.2.1, il cui dominio di individui è costituito da un singolo insieme z e la cui tavola è data da

$z \in z$	**F**

Questo modello ci permette di mostrare che P è indipendente da E, U e C, infatti:

1. È ovvio che E è vero in $\mathcal{A}$, in quanto in $\mathcal{A}$ non ci sono due insiemi distinti.

2. Si ha $\bigcup z = z$. Quindi U è valido.

3. Nel modello $\mathcal{A}$ non c'è alcun insieme il cui elemento sia z. Dunque nel modello $\mathcal{A}$ P non è valido.

4. Nel modello $\mathcal{A}$ si ha che z è un insieme di scelta di z. Così, nel modello $\mathcal{A}$ vale C.

Per dimostrare che l'assioma della scelta è indipendente dai tre rimanenti assiomi, consideriamo il modello $\mathcal{F}$ il cui dominio di individui consiste degli insiemi

$$a_1, b_1, c_1, a_2, b_2, c_2, a_3, b_3, c_3, \ldots$$

e che è descritto da:

$$
\begin{array}{ll}
a_1 = \{a_2, b_1\} & b_1 = \{c_2\} \\
a_2 = \{a_1, b_2\} & b_2 = \{b_1\} \\
a_3 = \{a_2, b_3\} & b_3 = \{b_2\} \\
a_4 = \{a_3, b_4\} & \ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots & \ldots\ldots\ldots \\
a_n = \{a_{n-1}, b_n\}, \text{ per } n > 1 & b_n = \{b_{n-1}\}, \text{ per } n > 1 \\
\ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots \\
c_1 = \{a_1, b_2, c_2\} & \\
c_1 = \{a_1, b_2, c_2\} & \\
c_2 = \{a_2, b_1, b_3, c_1\} & \\
c_3 = \{a_1, a_3, b_2, b_4, c_2\} & \\
c_4 = \{a_2, a_4, b_1, b_3, b_5, c_1, c_3\} & \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\
c_{2n} = \{a_2, a_4, \ldots, a_{2n}, b_1, b_3, \ldots, b_{2n+1}, c_1, c_3, \ldots, c_{2n-1}\} \quad \text{per } n \geqslant 1 & \\
c_{2n+1} = \{a_1, a_3, \ldots, a_{2n+1}, b_2, b_4, \ldots, b_{2n+2}, c_2, c_4, \ldots, c_{2n}\} \quad \text{per } n \geqslant 1 & \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots &
\end{array}
\tag{2.14}
$$

Ora, si vede che nel modello $\mathcal{F}$:

1. Due insiemi indicati con lettere diverse hanno elementi diversi. Dunque nel modello $\mathcal{F}$ vale E.

2. Si può vedere facilmente che nel modello $\mathcal{F}$

$$
\begin{array}{llll}
\bigcup a_1 = c_1 & \text{e} & \bigcup a_n = a_{n-1}, & \text{per } n > 1 \\
\bigcup b_1 = c_2 & \text{e} & \bigcup b_n = b_{n-1}, & \text{per } n > 1 \\
\bigcup c_1 = c_2 & \text{e} & \bigcup c_n = c_{n-1}, & \text{per } n > 1
\end{array}
$$

   Dunque nel modello $\mathcal{F}$ vale U.

3. Si vede facilmente che nel modello $\mathcal{F}$ per $n \geq 1$

$$\mathscr{P}(a_n) = a_{n+1}, \quad \mathscr{P}(b_n) = b_{n+1}, \quad \mathscr{P}(c_n) = c_{n+1}$$

   Quindi P è valido.

4. Si vede che a_1 è un insieme disgiunto e che nessuno dei suoi elementi è un insieme vuoto, poiché

$$a_1 = \{a_2, b_1\} = \{\{a_1, b_2\}, \{c_2\}\}$$

   Tuttavia, né $\{a_1, c_2\}$ né $\{b_2, c_2\}$ esistono nel modello $\mathcal{F}$. Dunque in questo modello l'insieme a_1 non può avere un insieme di scelta. Di conseguenza, C non è valido nel modello $\mathcal{F}$.

Per quanto osservato sui modelli $\mathcal{A}$, $\mathcal{B}$, $\mathcal{D}$, $\mathcal{E}$ e $\mathcal{F}$ si conclude che E, P, U e C formano un sistema di assiomi consistente e indipendente.

2.4 L'Assioma di Regolarità [R]

Gli assiomi introdotti finora non escludono l'esistenza di insiemi che sono elementi di se stessi o l'esistenza di due insiemi distinti ciascuno dei quali è un elemento dell'altro. Pur non dando problemi allo sviluppo della matematica, questi insiemi sono piuttosto contrari all'intuizione. Intuitivamente ci aspetteremmo che a partire da un qualunque insieme s, una qualunque $\in$-catena del tipo

$$\cdots \in e_4 \in e_3 \in e_2 \in e_1 \in s \tag{2.15}$$

debba terminare con $\emptyset$ in un numero finito di passi, quindi che non esistano $\in$-catene discendenti infinite.
A questo proposito, storicamente, venne introdotto l'assioma di fondazione (FA), che attualmente viene presentato in una forma più forte, come assioma di regolarità (R), quasi equivalente al primo.
Vediamo preliminarmente due definizioni:

Def 2.12.
- *Un insieme a si dice ben fondato se non esiste una successione $\in$-discendente con inizio da a, cioè una successione $(a_m)_{m\geq 0}$ tale che*

$$\ldots \in a_{n+1} \in a_n \in a_{n-1} \in \ldots \in a_2 \in a_1 \in a_0 = a$$

  Abbreviamo questa proprietà con WF(a) (WF sta per well founded, "ben fondato").

- *Un insieme a si dice regolare se a è vuoto oppure se contiene un elemento disgiunto da esso. Formalmente: $a = \emptyset$ oppure $\exists b(b \in a \wedge a \cap b = \emptyset$.*
  Abbreviamo questa proprietà con Reg(a).

Enunciamo dunque i due assiomi che abbiamo menzionato:
Assioma di fondazione: Ogni insieme è ben fondato.

$$\forall x WF(x) \tag{[FA]}$$

Assioma di regolarità: Ogni insieme è regolare.

$$\forall x Reg(x) \tag{[R]}$$

FA implica immediatamente l'impossibilità di $\in$-cicli, rispettando l'intuizione che ha spinto ad aggiungere questo assioma, attualmente però è visto come una conseguenza dell'assioma di regolarità, infatti:

Teorema 2.4. *R implica FA.*

Dimostrazione. Supponiamo che FA non valga e a non sia ben fondato, a causa della $\in$-successione $\sigma = (a_m)_{m\geq 0}$. Dato che le successioni sono funzioni, possiamo considerare come dato l'insieme $b = \{a_m; m \in \omega\} = Im(\omega)$: esso non è regolare. Infatti, dato un suo elemento a_j qualunque, si ha subito $a_{j+1} \in a_j \cap b \neq \emptyset$. Dunque R non vale. □

Corollario 2.10. *R implica che non ci sono insiemi in numero finito $a_1, a_2, ..., a_n$ tali che per ogni i esista un j con $a_i \in a_j$ per $i, j = 1, 2, ..., n$. In particolare, per $n = 1$ si ha: nessun insieme è elemento di se stesso.*

Dimostrazione. Senza perdita di generalità possiamo supporre che ci siano degli insiemi a_1, a_2, a_3 tali che $a_2 \in a_3$, $a_3 \in a_1$ e $a_1 \in a_2$. Ma questo implica l'esistenza di una $\in$-catena discendente infinita

$$\ldots a_3 \in a_1 \in a_2 \in a_3 \in a_1 \in a_2 \in a_3$$

che contraddice il Teorema 2.4. □

Per dimostrare l'implicazione inversa del teorema 2.4 è necessario sfruttare l'assioma della scelta, dunque FA implica R solo nei modelli in cui vale C.

