L'indipendenza dell'assioma di scelta dalla teoria degli insiemi di Zermelo Fraenkel

Autore: Fontanella Laura

Roma (Italia), 28 novembre 2006

A mamma.

Indice

Introduzione

Nel XIX secolo, in seguito alla scoperta di alcuni risultati sorprendenti della geometria, si diffuse tra i matematici un nuovo interesse: quello per i fondamenti della matematica. Fino ad allora, pochi matematici si erano chiesti su che cosa si fondassero i loro risultati. Eppure la loro materia era storicamente considerata la scienza per antonomasia, emblema del rigore e della certezza. Si fece avanti l'idea che la matematica dovesse fondarsi su pochi principi evidenti da cui era possibile dimostrare ogni teorema. Quali dovevano essere questi principi? Era possibile formularli, oppure l'evidenza che storicamente era stata attribuita alla matematica non le era propria? Immanuel Kant aveva consacrato la Critica della Ragion Pura al tentativo di spiegare come fossero possibili i giudizi sintetici a priori. Dalla risposta a questa domanda dipendeva la legittimità della fisica, della metafisica e della matematica pura. Kant, infatti, riteneva che la matematica si fondasse su giudizi sintetici a priori. Con Frege, fondatore del logicismo, si fece avanti, invece, l'idea che le proposizioni della matematica fossero analitiche. In altri termini, Frege riteneva che ogni proposizione della matematica fosse vera in virtù esclusivamente del significato dei suoi termini. Che la somma degli angoli interni di un triangolo fosse di 180 gradi era, secondo Frege, una *proprietà del concetto di triangolo*. La matematica dunque si fondava sulla logica, per Frege, e all'evidenza della logica doveva la sua certezza. Prese avvio, allora, un processo di rigorizzazione dei concetti della matematica, alcuni dei quali erano stati fino ad allora considerati intuitivi. A questo scopo Cantor formulò la teoria degli insiemi. I numeri naturali, reali, persino le funzioni possono essere visti come degli insiemi. La teoria degli insiemi, dunque, può fondare la matematica. Tuttavia, ad una teoria matemat-

ica si richiede la non contraddittorietà. Nel 1931, Gödel dimostrò che ogni teoria capace di esprimere e dimostrare almeno quanto esprime e dimostra l'aritmetica elementare non è capace di dimostrare la sua non contraddittorietà. La geometria può essere fondata sull'aritmetica, ma qualunque teoria che voglia fondare l'aritmetica non può, per il teorema di Gödel, dimostrare la sua non contraddittorietà.
La crisi dei fondamenti della matematica sopra accennata, ha spinto i matematici a esaminare criticamente alcune assunzioni prima ritenute evidenti. Al momento della formulazione della sua teoria degli insiemi, ad esempio, Cantor assunse un principio, noto come l'assioma di scelta, di cui molto spesso si faceva e si continua a fare uso per la dimostrazione di teoremi. Alcuni matematici, suoi contemporanei, ne misero in dubbio la validità innaugurando un dibattito che si è protratto sino ad oggi. La teoria degli insiemi nata per questi scopi fondazionali è stata più volte riformulata. Oggi il principale sistema assiomatico è la teoria degli insiemi di Zermelo-Fraenkel. In questa teoria l'assioma di scelta non è dimostrabile né refutabile. Il dibattito sulla legittimità dell'assioma, dunque, è ancora aperto, e si lega alla necessità o meno di riformulare, ancora una volta, la teoria degli insiemi. Dobbiamo accettare l'assioma di scelta oppure no? Sarà possibile riformulare la teoria in modo che sia possibile dimostrare o refutare l'assioma di scelta? Come si devono considerare tutti quei teoremi che si dimostrano utilizzando tale assioma dal momento che l'assioma non è evidente e non è dimostrabile?
Nel capitolo seguente, le tematiche qui introdotte sulla crisi dei fondamenti della matematica nel XIX secolo, sulla nascita dell teoria degli insiemi e sulle varie posizioni che è possibile assumere ripetto alla legittimità o illegittimità dell'assioma di scelta, verranno approfondite. Successivamente verranno presentati gli assiomi della teoria degli insiemi di Zermelo-Fraenkel e si dimostreranno i principali teoremi della teoria. Si tratterà poi dell'assioma di scelta, delle sue varie formulazioni, nonché dei teoremi che si dimostrano tramite questo assioma. Solo allora sarà possibile introdurre le nozioni necessarie ad affrontare la dimostrazione dell'indipendenza dell'assioma di scelta. Ci limiteremo a dimostrare rigorosamente solo la consistenza dell'assioma di scelta e non anche la consistenza della sua negazione. Quanto sarà trattato, tuttavia, fornirà gli

strumenti necessari per uno studio più dettagliato della dimostrazione dell'indipendenza dell'assioma. Il lettore, dunque, se interessato, potrà misurarsi con la prova della consistenza della negazione senza problemi.

Capitolo 1

Matematica e Teoria degli Insiemi: la crisi dei fondamenti

La *teoria degli insiemi* che si colloca nell'ambito della logica, ha svolto un importante ruolo fondazionale per la matematica. Prima della metà del XIX secolo il concetto di *insieme* veniva considerato primitivo ed intuitivo, insieme ad altre nozioni fondamentali come quelle di numero naturale, numero irrazionale, successore ecc.... Inoltre la matematica era storicamente fondata su un certo numero di principi ritenuti evidenti, condivisi, da cui ogni proposizione o teorema poteva essere dimostrato: gli *assiomi*. Ma non tutti i matematici erano consapevoli del carattere assiomatico di questa disciplina ,soprattutto non se ne interessavano. Nella seconda metà dell'ottocento, alcuni risultati sorprendenti della geometria, spinsero la comunità scientifica a interrogarsi sui fondamenti della matematica e sulla natura dei concetti su cui riposava questa scienza. Ne derivò un connubio fecondo di matematica e filosofia, che non aveva avuto precedenti. Tra i matematici che si impegnarono in questo programma fondazionale, George Cantor (1845-1918) propose di fondare l'intera matematica sulla "teoria degli insiemi" di cui egli è considerato il fondatore. Nel corso della storia, la scoperta di alcuni paradossi in seno alla definizione di insieme formulata da Cantor, portarono alla formalizzazione di nuovi sistemi di assiomi per la teoria degli insiemi. Oggi i principali sono due: la *teoria degli insiemi di Zermelo-Fraenkel*, noto anche con l'acronimo di ZF, e la *teoria degli insiemi di Von Neumann-Bernays-Gödel*. Noi ci occuperemo del primo sistema; mostreremo che esiste un principio, l'*assioma di scelta*, che non è dimostrabile né refutabile tramite gli assiomi di ZF, si dice che tale assioma è *indipendente* dagli assiomi della teoria. L'assioma di scelta dice che: dato un insieme di insiemi non vuoti e a due a due disgiunti, posso *scegliere* da ognuno di questi insiemi un solo elemento. L'indipendenza dell'assioma ci sorprende per diverse ragioni che cercherò di chiarire meglio nel seguito:

la più importante, è che non solo c'è una proprietà che la teoria *non sa* se è vera o se è falsa, ma proprio di questa proprietà si fa un uso smodato in ogni branca della matematica.
Cominciamo col fornire maggiori dettagli sulla nascita della teoria degli insiemi.

Le geometrie non euclidee

La crisi della matematica classica del XIX sec. si manifestò prima di tutto nella geometria: la geometria euclidea, con la sua struttura assiomatico-deduttiva, si basava su un ristretto numero di assiomi. C'era, poi, un principio cui si ricorreva spesso che non era di natura assiomatica in quanto non evidente: il postulato delle rette parallele. Può essere così enunciato: per un punto esterno a una retta passa una, e una sola, retta parallela alla retta data. Fin dall'antichità se ne era cercata una dimostrazione dagli altri assiomi, senza ottenere alcun risultato soddisfacente. Nel XIX secolo i matematici Gauss, Bolyai, Lobaceswski e Riemann teorizzarono delle geometrie alternative che non assumevano il quinto postulato come vero, le "geometrie non euclidee". In altri termini, tramite le geometrie non euclidee si era dimostrata l'indipendenza del postulato dagli altri assiomi della geometria. Alla sorpresa per un tale risultato, seguì il tentativo di fondare la matematica su una base più certa. Nell'analisi, ad esempio, era centrale il concetto di limite, e questo era tradizionalmente fondato sull'intuizione geometrica. Il tentativo di emancipare questa, ed altre branche della matematica, dalla geometria fu accompagnato dall'esigenza, sentita ora più che mai, di una rigorizzazione dei principali oggetti matematici. I matematici Weierstrass (1815-1897), Dedekind (1831-1916) e Cantor (1845-1918) formularono una definizione del concetto di *numero irrazionale*, fino ad allora fondato sull'intuizione del continuo geometrico, riconducendolo ai numeri interi e a operazioni su di essi. Con queste definizioni l'aritmetica diveniva il fondamento dell'analisi matematica. Spontanea si poneva allora la domanda: su che cosa si fonda l'aritmetica? È questa un fondamento sicuro?

1.1 La teoria degli insiemi di Cantor

Venne, allora, da Cantor la proposta di fondare l'intera matematica sulla teoria degli insiemi. Definì *insieme* ogni "riunione M in un tutto, di oggetti m (elementi di M) della nostra intuizione o del nostro pensiero". Nella sua teoria ogni numero diveniva un insieme. Così gli interi erano insiemi, e definiva un insieme *finito* come un insieme che può essere messo in corrispondenza biunivoca con un intero, che si dice il suo *cardinale*. I cardinali comprendevano oltre ai numeri naturali, anche i numeri transfiniti, cioè associati a insiemi infiniti.
Cantor dimostrò che esistono diversi infiniti. L'insieme dei numeri naturali e quello dei numeri razionali sono infiniti ed hanno la stessa cardinalità. Invece l'insieme dei numeri reali che è anch'esso infinito non ha la stessa cardinalità dell'insieme dei numeri naturali, vale a dire non è possibile stabilire una corrispondenza biunivoca tra l'insieme dei numeri reali e quello dei numeri naturali. Pur essendo entrambi infiniti, l'insieme dei numeri reali è un infinito più grande di quello dei numeri naturali. Questa è una caratteristica importante della teoria degli insiemi: ammette degli insiemi infiniti. Come si vedrà nel Capitolo 4, l'assioma di scelta sarebbe dimostrabile se tutti gli insiemi dell'universo fossero finiti, poiché se vogliamo scegliere un solo elemento per ogni insieme di una famiglia di insiemi, allora possiamo certamente fare un numero finito di scelte. Il problema si pone per le famiglie infinite: come definire una regola che permetta di fare infinite scelte? Sottolineo questo aspetto, perché alcuni matematici parteggiano per una particolare filosofia che si chiama *finitismo*: secondo la quale esistono solo insiemi finiti, e gli in-

siemi infiniti non vanno considerati più che utili astrazioni. Introdurre questa linea di pensiero è, credo, indispensabile per la nostra trattazione, ne parleremo ancora nel Capitolo 4.
Tornando alla teoria degli insiemi, nella teoria degli insiemi *contemporanea*, non solo i numeri (naturali e transfiniti) vengono caratterizzati come insiemi ma ogni oggetto matematico è un insieme con determinate caratteristiche. Le funzioni, ad esempio, sono insiemi di coppie che soddisfano certe proprietà; le formule stesse, cioè enunciati del linguaggio nella formalizzazione logica matematica, sono particolari insiemi. Dunque, è a pieno titolo, pare, che la teoria degli insiemi può proporsi come fondamento dell'intera matematica. Quanto segue servirà a chiarire perché, oggi, non riteniamo che quanto appena detto sia possibile.

1.2 Il logicismo di Frege

Nello stesso periodo, Gottlob Frege (1848-1925) credette di pervenire alla definitiva fondazione della matematica sulla logica. In particolare, egli si propose di definire in termini puramente logici i concetti fondamentali della matematica quali quello di "numero naturale", e di dimostrare a partire da principi logici le verità della matematica, a cominciare dagli assiomi dell'aritmetica. Nella definizione del suo programma, Frege si confrontò in primo luogo con la filosofia kantiana, secondo la quale i giudizi della matematica sono sintetici a priori. Nella Critica dell Ragion Pura, Kant riduceva l'ambito di indagine della sua opera -come sono possibili una matematica pura , una fisica pura , una metafisica come scienza?- alla questione: come sono possibili giudizi sintetici a priori? Da questa domanda dipendeva, dunque la legittimità della matematica pura, della fisica e della metafisica. Al contrario di Kant, Frege riteneva, invece, che le proposizioni matematiche fossero analitiche: vere esclusivamente in virtù del significato dei termini che le componevano. Un esempio di giudizio analitico è dato dalla frase "ogni scapolo è un uomo non ammogliato". In questa frase, non si fa altro che esplicitare una verità contenuta già nella definizione del soggetto ("scapolo"). Analogamente nella dimostrazione delle verità matematiche, sosteneva Frege, si fa uso esclusivamente di definizioni rigorose e di leggi logiche generali: cioè i teoremi matematici esplicitano quanto è già contenuto nelle definizioni. Una formula come "$6 + 1 = 7$", per esempio, non si basa sull'intuizione, ma esplicita il concetto di 7 come "successore di 6". L'aritmetica, base della matematica, veniva da lui fondata su concetti e principi della logica: la matematica è certa perché non è altro che un immensa tautologia. Per realizzare il programma *logicista*, Frege ideò un linguaggio simbolico e definì esplicitamente delle regole logiche nell'*Ideografia* del 1879. Questo particolare linguaggio permetteva di scrivere senza ambiguità tutta la logica e la matematica. Non ci si poteva servire a questo scopo del linguaggio ordinario, troppo ambiguo. La logica su cui voleva fondarsi Frege, cioè, era una logica *matematica*: una logica diversa da come era stata pensata fino ad allora, un'altra logica rispetto a quella formulata da Aristotele o dai pensatori medioevali, in quanto questa nascente logica doveva avere lo stesso rigore che aveva fatto della matematica la scienza per antonomasia. Il XIX secolo è infatti il secolo della matematizzazione della logica; poteva essere matematizzata e poteva servire come strumento per la matematica ma, ancora più che questo: la logica era di natura matematica. Il matematico Boole (1815-1864), infatti, mostrò che essa poteva essere assimilata a un anello, cioè a l'insieme $\{0, 1\}$ (vero e falso) munito di due operazioni $\wedge, \vee$ (congiunzione e disgiunzione) e di un elemento neutro per ognuna delle operazioni: V, F. Questo anello soddisfa delle particolari proprietà come l'associatività e la commutatività e si chiama *algebra di Boole dei valori di verità.*

Un concetto, secondo Frege, ha due dimensioni: *l'intensione o senso*, cioè l'insieme delle caratteristiche che un oggetto deve possedere per cadere sotto quel determinato concetto, e l'*estensione o significato,* vale a dire l'insieme degli oggetti che cadono sotto quel determinato concetto. Sulla base di questa distinzione, formulò due assiomi logici della teoria degli insiemi che egli riteneva ovvi. Il primo è il principio di estensionalità: se sotto due concetti cadono gli stessi oggetti e solo essi, allora i due concetti sono uguali. Per esempio "x è la stella del mattino" e "x è la stella della sera" sono due concetti uguali perché sotto di essi cade

lo stesso oggetto: Venere. Il secondo assioma è il cosiddetto principio di *astrazione o comprensione*: ogni concetto individua un insieme, l'insieme di tutti e soli gli individui che soddisfano le condizioni definite dal concetto. Questo assioma è filosoficamente molto impegnativo, in quanto implica due idee:
(a) esiste una classe per ogni molteplicità di enti caratterizzabili da una stessa condizione;
(b) è possibile formare classi di classi.

Le classi hanno, pertanto, una esistenza in sé, indipendente dal fatto che noi le pensiamo oppure no. Questa è la cosiddetta "componente platonica del pensiero di Frege": le classi, come le idee universali di Platone, sono *sostanze* che esistono indipendentemente dall'uomo, che non le costruisce ma le scopre.

La crisi del logicismo: Russell e Zermelo

Il programma logicista fu messo in crisi dalla scoperta di antinomie derivabili dai "principi indubitabili" della logica e della teoria degli insiemi. Nel 1902 Bertrand Russell (1872-1970), scoprì che dall'assioma di astrazione è derivabile una contraddizione. Si consideri la proprietà "non essere elemento di se stesso". A essa, come a ogni proprietà, corrisponde una classe R, cui appartengono tutti gli insiemi che non contengono se stessi. Ci chiediamo: la classe R appartiene a se stessa? Supponiamo che R appartenga a se stessa, allora deve soddisfare la proprietà sopraenunciata: non deve appartenere se stessa. Ciò è ovviamente contraddittorio. Supponiamo allora che R non appartenga a se stessa: allora godendo della proprietà di non appartenere a se stessa, dovrà appartenere a R cioè a se stessa. Anche questo è contraddittorio. Russell espresse l'antinomia in un modo intuitivo: "un certo villaggio ha tra i suoi abitanti un solo barbiere. Egli è un uomo ben sbarbato, che rade tutti e solamente gli uomini del villaggio che non si radono da soli. Ora: chi rade il barbiere? E' plausibile sostenere che egli si faccia la barba da solo. Se così fosse, tuttavia, sarebbe violata la premessa secondo cui il barbiere rade tutti coloro che non si radono da soli. Però se non si rade da solo, dovrà essere rasato dal barbiere, cioè si raderà da se stesso: il che è ancora contradditorio".

Russell aderiva, comunque, al programma logicista. Nei *Principia Mathematica* (1910-1913), scritti insieme a Whitehead, egli si propose di riedificare l'edificio della logica e della matematica, in modo da evitare l'insorgere delle antinomie. Dal punto di vista filosofico, tuttavia, Russell non riuscì a fornire alla matematica le basi logiche assolutamente certe che Frege avrebbe voluto.

Più tardi E.Zermelo (1871-1953) riuscì a riformulare la teoria degli insiemi in modo da evitare questi e altri paradossi, ma fu costretto a introdurre un nuovo assioma: l'assioma di *scelta* che, come abbiamo detto, non è logicamente evidente.

1.3 Brower e l'intuizionismo

Al logicismo si opposero, in primo luogo, i matematici *intuizionisti*. In Francia il matematico Poincaré, anticipò queste critiche, rifiutando ogni possibile fondazione della matematica su basi logiche. Si consideri il principio di induzione matematica: esso è un giudizio sintetico a priori. È a priori: le sue conclusioni sono assolutamente certe e non si fonda sull' esperienza; è sintetico: esso amplia il contenuto della conoscenza estendendo a una successione indefinita di enti ciò che si suppone valido per alcuni di essi. Non si tratta quindi di una verità analitica, come pensavano i logicisti, per i quali tutta la matematica è una tautologia, in cui le conclusioni dicono ciò che è già contenuto nelle premesse.