Teorema 2.5. *Se vale C, FA implica R.*

Dimostrazione. Per contrapposizione, $a = a_0$ sia un insieme non regolare: $a \neq \emptyset$ e, scelto $a_1 \in a$, $a_1 \cap a$ non è vuoto e quindi si può scegliere $a_2 \in a_1 \cap a$; poiché $a_2 \in a$, si può scegliere $a_3 \in a_2 \cap a$, ... In questo modo si ottiene una successione, definita per induzione

$$\ldots, \in a_n \in \ldots \in a_1 \in a_0$$

che prova che $a_0 = a$ non è ben fondato e quindi FA non vale. C è usato per ottenere una funzione di scelta (la successione degli a_n) per la famiglia di insiemi non vuoti $\{a \cap b; b \in a\} \subseteq \mathscr{P}(a)$. □

2.4.1 Indipendenza di R da E + S + P + U + C

È possibile dimostrare che R forma con gli altri sei assiomi di ZF un sistema di assiomi consistente e indipendente, lo vedremo più avanti quando avremo a disposizione strumenti più avanzati. Per ora, utilizzando un semplice modello finito è possibile dimostrare l'indipendenza di R da E, S, P, U e C. Introduciamo il

Modello 7: Il dominio di individui consiste di 0, 1, 2, 3, ... e $x \in y$ è definita come nel Modello 1 ($(x \in y) \equiv x$ appare come esponente nell'unica rappresentazione binaria di y, se $y > 0$, e 0 è l'insieme vuoto) fatta eccezione per $0 \in y$ che è sostituito con $1 \in y$ e per $1 \in y$ che è sostituito con $0 \in y$.

In questo modello si ha dunque: $0 = \emptyset$, $1 = \{1\}$, $2 = \{0\}$, $11 = \{1, 0, 3\}$, $290 = \{8, 0, 5\}$, $6 = \{2, 0\}$, $141 = \{3, 2, 7, 1\}$, ...

Dato che $1 = \{1\}$, per il Corollario 2.10, R non può essere valido nel Modello 7. Tuttavia, per quanto già visto per il Modello 1, si può facilmente verificare che E, S, P, U e C sono validi nel Modello 7.

2.5 Alcune prove di indipendenza

È possibile dimostrare che l'assunzione di consistenza di E + S + P + U + I implica la consistenza di questi assiomi con l'aggiunta di C e R. Per il Teorema del modello possiamo dunque affermare che esiste un modello nel quale E, S, P, U, I, C e R sono validi. Denotiamo questo modello con

$$(S, \in)$$

Osservazione 2.9. *Dato che tutti e sette gli assiomi sono validi nel Modello* $(S, \in)$*, un qualsiasi insieme la cui esistenza è dimostrata basandosi su questi assiomi è un individuo del Modello* $(S, \in)$*.*

I sette assiomi precedenti formano un sistema di assiomi indipendenti, per dimostrarlo occorre esibire sette modelli in ciascuno dei quali uno dei sette assiomi cade mentre i rimanenti sei assiomi restano validi. Ora esibiremo tre di questi modelli rimandando i restanti al prossimo capitolo, quando avremo introdotto ulteriori tecniche di teoria degli insiemi e aritmetica transfinita.

2.5.1 Un modello per ¬E + S + P + U + I + C + R

Introduciamo il:
Modello 8: Sia $(S', \in')$ il modello il cui dominio di individui S' è quello del modello $(S, \in)$ con l'eccezione dell'insieme vuoto $\emptyset$ di S e dove:

$$x \in' y \text{ se e solo se } x \in y \text{ e } x \notin \emptyset$$

Denoteremo i simboli di uguaglianza in S e S' rispettivamente con $=$ e $='$.
In $(S', \in')$ $\{\{\emptyset\}\}$ e $\{\emptyset, \{\emptyset\}\}$ hanno gli stessi elementi, tuttavia $\{\{\emptyset\}\} \in' \{\{\{\emptyset\}\}\}$ mentre $\{\emptyset, \{\emptyset\}\} \notin' \{\{\{\emptyset\}\}\}$, dunque $\{\{\emptyset\}\} \neq' \{\emptyset, \{\emptyset\}\}$. Quindi E non è valido nel modello 8.
Ora, sia $P'(x, y)$ un predicato funzionale in x su di un insieme s nel Modello $(S', \in')$. Sia $P''(x, y)$ una formula tale che $P'(x, y) \equiv P''(x, y)$ e tale che l'unico simbolo di teoria degli insiemi che compare in $P''(x, y)$ sia $\in'$. Sia $P(x, y)$ una formula che sia ottenuta dalla $P''(x, y)$ sostituendo ogni formula fondamentale $u \in' v$ che compare in $P''(x, y)$ con $(u \in v) \wedge (u \neq \emptyset)$.
Si verifica facilmente che

$$A(x, y) \equiv P(x, y) \wedge (\emptyset \in y)$$

così come

$$B(x, y) \equiv P(x, y) \wedge (\emptyset \notin y)$$

sono predicati binari funzionali in x su s nel modello $(S, \in)$. Tuttavia, dal momento che l'assioma di sostituzione è valido in $(S, \in)$, l'insieme a degli associati di s rispetto a $A(x, y)$ così come l'insieme b degli associati degli elementi di s rispetto a $B(x, y)$ esistono

in $(S, \in)$. Ma allora ovviamente, esiste in $(S, \in)$ anche l'insieme $a \cup b$.
Ora, se $a \cup b \neq \emptyset$, allora $a \cup b$ è l'insieme degli associati degli elementi di s rispetto a $P'(x, y)$ nel modello $(S', \in')$. D'altra parte, se $a \cup b = \emptyset$, allora $\{\emptyset\}$ è l'insieme degli associati degli elementi di s rispetto a $P'(x, y)$ in $(S', \in')$.[7] Così, l'assioma di sostituzione è valido in $(S', \in')$.
Sia ora s un insieme in $(S', \in')$ e $\mathscr{P}(s)$ sia l'insieme potenza di s in $(S, \in)$. Per l'assioma di sostituzione, l'insieme p degli associati di $\mathscr{P}(s)$ rispetto al predicato $y = x \cup \{\emptyset\}$ esiste. Ma allora, l'insieme $p \cup \mathscr{P}(s)$ è l'insieme potenza di s in $(S', \in')$ e quindi l'assioma delle potenze è valido in $(S', \in')$.
Sia ora s un insieme in $(S', \in')$ e u sia l'insieme unione di s in $(S, \in)$. È ovvio, per come è definito $\in'$, che se $\bigcup s \neq \emptyset$, allora u è l'insieme unione di s in $(S', \in')$ e, se $\bigcup s = \emptyset$ allora $\{\emptyset\}$ è l'insieme somma di s in $(S', \in')$. Dunque l'assioma dell'unione è valido in in $(S', \in')$.
L'insieme ω in $(S', \in')$ è un insieme tale che l'insieme vuoto $\{\emptyset\}$ di $(S', \in')$ è un elemento di ω in $(S', \in')$ ed è tale che, se $w \in' \omega$ allora il successivo immediato di w in $(S', \in')$, che è l'insieme $\bigcup\{w, \{w\}\}$, è un elemento di ω in $(S', \in')$. Dunque l'assioma di infinità è valido in $(S', \in')$.
Sia ora s un insieme disgiunto in $(S', \in')$ e nessuno dei suoi elementi sia $\{\emptyset\}$. Per l'assioma di sostituzione, l'insieme q degli associati degli elementi di s rispetto al predicato binario

$$(\forall t)(t \in y) \leftrightarrow ((t \in x) \wedge (t \neq \emptyset)))$$

che è un funzionale in x, esiste in $(S, \in)$. Ma allora esiste in $(S, \in)$ un insieme d tale che

$$(\forall t)((t \in d) \leftrightarrow ((t \in q) \wedge (t \neq \emptyset)))$$

Chiaramente, d è un insieme disgiunto in $(S, \in)$ e nessuno dei suoi elementi è $\emptyset$. Per l'assioma della scelta, d ha un insieme di scelta c in $(S, \in)$. Ma allora c è un insieme di scelta di s in $(S', \in')$. L'assioma della scelta vale dunque in $(S', \in')$.
L'assioma di regolarità vale in $(S, \in)$, ma allora per come è definito $\in'$ non può esistere una $\in'$-catena discendente infinita in $(S', \in')$. Dunque per il Teorema 2.5 l'assioma di regolarità è valido in $(S', \in')$.

Per quanto visto è possibile affermare che E è indipendente dai restanti sei assiomi.

2.5.2 Un modello per E + ¬S + P + U + I + C + R

Introduciamo il:
Modello 9: Sia $(B, \in)$ il modello il cui dominio di individui consiste dell'insieme B del modello $(S, \in)$, dove

$$A = \bigcup\{0, \mathscr{P}(\emptyset), \mathscr{P}(\mathscr{P}(\emptyset)), \ldots\}$$

[7] con $\emptyset$ ci riferiamo sempre all'insieme vuoto di $(S, \in)$

e

$$B = \bigcup \{A, \mathscr{P}(A), \mathscr{P}(\mathscr{P}(A)), \ldots\}$$

e dove

$$x \in y \text{ se e solo se } x \in y \text{ in } (S, \in).$$

Per quanto già visto nel Modello 6, nel nostro modello non vale S mentre sono validi E, P, U e I.
Sia s un insieme disgiunto in $(B, \in)$ e nessuno dei suoi elementi sia $\emptyset$. Per l'assioma della scelta, s possiede un insieme di scelta c in $(S, \in)$. Per fare vedere che c è un elemento di B è sufficiente osservare che ogni elemento x di c è elemento di un elemento X di s, dunque il rango di x è inferiore al rango di X. L'insieme c dunque non può avere rango superiore al rango di s. Poiché s è un elemento di B anche c lo è. c è dunque un insieme scelta di s in $(B, \in)$ e abbiamo così provato che l'assioma della scelta è valido in $(B, \in)$.
Per dimostrare che l'assioma di regolarità è valido in $(B, \in)$ osserviamo che:

Lemma 2.10. *Ogni elemento non vuoto x di B ha un elemento y tale che x e y non hanno elementi in comune.*

Dimostrazione. Osserviamo preliminarmente che se $x \in B$ allora $x \notin x$, poiché se si avesse $x \in x$ allora si avrebbe $r(x) < r(x)$ che è impossibile.
Per assurdo si supponga che ogni elemento non vuoto x_i di x abbia un elemento in comune con x. Allora si possono presentare due casi:

$$x_1 \in x,\ x_2 \in x_1,\ x_3 \in x_2,\ \ldots,\ x_{n+1} \in x_n,\ \ldots$$

continua indefinitamente, oppure

$$x_1 \in x,\ x_2 \in x_1,\ \ldots,\ x_k \in x_n$$

per qualche $k \leq n$.
Ma dato che ogni elemento di B ha un rango, il primo caso è impossibile perché sappiamo che $y \in x$ implica $r(y) < r(x)$ e non esiste una successione infinita strettamente decrescente di numeri naturali. Il secondo caso è anch'esso impossibile: identifichiamo x con x_0 e consideriamo la successione degli indici degli insiemi

$$x_k \in x_n \in \ldots \in x_2 \in x_1 \in x_0$$

La successione è strettamente decrescente e si dovrebbe avere quindi $k > n$, che porta all'assurdo. □

Allora l'assioma di regolarità vale in $(B, \in)$

Per quanto visto è possibile affermare che S è indipendente dagli altri sei assiomi.

2.5.3 Un modello per E + S + P + U + ¬I + C + R

Introduciamo il:
Modello 10: Sia $(D, \in')$ il modello il cui dominio di individui consiste dell'insieme del modello $(S, \in)$ e dove

$$(x \in y) \text{ se e solo se}$$
$$(x \text{ appare come esponente nell'unica rappresentazione binaria di y, se } y > 0, \text{ e}$$
$$0 \text{ è l'insieme vuoto})$$

Per quanto già visto riguardo il Modello 1 nella sezione 2.2.2, nel nostro modello non vale I mentre valgono E, S, P e U.
Sia s un insieme disgiunto in $(D, \in')$ e nessuno dei suoi elementi sia $\emptyset$. Per l'assioma della scelta, s ha un insieme di scelta c in $(S, \in)$. Dato che, in corrispondenza a ogni insieme costituito da un numero finito di numeri naturali, esiste un numero naturale i cui elementi in $(D, \in')$ sono questi numeri naturali, c è un insieme di scelta di s anche in $(D, \in')$. Dunque l'assioma della scelta è valido in $(D, \in')$.
Per quanto riguarda l'assioma di regolarità, poiché non c'è nessuna successione infinita strettamente decrescente di numeri naturali, esso è valido in $(D, \in')$.

Per quanto visto è possibile affermare che I è indipendente dagli altri sei assiomi.

Capitolo 3

Prove avanzate di indipendenza

3.1 Numeri ordinali e cardinali

In questa sezione vedremo una breve introduzione ai numeri ordinali e cardinali: ne daremo la definizione e ne enunceremo, senza dimostrarle, le principali proprietà di cui faremo uso nelle sezioni seguenti.[1]

Preliminarmente, vediamo alcune definizioni utili allo sviluppo della teoria degli ordinali.

Def 3.1. *Una corrispondenza biunivoca tra due insiemi a e b è una funzione biettiva $f : a \xrightarrow[su]{1-1} b$ e si scrive $a \overset{f}{\sim} b$.*
Se esiste una corrispondenza biunivoca tra a e b si dice che essi sono equipotenti, e si scrive $a \sim b$.

Def 3.2. *Se a e b sono ordinati da $<_a$ e $<_b$ rispettivamente, una similitudine è una corrispondenza biunivoca f tra i due insiemi tale che*

$$(\forall x \in a)(\forall y \in a)(x <_a y \leftrightarrow f(x) <_b f(y))$$

se una tale similitudine esiste, si dice che a e b sono simili: $a \approx b$.

Osservazione 3.1. *Queste definizioni sono molto generali, ma divengono assai utili nel caso di buoni ordinamenti. Salvo avviso in contrario, ci si restringe a quest'ultima situazione.*

Def 3.3. *Una relazione d'ordine R su A è un buon ordinamento per A se per ogni $\emptyset \neq X \subseteq A$, X ha minimo rispetto a R.*

Se due *buoni* ordinamenti sono simili si dice che hanno lo stesso *tipo d'ordine*.

[1] Rimandiamo a [4] o a [1] per le dimostrazioni.

Def 3.4. • *Se* $(A, <_a) \approx (B, <_b)$ *i due buoni ordinamenti hanno tipi uguali: si scrive*

$$tipo(A, <_a) = tipo(B, <_b)$$

o semplicemente, lasciando sottintese le relazioni, $tipo(A) = tipo(B)$

- *Si chiama segmento iniziale di* A *(rispetto alla relazione* $<_a$*) determinato da* $x \in A$ *l'insieme* $seg(x) = \{y \in A; y <_a x\}$*. Se è necessario specificare, si scrive* $seg(x; A; <_a)$*.*
- *Se* $(A, <_a)$ *risulta simile a un segmento iniziale* $seg(z) = seg(z; B; <_b)$ *di* B*, si dice che il tipo di* A *è minore di quello di* B*:* $tipo(A, <_a) < tipo(B, <_b)$*.*
- $tipo(A) \leq tipo(B)$ *significa che* $tipo(A) < tipo(B)$*, oppure che* $tipo(A) = tipo(B)$*.*

Proposizione 3.1. *Vale la legge di tricotomia per i tipi di buon ordine: per ogni coppia di buoni ordinamenti* $(A, <_a), (B, <_b)$ *o essi sono simili o uno è simile a un segmento iniziale dell'altro.*

Def 3.5. *Un insieme* a *si dice numero ordinale se è transitivo e bene ordinato da* $\in$ *o, più esattamente da* $\in_a$*, dove*

$$x \in_a y \iff x \in a \wedge y \in a \wedge x \in y$$

Vediamo alcune prime proprietà dei numeri ordinali.