L'idea della scuola intuizionista era che solo le entità matematiche che possono essere *costruite* esistono. Il vero fondatore della scuola intuizionista è considerato il matematico Brower (1881-1966). Brower, per questa via, arrivò a mettere in discussione i principi della logica classica. Una proposizione matematica non descrive un fatto oggettivo, ma asserisce che è stata effettuata una certa costruzione. Come affermò un seguace di Brower, Heyting, la formula "$2+2 = 3+1$" non descrive un fatto oggettivo, ma asserisce che "ho effettuato le costruzioni mentali indicate da $2+2$ e da $3+1$ e ho trovato che portano allo stesso risultato". Questo comporta una reinterpretazione dei connettivi logici: la negazione "non A" significa che effettuata la costruzione A ne deriva una contraddizione, mentre la disgiunzione "A o B" dice che è stata effettuta la cotruzione A oppure la costruzione B. A questo punto gli intuizionisti devono respingere uno dei principi della logica classica, quello del terzo escluso (A o non-A): esso significherebbe, infatti, che di ogni proposizione A è possibile costruire una dimostrazione, oppure non-A è vera senza bisogno di dimostrarla. Ampie parti della matematica, basate su dimostrazioni che si servivano del principio del terzo escluso come le *dimostrazioni per assurdo* vennero respinte come "metafisiche" dagli intuizionisti. Brower e la sua scuola, tuttavia, procedettero alla costruzione di una nuova matematica, , in cui furono recuperati molti risultati di quella classica. In questo modo l'intuizionismo ha portato alla nascita del *Costruttivismo*. Il costruttivismo rifiuta l'assioma di scelta, perché l'assioma stabilisce che esiste una funzione di scelta che ci permette di scegliere un solo elemento dagli insiemi di una famiglia di insiemi non vuoti (è un'altra delle formulazioni dell'assioma di scelta vedi il Capitolo 4), non ci dice come possiamo definire questa funzione. Dunque l'assioma di scelta non è costruttivo. Tutto ciò sarà più chiaro nel Capitolo 4.

1.4 Il formalismo di Hilbert

Il formalismo è la posizione assunta da coloro che ritengono che ogni teorema non costituisca una verità assoluta, ma una verità relativa: una dimostrazione è qualcosa che lega la verità delle premesse alla verità della conclusione. Nella prospettiva *formalista*, il matematico David Hilbert (1862-1943) affrontò il problema dei fondamenti della matematica. Le diverse teorie matematiche, come la teoria degli insiemi, la geometria elementare o l'aritmetica, sono strutture assiomatico-deduttive. Classicamente, sulla base del modello euclideo, le teorie si fondavano su principi (definizioni e assiomi) assunti come veri perché intuitivamente evidenti. Da essi venivano dedotti logicamente i diversi teoremi. La scoperta delle geometrie non euclidee aveva, però messo in crisi il criterio dell'evidenza intuitiva. Nel 1900 Hilbert pubblicò i *Fondamenti della geometria*, una nuova assiomatizzazione della geometria elementare, in cui i termini primitivi (punto, linea) erano introdotti senza far alcun appello al loro significato intuitivo: il loro significato è dato solo dalle mutue relazioni logiche tra di essi, specificate dagli assiomi. Infine, esplicite regole logiche governano le dimostrazioni. I termini possono poi ricevere diverse interpretazioni: per esempio, possiamo interpretare il termine "punto" come un ente geometrico inesteso come faceva Euclide, o come una coppia ordinata di numeri reali, come si fa in geometria analitica, o in infiniti altri modi. L'importante è il fatto che tutti i sistemi di enti che soddisfano le condizioni poste dagli assiomi rendono veri anche i teoremi. Hilbert, riflettendo sui sistemi assiomatici, aveva potuto definire con precisione le proprietà:

- la non contraddittorietà (da un sistema di assiomi non devono essere derivabili due proposizioni contraddittorie);
- la completezza (ogni enunciato deve essere dimostrabile o refutabile);
- l'indipendenza (nessun assioma deve essere derivabile dagli altri assiomi).

Particolarmente delicata ai fini della fondazione della matematica era la dimostrazione della non contraddittorietà dei sistemi. A questo scopo vi è una tecnica: una dimostrazione è una successione finita di simboli che possono essere *codificati*, associando ad ognuno di essi una successione di interi. Per dimostrare che una teoria non è contraddittoria, allora, sarà sufficiente dimostrare che per ogni x, x non è il codice di una contraddizione. Tale dimostrazione era ridotta, pertanto, alla prova di una proposizione dell'aritmetica.

I teoremi di incompletezza di Gödel

Il programma formalista fu messo in crisi da due famosi teoremi i "teoremi di incompletezza", dimostrati da Gödel (1906-78) nel 1931. Con essi dimostrò che la proposizione: "gli assiomi non sono contraddittori" non poteva essere dimostrata nell'aritmetica: una teoria non può "giustificare" se stessa all'interno della teoria. I teoremi di incompletezza di Gödel riguardano i sistemi formali "sufficientemente potenti", vale a dire capaci di esprimere e dimostrare almeno quanto esprime e dimostra l'arimetica elementare. Gödel dimostrò che ogni sistema sufficientemente potente, ssiomatizzabile e coerente, è sintatticamente incompleto (I teorema). Non è quindi possibile risolvere, come voleva il formalismo hilbertiano, il concetto semantico di verità in quello sintattico di dimostrabilità. Godel dimostrò poi che ogni sistema sufficientemente potente, assiomatizzabile e non contraddittorio, è incapace di dimostrare una proposizione che esprima la non contraddittorietà del sistema (II teorema). I metodi finitistici, appartenenti all'aritmetica elementare, a cui faceva appello Hilbert a fini fondazionali, non erano in grado di dimostrare la non contraddittorietà dell'aritmetica stessa. Gödel dimostrò, così, che la matematica non è un immensa tautologia, le proposizioni della matematica non possono essere analitiche: la verità di un enunciato della matematica non può dipendere da ciò che è contenuto nell'enunciato stesso.

Commenti

Il merito della teoria degli insiemi è stato quello di aver affrontato il problema dei fondamenti, mettendo in discussione (nel senso critico kantiano) gli assunti della matematica classica. Già prima della nascita della teoria degli insiemi, accettare quanto affermato dall'assioma di scelta non era cosa pacifica, e anche del postulato delle rette parallele si cercava una dimostrazione; tuttavia con la formulazione della teoria degli insiemi questo programma fondazionale venne svolto, per la prima volta, sistematicamente. I matematici si interessano dei fondamenti quando non ne possono più fare a meno. Trattare la tematica dei fondamenti della matematica ha, pertanto, un interesse forse più filosofico. Soprattutto è importante per la filosofia nella misura in cui essa si fonda sul terreno dell'opinione, di ciò che è dubbio o non è certo, e il suo obbiettivo è interrogarsi sulla natura del nostro sapere. Nel fare queste considerazioni, sposo il criticismo kantiano: compito della filosofia è criticare, interrogarsi, cioè, sui limiti e la leggittimità del sapere umano. Quale migliore occasione, allora, se non quella di indagare sui fondamenti di quella disciplina, la matematica, che a lungo è stata ritenuta la scienza per antonomasia? La critica ha una funzione positiva, mettiamo in questione certe assunzioni non per inferirne la falsità ma sempre per cercare una risposta. Quando ci rapportiamo a queste problematiche, allora, non dobbiamo dimenticare che è grazie alla matematica che possiamo inviare i satelliti sulla luna, fare previsioni, ecc... in un certo senso, la matematica "funziona". Gödel ha dimostrato che una teoria non può giustificare se stessa. Questo significa che la matematica non può dimostrare la sua evidenza. Che cos'è, allora, la matematica? Secondo alcune versioni del formalismo, l'oggetto della matematica è dato, letteralmente, dai simboli scritti. Per esempio la geometria euclidea viene considerata come un gioco che si basa sopra alcune stringhe chiamate assiomi e alcune regole di inferenza e consiste nel generare nuove stringhe dalle stringhe date mediante le regole; in tale gioco si può dimostrare il teorema di Pitagora, cioè si riesce a generare una stringa che corrisponde al suo enunciato. Ogni gioco del genere precedente è ugualmente accettabile e in matematica si possono solo giocare questi giochi, non dimostrare loro proprietà. Perché allora, come si diceva prima, la matematica funziona? Questa concezione della matematica non riesce a spiegare perché questa scienza è tanto utile da aver suscitato in Galilei, anzi, l'idea che le leggi della natura siano scritte in caratteri matematici. Diversa è allora la risposta che i realisti danno alla domanda così formulata. Il *realismo matematico* sostiene che le entità matematiche esistono indipendentemente dalla mente umana. Quindi gli umani non inventano la matematica, ma piuttosto la scoprono. Per questa posizione spesso si usa il termine *platonismo* in quanto essa si avvicina molto al credere di Platone in un mondo delle idee. Probabilmente la concezione di Platone deriva da Pitagora e dai suoi seguaci, i pitagorici, che pensavano che il mondo fosse, letteralmente, fatto di numeri. Analizziamo le due posizioni in riferimento all'assioma di scelta. Per un platonista l'indipendeza dell'assioma di scelta è, certo, un problema perché quanto è affermato dall'assioma, non è così evidente che si possa dire che esso esprima una verità matematica assoluta: è necessaria una dimostrazione o una refutazione. Dunque c'è probabilmente una verità di natura assiomatica che spiegherebbe o refuterebbe l'assioma di scelta e che non è stata ancora *scoperta*. Pertanto, la teoria dovrebbe essere riformulata o completata: non dimentichiamo che l'assioma non può essere dimostrato o refutato in *questa* teoria, che è già il risultato di una serie di revisioni e riformulazioni svolte in passato. La teoria degli insiemi che non sa rispondere alle domande più importanti? La teoria degli insiemi non solo non sa se l'assioma di scelta è vero o falso, ma non sa nemmeno se esiste un insieme infinito, o se il più piccolo insieme più grande dell'insieme dei numeri naturali è quello dei reali. Nella prospettiva di un platonista, allora, fino a quando qualcuno non avrà trovato un principio grazie al quale sia possibile dimostrare o refutare l'assioma di scelta, non possiamo sapere se tale assioma è vero o è falso e dubbia è anche la verità di tutti i teoremi che si dimostrano con esso.

Il vantaggio del formalista è, invece, che il gioco in cui, a partire dall'assioma di scelta, si dimostrano certi teoremi resta valido, perché legittime sono le regole di inferenza con cui questi risultati vengono dimostrati. Al gioco non è richiesto altro. Tuttavia questa linea di pensiero, come non è difficile immaginare, non va per la maggiore tra i matematici contemporanei. Anzi, è difficile immaginare che un matematico possa trovarsi d'accordo con questa visione nichilista.

La teoria degli insiemi che non sa rispondere alle domande più importanti? La teoria degli insiemi non solo non sa se l'assioma di scelta è vero o falso, ma non sa nemmeno se esiste un insieme infinito, o se il più piccolo insieme più grande dell'insieme dei numeri naturali è quello dei reali.

Un costruttivista, poi, rifiuta l'assioma di scelta proprio perché non ve ne è una dimostrazione costruttiva. D'altra parte non può neanche accettarne la falsità perché l'assioma non può essere refutato.

Un finitista, infine, ritiene che la questione sia priva di senso. Gli insiemi infiniti, egli sostiene, non esistono. Dunque l'assioma di scelta è vero perché è dimostrabile per tutti gli insiemi finiti (vedi il Capitolo 4). Tuttavia abbiamo già discusso del fatto che la teoria degli insiemi è intrinsecamente non finitista. Tra gli assiomi della teoria ve ne è uno che asserisce l'esistenza di un insieme infinito e uno dei motivi per cui l'assiomatizzazione di Zermelo-Fraenkel mette sostanzialmente d'accordo la maggior parte dei matematici, è che funziona bene per gli ordinali e i cardinali, che comprendono insiemi infiniti. Anche un finitista dunque vorrebbe una riformulazione della teoria, sebbene in un senso opposto a quello desiderato dalle altre filosofie matematiche appena discusse.

Mettendo in discussione gli assunti della matematica si è arrivati a mettere in discussione anche l'assioma di scelta. Vediamo, allora, come si inserisce storicamente l'assioma di scelta in questo quadro fondazionale.

1.5 Il principio del buon ordinamento

Quando Cantor formulò la teoria degli insiemi, con essa introdusse un principio noto come il "teorema del buon ordinamento": esiste un buon ordine su tutti gli insiemi. Cantor lo riteneva un principio fondamentale della sua teoria, tuttavia esso non convinceva alcuni matematici tra cui J. König che nel 1904 annunciò di aver dimostrato la falsità di questo principio. Successivamente Felix Hausdorff trovò un errore nella sua dimostrazione. Nel 1904, poi, Zermelo pubblicò una dimostrazione del principio di buon ordinamento che diveniva, quindi, un *teorema* della teoria degli insiemi, così come era stata formulata da Cantor. La dimostrazione riposava su un *postulato*, quello che oggi noi conosciamo come assioma di scelta (in questo contesto sarà chiamato "postulato di scelta"): data una famiglia di insiemi non vuoti e a due a due disgiunti esiste un insieme che ha in comune con ogni insieme della famiglia uno e un solo elemento (vedi il Capitolo 4). Il Teorema di Zermelo dette luogo ad un'acceso dibattito sulla legittimità del postulato di scelta.
Come abbiamo visto nel Paragrafo 1.2 dalla teoria degli insiemi di Cantor nacquero alcuni paradossi. In seguito alla scoperta di tali antinomie la comunità scientifica matematica si divise tra chi credeva non fosse più possibile attuare il programma logicista di Frege, che si era servito ampiamente del lavoro di Cantor, e chi invece sperava nella possibilità correggere quegli "errori" che avevano portato a tali scoperte paradossali. Della seconda schiera facevano parte Russell, come abbiamo visto, ma anche Zermelo che nel 1908 propose una nuova formulazione del-

la teoria degli insiemi che non cadeva nelle precedenti antinomie. Nel 1925, A.Fraenkel (1891-1965) produsse una nuova assiomatizzazione della teoria, ispirata alla teoria degli insiemi di Zermelo. Questo sistema è stato successivamente raffinato da T.Skolem, portando agli assiomi ora utilizzati. In questa teoria il postulato di scelta non è dimostrabile, né tantomeno refutabile: è un assioma.
Fermiamoci su alcune considerazioni. L'insieme dei numeri reali non è ben ordinato dalla relazione d'ordine $<$ che tutti conosciamo. Tuttavia, è possibile trovare una relazione d'ordine che ben ordini l'insieme dei numeri reali? Se tutti gli insiemi sono ben ordinabili come vuole il principio del buon ordine, allora dovremmo poter trovare un buon ordine anche per l'insieme dei numeri reali. È possibile farlo? La teoria degli insiemi non sa rispondere a questa domanda. L'indipendenza dell'assioma di scelta dalla teoria degli insiemi di Zermelo-Fraenkel è stata dimostrata da Cohen nel 1963.

Conclusioni

Riassumendo, abbiamo una teoria non completa: c'è una proposizione che non è dimostrabile né refutabile dentro la teoria. Tale teoria è nata con scopi fondazionali: doveva essere il fondamento di tutta la matematica. L'assioma di cui, nella teoria, non è possibile formulare una dimostrazione né una refutazione, è un principio centrale della matematica, dunque una tale teoria non può proporsi come il fondamento della matematica, se non sa rispondere ad una questione tanto importante. D'altra parte l'assioma di scelta non può andare a completare la teoria perché non è evidente, e quello che si vuole è un ristretto numero di assiomi semplici, indiscutibili con cui sia possibile dimostrare i grandi teoremi della matematica.
Con la dimostrazione dei teoremi di Gödel abbiamo capito che ogni teoria che voglia fondare la matematica è incompleta e, soprattutto, non può giustificare se stessa. Cioè non è vera solo in virtù del significato dei termini che compongono gli assiomi. Dunque non ci sconcerta tanto il fatto che questa assiomatizzazione venga meno agli obbiettivi fondazionali che gli erano stati storicamente attribuiti. Più grave è il fatto che la

teoria degli insiemi di Zermelo-Fraenkel, come abbiamo già spiegato, non sappia rispondere alle grandi questioni e tra queste c'è la legittimità o meno dell'assioma di scelta. Sulla validità dell'assioma poi, i matematici sono divisi forse più che per le altre questioni. Perché a questo assioma si ricorre spessissimo, e l'assioma di scelta sembra davvero indispensabile per la dimostrazione di numerosissimi teoremi. D'altro canto è difficile immaginare un buon ordine per i Reali e l'assioma di scelta ha delle conseguenze paradossali. L'assioma di scelta, infatti, permette di dimostrare che da una sfera è possibile ricavarne due identiche per dimensioni alla prima. Questo è il cosìddetto paradosso di Banach-Tarski, di cui si parlerà nel Capitolo 4. L'assioma di scelta allora è vero o falso? Oppure la matematica non si scopre ma si costruisce, e allora una tale domanda non ha senso. La matematica potrebbe essere solo una nostra astrazione, che per qualche motivo che non ci è chiaro riesce a spiegare bene la realtà nel senso che ci permette di fare previsioni, cioè "funziona" come si è detto più volte. Nelle Conclusioni di questo elaborato tutte queste tematiche verranno riesaminate e approfondite, ma con un riferimento più preciso alla teoria, che cominceremo a discutere dal prossimo capitolo.

Capitolo 2

Assiomi di Zermelo-Fraenkel

In questo capitolo mostreremo quali sono gli assiomi della *teoria degli insiemi* e in seguito vedremo quali strutture matematiche li soddisfano. Queste strutture, generalmente chiamate in letteratura *universi*, sono composte da un insieme munito di una relazione binaria detta *relazione di appartenenza*.

Consideriamo quindi una collezione[1] di oggetti che chiameremo d'ora in avanti *universo* e denoteremo con la lettera $\mathscr{U}$. Supporremo sempre che l'universo $\mathscr{U}$ sia non vuoto e munito di una relazione binaria, che noteremo con $\in$. Per indicare che un elemento x è in relazione con y tramite $\in$ scriveremo $x \in y$ e si leggerà x *appartiene a* y. Chiaramente $x \notin y$ si leggerà x *non appartiene a* y.

2.1 Assioma di estensionalità

Il primo assioma della teoria degli insiemi che consideriamo è il così detto *assioma di estensionalità* che esprime il fatto che non possono esistere due insiemi distinti che contengano esattamente gli stessi elementi. Questo concetto viene formalizzato come segue:

$$\forall x \forall y [\forall z (z \in x \iff z \in y) \Rightarrow x = y]. \tag{2.1}$$

[1] Si noti che non diciamo "insieme" in quanto per noi gli insiemi saranno solamente gli oggetti di $\mathscr{U}$.

Questo assioma ci suggerisce, inoltre, che un insieme è definito dai suoi elementi.

Assioma della coppia

L'*assioma della coppia* è l'assioma che garantisce l'esistenza, dati due elementi a e b, di un insieme c che ha come elementi a e b, ed essi soltanto. In realtà questo assioma non è essenziale in quanto è una conseguenza degli altri, ciò nonostante è pratico enunciarlo:

$$\forall x \forall y \exists z \forall t [t \in z \iff (t = x \vee t = y)]. \tag{2.2}$$

Come ci si potrà immaginare, l'insieme c che ha come soli elementi a e b viene denotato con $\{a, b\}$. Si noti che questo assioma implica in particolar modo, dato un elemento a, l'esistenza di un insieme $\{a\}$ che contiene a ed a soltanto. Un insieme con un unico elemento viene detto *singoletto*.