Teorema 3.1. α, β, γ *siano ordinali.*

1. $\alpha \notin \alpha$
2. *Se* $\alpha \in \beta$ *e* $\beta \in \gamma$*, allora* $\alpha \in \gamma$
3. *Se* $\alpha \approx \beta$*, allora* $\alpha = \beta$
4. *(Legge di tricotomia per gli ordinali) Vale sempre una e una sola delle seguenti tre possibilità:* $\alpha \in \beta$*,* $\alpha = \beta$*,* $\beta \in \alpha$
5. *Se* $\boldsymbol{C}$ *è una classe (non necessariamente un insieme) non vuota di ordinali, essa ha un (unico)* $\in$*-minimo, cioè esiste* $\alpha \in \boldsymbol{C}$ *tale che* $\alpha \in \boldsymbol{C} \wedge \forall \beta \in \boldsymbol{C}(\alpha \in \beta \vee \alpha = \beta)$*. Tale* α *viene indicato con* $min\boldsymbol{C}$ *e coincide con* $\bigcap \boldsymbol{C}$*.*
6. *Il successore insiemistico di* α*,* $\alpha^+ = \alpha \cup \{\alpha\}$ *è anch'esso un ordinale, diverso da* α*, e il minimo (rispetto a* $\in$*) ordinale maggiore di esso:* α^+ *si dice ordinale successore (di* α*). Inoltre,* $\alpha^+ = \beta^+$ *implica* $\alpha = \beta$*.*

Osservazione 3.2. *Il principio di minimo al punto (5) del precedente teorema sarà utilizzato spesso nelle dimostrazioni.*

Nel capitolo 2 abbiamo dato una definizione indiretta di numero naturale (definizione 2.4), definendo prima l'insieme ω, il più piccolo insieme induttivo, e poi chiamando numeri naturali i suoi elementi. Ora è possibile darne una definizione diretta da cui è molto più agevole ricavare le proprietà che finora abbiamo utilizzato giustificandole sulla base dell'intuizione. Definiamo quindi i numeri naturali come particolari numeri ordinali. È poi possibile dimostrare che l'insieme ω coincide con l'insieme di questi ordinali.

Def 3.6. *L'ordinale α è un numero naturale se è $\alpha = \emptyset$ oppure se è un successore e i suoi elementi sono tutti $\emptyset$ oppure successori.*

Proposizione 3.2. *Se $\mathscr{F}$ è una famiglia (insieme) di ordinali, $\bigcup \mathscr{F} = \bigcup_{\beta \in \mathscr{F}} \beta$ è un ordinale.*

Corollario 3.1. *$\bigcup \mathscr{F}$ è il minimo ordinale $\geq$ di tutti gli elementi di $\mathscr{F}$: viene indicato anche con $sup\mathscr{F}$.*

Corollario 3.2. *α è un ordinale successore se e solo se $\bigcup \alpha \subset \alpha$. In tal caso, se $\beta = \bigcup \alpha$, risulta $\alpha = \beta^+$. In caso contrario, $\alpha = \bigcup \alpha$.*

Questo corollario permette una partizione degli ordinali in tre classi disgiunte.

Def 3.7. *Ogni ordinale α è:*

- *l'ordinale zero: $\alpha = \emptyset = 0$, oppure*
- *un ordinale successore: $\exists \beta(\alpha = \beta^+)$, oppure*
- *un ordinale limite, per cui $\alpha = \bigcup_{\beta < \alpha} \beta$.*

Osservazione 3.3. *Una variante del principio di minimo verrà utilizzata per giustificare definizioni e dimostrazioni per induzione transfinita.*

Teorema 3.2. *Ogni insieme bene ordinato $(A, <_A)$ è simile ad esattamente un ordinale α, il suo tipo: $tipo(A, <_A) = \alpha$.*[2]

Osservazione 3.4. *Se si vuole attribuire un tipo a ogni insieme, non necessariamente bene ordinato, occorre l'assioma della scelta (come teorema del buon ordinamento): nel caso infinito questo tipo però non è unico.*

Facciamo ora un accenno all'aritmetica dei numeri ordinali. È possibile trovare i dettagli in [1] (Cap.VIII, §2).

[2]Dimostrazione in [1] (Cap.VIII, §1)

Def 3.8. *(Addizione tra ordinali) Siano α e β due ordinali.*

$$\alpha + \beta = tipo(A, <_A)$$

dove $A = (\{0\} \times \alpha) \cup (\{1\} \times \beta)$ e la relazione $<_A$ è il buon ordinamento di A ottenuto facendo precedere le coppie $(0, \gamma), \gamma < \alpha$, ordinate con $\in_\alpha$ a tutte le coppie $(1, \delta), \delta < \beta$, ordinate con $\in_\beta$.

Def 3.9. *(Moltiplicazione tra ordinali) Siano α e β due ordinali.*

$$\alpha \cdot \beta = tipo(\alpha \times \beta, <_{\alpha \cdot \beta})$$

dove $\alpha \times \beta = \bigcup_{\delta < \beta} \alpha \times \{\delta\}$ e $<_{\alpha \cdot \beta}$ è il buon ordinamento di $\alpha \times \beta$ ottenuto facendo precedere ogni $\alpha \times \{\delta\}$ a $\alpha \times \{\delta'\}$ (ordinati secondo $\in_\alpha$, cioè $<_\alpha$) se $\delta <_\beta \delta'$. Se $\delta = \delta'$ si utilizza l'ordinamento di α.

Possiamo ora definire il concetto di numero cardinale e di cardinalità di un insieme, per quest'ultimo aspetto è però indispensabile l'assioma della scelta. Segnaliamo il suo utilizzo in una definizione o in una dimostrazione con (C) premesso alle relative proposizioni.

Def 3.10.

- *Dato un ordinale α, la sua cardinalità è il minimo ordinale β equipotente ad α ($\beta \sim \alpha$): esso si indica con $|\alpha|$. Quindi, $\alpha \sim |\alpha|$ e anche $|\alpha| \leq \alpha$.*
- *Se $\alpha = |\alpha|$, esso si dice un (numero) cardinale.*
- *Se $(A; <_A)$ è un insieme bene ordinato e α è l'(unico) ordinale simile ad esso, (il suo tipo: teorema 3.2), si pone $|(A; <_A)| = |\alpha|$ e si può scrivere semplicemente $|A| = |\alpha|$.*
- *(C) Se A è un qualsiasi insieme, la sua cardinalità, indicata con $|A|$, è quella di un qualunque ordinale simile ad A dotato di un qualsiasi buon ordinamento: la definizione è ben posta per la seguente proposizione 3.3.*

Proposizione 3.3. *Per ordinali α, β sono equivalenti le seguenti affermazioni:*

1. $|\alpha| = |\beta|$
2. $|\alpha| \sim |\beta|$
3. $\alpha \sim \beta$

Dimostrazione. $1 \implies 2$ è ovvio; $2 \implies 3$ segue dalla equipotenza di un ordinale col suo numero cardinale; $3 \implies 1$ per il fatto che $|\alpha|$ e $|\beta|$ sono elementi minimi nella stessa classe di equipotenza. □

Vediamo ora alcuni risultati generali sui numeri cardinali.

Proposizione 3.4. *Se A è un insieme di cardinali $sup(A) = \bigcup_{\kappa \in A}$ è un cardinale, il minimo cardinale maggiore o uguale rispetto a tutti i $\kappa \in A$.*

Proposizione 3.5. *Dato un qualunque numero ordinale α, esiste un cardinale $\kappa > \alpha$.*

Dimostrazione. Basta provarlo per ordinali transfiniti. Si considerino i buoni ordinamenti R di α: essi costituiscono un insieme, dal momento che comunque $R \in \mathscr{P}(\alpha \times \alpha)$. Allora usando lo schema di sostituzione

$$K = \{tipo(\alpha; R) | R \text{ è un buon ordinamento di } \alpha\} = \{\beta | \beta \sim \alpha\}$$

è un insieme di ordinali. L'ordinale $sup(K)$ è allora ben definito ed è il numero cardinale cercato: inoltre risulta il minimo cardinale maggiore di α. □

Osservazione 3.5. *Osserviamo esplicitamente che per questo risultato non è necessario l'assioma della scelta. La dimostrazione infatti utilizza soltanto lo schema di sostituzione.*

Osservazione 3.6. *L'insieme K è anche detto classe-numero di α. $sup(K)$ è di fatto il minimo cardinale maggiore di $|\alpha|$ (come vedremo nella definizione 3.11, è il successore cardinale di $|\alpha|$)*

L'aritmetica cardinale è molto diversa da quella degli ordinali, anche se coincidono nel caso dei numeri naturali. Introduciamo inizialmente una diversa nozione di successore.

Def 3.11. *Se κ è un numero cardinale, il minimo cardinale strettamente maggiore di esso è il suo successore cardinale (immediato): lo indicheremo con $S(\kappa)$.*[3]

Proposizione 3.6. *Ogni cardinale transfinito è un ordinale limite.*

Dimostrazione. Se un cardinale κ è transfinito, il suo successore ordinale κ^+ è tale che $\kappa^+ \sim \kappa$ e quindi $\kappa^+ < S(\kappa)$. □

I cardinali transfiniti si possono ripartire in due classi, più ω:

Def 3.12. *Se il cardinale $\kappa > \omega$ non è un successore, si dice un cardinale limite. Quindi ω, che non è un cardinale successore, non è nemmeno un cardinale limite.*

Osservazione 3.7. *La nozione di cardinale limite è diversa da quella di ordinale limite: si è visto che tutti i cardinali transfiniti sono ordinali limite, anche i successori.*

[3]Più spesso viene indicato con κ^+, in questa trattazione è stata scelta una notazione differente per evitare di confondere la nozione di successore cardinale con quella di successore ordinale.

Seguendo la notazione introdotta da Cantor, ω, come primo cardinale transfinito, viene indicato con $\aleph_0$. Il simbolo $\aleph$ (alef) è la prima lettera dell'alfabeto ebraico, viene usata per indicare i cardinali transfiniti in generale.

Come si è visto, gli ordinali generalizzano le proprietà di induzione dei numeri naturali. Oltre a generalizzare lo schema di dimostrazione per induzione, questa proprietà, chiamata *induzione transfinita*, permette la definizione di costruzioni insiemistiche dipendenti da un ordinale. Vediamone un esempio:

Def 3.13. *La successione degli alef è definita per ricorsione transfinita su tutti gli ordinali con*

- $\aleph_0 = \omega$
- $\aleph_{\alpha+1} = S(\aleph_\alpha)$
- $\aleph_\alpha = \bigcup_{\beta<\alpha} \aleph_\beta$ *se* α *è un ordinale limite. In questo caso, per la proposizione 3.4,* $\aleph_\alpha$ *è il minimo cardinale strettamente maggiore di ogni* $\aleph_\beta$*,* $\beta < \alpha$*. Quindi* $\aleph_\alpha$ *è un cardinale limite se e solo se* α *è un ordinale limite (con l'eccezione di* ω*).*

Vediamo ora come è possibile definire sui numeri cardinali delle operazioni di somma e prodotto. Come per la nozione di successore anche queste operazioni sono distinte da quelle sui numeri ordinali, anche se coincidono nel caso dei numeri naturali.

Def 3.14. *Se* κ *e* λ *sono numeri cardinali*

- $\kappa \oplus \lambda = |\kappa + \lambda| = |(\{0\} \times \kappa) \cup (\{1\} \times \lambda)|$
- $\kappa \otimes \lambda = |\kappa \times \lambda|$

L'operazione più caratteristica dell'aritmetica ordinale è l'elevamento a potenza, dal momento che l'addizione e la moltiplicazione sono piuttosto banali:

Def 3.15. *(C) Se* κ, λ *sono cardinali* κ^λ *è* $|F(\lambda; \kappa)|$*.*
L'assioma della scelta è indispensabile per assicurare un buon ordinamento per $F(\lambda; \kappa)$*, l'insieme delle funzioni* $f : \lambda \longrightarrow \kappa$*.*

Un risultato notevole è quello relativo all'insieme potenza:

Proposizione 3.7. *(C) Per ogni insieme* A*,* $|\mathscr{P}(A)| = 2^{|A|}$*.*
(Senza C, si ha che $\mathscr{P}(A) \sim F(A, 2)$*)*

Dimostrazione. Se $B \subseteq A$, lo si può mettere in corrispondenza biunivoca con la sua funzione caratteristica χ_B di dominio A: poiché $2 = \{0; 1\}$, ciò crea una corrispondenza biunivoca di $\mathscr{P}(A)$ con $F(A; 2)$. □

Il ben noto Teorema di Cantor[4] mette in luce il fatto che grazie all'assioma della potenza è possibile costruire insiemi di cardinalità sempre maggiore, ma come si collocano nella successione degli alef gli insiemi così generati? Questa domanda è alla base dell'ipotesi formulata da Cantor conosciuta oggi come Ipotesi del Continuo:

Def 3.16.
- *(C) L'ipotesi del continuo [CH] è l'asserzione* $2^{\aleph_0} = \aleph_1$
- *(C) L'ipotesi generalizzata del continuo [GCH] è l'asserzione* $\forall\alpha, 2^{\aleph_\alpha} = \aleph_{\alpha+1}$

Naturalmente, GCH implica CH. Cantor non riuscì mai a provare né l'una né l'altra ipotesi, né riuscì a refutarle. Si scoprì solo dopo che ciò era di fatto impossibile.
È stato infatti dimostrato da Gödel (1938) che GCH è consistente con gli assiomi di ZFC, ci riuscì presentando un modello di ZF in cui sono validi sia C che GCH. Successivamente Cohen (1963) riuscì a dimostrare l'indipendenza di CH (e a maggior ragione di GCH) da ZFC, utilizzando la tecnica del forcing, da lui inventata, per costruire un modello di ZFC in cui CH non vale.[5]
Questi risultati di consistenza e indipendenza ci permettono di trattare CH e GCH come gli altri assiomi che abbiamo già visto, cosa che ci tornerà utile nella sezione 3.3.
È stato inoltre dimostrato che in ZF:

1. (Sierpinski) GCH implica C[6];
2. (Solovay) CH non implica C, e di conseguenza nemmeno GCH;
3. (Solovay) C e CH insieme non implicano GCH.

3.2 Il P-modello

In questo capitolo, sia $(K, \in)$ un modello per il nostro sistema fondamentale costituito da E, S, P, U e I. Allora, basandoci su $(K, \in)$ costruiamo il corrispondente P-modello $(P, \in)$ per il nostro sistema fondamentale di assiomi, nel quale, come di fatto avverrà, sia anche valido l'assioma di regolarità. Dunque dimostreremo la consistenza di R con il nostro sistema fondamentale di assiomi dando esplicitamente un modello $(P, \in)$ per l'intero sistema di assiomi in questione. Mostreremo poi che se l'assioma di regolarità è valido nel modello originario $(K, \in)$, allora il modello $(K, \in)$ coincide con il modello $(P, \in)$. Inoltre faremo vedere che se l'assioma della scelta è valido nel modello originario $(K, \in)$, allora l'assioma della scelta continua a essere valido nel modello $(P, \in)$.

[4]Dato un qualunque insieme A, $\mathscr{P}(A)$ ha cardinalità strettamente maggiore di A
[5][4]
[6][1], cap.X, Proposizione 13. La forma di GCH che abbiamo esposto necessita dell'assioma della scelta. Dovendo dimostrare che GCH implica C, Sierpinski utilizza una forma diversa di GCH, che non necessita di C.

Seguiremo la trattazione di [1]. In [4] (cap.III) la consistenza dell'assioma di regolarità è invece studiata attraverso l'introduzione della classe propria **WF** degli insiemi ben fondati. Tale classe è un sottomodello del modello $(K, \in)$ per il sistema costituito da E, S, P, U e I, costruita partendo da $\emptyset$ e iterando l'operazione di potenza di un insieme.
Come si è detto sopra, sia $(K, \in)$ un modello per il nostro sistema fondamentale di assiomi (E, S, P, U e I). Per ogni ordinale u (del modello $(K, \in)$) sia B_u l'insieme (del modello $(K, \in)$), dato da:

$$B_u = \mathscr{P}\left(\bigcup_{v<u} B_v\right) \tag{3.1}$$

essendo $\mathscr{P}(x)$ l'insieme potenza (naturalmente nel modello $(K, \in)$) di x. Così, per esempio,

$$B_0 = \{\emptyset\}, B_1 = \{\emptyset, \{\emptyset\}\}, \ldots$$

dove $\emptyset$ è l'insieme vuoto del modello $(K, \in)$.
Osserviamo che la successione dei B_u cresce con u: se $u < v$ si ha che $B_u \subseteq B_v$.

Def 3.17. *Per P-modello corrispondente al modello $(K, \in)$ si intende il modello $(P, \in)$ definito nel seguente modo:*

x è un insieme di $(P, \in)$ se e solo se $x \in B_u$ per qualche ordinale u.

B_u essendo dato dalla (3.1).
La relazione di appartenenza $\in$ in $(P, \in)$ è la stessa di quella del modello $(K, \in)$.