Definizione 2.1.1 *Siano a, b due insiemi tali che $a \neq b$:*

(i) l'insieme $\{a, b\}$ viene chiamato coppia*,*

(ii) l'insieme $\{\{a\}, \{a, b\}\}$ viene chiamato coppia ordinata*.*

Si faccia attenzione al fatto che, a differenza di molte altre branche della matematica, in teoria degli insiemi il termine “coppia” non fa riferimento implicito alla “coppia ordinata”.

Definizione 2.1.2 *Per ogni $n > 0$ definiamo la n-upla $(a_1, a_2, \ldots, a_n)$ per induzione come $(a_1, (a_2, \ldots, a_n))$.*

Gli assiomi che abbiamo introdotto fino a questo punto della trattazione non sono sufficienti per affermare, dati tre elementi distinti a, b, c, l'esistenza di un insieme che contenga essi ed essi soltanto (ovvero $\{a, b, c\}$). Al fine di ovviare a questo problema introduciamo l'assioma seguente.

2.2 Assioma dell'unione

L'assioma dell'unione, chiamato anche *assioma della somma*, che stiamo per riportare ci permette di costruire, dato un insieme a, l'(unico) insieme b i cui elementi sono gli elementi degli elementi di a. Questo insieme b viene chiamato l'*unione* degli elementi di a e si scrive $b = \bigcup a$ o, volendo essere precisi, $b = \bigcup_{x\in a} x$. L'assioma dell'unione è il seguente:

$$\forall x \exists y \forall z[z \in y \iff \exists t(t \in x \wedge z \in t)]. \tag{2.3}$$

Ora possiamo costruire, dati tre insiemi a, b, c, l'insieme $\{a, b, c\}$ che chiaramente sarà $\bigcup\{\{a, b\}, \{c\}\}$. Questa costruzione è generalizzabile in maniera ovvia a qualsiasi numero finito di insiemi $a_1, \ldots, a_n$ portando alla creazione dell'insieme $\{a_1, \ldots, a_n\}$.

Anche l'usuale unione insiemistica, denotata da $a\cup b$, di due insiemi a e b è una conseguenza di questo assioma ed è qui definita come l'insieme $\bigcup\{\{a\}, \{b\}\}$. In generale, dato un numero finito di insiemi $a_1, \ldots, a_n$, l'insieme $\bigcup\{a_1, \ldots, a_n\}$ è chiamato *unione degli insiemi* $a_1, \ldots, a_n$ ed è scritto $a_1 \cup \ldots \cup a_n$.

2.3 Assioma dell'insieme delle parti

L'assioma dell'insieme delle parti esprime il fatto che, per ogni insieme a, esiste un insieme i cui elementi sono tutti i sottoinsiemi di a e lo denotiamo con $\mathscr{P}(a)$. Questo insieme viene usualmente chiamato *l'insieme delle parti di a.*

$$\forall x \exists y \forall z[z \in y \iff z \subseteq x]. \tag{2.4}$$

Si osservi che il simbolo "$\subseteq$" non fa parte del nostro linguaggio in quanto l'universo considerato è munito solo della relazione binaria di appartenenza. la formula $z \subseteq x$, quindi, non è altro che uno zucchero sintattico per esprimere l'enunciato $\forall y(y \in z \Rightarrow y \in x)$.

Relazioni funzionali

Consideriamo una relazione $k+1$-aria $R(x_1, \ldots, x_k, x_{k+1})$. Si dice che è una *relazione funzionale a k argomenti* se si ha

$$\forall x_1 \ldots \forall x_k \forall z \forall w[R(x_1, \ldots, x_k, z) \wedge R(x_1, \ldots, x_k, w) \Rightarrow z = w]$$

Si chiama *dominio* della relazione funzionale R la formula $\exists z R(x_1, \ldots, x_k, z)$. L'*immagine* della relazione funzionale R è, invece, la formula $\exists x_1 \ldots \exists x_k$ $R(x_1, \ldots, x_k, z)$. Data una relazione funzionale $R(x_1, \ldots, x_k, z)$, scriveremo spesso $z = \varphi(x_1, \ldots, x_k)$ per indicare tale relazione. Definiamo cioè, una nuova relazione: $z = \varphi(x_1, \ldots, x_k)$ se e soltanto se $R(x_1, \ldots, x_k, z)$.

Definizione 2.3.1 *Sia $R(x, y)$ una relazione funzionale, se il dominio e l'immagine di R sono insiemi, allora la collezione delle coppie (x, y) tali che $R(x, y)$ si chiama* funzione.

2.4 Schema d'assiomi di rimpiazzamento

Sia $E(x, y, a_1, \ldots, a_k)$ un enunciato i cui paramentri sono $a_1, \ldots, a_k$ tale che E definisca una relazione funzionale ad un argomento e sia a un insieme arbitrario. Vogliamo imporre che il nostro universo $\mathscr{U}$ soddisfi la condizione seguente: esiste un insieme b i cui elementi sono esattamente le immagini degli elementi di a che si trovano nel dominio di questa relazione funzionale. Si noti che il seguente non è un singolo assioma bensì, al variare della formula, esso forma una lista infinita (numerabile) di assiomi. In questo senso viene chiamato *schema di assiomi*:

$$\begin{aligned} &\forall x_1 \ldots \forall x_k \\ &\{\forall x \forall y \forall y'((E(x, y, x_1, \ldots, x_k) \wedge E(x, y, x_1, \ldots, x_k) \Rightarrow y = y') \\ &\Rightarrow \forall t \exists u \forall y[y \in u \iff \exists x(x \in t \wedge E(x, y, x_1, \ldots, x_k))]\} \end{aligned} \tag{2.5}$$

dove $E(x, y, x_1, \ldots, x_k)$ è una formula qualunque senza parametri (con almeno due variabili libere x e y).

Schema di comprensione

Dati un insieme a e una formula $A(x, a_1, \ldots, a_k)$ i cui parametri sono $a_1, \ldots, a_k$ e ad una variabile libera, esiste un insieme i cui elementi sono gli elementi di a che soddisfano la formula. Lo *schema di comprensione* consiste allora nell'insieme dei seguenti assiomi:

$$\forall x_1 ... \forall x_k \forall x \exists y \forall z [z \in y \iff (z \in x \wedge A(z, x_1 ... x_k))] \tag{2.6}$$

dove $A(x, x_1 ... x_k)$ è una formula qualunque senza parametri e ad almeno una variabile libera x. Questo schema di assioma, in realtà, è derivabile dallo schema di rimpiazzamento. In effetti ponendo $E(x, y, a_1, \ldots, a_k)$ la formula "$y = x \wedge A(x, a_1..a_k)$" si ottiene una relazione funzionale ad un argomento di cui $A(x, a_1..a_k)$ è il dominio. Per l'assioma di rimpiazzamento esiste l'insieme delle immagini degli elementi di a che appartengono al dominio. Chiamiamo b questo insieme, b è allora formato dagli elementi di a che sono nella collezione $A(x, a_1, \ldots, a_k)$. Da adesso in poi si utilizzerà la notazione $b = \{x \in a; A(x, a_1, \ldots, a_k)\}$ per rappresentare questo insieme.

Proposizione 2.4.1 *Dati due insiemi a e b, $a \times b$: la collezione delle coppie (x, y) tali che $x \in a$ e $y \in b$ detto* prodotto cartesiano di a e b, *è un insieme.*

Proof. $a \times b = \{z \in \mathscr{P}(\mathscr{P}(a \cup b)); \exists x \exists y [z = (x, y) \wedge x \in a \wedge y \in b]\}$ che è un insieme per l'assioma di comprensione. ■

Corollario 2.4.2 *Una funzione è un insieme.*

Proof. Una funzione f è una collezione di coppie (x, y) tali che $x \in a$ e $y \in b$ dove a, b sono rispettivamente il dominio e l'immagine della funzione. Allora per l'assioma di comprensione, f è un insieme: $f = \{z \in a \times b; \exists x \exists y (z = (x, y) \wedge R(x, y))\}$. ■

A questo punto siamo in grado di dimostrare l'esistenza dell'insieme vuoto.

Teorema 2.4.3 *Esiste un insieme, e uno solo, che non ha elementi.*

Proof. Sia a un insieme qualsiasi dell'universo per l'assioma di comprensione esiste l'insieme $\{x \in a; x \neq x\}$. Questo insieme non ha elementi, la sua unicità è una conseguenza dell'assioma di estensionalità. ■

L'insieme vuoto sarà denotato con il simbolo: $\emptyset$. Questo insieme ci permette di definire l'ultimo degli assiomi della teoria non ancora enunciato. Prima, però, è opportuno dare una dimostrazione del fatto che *l'assioma della coppia si deriva dall'assioma delle parti e da quello di rimpiazzamento.*

Proof. Ogni insieme d che è un sottoinsieme di $\emptyset$ è vuoto. Dunque esiste $\mathscr{P}(\emptyset)$ e ha $\emptyset$ come unico elemento. Questo dimostra l'esistenza di $\{\emptyset\}$. Ora se $d \subseteq \{\emptyset\}$ ciò vorrebbe dire che $d = \emptyset$ oppure $d = \{\emptyset\}$. Dunque $\mathscr{P}(\{\emptyset\})$ ha due elementi distinti $\emptyset$ e $\{\emptyset\}$ e questo dimostra l'esistenza di $\{\emptyset, \{\emptyset\}\}$. Siano allora a, b due insiemi qualsiasi. La relazione $(x = \emptyset \wedge y = a) \vee (x = \{\emptyset\} \wedge y = b)$ è una relazione funzionale a un argomento. Applicando lo schema di riflessione a questa relazione e all'insieme $\{\emptyset, \{\emptyset\}\}$ si ottiene un insieme c che ha per unici elementi a e b. ■

2.5 Ordinali

A partire da $\emptyset$, possiamo definire la classe[2] degli ordinali On. L'idea è questa: $\emptyset$ è l'ordinale 0. Se α è un ordinale, allora anche $\alpha \cup \{\alpha\}$ lo è, e si chiama il *successore* di α. Dunque il successore di 0 è $1 = \{\emptyset\}$. Il successore di 1 è l'insieme $\{\emptyset, \{\emptyset\}\}$ che chiameremo 2, e così via. In tal modo ogni ordinale contiene tutti gli ordinali che lo precedono, infatti, ad esempio, $2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$. Ma questa non è una definizione rigorosa.

Definizione 2.5.1 *Un insieme è* transitivo *se soddisfa la seguente proprietà:* $\forall x (x \in \alpha \Rightarrow x \subseteq \alpha)$.

[2]Una classe è una collezione di insiemi dell'universo che soddisfano una determinata proprietà. Il termine viene usato, prevalentemente, per quelle collezioni di insiemi che non sono a loro volta insiemi.

Definizione 2.5.2 *Un insieme ordinato*[3] a *è* ben ordinato *quando ogni sottoinsieme non vuoto di* a *ha un minimo.*

Definizione 2.5.3 *Un insieme* α *è un* ordinale *se, e soltanto se è transitivo e ben ordinato per l'appartenenza.*

Notazione 2.5.4 *D'ora in avanti scriveremo* $\alpha \varepsilon On$ *per intendere* "α è un ordinale".[4]

Nessun ordinale appartiene a se stesso: si consideri un ordinale α, nessuno dei suoi elementi appartiene a se stesso, perché $\in$ è una relazione d'ordine stretto su α. Dunque α non può appartenere a se stesso.

Lemma 2.5.5 *Sia* α *un ordinale. Se* β *è un elemento di* α*, allora* β *è un ordinale.*

Proof. Se $\beta \in \alpha$, allora $\beta \subset \alpha$ dunque, poiché α è ben ordinato da $\in$, anche β è ben ordinato da $\in$. Inoltre β è transitivo: sia $\sigma \in \beta$, poiché α è transitivo, $\sigma \in \alpha$. Allora per ogni $\gamma \in \sigma$, dal fatto che $\in$ è un ordine su α e γ, σ, β sono elementi di α, segue che $\gamma \in \sigma \wedge \sigma \in \beta \Rightarrow \gamma \in \beta$. ■

Osservazione 2.5.6 *Il Lemma 2.5.5 ci permette di affermare che ogni ordinale è l'insieme degli ordinali che lo precedono.*

Lemma 2.5.7 *Siano* α, β *due ordinali, le seguenti affermazioni sono equivalenti:*

(i) $\alpha < \beta$

(ii) $\alpha \in \beta$

---

[3] Un ordine è una relazione transitiva e antisimmetrica.

[4] Riserviamo il simbolo $\in$ alla relazione di appartenenza tra due insiemi. Come dimostreremo in seguito, la classe degli ordinali non è un insieme dunque, tale scelta ci impedisce di scrivere $\alpha \in On$. Tuttavia $x \varepsilon On$, così come l'abbiamo appena definita, è un predicato, cioè una relazione unaria.

(iii) $\alpha \subset \beta$

La dimostrazione che il punto *iii.* equivale ai precedenti non è immediata. Eccone dunque una dimostrazione.
Proof. *ii.* $\Rightarrow$ *iii.* è vero per il Lemma 2.5.5.
Supponiamo *iii.* Sia γ il primo ordinale di $\beta - \alpha$ (γ esiste perché β è ben ordinato). Allora $\alpha = \{x \in \beta; x < \gamma\}$: infatti se $x \in \alpha$, allora $x \in \beta$ perché, per ipotesi, $\alpha \subset \beta$. Dunque $x \in \beta$ e $x < \gamma$ perché, poiché α è transitivo, allora si ha che, dati due insiemi y, x, se $x \in \alpha$ e $y < x$, allora $y \in \alpha$. Dunque se fosse $x \geq \gamma$,[5] si avrebbe $\gamma \in \alpha$ che contraddice la definizione di γ. Viceversa, se $x \in \beta$ e $x < \gamma$, allora $x \in \alpha$ (per definizione di γ). D'altra parte $\alpha = \{x \in \beta; x < \gamma\} = \{x \in b, x \in \gamma\} = \beta \cap \gamma = \gamma$ (perché β è transitivo dunque $\gamma \subset \beta$). Dunque $\alpha = \gamma$, quindi $\alpha \in \beta$. ■

Dalla definizione di ordinale possiamo dedurre che:

Osservazione 2.5.8 *Se α è un ordinale, allora $\alpha \cup \{\alpha\}$ è un ordinale.*

La transitività è evidente. Inoltre sia $a \subseteq \alpha \cup \{\alpha\}$ non vuoto, se a è tutto contenuto in (o uguale a) α, allora ha un minimo perché α è ben ordinato. Altrimenti $a = b \cup \{\alpha\}$ con $b \subset \alpha$. L'elemento minimo di b è anche più piccolo di α perché $b \subset a \subset \alpha$. Abbiamo dimostrato che ogni sottoinsieme non vuoto di $\alpha \cup \{\alpha\}$ ha un minimo.

Il *successore* di α è, per definizione, il più piccolo ordinale superiore (secondo la relazione di appartenenza) ad α.

Lemma 2.5.9 *Per ogni ordinale α, $\alpha \cup \{\alpha\}$ è il suo successore.*

Proof. Sia σ un ordinale superiore ad α. Allora $\alpha \in \sigma$ e poiché, per ipotesi, σ è un ordinale, allora è transitivo, dunque $\alpha \subset \sigma$. Questo dimostra che $\alpha \cup \{\alpha\} \subseteq \sigma$. Per l'Osservazione2.5.5, $\alpha \cup \{\alpha\} \leq \sigma$. ■

Il successore di un ordinale α si denota con $\alpha + 1$. Viceversa, α si dice il *predecessore* di $\alpha + 1$.

[5] si ricorda che β è ben ordinato quindi è anche totalmente ordinato

2.6 Assioma dell'infinito

L'assioma dell'infinito è la seguente formula:

$$\exists w(\emptyset \in w \wedge \forall y(y \in w \Rightarrow y \cup \{y\} \in w)). \tag{2.7}$$

L'assioma è equivalente alla proposizione:

"Esiste un ordinale infinito".

Vediamo perché.

Un ordinale α si dice *finito* quando: ogni ordinale β più piccolo o uguale ad α e diverso da $\emptyset$, ha un predecessore. Se esiste un ordinale non finito, allora chiamiamo w il primo tra questi. Si ha che w è l'insieme di tutti gli ordinali finiti: perché se α è un ordinale finito, non si può avere $w \leq \alpha$, altrimenti w sarebbe finito. Ne segue che $\alpha < w$.[6]

Diamo ancora una definizione:

Definizione 2.6.1 *Un ordinale α si dice* limite, *quando è non vuoto e soddisfa la formula $\forall\beta(\beta \in \alpha \Rightarrow (\beta + 1 \in \alpha))$.*

Un ordinale limite è un ordinale che non ha predecessori. Dunque un ordinale limite è non finito. Inoltre w è un ordinale limite. Infatti, se $\alpha \in w$, allora $\alpha + 1 \in w$: perché $\alpha + 1$ è finito. Abbiamo dimostrato che:

Osservazione 2.6.2 *L'affermazione "esiste un ordinale limite" è equivalente all'affermazione "esiste un ordinale non finito".*

Se esiste un ordinale limite, allora soddisfa chiaramente la Formula 2.7. Viceversa, supponiamo che questa formula sia vera e, sia a un insieme che soddisfa la formula, consideriamo il primo ordinale che non è elemento di a, sia α. Allora $\alpha \neq \emptyset$ e α non ha predecessori: se $\alpha = \beta \cup \{\beta\}$, si avrebbe β inferiore a α, cioè $\beta \in \alpha$, dunque $\beta \cup \{\beta\} \in \alpha$, che è una contraddizione. Ciò vuol dire che esiste un ordinale infinito: α. Abbiamo dimostrato che:

Osservazione 2.6.3 *l'affermazione "esiste un ordinale infinito" è equivalente alla Formula 2.7.*

---

[6]Questa dimostrazione riposa sul fatto che di due ordinali distinti ce ne è uno inferiore all'altro. Per la dimostrazione si veda il Corollario2.6.5

La teoria degli insiemi di Zermelo-Fraenkel

Riportiamo qui di seguito la lista degli assiomi della teoria degli insiemi di Zermelo-Fraenkel, di cui si è trattato in questo capitolo:

Assioma di Estensionalità:

$$\forall x \forall y [\forall z (z \in x \iff z \in y) \Rightarrow x = y];$$

(Assioma della Coppia:

$$\forall x \forall y \exists z \forall t [t \in z \iff (t = x \vee t = y)];)$$

Assioma dell'Unione:

$$\forall x \exists y \forall z [z \in y \iff \exists t (t \in x \wedge z \in t)];$$

Assioma dell'Insieme delle Parti:

$$\forall x \exists y \forall z [z \in y \iff z \subseteq x];$$

Assiomi di Rimpiazzamento:

Sia $E(x, y, x_1, \ldots, x_k)$ una formula qualunque senza parametri (con almeno due variabili libere x e y)

$$\begin{aligned} \forall x_1 \ldots \forall x_k \{ \forall x \forall y \forall y' ((E(x, y, x_1, \ldots, x_k) \wedge E(x, y, x_1, \ldots, x_k) \Rightarrow y = y') \\ \Rightarrow \forall t \exists u \forall y [y \in u \iff \exists x (x \in t \wedge E(x, y, x_1, \ldots, x_k))] \}; \end{aligned}$$

(Assiomi di Comprensione:

Sia $A(x, x_1 ... x_k)$ una formula qualunque senza parametri e ad almeno una variabile libera x.

$$\forall x_1 ... \forall x_k \forall x \exists y \forall z [z \in y \iff (z \in x \wedge A(z, x_1 ... x_k))];)$$

Assioma dell'Infinito:

$$\exists w (\emptyset \in w \wedge \forall y (y \in w \Rightarrow y \cup \{y\} \in w)).$$

Proprietà degli ordinali

Lemma 2.6.4 *Ogni insieme di ordinali ha un limite superiore, che è l'unione degli elementi di questo insieme ed è un ordinale.*

Proof. Sia a un insieme di ordinali, e $\beta = \bigcup_{\alpha \in a} \alpha$. Se x è un sottoinsieme non vuoto di β, si ha $x \cap \alpha_0 \neq \emptyset$ per un certo ordinale $\alpha_0 \in a$. Allora $x \cap \alpha_0$ ha un più piccolo elemento, in quanto è un sottoinsieme non vuoto di un insieme ben ordinato α_0. Il più piccolo elemento di $x \cap \alpha_0$ è chiaramente il più piccolo elemento di x. Ciò dimostra che β è ben ordinato dalla relazione di appartenenza $\in$. Inoltre, se $x \in \beta$ e $y \in x$, si ha $x \in \alpha$ per un certo $\alpha \in a$, dunque $y \in \alpha$, quindi $y \in \beta$. Questo dimostra che β è un ordinale. Si ha $\beta \geq \alpha$ per ogni $\alpha \in a$; Inoltre, se $\gamma \geq \alpha$ per ogni $\alpha \in a$, allora $\alpha \subseteq \gamma$ per ogni $\alpha \in a$, dunque $\beta \subseteq \gamma$, cioè $\gamma \geq \beta$. ■

Corollario 2.6.5 *Dati due ordinali α, β, si ha $\alpha < \beta$ oppure $\beta < \alpha$ oppure $\alpha = \beta$.*

Lemma 2.6.6 *Ogni insieme transitivo di ordinali è un ordinale.*

Proof. Sarà sufficiente dimostrare che se a è un insieme transitivo di ordinali, allora a è ben ordinato dalla relazione di appartenenza. Per il Lemma 2.6.6, a ha un limite superiore α che è l'unione degli elementi di a. Se $\beta \in a$, allora $\beta \subseteq \alpha$. Dunque $\beta = \alpha$, oppure $\beta \in \alpha$. Ciò dimostra che $a \subseteq \alpha + 1$, che è un insieme ben ordinato per l'appartenenza. Pertanto, anche a è ben ordinato per l'appartenenza. ■

Teorema 2.6.7 *La classe degli ordinali non è un insieme.*

Proof. Se la classe degli ordinali fosse un insieme, allora sarebbe un insieme transitivo di ordinali. Dunque, per il Lemma 2.6.6, On sarebbe un ordinale. Potremmo affermare, allora, che $On \in On$, ma nessun ordinale appartiene a se stesso. Contraddizione. ■

Teorema 2.6.8 *Se due ordinali α, β sono isomorfi, allora sono uguali.*

Proof. Per ipotesi esiste un isomorfismo $f : \alpha \to \beta$. In particolare f è una funzione strettamente crescente. Supponiamo, per assurdo, che esista γ il più piccolo elemento di α tale che $f(\gamma) < \gamma$. Allora $f(f(\gamma)) < f(\gamma)$ perché f è crescente. Ma $f(\gamma)$ è un ordinale più piccolo di γ, dunque il fatto che $f(f(\gamma)) < f(\gamma)$ contraddice la definizione di γ. Pertanto per ogni $\gamma \in \alpha$, $\gamma \leq f(\gamma) \in \beta$ dunque $\gamma \in \beta$. Cioè $\alpha \subseteq \beta$. Analogamente si dimostra che $\beta \subseteq \alpha$ (anche f^{-1} è strettamente crescente). Ne concludiamo che $\alpha = \beta$. ■

Definizione 2.6.9 *Un* buon ordine su una classe *X, è una relazione d'ordine totale* $<_X$ *su* X *tale che per ogni elemento* x *di* X, *la collezione* $S_x(<_X)$ *degli* $y \in X$ *tali che* $y <_X x$ *è un insieme ben ordinato.*

Dato un insieme a, per ogni $x \in a$ $S_x(a) = \{y \in a; y <_a x\}$ è un *segmento iniziale* di a.

Teorema 2.6.10 *Ogni insieme ben ordinato* $(a, <_a)$ *è isomorfo a un unico ordinale.*

Proof. *Unicità.* Se f è un isomorfismo di a su un ordinale α e g è un isomorfismo di a su β, allora $g \circ f^{-1}$ è un isomorfismo di α su β. Dunque $\alpha = \beta$.
Esistenza. Poniamo $b = \{x \in a; S_x(a)$ è isomorfo a un ordinale $\}$, dove $S_x(a) = \{y \in a; y <_a x\}$. Per ogni $x \in b$ chiamo $\beta(x)$ l'ordinale isomorfo a $S_x(a)$. L'insieme $\{\beta(x); x \in b\}$ è un insieme transitivo di ordinali: se $\alpha \in \beta(x)$ per un certo $x \in b$ allora α è isomorfo a un segmento iniziale (stretto) di $S_x(a)$: tale isomorfismo si ottiene dalla restrizione a α della funzione inversa dell'isomorfismo tra $S_x(a)$ e $\beta(x)$. Dunque α è della forma $\beta(y)$ per un certo $y <_a x$. Pertanto $\{\beta(x); x \in b\}$ è un ordinale. Allora la funzione che ad ogni x associa $\beta(x)$ è un isomorfismo tra b e un ordinale. Se $b \neq a$ allora $b = S_{x_0}(a)$ per un certo $x_0 \in a$. Ma abbiamo appena dimostrato che b è isomorfo a un ordinale dunque $x_0 \in b = S_{x_0}(a)$, contraddizione. Allora $b = a$ dunque si ha un isomorfismo tra a e un ordinale. ■

Teorema 2.6.11 *Sia X una classe che non è un insieme e R un buon ordine su X, esiste una relazione funzionale che stabilisce un isomorfismo tra X e On.*

Proof. Per ogni $x \in X$ esiste un unico ordinale isomorfo a $S_x(<_X)$. Posso allora definire la relazione funzionale $\alpha = H(x)$ tramite la formula "α è un ordinale isomorfo a $S_x(<_X)$". Tale relazione, inoltre, stabilisce un isomorfismo tra X e On : se $x <_X y$, allora $S_x(<_X) \subset S_y(<_X)$, pertanto $H(x) \in H(y)$. L'immagine di H è un insieme transitivo di ordinali che non è un insieme, quindi è la classe On. Dimostriamo dunque che l'immagine è transitiva: sia $H(x)$ un elemento dell'immagine di H, sia $\alpha \in H(x)$. L'isomorfismo tra $H(x)$ e $S_x(<_X)$ associa a α l'insieme $S_y(<_X)$ per $y <_X x$. Cioè $\alpha = H(y)$. Dimostriamo, infine, che l'immagine di H non è un insieme: si consideri J^{-1} che ha per dominio l'immagine di H, e ha X per immagine. Per lo schema di rimpiazzamento, poiché X non è un insieme, il dominio di J^{-1} non può essere un insieme. ■

Capitolo 3

Assioma di fondazione

Gli assiomi di cui si è parlato nel capitolo precedente, formano la teoria degli insiemi di Zermelo-Fraenkel, a cui ci si riferirà con l'abbreviazione ZF. Il seguente assioma, invece, non fa parte della teoria, si tratta dell'*assioma di fondazione* (d'ora in avanti AF). L'enunciato dell'assioma è il seguente:

$$\forall x[x \neq \emptyset \Rightarrow \exists y(y \in x \wedge y \cap x = \emptyset)].$$

L'assioma dice che: ogni insieme non vuoto, ha un elemento che non ha alcun elemento in comune con l'insieme in questione. Questo assioma implica che non esistono successioni infinite discendenti. Non esiste, cioè, alcuna successione $(u_n)_{n \in w}$ (una *successione infinita* è una funzione di dominio w) tale che per ogni $n \in w$, $u_{n+1} \in u_n$. L'immagine di questa successione sarebbe un insieme per l'assioma di rimpiazzamento, e contraddirebbe dunque AF. In particolare, allora, l'assioma di fondazione implica che $\forall x(x \notin x)$. L'assioma di fondazione, si è detto, non fa parte della teoria nel senso che è indipendente dagli assiomi di ZF (in questo contensto l'indipendenza dell'assioma di fondazione non verrà trattata, per la dimostrazione si veda [Krivine, 1998]).

3.1 Definizioni per induzione sugli ordinali

Si consideri una formula a una variabile libera $E(x)$. Affiché $E(\alpha)$ sia vera per ogni ordinale α, è necessario e sufficiente che, per ogni ordinale α, se $E(\beta)$ è vera per ogni $\beta < \alpha$, allora $E(\alpha)$ è vera; in altri termini è necessario e sufficiente che sia vera la formula che segue:

$$\forall\alpha(\forall\beta(\beta < \alpha \Rightarrow E(\beta)) \Rightarrow E(\alpha)).$$

La dimostrazione è immediata: Supponiamo $\forall\alpha(\forall\beta(\beta < \alpha \Rightarrow E(\beta)) \Rightarrow E(\alpha))$, allora se $E(\alpha)$ è falso per un certo $\alpha \varepsilon On$, consideriamo il primo di tali ordinali. Si ha che per ogni $\beta < \alpha$, $E(\beta)$ è vero e dunque, per ipotesi, $E(\alpha)$ è vero. Contraddizione.

Questo principio ci fornisce un metodo di dimostrazione che si chiama *dimostrazione per induzione sugli ordinali*. Quando vogliamo dimostrare che una proprietà è vera per tutti gli ordinali, potremo supporre per *ipotesi induttiva* che, dato un ordinale α tale proprietà è vera per tutti gli ordinali più piccoli di α. Sarà sufficiente dimostrare, allora, che l'ipotesi induttiva implica che la proprietà è vera per α. Nella maggior parte delle dimostrazioni per induzione, però, dovremo trattare separatamente il caso in cui $\alpha = 0$, il caso in cui α è un ordinale successore, e il caso in cui α è un ordinale limite. Nel paragrafo seguente si da qualche esempio di dimostrazione per induzione sugli ordinali. I risultati così ottenuti, saranno indispensabili per il seguito.

3.2 La gerarchia cumulativa

In ogni modello $\mathscr{U}$ di ZF, è possibile definire una collezione V costruita come segue. Si associa ad ogni ordinale α un insieme V_α, secondo la seguente definizione:

- $V_0 = \emptyset$,
- $V_{\alpha+1} = \mathscr{P}(V_\alpha)$,
- $V_\alpha = \bigcup_{\beta\in\alpha} V_\beta$ se α è un ordinale limite.

La precedente è la definizione di una relazione funzionale $y = V_\alpha$ di dominio On.

La collezione V è uguale all'unione, nel senso intuitivo, dei V_α (per $\alpha\varepsilon On$).

Notazione 3.2.1 *Definiamo la relazione* $x\varepsilon V$:

$$x\varepsilon V \iff \exists\alpha(\alpha\varepsilon On \wedge x \in V_\alpha).$$

Il metodo della dimostrazione per induzione sugli ordinali di cui si è trattato in questo capitolo ci permette di dimostrare che, per ogni $\alpha \in On$, V_α è un insieme transitivo.

Lemma 3.2.2 *Per ogni* $\alpha\varepsilon On$, V_α *è un insieme transitivo.*

Proof. Se $\alpha = 0$ la condizione di transitività è banalmente soddisfatta. Se α è, invece, un ordinale successore, precisamente $\alpha = \beta + 1$, allora sia $x \in V_{\beta+1}$ un insieme qualsiasi dell'universo. Per definizione di $V_{\beta+1}$, $x \subseteq V_\beta$. Allora, per ogni $y \in x$, si ha $y \in V_\beta$. Per ipotesi di induzione V_β è transitivo dunque $y \subseteq V_\beta$ e quindi $y \in V_{\beta+1}$. Dimostriamo, infine, che il lemma è vero per α ordinale limite. Sia $x \in V_\lambda$, con λ ordinale limite. $V_\lambda = \bigcup_{\sigma\in\lambda} V_\sigma$ dunque, $x \in V_\sigma$ per un certo ordinale $\sigma < \lambda$. Per ipotesi di induzione V_σ è transitivo, dunque $x \subseteq V_\sigma$. Pertanto, sia $y \in x$, si ha $y \in V_\sigma$ e ,quindi, $y \in \bigcup_{\sigma<\alpha} V_\sigma$. ■

Ancora per induzione[1], è possibile dimostrare che, dati due ordinali α, β :

$$\alpha \leq \beta \Rightarrow V_\alpha \subseteq V_\beta.$$

Questi risultati ci permettono, allora, di affermare che per ogni α:

$$V_\alpha = \bigcup_{\sigma<\alpha} \mathscr{P}(V_\sigma).$$

È ovvio per $\alpha = 0$. Altrimenti, supponiamo $\alpha = \beta+1$, se $x \in V_{\beta+1}$ allora $x \in \mathscr{P}(V_\beta)$, dunque $x \in \bigcup_{\sigma<\alpha} \mathscr{P}(V_\sigma)$. Viceversa: se $x \in \bigcup_{\sigma<\alpha} \mathscr{P}(V_\sigma)$,

[1] L'induzione si fa su β.

allora $x \subseteq V_\sigma$ per un certo ordinale $\sigma < \alpha$. $\sigma \leq \beta$ perché α è il successore di β, dunque per quanto abbiamo detto sopra, $V_\sigma \subseteq V_\beta$. Pertanto $x \subseteq V_\sigma$ implica $x \subseteq V_\beta$, cioè $x \in V_{\beta+1}$. Se, infine, α è un ordinale limite allora, per definizione, $V_\alpha = \bigcup_{\sigma\in\alpha} V_\sigma$. Sia dunque $x \in V_\alpha$, $x \in V_\sigma$ per un certo $\sigma < \alpha$. Poiché V_σ è transitivo, allora si ha anche $x \subseteq V_\sigma$, cioè $x \in \mathscr{P}(V_\sigma)$. Dunque $x \in \bigcup_{\sigma\in\alpha} \mathscr{P}(V_\sigma)$. Viceversa: sia $x \in \bigcup_{\sigma\in\alpha} \mathscr{P}(V_\sigma)$; esiste un ordinale $\sigma < \alpha$ tale che $x \subseteq V_\sigma$. Allora $x \in V_{\sigma+1}$. Poiché α è un ordinale limite, anche $\sigma + 1 \in \alpha$, dunque $x \in \bigcup_{\sigma<\alpha} V_\sigma$.

3.3 IL rango di un insieme

Definizione 3.3.1 *Dato un inseme a, il* rango di a *(nel seguito $rg(a)$) è il più piccolo ordinale α tale che $a \in V_\alpha$.*

Il rango è sempre un ordinale successore: se un insieme $x \in V_\alpha$ e α è un ordinale limite, allora si ha $x \in \bigcup_{\beta\in\alpha} V_\beta$, cioè $x \in V_\beta$ per un ordinale $\beta < \alpha$. Pertanto α non può essere il rango di x.

Dimostriamo ora una proprietà che sarà utilizzata in seguito.

Lemma 3.3.2 *Un insieme x è in V se e soltanto se ogni elemento di x è in V. Inoltre se $rg(x) = \alpha$ allora per ogni $y \in x$ si ha che $rg(y) < \alpha$.*

Proof. Sia a un insieme di V di rango $\alpha = \beta + 1$; allora $a \in V_{\beta+1}$ cioè $a \subseteq V_\beta$. Questo vuol dire che ogni elemento di a è in V, e ha un rango inferiore o uguale a β, dunque minore di α. Viceversa, sia a un insieme tale che ogni elemento di a è in V. L'insieme dei ranghi degli elementi di a è un insieme di ordinali, che ammette, per il Lemma 2.6.4, un ordinale α per estremo superiore. Dunque $a \subseteq V_{\alpha+1}$, quindi a è in V. ■

Un'altra proprietà importante è la seguente:

Lemma 3.3.3 *Ogni ordinale α è in V e $rg(\alpha) = \alpha + 1$.*

Proof. Sia α il primo ordinale tale che $\alpha \notin V_{\alpha+1}$, se esiste. Allora $\beta \in \alpha \Rightarrow \beta \in V_{\beta+1}$; dunque:

$$\alpha \subseteq \bigcup_{\beta\in\alpha} V_{\beta+1} = \bigcup_{\beta\in\alpha} \mathscr{P}(V_\beta) = V_\alpha$$

Ciò vuol dire che $\alpha \in V_{\alpha+1}$, contrariamente all'ipotesi. Sia α il primo ordinale tale che $\alpha \in V_\alpha$, se esiste; si ha $\alpha \in \bigcup_{\beta\in\alpha} \mathscr{P}(V_\beta)$; esiste, pertanto, $\beta < \alpha$ tale che $\alpha \in \mathscr{P}(V_\beta)$; ne segue $\alpha \subseteq V_\beta$ e, poiché $\beta \in \alpha$, $\beta \in V_\beta$, contrariamente alla definizione di α. ■

3.4 Chiusura transitiva di un insieme

Definiamo la nozione di *chiusura transitiva*.

Teorema 3.4.1 *Per ogni insieme x esiste un insieme transitivo $Ct(x)$ che contiene x, e che è contenuto in ogni insieme transitivo contenente x. Un tale insieme si chiama* chiusura transitiva di x.

Proof. Si definisce, per induzione, una funzione f di dominio w, ponendo: $f(0) = x$; $f(n+1) = \bigcup_{y\in f(n)} y$. Si pone poi, $a = \bigcup_{n\in w} f(n)$: a è l'insieme che stiamo cercando, cioè $Ct(x)$. È evidente, infatti, che $x \subseteq a$. Inoltre, a è transitivo: se $y \in a$, allora $y \in f(n)$ per un certo $n \in w$, dunque $y \subseteq f(n+1)$ e $y \subseteq a$. Se z è un insieme transitivo che contiene x, si dimostra per induzione che $f(n) \subseteq z$ per ogni $n \in w$. È vero per $n = 0$; se $f(n) \subseteq z$ con $y \in f(n)$ allora $y \in z$, dunque $y \subseteq z$. Pertanto $\bigcup_{y\in f(n)} y \subseteq z$, cioè $f(n+1) \subseteq z$. Poiché z contiene $f(n)$ per ogni n, allora $a \subseteq z$. ■

3.5 Indipendenza di $\forall x(x\varepsilon V)$

Teorema 3.5.1 *L'assioma di fondazione equivale all'affermazione:* "ogni insieme dell'universo è in V *(affinché l'universo soddisfi l'assioma di fondazione, è necessario e sufficiente che V sia l'universo intero).*

Proof. Supponiamo che ogni insieme dell'universo sia in V e sia a un insieme non vuoto. Sia, inoltre, b un elemento di a di rango minimo α. Ogni elemento di b è di rango minore di α, quindi non può essere elemento di a. Questo vuol dire che $b \cap a = \emptyset$, ne segue l'assioma di fondazione.