Deduciamo ora alcune proprietà del modello $(P, \in)$, dedotte da risultati che valgono in $(K, \in)$.
Dalla (3.1) discende che se $x \in B_u$ e $y \in x$ allora $y \in \bigcup_{v<u} B_v$. Pertanto risulta $y \in B_k$ per qualche $k < u$, il che, sempre per la (3.1), comporta che sia $y \subseteq \bigcup_{v<k} B_v$. Ma dato che $k < u$, si ha $y \subseteq \bigcup_{v<u} B_v$ che, per la (3.1), implica $y \in B_u$. Dunque, per ogni ordinale u,

$$x \in B_u \text{ implica } x \subseteq B_u \text{ (cioè } B_u \text{ è transitivo)} \tag{3.2}$$

Lemma 3.1. *Sia x un insieme di $(P, \in)$. Allora $y \in x$ in $(P, \in)$ se e solo se $y \in x$ in $(K, \in)$*

Dimostrazione. Sia $y \in x$ in $(P, \in)$. Allora, dato che la relazione di appartenenza "$\in$" in $(P, \in)$ è la stessa che in $(K, \in)$, si vede che $y \in x$ in $(K, \in)$.
Viceversa sia $y \in x$ in $(K, \in)$. Allora, dato che $x \in B_u$ per qualche ordinale u, dalla (3.2) si vede che $y \in B_u$. Così dalla definizione di P-modello discende che y è un insieme di $(P, \in)$ e pertanto $y \in x$ in $(P, \in)$. □

Dalla (3.1) discende che per ogni ordinale v e ogni ordinale u

$$v < u \text{ se e solo se } B_v \in B_u \tag{3.3}$$

che per la (3.2) implica la

$$v \leq u \text{ se e solo se } B_v \subseteq B_u \tag{3.4}$$

Ma allora, dalla (3.1) e dalla (3.4) discende

$$B_{u+1} = \mathscr{P}\left(\bigcup_{v \leq u} B_v\right) = \mathscr{P}\left(B_u\right) \tag{3.5}$$

Osserviamo poi che per ogni ordinale u si ha:

$$x \in B_u \text{ implica } \mathscr{P}(x) \in B_{u+1} \tag{3.6}$$

$$x \in B_u \text{ implica } (\bigcup x) \in B_u \tag{3.7}$$

$$u \in B_u \tag{3.8}$$

Queste proprietà si provano per induzione transfinita o, equivalentemente, attraverso il principio di minimo.
Introduciamo la seguente definizione, che è una generalizzazione della definizione 2.7 che abbiamo visto nel Capitolo 2.

Def 3.18. *Per ogni insieme x del modello $(P, \in)$, il numero ordinale $r(x)$ si dice P-classe (rango) di x se e solo se $r(x)$ è il più piccolo ordinale tale che $x \in B_{r(x)}$*
Cioè $r(x) = u$ implica $x \in B_u$.

Chiaramente, in virtù della (3.1) e della definizione precedente, dati comunque gli insiemi x e y del modello $(P, \in)$, si ha

$$x \in y \text{ implica } r(x) < r(y) \tag{3.9}$$

Dimostriamo ora la

Proposizione 3.8. *Per ogni insieme x del modello $(P, \in)$ si ha:*

$$r(x) = \bigcup_{y \in x} (r(y) + 1) \tag{3.10}$$

Dimostrazione. Sia $u = \bigcup_{y \in x}(r(y) + 1)$. Ma allora, per ogni $y \in x$ si ha $r(y) < u$. Pertanto $x \subseteq \bigcup_{v<u} B_v$ e quindi $x \in B_u$. Così $r(x) \leq u$. D'altra parte, dalla (3.9) discende che se $y \in x$, allora risulta $r(y) < r(x)$, che implica $r(y) + 1 \leq r(x)$. Dunque, $u \leq r(x)$. Di conseguenza, $u = r(x)$. □

Similmente, basandosi sulla definizione 3.18 si può verificare subito che per ogni insieme x del modello $(P, \in)$ si ha:

$$r(\mathscr{P}(x)) = r(x) + 1 \tag{3.11}$$

dove, al solito, $\mathscr{P}(x)$ è l'insieme potenza di x, e

$$r(\bigcup x) = \bigcup r(x) = \bigcup_{y \in x} r(y) \tag{3.12}$$

Proposizione 3.9. *Per ogni numero ordinale u:*

$$r(u) = u \tag{3.13}$$

Dimostrazione. Proviamolo per induzione. $B_0 = \{0\}$, dunque $r(0) = 0$ e il caso base è verificato. Supponiamo ora che $\forall v < u, r(v) = v$. Sfruttiamo allora la proposizione 3.8: $r(u) = \bigcup_{v \in u}(r(v) + 1) = \bigcup_{v<u}(v + 1) = u$. □

Proposizione 3.10. *L'assioma di estensione è valido in $(P, \in)$.*

Dimostrazione. Dato che gli insiemi di $(P, \in)$ sono anche insiemi di $(K, \in)$, è sufficiente il lemma 3.1 per concludere che in $(P, \in)$ vale l'assioma di estensione. □

Proposizione 3.11. *Lo schema di sostituzione è valido in $(P, \in)$.*

Dimostrazione. Si denoti con $M(x)$ la formula scritta nel linguaggio di $(K, \in)$ ed equivalente a:

$$\text{"}x \in B_u \text{ per qualche ordinale } u\text{"} \tag{3.14}$$

Sia ora s un insieme di $(P, \in)$ e sia $F(x, y)$ un predicato binario che sia funzionale in x su s in $(P, \in)$. Sulla base della (3.14) si denoti con $F'(x, y)$ la formula ottenuta da $F(x, y)$ con la sostituzione di $(\forall z)(\ldots)$, ogni volta che questa interviene in $F(x, y)$, con $(\forall z)(M(z) \rightarrow \ldots)$ e la sostituzione di $(\exists z)(\ldots)$, ogni volta che questa interviene in $F(x, y)$, con $(\exists z)(M(z) \wedge \ldots)$ per ogni variabile limitata z di $F(x, y)$. Sia inoltre

$$F^*(x, y) \equiv F'(x, y) \wedge M(x) \wedge M(y)$$

Chiaramente

$$F(a, b) \text{ è vera nel modello } (P, \in) \text{ se e solo se } F^*(a, b) \text{ è vera nel modello } (K, \in). \tag{3.15}$$

Tramite il lemma 3.1, si vede che $F^*(x, y)$ è funzionale in x su s in $(K, \in)$. Dato che lo schema di sostituzione è valido in $(K, \in)$, l'insieme t i cui elementi sono precisamente gli associati degli elementi di s tramite $F^*(x, y)$, esiste in $(K, \in)$. Per mostrare che lo schema di assioma di sostituzione è valido in $(P, \in)$, stanti il lemma 3.1 e la (3.15), è

sufficiente provare che t è un insieme di $(P, \in)$. In virtù della (3.15), è chiaro che gli elementi y di t sono insiemi di $(P, \in)$. Basandosi sulla definizione di P-classe, sia

$$u = \sup_{y \in t} r(y)$$

Ma allora, dalla (3.4) discende che $y \in B_u$ per ogni $y \in t$, che implica $t \subseteq B_u$. Ma allora la (3.5) comporta che $y \in B_{u+1}$. Così, dalla definizione 3.17 si trae che t è un insieme di $(P, \in)$. Lo schema di sostituzione è dunque valido in $(P, \in)$. □

Proposizione 3.12. *L'assioma delle potenze è valido in* $(P, \in)$.

Dimostrazione. Sia x un insieme di $(P, \in)$. Dunque $x \in B_u$ per qualche ordinale u. Pertanto la (3.6) ci dice che $\mathscr{P}(x) \in B_{u+1}$. Ma allora dalla definizione 3.17 e dal lemma 3.1 discende che $\mathscr{P}(x)$ è l'insieme potenza di x in $(P, \in)$. □

Proposizione 3.13. *L'assioma dell'unione è valido in* $(P, \in)$.

Dimostrazione. Sia x un insieme di $(P, \in)$. Dunque $x \in B_u$ per qualche ordinale u. Pertanto dalla (3.7) si trae $\bigcup x \in B_u$. Ma allora dalla definizione 3.17 e dal lemma 3.1 discende che $\bigcup x$ è l'insieme unione di x in $(P, \in)$. □

Proposizione 3.14. *L'assioma dell'infinito è valido in* $(P, \in)$.