Per dimostrare l'affermazione reciproca usiamo il Teorema 3.4.1: dato un insieme a esiste la chiusura transitiva di a, $Ct(a)$ è un insieme transitivo. Supponiamo, allora, che AF sia soddisfatto e che esista un insieme a che non è in V. Sia b un insieme transitivo contenente a (un tale insieme esiste in quanto esiste $Ct(a)$), e sia $c = \{x \in b; x \notin \mathrm{V}\}$. Allora $c \neq \emptyset$: infatti $a \subseteq b$ (a è non vuoto altrimenti sarebbe in V) e poiché $a \notin V$, esiste un elemento x_0 di a che non è in V; cioè $x_0 \in c$. Per ogni $x \in c$, $c \cap x \neq \emptyset$: perché se $x \in c$, c'è un elemento y di x che non è in V (altrimenti x stesso sarebbe in V). Poiché b è transitivo, $y \in b$, allora $y \in c$ per definizione di c e $x \cap c \neq \emptyset$. L'insieme c contraddice l'assioma di fondazione. ∎

Capitolo 4

Assioma di scelta

In questo capitolo si tratterà dell'assioma di scelta. Una prima parte sarà dedicata alle diverse formulazioni dell'assioma, si tratterà, in seguito, del ruolo che esso gioca nella matematica, cioè si enuncieranno alcuni dei principali teoremi che, almeno sino ad oggi, è possibile dimostrare solo utilizzando l'assioma di scelta.
Dobbiamo a Russell una celebre illustrazione dell'assioma di scelta. Immaginiamo di avere un insieme infinito di paia di scarpe e, supponiamo di voler costruire un nuovo insieme prendendo una scarpa (e una sola) per ogni paio. Possiamo decidere di prendere, ad esempio, tutte e sole le scarpe destre. Sostituiamo allora, le scarpe con paia di calzini: non possiamo distinguere un calzino destro da una corrispondente calzino sinistro. Dunque, non possiamo costruire l'insieme cercato procedendo come prima. Abbiamo bisogno di utilizzare l'assioma di scelta per il quale: dato un insieme a di insiemi non vuoti (l'insieme di paia di scarpe), esiste un insieme che ha, in comune con ogni insieme di a, un solo elemento (l'insieme che ha una sola scarpa di ogni paio). In altre parole l'assioma di scelta ci dice che, esiste una regola che ci permette di *scegliere* da ogni insieme di a, un solo elemento.

4.1 L'assioma di scelta

L'assioma di scelta (in seguito AC-dall'inglese Axiom of Choice-) è il seguente assioma:

Assioma 4.1.1 AC_i[1]*:*

$$\forall x((\emptyset \notin x \wedge \forall y \forall z(y \in x \wedge z \in x \wedge y \neq z \Rightarrow y \cap z = \emptyset)) \Rightarrow$$

$$\exists u \forall y(y \in x \Rightarrow \exists k(y \cap u = \{k\}))).$$

L'assioma dice che dato un insieme a di insiemi non vuoti e a due a due disgiunti, esiste un insieme che ha un solo elemento in comune con ognuno degli elementi di a.
Si osservi che se a è l'insieme quoziente rispetto ad una relazione di equivalenza, allora c è l'insieme dei rappresentanti. L'assioma di scelta, anzi, è equivalente all'affermazione: ogni insieme di classi di equivalenza, ammette un'insieme di rappresentanti. Questo ci fornisce già dei chiarimenti sul perché l'assioma di scelta è tanto importante.

Teorema 4.1.2 $AC \iff$ *"per ogni insieme A, sia R una relazione di equivalenza su A, A/R -l'insieme quoziente modulo $R-$ ammette un insieme di rappresentanti".*

Proof. Supponiamo l'assioma di scelta e siano A un insieme e R una relazione di equivalenza su A. A/R è una famiglia di insiemi non vuoti e a due a due disgiunti. Per l'assioma di scelta, dunque, esiste un insieme che ha in comune con ogni classe di A/R uno e un solo elemento che possiamo scegliere come suo rappresentante.
Viceversa, sia A una famiglia di insiemi non vuoti e a due a due disgiunti. Possiamo definire una relazione di equivalenza R su $\bigcup A$: Siano a, b due insiemi di $\bigcup A$, aRb se e soltanto se "a e b appartengono allo stesso insieme di A". Per ipotesi allora esiste l'insieme dei rappresentanti c. Chiaramente c ha in comune con ogni insieme di a un solo elemento. ■

[1] AC_i sta per "assioma di scelta formulazione insiemistica"

Nota 4.1.3 *La condizione "gli insiemi della famiglia di insiemi non vuoti a, sono a due a due disgiunti" è necessaria affinché l'assioma non sia palesemente falso.*

Supponiamo, infatti, che $a = \{\{p, s\}, \{s, t\}, \{t, p\}\}$. Per soddisfare l'assioma di scelta, dovrei trovare un insieme che abbia in comune con ogni insieme di a *un solo elemento.* Gli insiemi di a si intersecano. Si scelga, ad esempio, p per il primo dei tre. Si è costretti a scegliere t per il secondo insieme dei tre (altrimenti $c \cap \{p, s\} = \{p, s\}$), ma così $c \cap \{t, p\} = \{t, p\}$. Se, invece, si sceglie s per il primo dei tre insiemi, allora si è costretti a scegliere t per il terzo. Ancora una volta, l'insieme costruito non soddisfa l'assioma di scelta: $c \cap \{s, t\} = \{s, t\}$.

4.2 Le principali formulazioni

L'assioma di scelta si presta a numerose formulazioni. Qui di seguito si trovano altre formulazioni dell'assioma di scelta (equivalenti modulo $ZF + AF$).

La funzione di scelta

Definizione 4.2.1 *Sia a un insieme di insiemi non vuoti, $f : a \to \bigcup a$ è una* funzione di scelta per *a se, e soltanto se, per ogni $x \in a$, $f(x) \in x$.*

Assioma 4.2.2 *AC_f: Per ogni insieme a di insiemi non vuoti, esiste una funzione di scelta per a.*

L'assioma ci assicura che esiste una regola, la funzione f, grazie alla quale possiamo scegliere da ogni insieme di a un solo elemento. Però non ci dice qual'è questa regola, si tratta, cioè, di un assioma *"non costruttivo"*, nel senso che asserisce l'esistenza di una funzione di scelta (la regola di cui si parla sopra) ma senza spiegarci come possiamo costruirla. Il problema è, dunque, che a dispetto del carattere non costruttivo dell'assioma di scelta, questo principio sembra essere indispensabile per la *costruzione* di diversi oggetti matematici con i quali si dimostrano importantissimi teoremi. Di questo si parlerà nella fine di questo capitolo.

Il Lemma di Zorn

Definizione 4.2.3 *Sia $(a, <)$ un insieme ordinato:*

(i) m è un elemento massimale *di a se, e soltanto se, non esiste $w \in a$ tale che $m < w$.*

(ii) c è un maggiorante *di $b \subseteq a$ se, e soltanto se, per ogni $x \in b$, $x \geq c$.*

(iii) $b \subseteq a$ è una catena *se, e soltanto se, $(b, <)$ è totalmente ordinato.*

Assioma 4.2.4 *AC_z(Lemma di Zorn): Se $(a, <)$ è un insieme non vuoto, ordinato e tale che ogni catena di a ha un maggiorante, allora a ha un elemento massimale.*

4.3 L'equivalenza delle formulazioni

Le seguenti affermazioni sono ancora equivalenti all'assioma di scelta.

Assioma 4.3.1 *$AC_{\mathscr{P}}$: Per ogni insieme a, esiste $f : \mathscr{P}(a) - \{\emptyset\} \rightarrow a$ tale che per ogni $x \in \mathscr{P}(a) - \{\emptyset\}$, $f(x) \in x$.*

Assioma 4.3.2 *AC_{ord}: Per ogni insieme a, esiste un ordinale α e una funzione biiettiva $f : a \rightarrow \alpha$.*

Dimostriamo in $ZF + AF$ l'equivalenza degli assiomi fin ora enunciati enunciati. Si dimostrerà che $AC_i \Rightarrow AC_f \Rightarrow AC_{\mathscr{P}} \Rightarrow AC_{ord} \Rightarrow AC_z \Rightarrow AC_i$.

$AC_i \Rightarrow AC_f$: Sia a un insieme non vuoto. Per ogni $x \in a$, sia $x' = x \times \{x\}$.

$a' = \{x'; x \in a\}$ è un insieme per l'assioma di rimpiazzamento e gli elementi di a' sono disgiunti e non vuoti. Per AC_i esiste un insieme c tale che per ogni $x' \in a'$, $c \cap x'$ è un singoletto. Si definisce $f : a \rightarrow \bigcup a$ come la funzione che ad ogni $x \in a$ associa $f(x) = (c \cap x')$. f è una funzione di scelta per a.

$AC_f \Rightarrow AC_{\mathscr{P}}$: Sia a un insieme, $\mathscr{P}(a) - \{\emptyset\}$ è un insieme di insiemi non vuoti. Per AC_f esiste una funzione $f : (\mathscr{P}(a) - \{\emptyset\}) \to \bigcup(\mathscr{P}(a) - \{\emptyset\})$ tale che per ogni $x \in (\mathscr{P}(a) - \{\emptyset\})$, $f(x) \in x$. Ma $\bigcup(\mathscr{P}(a) - \{\emptyset\}) = a$, dunque abbiamo dimostrato $AC_{\mathscr{P}}$.

$AC_{\mathscr{P}} \Rightarrow AC_{ord}$: Siano a un insieme non vuoto e $f : \mathscr{P}(a) - \{\emptyset\} \to a$ tale che per ogni $x \in \mathscr{P}(a) - \{\emptyset\}$, $f(x) \in x$. Si definisce per induzione una relazione funzionale di dominio On :

$$h(\alpha) = \begin{cases} f(a - h[\alpha]) = f(a - \{h(\beta); \beta < \alpha\}) & \text{se } h[\alpha] \subset a \text{ e } h[\alpha] \neq a \ (*), \\ a & \text{altrimenti.} \end{cases}$$

Se la condizione $(*)$ è soddisfatta allora, per la proprietà di f, si ha che $h(\alpha) \in (a - h[\alpha])$; pertanto $h(\alpha) \in a$ oppure $h(\alpha) = a$; La condizione $(*)$ è equivalente a $a - h[\alpha] \neq \emptyset$. Si dimostra, allora, che esiste $\alpha \varepsilon On$ tale che $h(\alpha) = a$. Se così non fosse, infatti, per ogni $\alpha \varepsilon On$, si avrebbe $h[\alpha] \subset a$, $h[\alpha] \neq a$ e $h(\alpha) \in a$. h è iniettiva: se $\beta < \alpha$, $h(\alpha) = f(a - \{h(\beta); \beta < \alpha\}) \notin \{h(\beta); \beta < \alpha\}$, pertanto $h(\alpha) \neq h(\beta)$. Se $x = \{z \in a; \exists \alpha \in On(h(\alpha) = z)\}$, h è una biiezione tra On e x. Esiste, allora, $h^{-1} : x \to On$, e questo contraddice l'assioma di rimpiazzamento perché, per l'assioma di comprensione, x è un insieme (sottoinsieme di a). Dunque On è un insieme.

$AC_{ord} \Rightarrow AC_z$: Sia $(a, <)$ un insieme ordinato. Se c è una $<$-catena massimale per l'inclusione in a, cioè c è una $<$-catena e per ogni catena c' di a, $c \not\subset c'$, e m è un maggiorante di c, allora m è un elemento $<$-massimale di a. Infatti se m non è massimale, allora esiste $z \in a$ tale che $m < z$. Ma allora $c \cup \{z\}$ è una catena e $c \subset c \cup \{z\}$, e questo contraddice la massimalità di c. Per dimostrare AC_z, è sufficiente mostrare che se $(a, <)$ è un insime ordinato, allora esiste in a un catena massimale per l'inclusione. Siano $\alpha \in On$ e $h : \alpha \to a$ una biiezione. Si definisce per

$\beta < \alpha$,

$$M_\beta = \begin{cases} \bigcup_{\delta<\beta} M_\delta \cup \{h(\beta)\} & \text{se questa è una catena,} \\ \bigcup_{\delta<\beta} M_\delta & \text{altrimenti.} \end{cases}$$

$\bigcup_{\beta<\alpha} M_\beta$ è una catena massimale per l'inclusione.

$AC_z \Rightarrow AC_i$: Sia a un insieme di insiemi non vuoti e a due a due disgiunti. Siano $b = \cup a$ e $x = \{c \subseteq b; \forall z \in a(\#(c \cap z) \leq 1)\}$[2]. Se $c \in x$, allora $c \cap z$ è uguale all'insieme vuoto oppure è un singoletto. Inoltre $x \neq \emptyset$ perché $\emptyset \in x$. Infine se $c \in x$, allora $c \in \mathscr{P}(b)$. Poiché $x \subset \mathscr{P}(b)$, allora x è ordinato per inclusione. Questi fatti ci permettono di dimostrare, allora, che: se $y \subseteq x$ è totalmente ordinato, allora $\bigcup y \in x$. Infatti se $z \in a$ si danno due possibiltà (per y): se $\forall s \in y(s \cap z = \emptyset)$, allora $z \cap (\cup y) = \emptyset$ e $\cup y \in x$. Se $\exists s \in y(s \cap z = \{u\})$, allora $z \cap (\cup y) = \{u\}$, perché se $v \in z \cap (\cup y)$, allora esiste $s' \in y(v \in s' \cap z)$. Poiché y è totalmente ordinato per inclusione, allora $s \subseteq s'$ oppure $s' \subseteq s$; pertanto $s \cup s' = s$ oppure $s \cup s' = s'$ e $z \cap (s \cup s')$ è un singoletto, e ciò implica $u = v$. $\bigcup y$ è un maggiorante per y. Abbiamo stabilito che ogni sottoinsieme totalmente ordinato di x ha un limite superiore (maggiorante) in x; Per AC_z, x ha un elemento massimale m. Dimostriamo infine, che per ogni $z \in a$, $m \cap z$ è un singoletto. Se esistesse $z \in a$ tale che $m \cap z = \emptyset$ e $t \in z$ (esiste perché gli elementi di a sono non vuoti), allora $m \cup \{t\} \in x$ (nessuna interferenza perché gli elementi di a sono a due a due disgiunti, quindi aggiungere un elemento di z a m non aumenta l'intersezione di m con gli altri elementi di a), e ciò contraddice la massimalità di m.

Il teorema di Zermelo

Diamo qui di seguito altre formulazioni di AC :

Assioma 4.3.3 *AC_{bo}(Teorema di Zermelo): Ogni insieme può essere ben ordinato.*

[2]"$\#(c \cap z)$" sta per: la cardinalità di "$(c \cap z)$".

Cioè per ogni insieme a, esiste $R \subset a \times a$ tale che (a, R) è ben ordinato.

Definizione 4.3.4 *Sia* $\{a_i; i \in I\}$ *una famiglia di insiemi con indici in* I, *il* prodotto *di* $\{a_i; i \in I\}$ *è l'insieme* $\{f : I \to \bigcup_{i \in I} a_i; \forall i \in I f(i) \in a_i\}$.

Assioma 4.3.5 AC_π : *Il prodotto di una famiglia di insiemi non vuoti è non vuoto.*

Teorema 4.3.6 $AC_{bo} \iff AC_{ord}$.

Proof. *Se* AC_{ord}, *allora* AC_{bo}*:* Sia a un insieme qualsiasi, per AC_{ord} esistono un ordinale α e una biiezione $\varphi : a \to \alpha$. Definiamo una relazione R di buon ordine su a :

$$\text{per ogni } x, y \in a, \quad R(x, y) \iff \varphi(x) \in \varphi(y)$$

Poiché $\in$ è un buon ordine su α, allora R è un buon ordine su a.
Se AC_{bo}, *allora* AC_{ord}*:* Sia a un insieme qualunque, per AC_{bo} esiste un buon ordine R su a. Definiamo una funzione $\varphi : a \to On$

$$\text{per ogni } x \in a, \varphi(x) = \{\varphi(y); yRx\}.$$

L'immagine della funzione appena definita è un ordinale α. Dunque abbiamo definito una biiezione tra a e α. ■

Osservazione 4.3.7 *Tutti gli insiemi numerabili sono ben ordinabili*

Infatti sia f una funzione biunivoca tra un insieme numerabile a e w, definisco un ordine su a : per ogni $x, y \in a$, $x <_a y$ se e soltanto se $f(x) \in f(y)$.

Teorema 4.3.8 $AC_\pi \iff AC_f$

Proof. *Se* AC_π, *allora* AC_f*:* Sia a un insieme di insiemi non vuoti. Consideriamo l'identità su a, essa associa ad ogni $i \in a$ un insieme $a_i = i$. L'immagine è una famiglia di insiemi non vuoti $\{a_i; i \in a\}$ (detto in altri termini: posso sempre fare di un insieme di insiemi non vuoti a, una

famiglia di insiemi non vuoti, indicizzando ogni elemento di a con se stesso). Per AC_π, esiste una funzione $f : a \to \bigcup_{i\in a} a_i$ tale che per ogni $i \in a$, $f(i) \in a_i$. Ma $a_i = i$, dunque esiste una finzione di scelta su a.
Se AC_f, allora AC_π: Sia $a = \{a_i; i \in I\}$ una famiglia di insiemi. a è un insieme di insiemi non vuoti, dunque per AC_f esiste una funzione $f : a \to \bigcup a$ tale che per ogni a_i, $f(a_i) \in a_i$. Poiché a è una famiglia con indici in un insieme I, allora esiste una funzione $g : I \to a$ che ad ogni $i \in I$ associa a_i. Componendo f e g otteniamo una funzione $g \circ f : I \to \bigcup a = \bigcup_{i\in I} a_i$ tale che per ogni $i \in I$, $g \circ f = f(g(i)) = f(a_i) \in a_i$. $g \circ f$ appartiene al prodotto della famiglia di insiemi a, che dunque è non vuoto. ■

L'assioma delle scelte dipendenti

Quella che segue è una forma debole dell'assioma di scelta.

Assioma 4.3.9 *AC_{Dip}(Assioma delle scelte dipendenti): Sia a un insieme non vuoto e R una relazione binaria su a tale che $\forall x(x \in a \Rightarrow \exists y(y \in a \wedge yRx))$, allora esiste $f : w \to a$ tale che $\forall n \in w(f(n+1)Rf(n))$.*

Nel Capitolo 3 si è detto che l'assioma di fondazione impedisce l'esistenza di una successione infinita discendente. In realtà per un modello di $ZF + AC_{Dip}$, è anche vero che se l'assioma di fondazione è falso, allora esiste una successione infinita discendente.

Proposizione 4.3.10 $\neg AF + AC_{Dip} \Rightarrow$ "esiste una successione infinita discendente".

Proof. $\neg AF$ è la formula $\exists k(k \neq= \emptyset \wedge \forall x(x \in a \Rightarrow \exists y(y \in a \wedge y \in x)))$. Se tale formula è vera allora, per AC_{Dip}, esiste una funzione $f : w \to a$ tale che $\forall n \in w[f(n+1) \in f(n)]$. Cioè esiste una successione infinita discendente. ■

Nota 4.3.11 *Si osservi che l'assioma di scelta è indispensabile per dimostrare la Proposizione 4.3.10.*

Si potrebbe pensare, infatti, che la funzione f di cui si parla nella dimostrazione sia facilmente definibile: si prende per $f(n)$, di ogni insieme b di a un elemento che questo insieme ha in comune con a. Invece possono esserci più elementi che b ha in comune con a, in tal caso non possiamo affermare di poterne sempre scegliere uno tra questi, senza ricorrere all'assioma di scelta.

Teorema 4.3.12 $AC \Rightarrow AC_{Dip}$.

Proof. Sia a un insieme non vuoto e R una relazione binaria su a tale che $\forall x(x \in a \wedge \exists y(y \in a \wedge yRx))$. Sia f una funzione di scelta per $\mathscr{P}(a) - \emptyset$; $f : \mathscr{P}(a) - \emptyset \rightarrow \bigcup(\mathscr{P}(a) - \emptyset)$. La funzione $h : w \rightarrow a$ definita da $h(0) = f(a)$; $h(n+1) = f(\{z \in a;\ zRh(n)\})$ è ben definita $(\forall n \in w\{z \in a;\ zRh(n)\} \in \mathscr{P}(a) - \emptyset)$ e soddisfa: $\forall n \in w(f(n+1)Rf(n))$. ■

4.4 L'assioma di scelta in matematica

Come si è già accennato, in matematica si fa costantemente uso dell'assioma di scelta. Si tratteranno, qui, alcuni teoremi che, attualmente, non possiamo dimostrare senza assioma di scelta. Prima, però, analizziamo alcune ragioni che potrebbero indurci a rifiutare l'assioma di scelta.
Abbiamo già osservato che l'assioma di scelta è diverso, per alcuni aspetti, dagli altri assiomi. Gli assiomi di ZF, infatti, (eccetto l'assioma dell'infinito) asseriscono l'esistenza di insiemi che sono intuitivamente costruibili in modo ovvio. L'assioma di scelta, invece, non indica la costruzione effettiva di un nuovo insieme, ne garantisce solo l'esistenza. Questo costringerebbe un intuizionista come abbiamo visto nel Capitolo 1 a rifiutarlo.
C'è almeno un altro aspetto indesiderabile dell'assioma di scelta. Secondo il formalismo, abbiamo detto, una dimostrazione è qualcosa che lega la verità delle premesse alla verità della conclusione. Ora, sembra che noi siamo più sicuri delle conclusioni che delle premesse. L'assioma di scelta, ad esempio, se da una lato ci permette di dimostrare importanti

teoremi, dall'altro implica la costruzione di oggetti matematici controintuitivi: con l'assioma di scelta si dimostra che da una sfera è possibile ricavare due sfere di raggio pari alla sfera originale. Se accettiamo l'assioma di scelta dovremmo allora essere capaci di compiere tale magia. Il paradosso appena enunciato è noto come il *paradosso di Banach-Tarski*: una sfera può essere scomposta in un numero finito di parti, con le quali si può poi ricomporre una sfera di raggio doppio.
Sebbene questo paradosso sia una conseguenza dell'assioma di scelta, non dimostra che l'assioma di scelta è necessariamente controintuitivo, potrebbe essere controintuitiva piuttosto la teoria delle misure.

Vediamo ora, invece, in quali casi si fa uso dell'assioma di scelta. Ecco alcuni esempi tipici. Dei seguenti teoremi darò solo un'idea della dimostrazione. Cercherò poi di spiegare perché tali teoremi sono molto importanti.

Il Teorema di Rappresentazione di Stone

Ci occupiamo prima di tutto del Teorema di Rappresentazione di Stone (per ulteriori dettagli si veda [Johnstone, 1982]).

Teorema 4.4.1 Teorema di rappresentazione di Stone
Ogni algebra Booleana è isomorfa all'algebra di sottoinsiemi clopen *(ovvero,* aperti *e* chiusi *al contempo) del suo Spazio di Stone.*

Proof. Sia $S(\mathscr{A})$ lo spazio di Stone di $\mathscr{A}$. Notiamo $\mathscr{B}(S(\mathscr{A}))$ l'algebra di Boole degli aperti-chiusi di $S(\mathscr{A})$. Definiamo un applicazione H di dominio $\mathscr{A}$ tale che per ogni elemento a di $\mathscr{A}$:

$$H(a) = \{h \in S(\mathscr{A}); h(a) = 1\}.$$

La funzione appena definita si dimostra essere un isomorfismo di algebre di Boole di $\mathscr{A}$ su $\mathscr{B}(S(\mathscr{A}))$. Nella dimostrazione del teorema si sfrutta il seguente lemma: lo spazio di Stone di un algebra booleana $\mathscr{A}$ è uno spazio topologico booleano. Per la dimostrazione del lemma ci si serve del teorema di Tychonoff che si dimostra utilizzando l'assioma di scelta. Il teorema afferma che:

Il prodotto di tutte le famiglie di spazi topologici compatti è uno spazio topologico compatto. ■

É possibile dimostrare che tutte le algebre di Boole finite "possono essere decomposte" in un prodotto finito di algebre dei valori di verità (si veda l'Introduzione Sezione 1.2). Questo e' in generale non vero per le algebre infinite. Il teorema di Stone ci permette di affermare che ogni algebra di Boole (finita o infinita) può essere immersa nel prodotto di algebre direttamente indecomponibili, cioè le algebre dei valori di verità. Inoltre ogni fattore del prodotto può essere indicizzato dagli elementi di uno spazio topologico Booleano. Questo risultato è importante perché stabilisce un dualismo tra le algebre di Boole e gli spazi topologici booleani. Infine, il teorema di Stone ci permette di stabilire altre dualità oltre a quella tra algebre di Boole e spazi booleani: tra filtri e sottoinsiemi chiusi; tra ideali e sottoinsiemi aperti; tra omomorfismi e funzioni continue.

Il Teorema di Compattezza

Un altro teorema importante la cui dimostrazione richiede l'assioma di scelta è il Teorema di Compattezza
(per ulteriori dettagli si veda [Cori and Lascar, 1993])

Teorema 4.4.2 Teorema di Compattezza: *Sia $\mathscr{L}$ un linguaggio del primo ordine e T una teoria di $\mathscr{L}$. Se T è finitamente soddisfacibile (significa che ogni sottoinsieme finito e non vuoto della teoria ha un modello), allora T è soddisfacibile.*

Proof. Si dice che una teoria T di un linguaggio $\mathscr{L}$ ha dei testimoni in $\mathscr{L}$ quando per ogni formula con esattamente una variabile libera $F(x)$ di $\mathscr{L}$, esiste un simbolo di costante c_F di $\mathscr{L}$ tale che la formula chiusa $\exists x F(x) \Rightarrow F(C_F)$ sia una formula di T. Si dimostrano prima due lemmi:

Lemma 4.4.3 *(senza AC) Sia $\mathscr{L}$ un linguaggio e T una teoria di $\mathscr{L}$ fintamente soddisfacibile. Esistono un linguaggio $\mathscr{L}'$ estensione di $\mathscr{L}$, ottenuto aggiungendo ad $\mathscr{L}$ dei simboli di costante, ed una teoria T' estensione di T di $\mathscr{L}'$, tali che:*

(i) T' è finitamente soddisfacibile

(ii) T' ha dei testimoni in $\mathscr{L}'$

Lemma 4.4.4 *(con AC) Sia T una teoria di un linguaggio $\mathscr{L}$ finitamente soddisfacibile. Esiste un estensione T' di T (in $\mathscr{L}$) finitamente soddisfacibile e massimale (cioè per ogni formula chiusa F di $\mathscr{L}$, si ha che $F \in T'$ oppure $\neg F \in T'$).*

Applicando i due lemmi si ottiene da una teoria soddisfacibile (la teoria T dell'enunciato del teorema), una teoria T' che la contiene e che è finitamente soddisfacibile e massimale. Si costruisce allora un modello di T'. Il modello ottenuto sarà anche un modello di T. Guardiamo, però, la dimostrazione del secondo lemma che più ci interessa perché richiede l'assioma di scelta.
Sia $\mathscr{E} = \{\mathscr{B}; \mathscr{B}$ è un insieme di formule chiuse di $\mathscr{L}, T \subseteq \mathscr{B}$, $\mathscr{B}$ è finitamente soddisfacibile $\}$. $\mathscr{E}$ è un insieme ordinato. Ogni sottoinsieme non vuoto e totalmente ordinato di $\mathscr{E}$ ha un maggiorante. *Per il lemma di Zorn* esiste un elemento massimale T' di $\mathscr{E}$. Si dimostra infine che T' è finitamente soddisfacibile e massimale, e soddisfa perciò la conclusione del lemma. ■

È opportuno spiegare perché questo risultato è tanto importante. Il teorema di Compattezza è un teorema centrale della teoria dei modelli. Molto poco di questa teoria può essere detto senza assumere l'assioma di scelta. Esso dice che data una teoria, se ogni sottoinsieme finito della teoria ammette un modello (è vero sotto un certo "punto di vista"), allora la teoria in questione ammette un modello. Questo teorema ci permette di dimostrare dei risultati fondamentali per l'algebra:

- La teoria dei gruppi finiti non è assiomatizzabile, cioè non esiste una teoria che è soddisfatta da tutti e soli quei modelli che sono gruppi finiti.

- La teoria dei gruppi infiniti non è finitamente assiomatizzable, cioè non esiste una formula che è soddisfatta da tutti e soli quei modelli che sono gruppi infiniti.

- La teoria dei campi di caratteristica diversa da 0 non è assiomatizzabile.
- La teoria dei campi di caratteristica 0 non è finitamente assiomatizzabile.

In quanto rende possibile dimostrare questi e altri risultati, il teorema di Compattezza, può essere considerato la colonna portante della teoria dei modelli.

Il Teorema di Compattezza per i linguaggi numerabili

In realtà il teorema di Compattezza è sempre dimostrabile per linguaggi numerabili. Diamo qui di seguito una dimostrazione di questo risultato che non fa appello all'assioma di scelta. Sarà sufficiente dimostrare il Lemma

Lemma 4.4.4 *(senza AC)Sia T una teoria di un linguaggio* numerabile *$\mathscr{L}$ finitamente soddisfacibile. Esiste, allora un estensione T' di T finitamente soddisfacibile e massimale.*

Proof. Poiché il linguaggio è numerabile possiamo enumerare le sue formule chiuse, ottenendo la successione $A_0, A_1, ..., A_n, ...$ .Costruiamo poi, per induzione, una famiglia di teorie $\{T_n; n \in \mathbb{N}\}$ tale che:

(i) T_n è una teoria finitamente soddisfacibile

(ii) T_n contiene la formula chiusa A_n oppure la formula chiusa $\neg A_n$.

La teoria T' che cerchiamo è l'unione delle teorie della famiglia appena definita, $T = \bigcup_{n\in\mathbb{N}} T_n$. ■

Si osservi che nel caso di un linguaggio più che numerabile questa dimostrazione può essere adattata enumerando l'insieme delle formule chiuse del linguaggio con il suo cardinale. Ma perché a un insieme possiamo associare un cardinale è necesario che tale insieme sia ben ordinabile e, per questo, è necessario l'assioma di scelta.

Il Teorema di Hann-Banch

Tra i teoremi che si dimostrano con l'assioma di scelta abbiamo anche il Teorema di Hahn Banach (per maggiori dettagli si veda [Narici and Beckenstein, 1997])

Teorema 4.4.5 *Teorema di Hann-Banach.*
Sia V uno spazio vettoriale sul campo di scalari $\mathbb{K}$, sia $N : V \to \mathbb{R}$ una funzione sublineare, sia U un sottospazio vettoriale di V e sia $\varphi : U \to \mathbb{K}$ una funzione lineare tale che $|\varphi(x)| \leq N(x)$ per ogni x in U. Allora esiste un'applicazione lineare $\psi : V \to \mathbb{K}$ che estende φ e tale che $|\psi(x)| \leq N(x)$ per ogni x in V.

Il teorema di Hann-Banach è uno strumento centrale nell'analisi funzionale. Permette di estendere operatori lineari definiti su un sottospazio di qualche spazio vettoriale a tutto lo spazio, e mostra, inoltre che ci sono "abbastanza" funzionali lineari continui definiti su ogni spazio normato da rendere lo studio dello spazio duale interessante.

Altri risultati importanti

Cito ancora qualche teorema (per approfondimenti si vedano [Piacentini-Cattaneo, 1996] e [Sernesi, 1989]).

Teorema 4.4.6 *Ogni spazio vettoriale ammette una base.*

Proof. Si consideri l'insieme H di tutti i sottoinsiemi di V linearmente indipendenti, ordinato rispetto all'inclusione. L'ipotesi del Lemma di Zorn è soddisfatta, perché l'unione di una catena di elementi di H è ancora un insieme linearmente indipendente. Un elemento massimale di H è ancora una base. $\blacksquare$

Teorema 4.4.7 *Se A è un anello commutativo unitario, allora ogni elemento x non invertibile appartiene a un ideale massimale.*

Proof. Si consideri l'insieme degli ideali di A propri (cioè non contenenti 1) a cui x appartiene; tale insieme è non vuoto perché contiene xA (dal fatto che x non è invertibile segue che $1 \notin A$) ed è ordinato dall'inclusione. É facile arrivare alla conclusione, se si osserva che l'unione di ideali propri è, a sua volta, un ideale proprio (perché l'anello contiene l'elemento 1). ■

Il Finitismo

Le dimostrazioni dei precedenti teoremi ci lasciano intendere che l'assioma di scelta sembra essere indispensabile quando si ha a che fare con insiemi infiniti più che numerabili. Abbiamo visto, ad esempio, che certi risultati a cui si applica il teorema di Stone sono dimostrabili per gli insiemi finiti senza ricorrere all'assioma di scelta. Analogamente il teorema di compattezza può essere dimostrato per i linguaggi numerabili senza utilizzare l'assioma, fondando la dimostrazione sul fatto che le formule di un tale linguaggio possono essere sempre enumerate. Questo è dovuto al fatto che gli insiemi finiti e infiniti numerabili sono sempre ben ordinabili. Dunque la nostra trattazione sull'assioma di scelta si lega all'esistenza di insiemi infiniti: se non esistessero insiemi infiniti (basterebbe negare l'esistenza degli insiemi infiniti più che numerabili), l'assioma di scelta sarebbe banalmente vero. La supposizione che insiemi infiniti esistano, l'abbiamo visto nell'Introduzione, non è così pacifica come può sembrare. Un finitista non crede nell'esistenza di collezioni infinite, supportato dal fatto che ogni oggetto dell'universo fisico noto è finito. Gli insiemi infiniti, sosterrebbe, sono utili finzioni giustificate dal fatto che risultano, a posteriori, pratiche per la risoluzione di problemi. A questo proposito, si noti che l'esistenza di insiemi infiniti è un prodotto della moderna teoria degli insiemi: l'assioma dell'infinito asserisce, appunto, che esiste un insieme infinito. Sottolineare questo aspetto era, credo, rilevante per la nostra discussione, sebbene attualmente il finitismo non abbia grande credito. L'esperienza matematica, infatti, sembra dare ragione del fatto che gli insiemi infiniti esistono. Nella pratica matematica, si ha sempre a che fare con l'insieme dei numeri naturali o con quello dei reali, ad esempio, che sono insiemi infiniti.

Nei prossimi capitoli, introdurremo le nozioni che ci servono per dimostrare, finalmente, l'indipendenza dell'assioma di scelta.

Capitolo 5

Schema di Riflessione

In questo capitolo, introdurremo le nozioni necessarie ad affrontare la dimostrazione dell'indipendenza dell'assioma di scelta dall teoria degli insiemi ZF. Nel capitolo che seguirà, il teorema che asserisce l'indipendenza dell'assioma di scelta non verrà interamente dimostrato. Ci limiteremo, infatti, a dimostrare la consistenza dell'assioma di scelta. Tuttavia, quanto sarà trattato nel presente capitolo, è necessario anche alla dimostrazione della consistenza della *negazione* dell'assioma di scelta.

5.1 Relativizzazione di formule

Ogni classe X, è una collezione di insiemi dell'universo che soddisfano una determinata relazione unaria, la denoteremo $x \varepsilon X$ (con x simbolo di variabile). Date una classe (risp. insieme) X, e una formula $E(x_1, \ldots, x_k)$ a k variabili a parametri in X. Si denota $E^X(x_1, \ldots, x_k)$ la formula E *relativizzata a* X e si definisce per induzione nel modo seguente:

- Se E è una formula atomica a parametri in X o senza parametri, allora la relativizzata di E a X è la formula E stessa.
- Se E è la formula $\neg F$, allora E^X è $\neg F^X$.
- Se E è la formula $F \vee G$, allora E^X è $F^X \vee G^X$.

- Se E è la formula $\exists x F(x, x_1, \dots, x_k)$, allora E^X è $\exists x \varepsilon X(F^X(x, x_1, \dots, x_k))$. (risp. $\exists x \in X(F^X(x, x_1, \dots, x_k))$.)

Allora se $E(x_1, \dots, x_k)$ è $\forall x F(x, x_1, \dots, x_k)$, allora $E^X(x, x_1, \dots, x_k)$ è $\forall x \varepsilon X(F^X(x, x_1, \dots, x_k))$ (risp. $\forall x \in X(F^X(x, x_1, \dots, x_k)))$.

È necessario, allora, fare un' osservazione importante: si consideri una formula $E(a_1, \dots, a_k)$ a parametri in una classe (risp. un insieme) X, allora $E^X(a_1, \dots, a_k)$ è vera nell'universo se, e soltanto se $E(a_1, \dots, a_k)$ è vera in X.