Dimostrazione. L'insieme di tutti i numeri naturali è un numero ordinale ω tale che $\emptyset \in \omega$ e tale che, se $x \in \omega$, allora $(x \cup \{x\}) \in \omega$. Ma allora dalla 3.8 si trae che $\omega \in B_\omega$ e pertanto ω è un insieme di $(P, \in)$. L'assioma dell'infinito è dunque valido in $(P, \in)$. Osserviamo che l'insieme ω di $(P, \in)$ è lo stesso insieme ω di $(K, \in)$. □

Osservazione 3.8. *Da queste due ultime proposizioni si vede che se x è un insieme del modello $(P, \in)$, l'insieme potenza, così come l'insieme unione di x in $(P, \in)$ coincidono rispettivamente con l'insieme potenza e l'insieme unione di x nel modello originario $(K, \in)$.*

Proposizione 3.15. *L'assioma di regolarità è valido in* $(P, \in)$.

Dimostrazione. Sia s un insieme non vuoto di $(P, \in)$ e sia

$$r = \min_{x \in s} r(x)$$

che esiste sempre. Chiaramente, s ha un elemento t la cui P-classe è r. Ma allora dalla (3.9) discende che s non può avere un elemento in comune con t. Dunque l'assioma di regolarità è valido in $(P, \in)$. □

Osservazione 3.9. *Questa proposizione mostra che l'assioma di regolarità è consistente con il nostro sistema fondamentale costituito da E, P, U, I e S. Come si è detto all'inizio di questa sezione e come mostrano le proposizioni appena viste, tale consistenza si dimostra dando esplicitamente un modello per l'intero sistema di assiomi in questione. Chiaramente* $(P, \in)$ *è un tale modello.*
P è inoltre un sottomodello di K, dato che è un suo sottoinsieme e la relazione di appartenenza ha la stessa interpretazione.

Lemma 3.2. *Se ogni elemento* x *di un insieme* s *del modello* $(K, \in)$ *è un insieme del modello* $(P, \in)$*, allora* s *è un insieme di* $(P, \in)$*.*

Dimostrazione. Sia $u = (\sup_{x \in s} r(x)) + 1$. Ma allora dalla (3.1) si trae che $s \in B_u$, che dimostra il lemma. □

Basandoci sul lemma 3.2 dimostriamo ora la seguente notevole proposizione.

Proposizione 3.16. *Se l'assioma di regolarità è valido nel modello originario* $(K, \in)$*, allora* $(K, \in)$ *coincide con il P-modello* $(P, \in)$*, ossia se* s *è un insieme di* $(K, \in)$*, allora* s *è un insieme di* $(P, \in)$*.*

Dimostrazione. Supponiamo per assurdo che s sia un insieme di $(K, \in)$ e s *non* sia un insieme di $(P, \in)$. Allora dal lemma 3.2 discende che s ha un elemento q tale che q non è un insieme di $(P, \in)$. Similmente, q ha un elemento p tale che p non è un insieme di $(P, \in)$. Così, la $\in$-catena discendente $(\ldots \in)p \in q \in s$, che inizia con s, è tale che nessuno degli insiemi che in essa intervengono è un insieme di $(P, \in)$. Sia C l'insieme (del modello $(K, \in)$) di tutti quegli insiemi che intervengono in tali catene finite. Chiaramente, C ha un elemento in comune con ogni elemento di se stesso. Ma ciò contraddice l'ipotesi della proposizione. Dunque la nostra supposizione è falsa e la proposizione è dimostrata. □

L'importanza della proposizione 3.16 risulta dai seguenti corollari.

Corollario 3.3. *Ogni modello per il sistema costituito dagli assiomi di estensione, delle potenze, dell'unione, di infinità,* ***di regolarità*** *e dallo schema di sostituzione è un P-modello.*

Corollario 3.4. *Nella teoria degli insiemi con sistema fondamentale di assiomi dato dagli assiomi di estensione, delle potenze, dell'unione, di infinità,* ***di regolarità*** *e dallo schema di sostituzione ogni insieme ha una P-classe.*

Come si vede dalla (3.1) e dalla definizione 3.17, la P-classe di un insieme di un insieme s del modello $(P, \in)$ ci dà il grado di complessità del procedimento, mediante raggruppamenti, di costruzione dell'insieme s a partire dall'insieme vuoto $\emptyset$. Per esempio, si ha

$$r(\emptyset) = 0 \text{ e } r(\{\emptyset, \{\emptyset\}\}) = 2$$

Inoltre, come si vede dalla (3.1)

$$r(\{\emptyset, \{\emptyset, \{\emptyset\}\}\} = r(\{0, 2\}) = 3$$

In base a quanto sopra e al fatto che la P-classe $r(s)$ di un insieme s di un P-modello $(P, \in)$ è un numero ordinale, si è soliti dire che:

$$s \text{ è } \textit{ben formato da } \emptyset \text{ in } r(s) \text{ passi.}$$

In virtù di questo, si è soliti dire che ogni insieme di un P-modello $(P, \in)$ è *ben fondato*. Un insieme ben fondato ha delle proprietà significative che si avvicinano di più alla nostra nozione intuitiva di insieme (di qui il "ben").
Basandosi sulla nozione di insieme ben fondato, il corollario 3.4 si può riformulare come segue.

Corollario 3.5. *Nella teoria degli insiemi con sistema fondamentale di assiomi dato dagli assiomi di estensione, delle potenze, dell'unione, di infinità,* ***di regolarità*** *e dallo schema di sostituzione ogni insieme è ben fondato.*

Il fatto che ogni insieme di P sia ben fondato offre il seguente vantaggio: che per ogni ordinale u si può considerare ed è assicurata l'esistenza dell'*insieme di tutti gli insiemi di P-classe u* (dalla definizione 3.18).

Proposizione 3.17. *Se l'assioma della scelta è valido nel modello originario $(K, \in)$, allora l'assioma della scelta resta valido nel corrispondente P-modello $(P, \in)$.*

Dimostrazione. Supponiamo che l'assioma della scelta sia valido in $(K, \in)$ e sia $d \neq \emptyset$ un insieme disgiunto di $(P, \in)$ tale che $\emptyset \notin d$. Allora dal lemma 3.1 si trae che d è disgiunto anche in $(K, \in)$. Ma, dato che in $(K, \in)$ è valido l'assioma della scelta, ne segue che d ha un insieme di scelta c in $(K, \in)$. Chiaramente $c \subseteq \bigcup d$ e pertanto $c \in \mathscr{P}(\bigcup d)$ in $(K, \in)$. Ma allora, per l'osservazione 3.8 si vede che $\mathscr{P}(\bigcup d) \in B_u$ per qualche ordinale u e pertanto dalla (3.2) segue che $\mathscr{P}(\bigcup d) \subseteq B_u$: dunque $c \in B_u$. L'assioma della scelta è dunque valido in $(P, \in)$. □

3.3 Indipendenza degli assiomi della teoria degli insiemi

Per quanto visto finora sappiamo che, poggiando sull'assunzione di consistenza del sistema fondamentale di assiomi composto da E, P, U, I e dallo schema S, è possibile dimostrare la consistenza del sistema costituito da E, P, U, I, S, C, R e GCH.[7]

[7] Inserire GCH nel sistema di assiomi non è necessario per tutte le prove seguenti, tuttavia lo inseriamo per uniformità.

Pertanto, questo sistema di assiomi, per il Teorema del Modello, ha un modello che, stante la proposizione 3.16, coincide con il corrispondente P-modello

$$(P, \in) \tag{3.16}$$

Osservazione 3.10. *Sottolineiamo il fatto che nel P-modello $(P, \in)$ a cui facciamo riferimento sono validi gli assiomi si estensione, delle potenze, dell'unione, di infinità, della scelta, di regolarità, lo schema di sostituzione e l'ipotesi generalizzata del continuo.*

Vediamo ora come questo P-modello può aiutarci a dimostrare i risultati di indipendenza che non abbiamo ancora visto.