Teorema 5.1.1 *Sia $\mathscr{U}$ un modello di ZF. Se $\mathscr{M}$ è una classe (risp. insieme) non vuota e transitiva*[1] *dell'universo, allora $\mathscr{M}$ soddisfa:*

- *l'assioma di estensionalità,*
- *soddisfa l'assioma di fondazione se $\mathscr{U}$ lo soddisfa,*
- *e soddisfa l'assioma dell'infinito se e soltanto se $w \varepsilon \mathscr{M}$ (risp. $w \in \mathscr{M}$).*

Proof. *Assioma di estensionalità:* nell'universo $\mathscr{U}$ è vero l'assioma $\forall x \forall y(\forall z(z \in x \iff z \in y) \Rightarrow x = y)$. In particolare è vera in $\mathscr{U}$ la formula: $\forall x \varepsilon \mathscr{M} \forall y \varepsilon \mathscr{M}(\forall z(z \in x \iff z \in y) \Rightarrow x = y)$ (risp. $\forall x \in \mathscr{M} \forall y \in \mathscr{M}(\forall z(z \in x \iff z \in y) \Rightarrow x = y))$. Se in $\mathscr{U}$ è vero $a \neq b$ con $a, b \varepsilon \mathscr{M}$ (risp.$a, b \in \mathscr{M}$), allora esiste c in $\mathscr{U}$ tale che, ad esempio, $c \in a$ e $c \notin b$. Poiché $\mathscr{M}$ è transitivo, dal fatto che $c \in a$, segue che $c \varepsilon \mathscr{M}$ (risp.$\in \mathscr{M}$). Abbiamo dimostrato che $\forall x \varepsilon \mathscr{M} \forall y \varepsilon \mathscr{M}(x \neq y \Rightarrow \exists z \varepsilon \mathscr{M}(z \in x \iff z \in y))$ (risp. $\forall x \in \mathscr{M} \forall y \in \mathscr{M}(x \neq y \Rightarrow \exists z \in \mathscr{M}(z \in x \iff z \in y)))$, che equivale all'assioma di estensionalità relativizzato a $\mathscr{M}$. Dunque $\mathscr{M}$ soddisfa l'assioma di estensionalità.
Assioma di fondazione: nell'universo è vero $\forall x((x \neq \emptyset) \Rightarrow \exists z(z \in x \wedge z \cap x = \emptyset))$. Si consideri la formula $y = \emptyset : \forall k(k \notin y)$, essa implica che $\forall k \varepsilon \mathscr{M}(k \notin y)$[2]. Dunque l'insieme vuoto, è tale anche in $\mathscr{M}$. Viceversa,

[1] una classe transitiva $\mathscr{M}$ è una classe tale che se a è un insieme tale che $a \varepsilon \mathscr{M}$, allora per ogni insieme $b \in a$, $b \varepsilon \mathscr{M}$.

[2] Per non appesantire la dimostrazione ometterò il caso in cui $\mathscr{M}$ è un insieme. Il teorema si dimostra in modo evidentemente analogo.

un insieme vuoto $\emptyset^{\mathscr{M}}$ in $\mathscr{M}$, è tale anche in $\mathscr{U}$. Supponiamo, infatti, per assurdo, che $\exists k(k \in \emptyset^{\mathscr{M}})$, allora per la transitività di $\mathscr{M}$, $\exists k\varepsilon\mathscr{M}(k \in \emptyset^{\mathscr{M}})$. Contraddizione. Questo dimostra che se in $\mathscr{U}$ è vero l'assioma di fondazione allora, in particolare, è vero che $\forall x\varepsilon\mathscr{M}((x \neq \emptyset^{\mathscr{M}}) \Rightarrow \exists z(z \in x \wedge z \cap x = \emptyset^{\mathscr{M}}))$. Poiché $\mathscr{M}$ è transitivo, dal fatto che esiste $z \in x$ e $x\varepsilon\mathscr{M}$ segue che $z\varepsilon\mathscr{M}$. Si consideri, allora l'insieme $z \cap x$, tale insieme è uguale a $\{k \in x; k \in z\} = \{k \in \mathscr{M}; k \in x \text{ e } k \in z\} = (z \cap x)^{\mathscr{M}}$, poiché $\mathscr{M}$ è transitivo. Abbiamo dimostrato che in $\mathscr{U}$ è vero $AF^{\mathscr{M}}$, cioè l'assioma di fondazione relativizzato a $\mathscr{M}$. Dunque $\mathscr{M}$ soddisfa l'assioma di fondazione.

Assioma dell'infinito: Si dimostra, infine, che in $\mathscr{M}$ l'assioma dell'infinito è vero se e soltanto se $w\varepsilon\mathscr{M}$. Per ipotesi, in $\mathscr{U}$ è vero l'assioma $\exists w(\emptyset \in w \wedge \forall y(y \in w \Rightarrow y \cup \{y\} \in w))$. L'insieme che soddisfa tale formula è w, il primo ordinale infinito. Abbiamo già mostrato che $\emptyset = \emptyset^{\mathscr{M}}$, dunque in $\mathscr{U}$ è vero, in particolare, che $\emptyset^{\mathscr{M}} \in w \wedge \forall y\varepsilon\mathscr{M}(y \in w \Rightarrow y \cup \{y\} \in w)$. Se $y\varepsilon w$, allora chiaramente $\{y\} = \{y\}^{\mathscr{M}}$. Inoltre, dati due insiemi qualsiasi $a, b\varepsilon\mathscr{M}$, $a \cup b = \{k; k \in a \vee k \in b\} = \{k\varepsilon\mathscr{M}; k \in a \vee k \in b\}$, perché $\mathscr{M}$ è transitivo. Dunque se $y\varepsilon\mathscr{M}$, allora $y \cup \{y\} = (y \cup \{y\})^{\mathscr{M}}$. Ciò dimostra che $\mathscr{U}$ soddisfa $\exists w(\emptyset^{\mathscr{M}} \in w \wedge \forall y\varepsilon\mathscr{M}(y \in w \Rightarrow (y \cup \{y\})^{\mathscr{M}} \in w))$. Poiché $w\varepsilon\mathscr{M}$, allora $\mathscr{M}$ soddisfa l'assioma dell'infinito.

Viceversa, supponiamo che l'assioma dell'infinito AI sia vero in $\mathscr{M}$, allora $(AI)^{\mathscr{M}}$ è vero in $\mathscr{U}$. Si ha che $\exists x\varepsilon\mathscr{M}(\emptyset \in x \wedge \forall y\varepsilon\mathscr{M}(y \in x \Rightarrow y \cup \{y\} \in x))$. Sia a l'insieme di $\mathscr{M}$ che soddisfa tale assioma. Se, per assurdo, esistesse un insieme dell'universo u tale che $u \in a$ e $u \cup \{u\} \notin a$ allora, per ipotesi, u non è un oggetto di $\mathscr{M}$. D'altra parte, però, la transitività di $\mathscr{M}$ e l'ipotesi $u \in a$ ci impone $u\varepsilon\mathscr{M}$. Dunque possiamo affermare $\emptyset \in a \wedge \forall y(y \in a \Rightarrow y \cup \{y\} \in a))$. Nel Paragrafo 2.6 del Capitolo 2 abbiamo visto che l'insieme che soddisfa l'assioma dell'infinito è un ordinale non finito. Abbiamo definito, inoltre, w come il primo ordinale non finito. Questo dimostra che $w \in a$ oppure $w = a$. In entrambi i casi (per la transitività di $\mathscr{M}$) $w\varepsilon\mathscr{M}$. ■

5.2 Consistenza dell'assioma di fondazione

In questa sezione mostreremo che se siste un modello di ZF allora esiste un modello di $ZF + AF$. Nella dimostrazione di questo risultato supporremo, dunque, l'esistenza di un modello di ZF e, in questo, costruiremo la gerarchia V di cui si è parlato nel Capitolo 2, dimostreremo, infine che V è un modello di $ZF + AF$. Ogni risultato, come questo, della forma *se T è una teoria non contraddittoria, allora anche la teoria T' è non contraddittoria* si chiama *risultato di non contraddittorietà relativa.*

Teorema 5.2.1 *Se esiste un modello di ZF allora esiste un modello di $ZF + AF$*

Proof. Sia $\mathscr{U}$ un modello di ZF. V è una collezione transitiva dunque, per il Teorema 5.1.1, V soddisfa l'assioma di estensionalità. Inoltre tutti gli ordinali sono in V dunque, in parti colare w è in V. Ancora per il Teorema 5.1.1 V soddisfa l'assioma dell'infinito. Dimostriamo, ora, che V è un modello degli altri assiomi di $ZF + AF$.
Assioma dell'Unione: Per ipotesi $\mathscr{U}$ soddisfa l'assioma dell'unione. Inoltre se $a \varepsilon V$, allora $\bigcup a = (\bigcup a)^V$, infatti $x \in \bigcup a \iff \exists y(x \in y \wedge x \in a) \iff \exists y(x \in y \wedge y \in a \wedge y \varepsilon V) \iff \exists y(x \in y \wedge y \in a \wedge y \varepsilon V \wedge x \varepsilon V) \iff x \in (\bigcup a)^V$. Dunque per dimostrare che V soddisfa l'assioma dell'unione è sufficiente dimostrare che $\forall x \varepsilon V (\bigcup x \varepsilon V)$. Sia $a \varepsilon V$, allora se $b \in \bigcup a$, allora esiste c tale che $b \in c$ e $c \in a$. Poiché V è transitivo, allora $c \in a$ implica $c \varepsilon V$, dunque $b \varepsilon V$. Questo dimostra che tutti gli elementi di $\bigcup a$ sono in V. Per il Lemma 3.3.2 $\bigcup a \varepsilon V$.
Assioma dell'Insieme delle Parti: $\mathscr{U}$ soddisfa, per ipotesi, l'assioma dell'insieme delle parti. Inoltre per ogni insieme a di V, $\mathscr{P}(a) = \{x; x \subseteq a\} = \{x \varepsilon V; x \subseteq^V a\} = (\mathscr{P}(a))^V$. Allora è sufficiente dimostrare che $\forall x \in V (\mathscr{P}(x) \in V)$. Per la transtività di V, se a è un oggetto di V allora ogni insieme $b \in \mathscr{P}(a)$ è un insieme di elmenti di a, dunque per il Lemma 3.3.2 si ha $b \in V$. Pertanto $\mathscr{P}(a)$ è in V.
Assioma di Rimpiazzamento: Sia $a \varepsilon V$ e $R(x, y)$ una formula a parametri in V, che definisce in V una relazione funzionale. Tale relazione è definita nell'universo $\mathscr{U}$ dalla formula $V(x) \wedge V(y) \wedge R^V(x, y)$. Poiché $\mathscr{U}$ soddisfa l'assioma di rimpiazzamento, possiamo applicarlo alla precedente

relazione per affermare che esiste in $\mathscr{U}$ un insieme b i cui elementi sono le immagini degli elementi di a tramite questa relaizone funzionale. Questo insieme ha tutti i suoi elementi in V, dunque esso stesso è un oggetto di V.
Assioma di Fondazione: Sia x un insieme dell'universo che è nella collezione V. Allora ogni elemento di x è anch'esso nella collezione V. Sia b un elemento di x di rango minimo: allora $b \cap x = \emptyset$, perché altrimenti un elemento di $b \cap x$ sarebbe elemento di b, dunque di rango strettamente inferiore, in contraddizione con il fatto che abbiamo scelto b di rango minimo. ■

5.3 Schema di riflessione

Si considerino una collezione X e una formula $E(x_1, \ldots, x_k)$ a parametri in X. Si dice che X *conviene a* E quando ogni k-upla di elementi di X soddisfa $E(a_1, \ldots, a_k)$ se e soltanto se soddisfa $E^X(a_1, \ldots, a_k)$.

Osserviamo che se E è una formula senza quantificatori allora $E = E^X$, quindi qualsiasi collezione conviene a E. Una formula è in *forma prenessa* se è della forma $P_1P_2 \ldots P_nF$ con F formula senza quantificatori e ogni P_i per $1 \leq i \leq n$ è uguale a $\neg$ oppure a $\exists x$. Data una formula E in forma prenessa si dirà che *una formula* G *precede* E se è ottenuta eliminando un certo numero di segni $\neg$ e $\exists x$ di testa da E.
Data una formula è sempre possibile trovare una formula in forma prenessa ad essa equivalente e che abbia le stesse variabili libere e gli stessi parametri (si veda, ad esempio, [Cori and Lascar, 1993]).

Lemma 5.3.1 *Sia E una formula in forma prenessa senza parametri, e $(X_n)_{n\in w}$ una successione crescente di insiemi; Sia $X = \bigcup_{n\in w} X_n$. Se ogni X_n conviene alla formula E, e a tutte le formule precedenti, allora anche X conviene a E e a tutte le formule precedenti.*

Proof. Il lemma si dimostra per induzione sulla complessità della formula. Il lemma è evidente se E è senza quantificatori, perché in tal caso qualunque insieme conviene a E e non esistono formule precedenti di E. Se E è $\neg F$, X_n conviene a E e a tutte le precedenti, quindi a F e a tutte le precedenti. Dunque, per ipotesi di induzione, X conviene a F e a tutte le precedenti. Si ha allora:

$$\forall x_1 \in X \ldots \forall x_k \in X(F(x_1, \ldots, x_k) \iff F^X(x_1, \ldots, x_k)).$$

Poiché E è $\neg F$ e E^X è $\neg F^X$, è evidente che X conviene a E. Se E è $\exists x F(x, x_1, \ldots, x_k)$, X_n conviene a E e alle formule precedenti, dunque a F e alle formule precedenti. Ne segue, per ipotesi di induzione, che X conviene a F e alle formule precedenti. Si dimostra allora che X conviene a E. Siano $a_1, \ldots, a_k \in X$, se $E^X(a_1, \ldots, a_k)$ è vero, si ha $\exists x(x \in X \wedge F^X(x, a_1, \ldots, a_k))$; sia $a \in X$ tale che $F^X(a, a_1, \ldots, a_k)$. Poiché X conviene a F allora si ha $F(a, a_1, \ldots, a_k)$ e dunque $\exists x F(x, a_1, \ldots a_k)$; ne risulta che $E(a_1, \ldots, a_k)$ è vera. Viceversa, se $E(a_1, \ldots, a_k)$ è vera, si ha $a_1, \ldots, a_k \in X_n$ per un n sufficientemente grande; poiché X_n conviene a E si ha $E^{X_n}(a_1, \ldots, a_k)$ cioè:

$$\exists x[x \in X_n \wedge F^{X_n}(x, a_1, \ldots, a_k)].$$

Di conseguenza esiste un elemento a di X_n tale che $F^{X_n}(a, a_1, \ldots, a_k)$. Poiché X_n conviene a F, si ha $F(a, a_1, \ldots, a_k)$; poiché X conviene a F, allora $F^X(a, a_1, \ldots, a_k)$ e quindi $\exists x(x \in X \wedge F^X x, a_1, \ldots, a_k)$. Questo dimostra che $E^X(a_1, \ldots, a_k)$ è vera. ■

Si osservi che il lemma appena dimostrato è uno schema di teorema (per ogni formula E ci fornisce un enunciato vero). Lo *schema di riflessione* è uno schema di teorema che si dimostra nella teoria ZF con l'assioma di fondazione.

Teorema 5.3.2 *(con AF) Sia $E(x_1, \ldots, x_k)$ una formula senza parametri; allora per ogni ordinale α, esiste un ordinale limite $\beta > \alpha$ tale che V_β conviene a E.*

Proof. Si dimostra per induzione (nel senso intuitivo) sulla complessità di E che si suppone in forma prenessa, che per ogni ordinale α esiste un ordinale β superiore a α tale che V_β conviene a E e a tutte le formule precedenti. È evidente per E formula senza quantificatori, perché in tal caso E e E^X per una collezione qualunque X, sono uguali. Pertanto

$V_{\alpha+w}$ conviene a E. Se E è la formula $\neg F$, allora esiste un ordinale limite $\beta > \alpha$ tale che V_β conviene a F e a tutte le formule precedenti; allora V_β conviene anche a E : infatti se $a_1, \ldots, a_k \in V_\beta$ allora $F(a_1, \ldots, a_k) \iff F^{V_\beta}(a_1, \ldots, a_k)$, e dunque $E(a_1, \ldots, a_k) \iff E^{V_\beta}(a_1, \ldots, a_k)$. Supponiamo che E sia della forma $\exists x F(x, x_1, \ldots, x_k)$; per ipotesi di induzione, per ogni ordinale α, esiste un ordinale limite $\beta > \alpha$ tale che V_β conviene a F e a tutte le formule precedenti. Si definisce una relazione funzionale $y = \varphi(x_1, ..., x_k)$ k-aria tramite l'enunciato:

$$y \text{ è un insieme di rango minimo tale che } F(x, x_1, ...x_k).$$

Per definizione di φ si ha grazie all'assioma di fondazione:

$$\exists x F(x, x_1, ..., x_k) \iff \exists x[(x \in \varphi(x_1, ..., x_k)) \wedge F(x, x_1, ..., x_k)].$$

Si definisce per induzione su w una successione di ordinali $(\beta_n)_{n\in w}$ nel modo seguente. β_0 è il più piccolo ordinale $> \alpha$, tale che V_{β_0} conviene a F e a tutte le formule precedenti. Supponiamo di aver definito β_i per ogni $i \geq 2n$, si pone: β_{2n+1} il primo ordinale $> \beta_{2n}$, tale che $V_{\beta_{2n+1}}$ contiene $\varphi(a_1, ..., a_k)$ per ogni $(a_1, ..., a_k)$ k-upla di elementi di $V_{\beta_{2n}}$. Un tale ordinale esiste esiste perché $\bigcup\{\varphi(a_1, ..., a_k); (a_1, ..., a_k) \in V^k_{\beta_{2n}}\}$ è nella gerarchia cumulativa V in quanto ogni elemento di questo insieme è chiaramente in V. Dunque tale insieme appartiene a V_γ per un certo ordianle γ e quindi è contenuto in V_γ. β_{2n+2} è il primo ordinale $> \beta_{2n+1}$ tale che $V_{\beta_{2n+2}}$ conviene a F e a tutte le formule precedenti. La successione β_n è strettamente crescente; dunque se $\beta = sup\beta_n$, β è un ordinale limite, e $V_\beta = \bigcup_{n\in w} V_{\beta_n} = \bigcup_{n\in w} V_{\beta_{2n}}$. Poiché ogni $V_{\beta_{2n}}$ conviene a F e a tutte le formule precedenti, anche V_β per il Lemma 2.4.1. Resta da dimostrare allora che V_β conviene a E. Siano $a_1, ...a_k \in V_\beta$ e n un intero sufficintemente grande perché $a_1, ...a_k \in V_{\beta_{2n}}$. Se $E(a_1, ..., a_k)$ è vero allora si ha $\exists x F(x, a_1, ..., a_k)$, dunque $\exists x[x \in \varphi(a_1, ..., a_k) \wedge F(x, a_1, ..., a_k)]$. Sia $a \in \varphi(a_1, ..., a_k)$ tale che $F(a, a_1, ..., a_k)$. Si ha $a_1, ..., a_k \in V_{\beta_{2n}}$, e dunque $a \in V_{\beta_{2n+1}}$, cioè $a \in V_\beta$. Poiché V_β conviene a F, si ha allora $F^{V_\beta}(a, a_1, ..., a_k)$, dunque $\exists x(x \in V_\beta \wedge F^{V_\beta}(x, a_1, ..., a_k))$. Pertanto $E^{V_\beta}(a_1, ..., a_k)$ è vera. Viceversa, se $E^{V_\beta}(a_1, ..., a_k)$ è vera, esiste $a \in V_\beta$ tale che $F^{V_\beta}(a_1, ..., a_k)$. Poiché V_β conviene a F, allora $F(a, a_1, ..., a_k)$ è vera e quindi si ha $E(a_1, ..., a_k)$. ■

Osservazione 5.3.3 *Se E è una formula chiusa, dire che V_β conviene a E equivale a dire che E è vera nell'universo se, e soltanto se, è vera in V_β. Ne segue che: se E è una formula chiusa che è vera nell'universo allora per ogni ordinale α esiste un ordinale $\beta > \alpha$ tale che E è vera in V_β.*

Capitolo 6

Indipendenza dell'assioma di scelta

Finalmente, abbiamo gli strumenti necessari ad affrontare la dimostrazione della consistenza dell'assioma di scelta che è l'argomento di questo capitolo. Ci limiteremo a dimostrare rigorosamente solo la consistenza dell'assioma di scelta e non anche la consistenza della sua negazione. Quanto è stato trattato, tuttavia, ci fornisce gli strumenti necessari per uno studio più dettagliato della dimostrazione di Cohen, che completa la dimostrazione dell'indipendenza dell'assioma. Il lettore, dunque, se interessato, potrà misurarsi con la prova della consistenza della negazione senza problemi.