3.3.1 Indipendenza di P

L'assioma delle potenze è indipendente da E, U, I, S, C, R e GCH (a maggior ragione questo vale senza GCH: in questa prova non viene utilizzato).
Definiamo preliminarmente una notazione: per ogni insieme x si ponga:

$$S_0(x) = \{x\} \; e \; S_{n+1}(x) = \bigcup S_n(x) \; per \; n = 0, 1, 2, \ldots \tag{3.17}$$

Dunque, in particolare si avrà:

$$S_1(x) = x, \;\; S_2(x) = \bigcup x, \;\; S_3(x) = \bigcup\bigcup x, \; \ldots$$

Servendoci di questa notazione, osserviamo che, poiché in $(P, \in)$ valgono E, P, U, I, S, C, R e GCH (Osservazione 3.10), l'insieme E dato da

$$E = \left\{ x \mid x \in B_{\aleph_1} \quad e \quad r(x) < \aleph_1 \quad e \quad |\bigcup_{n\in\omega} S_n(x)| < \aleph_1 \right\} \tag{3.18}$$

esiste nel modello $(P, \in)$ dato dalla (3.16).
Nella (3.18) $\aleph_1$ è il primo cardinale infinito non numerabile, e $B_{\aleph_1}$ è definito secondo la (3.1) della sezione precedente. Pertanto E è l'insieme di tutti gli insiemi x del modello $(P, \in)$ la cui P-classe $r(x)$ è minore di $\aleph_1$ e tali che $|x| < \aleph_1, |\bigcup x| < \aleph_1, |\bigcup\bigcup x| < \aleph_1, \ldots$
Introduciamo il:
Modello 11: Sia $(E, \in)$ il modello il cui dominio di individui sia l'insieme E e la cui relazione di appartenenza $\in$ è la stessa di quella del modello $(P, \in)$.
Chiaramente, dalla (3.18) e dalla (3.13) discende che ω è un insieme del modello $(E, \in)$. Tuttavia, essendo $|\mathscr{P}(\omega)| \geq \aleph_1$, si vede che $\mathscr{P}(\omega)$ non è un insieme del modello $(E, \in)$. Così l'assioma delle potenze non è valido nel modello $(E, \in)$. D'altra parte è facile verificare che i restanti assiomi sono validi nel modello $(E, \in)$.

Se, per esempio, x è un insieme del modello $(E, \in)$, allora dalla (3.12) si vede che $r(\bigcup x) < \aleph_1$, e dalla (3.17) discende che

$$|\bigcup_{n\in\omega} S_n(\bigcup x)| = |\bigcup_{\substack{n\in\omega \\ n\geq 2}} S_n(x)| < \aleph_1$$

Così, l'assioma dell'unione è valido nel modello $(E, \in)$.
Similmente, dato che l'estremo superiore di un insieme finito o numerabile di numeri ordinali finiti o numerabili è un ordinale finito o numerabile, si vede che anche lo schema di assioma di sostituzione è valido nel modello $(E, \in)$. ecc.

3.3.2 Indipendenza di U

L'assioma dell'unione è indipendente da E, P, I, S, C, R e GCH.
Sia $(P, \in)$ il P-modello dato dalla (3.16). Servendoci della notazione (3.17), introduciamo il
Modello 12: Prendiamo in considerazione il modello $(H, \in)$ definito al modo seguente:

x è un insieme del modello $(H, \in)$ se e solo se
x è un insieme del modello $(P, \in)$ e per ogni y, $y \in \bigcup_{n\in\omega} S_n(x)$ implica $|y| < \aleph_\omega$

Così, il dominio H di individui del modello $(H, \in)$ consiste degli insiemi x del modello $(P, \in)$ tali che $|x| < \aleph_\omega$ e tali che se $y \in x$, allora $|y| < \aleph_\omega$ e se $z \in y$ e $y \in x$ allora $|z| < \aleph_\omega$ e così via. Inoltre, la relazione di appartenenza "$\in$" del modello $(H, \in)$ è la stessa di quella del modello $(P, \in)$.
Da come è definito $(H, \in)$ discende che ω è un insieme del modello. Inoltre in virtù dell'osservazione 3.10 e dell'ipotesi generalizzata del continuo, si vede che l'insieme numerabile s dato da:

$$s = \{\omega, \mathscr{P}(\omega), \mathscr{P}(\mathscr{P}(\omega)), \mathscr{P}(\mathscr{P}(\mathscr{P}(\omega))), \ldots\} \tag{3.19}$$

è un insieme del modello $(H, \in)$. Tuttavia dato che $|\bigcup s| = \aleph_\omega$, l'insieme unione $\bigcup s$ dell'insieme s dato dalla (3.19) non è un insieme del modello $(H, \in)$. D'altra parte, si verifica facilmente che i restanti assiomi sono validi nel modello $(H, \in)$. Se, per esempio, x è un insieme del modello $(H, \in)$, allora $|\mathscr{P}(x)| < \aleph_\omega$ e si vede subito che anche $\mathscr{P}(x)$ è un insieme del modello $(H, \in)$. Pertanto l'assioma delle potenze è valido nel modello $(H, \in)$. ecc.

3.3.3 Indipendenza di R

L'assioma di regolarità è indipendente da E, P, U, I, S, C e GCH (anche in questa prova GCH non è necessario).

Introduciamo il
Modello 13: Sia $(P'', \in'')$ il modello il cui dominio P'' di individui è quello del modello $(P, \in)$ dato dalla (3.16) e dove

$$\begin{gathered} 0 \in'' y \text{ se } e \text{ solo se } 1 \in y \\ 1 \in'' y \text{ se } e \text{ solo se } 0 \in y \\ \text{Altrimenti, } x \in'' y \text{ se e solo se } x \in y \end{gathered} \tag{3.20}$$

Dato che $x \in 1$ se e solo se $x = 0$, dalla (3.20) si tra che $x \in'' 1$ se e solo se $x = 1$. Pertanto, nel modello $(P'', \in'')$ l'insieme 1 ha uno e un solo elemento 1. Dunque nel modello $(P'', \in'')$ l'insieme non vuoto 1 ha un elemento in comune con ogni altro elemento di se stesso. Così, l'assioma di regolarità non vale nel modello $(P'', \in'')$. D'altra parte, tenendo conto dell'osservazione 3.10 e per quanto già visto per il Modello 7, si verifica subito che i restanti assiomi sono validi nel modello $(P'', \in'')$.

Capitolo 4

Riepilogo

Riepiloghiamo con una tabella riassuntiva i modelli visti in questa tesi:

Modello	Sistema di assiomi	Paragrafi di riferimento
$\mathcal{A}$	E + S + ¬P + U + C	1.2.1, 1.3.2, 1.4.2, 2.3
$\mathcal{B}$	E + ¬S + P + U + C	1.2.2, 1.3.2, 1.4.2, 2.3
$\mathcal{C}$	¬E + S	1.2.2
1	E + S + P + U + ¬I	1.3.1, 1.4.1, 2.2.2
2	¬E + S + P + U	1.3.2, 1.4.2
3	E + S + ¬U	1.4.2
4	¬E + S + P + U + I	2.2.2
5	E + S + P + U + ¬I	2.2.2
6	E + ¬S + P + U + I	2.2.2
$\mathcal{D}$	¬E + U + P + C	2.3.1
$\mathcal{E}$	E + ¬U + P + C	2.3.1
$\mathcal{F}$	E + U + P + ¬C	2.3.1
7	E + S + P + U + C + ¬R	2.4.1
8	¬E + S + P + U + I + C + R	2.5.1
9	E + ¬S + P + U + I + C + R	2.5.2
10	E + S + P + U + ¬I + C + R	2.5.3
11	E + S + ¬P + U + I + C + R + GCH	3.3.1
12	E + S + P + ¬U + I + C + R + GCH	3.3.2
13	E + S + P + U + I + C + ¬R + GCH	3.3.3

Bibliografia

[1] Alexander Abian. *La teoria degli insiemi e l'aritmetica transfinita.* (trad. Giulia Maria Piacentini Cattaneo) Feltrinelli, 1972.

[2] Umberto Bottazzini. *Il flauto di Hilbert: storia della matematica.* UTET libreria, 2003.

[3] Paul Richard Halmos. *Teoria elementare degli insiemi.* Feltrinelli, 1981.

[4] Kenneth Kunen. *Set theory an introduction to independence proofs.* Elsevier, 2014.