6.1 Insiemi di formule

In questa sezione mostreremo che è possibile associare ad ogni formula logica un'insieme dell'universo, che chiameremo *formula*. Per non confondere le formule abituali con le formule che sono insiemi dell'universo, chiameremo *enunciati* le prime.
Ai connettivi logici $\vee, \neg$, ai simboli $\in, =$, e al quantificatore esistenziale $\exists$ associamo 5 insiemi distinti dell'universo

ad esempio $0, 1, 2, 3, 4$; che noteremo $\vee, \neg, \bigvee, \xi, \approx$. Scegliamo, poi, un insieme numerabile $\mathscr{V}$ i cui elementi chiamati *variabili* sono distinti dai precedenti: l'insieme degli interi ≥ 5. Se x è una variabile la coppia ordinata $(\bigvee, x)$ sarà denotata $\bigvee x$. Si definisce per induzione una funzione $n \mapsto \mathscr{F}_n$ di dominio w : $\mathscr{F}_0$ è l'insieme delle triple ordinate (ξ, x, y) e $(\approx, x, y)$ per $x, y \in \mathscr{V}$. Detto in altri termini

$$\mathscr{F}_0 = [\{\xi\} \times \mathscr{V}^2] \cup [\{\approx\} \times \mathscr{V}^2].$$

Gli elementi di $\mathscr{F}_0$ si chiamano *formule atomiche*. Per ogni intero n,

$$\mathscr{F}_{n+1} = \mathscr{F}_n \cup [\{\neg\} \times \mathscr{F}_n] \cup [\{\vee\} \times \mathscr{F}_n^2] \cup [(\{\bigvee\} \times \mathscr{V}) \times \mathscr{F}_n].$$

$\mathscr{F}_{n+1}$ è cioè l'insieme costituito dagli elementi di $\mathscr{F}_n$ e le coppie e le triple ordinate della forma $(\neg, \varphi), (\vee, \varphi, \psi), (\bigvee x, \varphi)$ per $\varphi, \psi \in \mathscr{F}_n$ e $x \in \mathscr{V}$. Si pone $\mathscr{F} = \bigcup_{n \in w} \mathscr{F}_n$; $\mathscr{F}$ è l'*insieme delle formule*.

Osservazione 6.1.1 *È chiaro, allora, che ogni enunciato senza parametri corrisponde una formula e ad ogni formula di lunghezza finita corrisponde un enunciato.*

Così costruito $\mathscr{F}$, possiamo dimostrare che $\mathscr{F} \subseteq V_w$, dimostrando per induzione su n che per ogni n, $\mathscr{F}_n \subseteq V_w$. In seguito le formule $(\xi, x, y), (\approx, x, y), (\neg, \varphi), (\vee, \varphi, \psi), (\bigvee x, \varphi)$ saranno denotate rispettivamente $x \xi y$, $x \approx y, \neg\varphi, \varphi \vee \psi, \bigvee x(\varphi)$. Le formule $(\neg\varphi) \vee \psi, \neg((\neg\varphi) \vee (\neg\psi)), \neg \bigvee x(\neg\varphi)$ saranno denotate rispettivamente $\varphi \Rightarrow \psi, \varphi \wedge \psi, \bigwedge x(\varphi)$ Una *formula φ a parametri* è, per definizione, una coppia ordinata (ψ, η), dove ψ è una formula e η una funzione che ha per dominio un sottoinsieme dell'insieme delle variabili libere di ψ.

Definiamo ora una relazione funzionale $Y = Val(\phi, X)$ dove ϕ è una formula e X un insieme non vuoto. In base alla definizione che daremo, se $\phi = A(x_1, ..., x_k)$, allora Y sarà l'insieme delle $k - uple$ di elementi che soddisfano $A^X(x_1, ..., x_k)$.
Chiamo $vl(\phi)$ l'insieme delle variabili libere di ϕ (si ricorda che $vl(\phi)$ è un insieme di interi $n \geq 5$).

- Se ϕ è $x \xi y$ (risp. $x \approx y$), $Val(\phi, X) = \{\delta \in X^{\{x,y\}}; \delta(x) \in \delta(y)$ (risp. $\delta(x) = \delta(y))\}$[1];

[1] X^Y è l'insieme delle funzioni di dominio Y a valori in X

- se ϕ è $\neg\psi$, $Val(\phi, X) = X^{vl(\psi)} \setminus Val(\psi, X)$;
- se ϕ è $\psi \vee \theta$, $Val(\phi, X) = \{\delta \in X^{vl(\psi)}$; la restrizione di δ a $vl(\psi)$ appartiene $Val(\psi, X)$ oppure la restrizione di δ a $vl(\theta)$ appartiene a $Val(\theta, X)\}$;
- se ϕ è $\bigvee x\psi$, $Val(\phi, X) = \{\delta \in X^{vl(\psi)}$; esiste un estensione γ di δ a $vl(\psi)$ tale che $\gamma \in Val(\psi, X)\}$.

6.2 Insiemi definibili in termini di ordinali

Si consideri un universo $\mathscr{U}$ che soddisfi l'assioma di fondazione. Si definisce la collezione DO degli *insiemi definibili in termini di ordinali.*

Definizione 6.2.1 *Per ogni insieme a, $a \varepsilon DO$ se e soltanto se* esistono un ordinale α e una formula $\varphi(x, \alpha_1, ..., \alpha_k)$ a una sola variabile libera e a parametri in $\alpha \varepsilon On$ e tale che[2] a è l'unico insieme di V_α che soddisfa $\varphi^{V_\alpha}(x, \alpha_1, ..., \alpha_k)$.

Lemma 6.2.2 *Sia a un insieme e $A(x, \alpha_1, ..., \alpha_k)$ un enunciato ad una sola variabile libera, e a parametri $\alpha_1, ..., \alpha_k$ in On, e tale che a è il solo insieme che soddisfa l'enunciato. Allora a è definibile in termini di ordinali.*

Proof. Possiamo applicare lo schema di riflessione, perché l'assioma di fondazione è supposto vero in $\mathscr{U}$. Pertanto esiste un ordinale $\alpha > \alpha_1, ...\alpha_k$ e sufficientemente grande perché $a \in V_\alpha$, tale che V_α conviene all'enunciato $A(x, \alpha_1, ..., \alpha_k)$. Allora a è il solo elemento di V_α che soddisfa l'enunciato $A^{V_\alpha}(x, \alpha_1, ..., \alpha_k)$. Cioè a è definibile in termini di ordinali. ■

Vogliamo dimostrare il viceversa del Lemma 6.2.2 ma per poterlo fare, abbiamo bisogno di introdurre due relazioni funzionali. Ciò sarà fatto nelle due sezioni che seguono.

[2]quanto segue si può scrivere nella teoria così: $Val(\psi, V_\alpha) = \{a\}$ dove ψ è la formula $\varphi(x, \alpha_1, ..., \alpha_k)$.

La collezione $\sigma(On)$

Sia C una collezione, una successione finita di oggetti di C è, per definizione, una funzione definita su un intero n, a valori in C. L'intero n si chiama *lunghezza* della successione. La collezione delle successioni finite di oggetti di C si denota $\sigma(C)$. Sulla collezione $\sigma(On)$ delle successioni finite di ordinali, definiamo una relazione d'ordine R ponendo:
$s < t$ (mod R) se e soltanto se:
$[sup(s) < sup(t)] \vee [sup(s) = sup(t) \wedge l(s) < l(t)] \vee [sup(s) = sup(t) \wedge l(s) = l(t) \wedge s \neq t \wedge s(n) < t(n)$ per il primo ordinale n tale che $s(n) \neq t(n)]$. $l(s)$ designa la lunghezza della successione s, $sup(s)$ il più grande valore assunto dalla funzione s (ogni insieme totalmente ordinato e finito ha un più grande elemento).
La relazione R così definita è una relazione di buon ordine: infatti, la collezione $S_t(R)$ delle successioni $s < t$ (mod R) ha tutti i suoi elemeti in $\sigma(\gamma + 1)$ con $\gamma = \sup(t)$ (in quanto le successioni di $S_t(R)$ sono inferiori modulo R a t, queste non possono avere un estremo superiore più grande di γ). Dunque è un insieme.
Sia allora X un insieme non vuoto i cui elementi sono tutti in $\sigma(On)$; sia γ il più piccolo ordinale della forma $sup(s)$ per $s \in X$; sia n il più piccolo intero della forma $l(s)$ per $s \in X$ e $sup(s) = \gamma$; si definisce, per induzione, un'applicazione f di dominio n : se $i \in n$, $f(i)$ è il primo ordinale della forma $s(i)$ per $s \in X$, $sup(s) = \gamma$, $l(s) = n$, e $s(j) = f(j)$ per ogni $j < i$. La funzione f così definita è il più piccolo elemento di X.
Chiaramente R è totale perché date due successioni s, t di $\sigma(On)$, quanto abbiamo appena dimostrato ci permette di affermare che $\{s, t\}$ è un insieme ben ordinato dunque $s < t \vee t < s \vee s = t$.
Possiamo concludere allora che R è una relazione di buon ordine. $\sigma(On)$ è pertanto una collezione ben ordinata che non è un insieme; esiste per il Teorema 2.6.11 una relazione funzionale $s = J(\alpha)$ che stabilisce un isomorfismo tra On e $\sigma(On)$.

Un buon ordine per V_w

In questa sezione si definirà una relazione funzionale che stabilisce una biezione tra V_w e w (senza assioma di scelta).

Lemma 6.2.3 *Se n è un intero, $\{0,1\}^n$ è equipotente a un intero e a uno soltanto.*

Proof. L'unicità è evidente perché due interi distinti non possono essere equipotenti. Il lemma si dimostra per induzione su n : se $\{0,1\}^n$ è equipotente all'intero k allora $\{0,1\}^{n+1}$ è equipotente a $k \times \{0,1\}$ cioè all'intero $2k$. ■

Si definisce per induzione su $n \in w$ una biiezione φ_n di V_n su un intero v_n. Per $n = 0$, $\varphi_n = \emptyset$ e $v_n = 0$; Supponiamo definita φ_n si definisce una biiezione $\psi_n : \mathscr{P}(V_n) \to \{0,1\}^{v_n}$, cioè $\psi_n : V_{n+1} \to \{0,1\}^{v_n}$ nel modo seguente:

$$\psi_n(X)(i) = 1 \iff \exists x \in X(i = \varphi_n(x))$$

per $X \subseteq V_n$, e $0 \leq i < v_n$. $\{0,1\}^{v_n}$ è un insieme di successioni finite di ordinali (insieme di successioni di lunghezza v_n di ordinali 0 e 1). Quindi è ben ordinata dalla relazione definita su $\sigma(On)$ nel paragrafo precedente. Per il Lemma 6.2.3 allora, l'ordinale isomorfo a questo insieme è un intero che sceglieremo per v_{n+1}. Si ha dunque una biiezione φ_{n+1} di V_{n+1} su v_{n+1} definita da $\varphi_{n+1} = H(\varphi_n)$ dove la relazione $\varphi' = H(\varphi)$ si enuncia:
esiste $d \in w$ e D tali che $\varphi : D \to d$, e φ' è la funzione di dominio $\mathscr{P}(D)$ ottenuta componendo l'applicazione $\psi : \mathscr{P}(D) \to \{0,1\}^d$ canonicamente dedotta da φ, e l'isomorfismo di $\{0,1\}^d$ munito del buon ordine R sui suoi ordinali. Questa relazione è definita da una formula senza parametri. Di conseguenza la relazione funzionale $n \longmapsto \varphi_n$ di dominio w, definita così per induzione è anch'essa senza parametri. Si ha, dunque, una relazione funzionale $n \longmapsto r_n$ senza parametri che a ogni intero n associa un buon ordine r_n su V_n (immagine tramite φ_n^{-1} del buon ordine dell'intero v_n). Si definisce allora un buon ordine r su V_w, ponendo $x < y \pmod r$ se e soltanto se: $rg(x) < rg(y)$ *oppure* $[rg(x) = rg(y) = n \wedge x < y$ *(mod r_n.)]*. Ogni segmento iniziale di questo buon ordine è isomorfo a un intero: l'insieme degli $x < x_0 \pmod r$ è contenuto in V_n, se n è il rango di x_0;

quindi il suo ordinale è un intero. Questo dimostra che il buon ordine r su V_w è isomorfo a w. L'isomorfismo dell'insieme ben ordinato (V_w, r) su w è la relazione funzionale cercata perché è definita da una formula senza parametri.
Questo risultato ci permette di affermare che possiamo associare ad ogni formula dell'universo un intero, in quanto abbiamo visto nel Paragrafo 6.1 che $\mathscr{F} \subseteq V_w$.

6.3 Insiemi ereditariamente definibili in termini di ordinali

Lemma 6.3.1 *Se a è definibile in termini di ordinali allora esiste un enunciato $A(x, \gamma)$ ad una variabile libera il cui unico parametro è l'ordinale γ, e che è soddisfatto solamente da a.*

Un tale enunciato si chiama *definizione di a in termini di ordinali*.
Proof. Nei precedenti paragrafi abbiamo mostrato che esistono due biiezioni, la prima J di On su $\sigma(On)$ e la seconda K di w su V_w. Poiché a è definibile in termini di ordinali, esiste un ordinale α_0 e una formula $\varphi_0(x, \alpha_1, ..., \alpha_k)$ a parametri in α_0 tale che l'unico insieme in V_α che soddisfa $\varphi_0^{V_\alpha}(x, \alpha_1, ..., \alpha_k)$ è a. Chiamiamo allora n_0 l'intero che K associa alla formula $\varphi_0(x, x_1, ..., x_k)$ senza parametri, e chiamiamo β_0 l'ordinale che J associa alla successione $(\alpha_1, ..., \alpha_k)$. Si consideri allora l'enunciato seguente $E(x, n_0, \alpha_0, \beta_0)$: *n è un intero β_0, α_0 sono ordinali la coppia ordinata $(K(n_0), J(\beta_0))$ è una formula ψ a parametri in α_0 e tale che x è l'unico insieme di V_{α_0} che soddisfa ψ relativizzata a V_{α_0}*. É chiaro che questo enunciato è soddisfatto solo da a e ha per soli parametri gli ordinali n_0, α_0, β_0. Se si vuole trovare un enunuciato a un solo parametro, si designa con γ_0 l'ordinale associato da J alla tripla (n_0, α_0, β_0), l'enunciato cercato sarà $A(x, \gamma_0)$: *esiste un intero n e α, β ordinali tali che $J(\gamma_0) = (n, \alpha, \beta)$ e $E(x, n, \alpha, \beta)$*. ■

La collezione DO non è transitiva. [3]

[3] Per la dimostrazione che DO non è transitiva cf. [Krivine, 1998] (esercizio 17).

Definiamo una sottocollezione di DO, la collezione HDO che è transitiva.

Definizione 6.3.2 *$x \varepsilon HDO$ se e soltanto se ogni elemento di $\{x\} \cup Ct(x)$ è definibile in termini di ordinali*

La collezione HDO si chiama collezione degli *insiemi ereditariamente definibili in termini di ordinali.* Si osservi che è definita da un enunciato senza parametri. La transitività di HDO segue dal fatto che: se $a \varepsilon HDO$, allora ogni $x \in a$ appartiene a $Ct(a)$ dunque per definizione $x \varepsilon HDO$.

Lemma 6.3.3 *Un insieme a è ereditariamente definibile in termini di ordinali se e soltanto se a è definibile in termini di ordinali e ogni suo elemento è ereditariamente definibile in termini di ordinali.*

Proof. La condizione è evidentemente necessaria. Supponiamo allora che ogni elemento di a si in HDO e che a sia in DO. $Ct(a) = a \cup \bigcup_{y \in a} Ct(y)$: infatti $Ct(a) \subseteq a \cup \bigcup_{y \in a} Ct(y)$ perché $a \subset a \cup \bigcup_{y \in a} Ct(y)$. Viceversa, per ogni $y \in a$, $Ct(y) \subset Ct(a)$, dunque tutti gli elementi di $a \cup \bigcup_{y \in a} Ct(y)$ sono anche elementi di $Ct(a)$. Allora $\{a\} \cup Ct(a) = \{a\} \cup a \cup \bigcup_{y \in a} Ct(y) = \{a\} \cup \bigcup_{y \in a} (Ct(y) \cup \{y\})$. Vogliamo dimostrare che per ogni $x \in \{a\} \cup Ct(a)$, x è definibile in termini di ordinali. Se $x \in \{a\} \cup Ct(a)$, allora $x \in \{a\} \cup \bigcup_{y \in a} (Ct(y) \cup \{y\})$. Dunque se $x \in (Ct(y) \cup \{y\})$ per un certo $y \in a$, allora, per ipotesi, x è definibile in termini di ordinali. Se invece $x \in \{a\}$, cioè $x = a$ allora, ancora una volta per ipotesi, x è definibile in termini di ordinali. ■

6.4 Indipendenza dell'assioma di scelta

Il seguente teorema dimostra la consistenza relativa dell'assioma di scelta: da un modello $\mathscr{U}_0$ di ZF, è possibile costruire un modello di $ZF + AF + AC$. Da $\mathscr{U}_0$ si potrà costruire un modello $\mathscr{U}$ di $ZF + AF$ nel quale sarà possibile costruire la collezione HDO. Il seguente teorema ci permetterà di concludere.

Teorema 6.4.1 *Sia $\mathscr{U}$ un modello di $ZF + AF$. La collezione HDO costruita in $\mathscr{U}$, soddisfa ZF, l'assioma di fondazione e l'assioma di scelta.*

assioma di estensionalità: HDO è un modello transitivo il Teorema 5.1.1 ci permette di concludere.

assioma di fondazione: HDO è un modello transitivo il Teorema 5.1.1 ci permette di concludere.

assioma dell'infinito: ogni ordinale α è chiaramente in DO (è definito dall'enunciato $x = \alpha$) dunque è anche in HDO. In particolare w è in HDO, che, dunque, per il Teorema 5.1.1 soddisfa l'assioma dell'infinito.

assioma dell'unione: Sia a in HDO, sia b l'unione degli elementi di a. É chiaro che ogni elemento di b è in HDO, dunque è sufficiente dimostrare che b è in DO per il Lemma 6.3.3. a è in DO dunque è l'unico oggetto che soddisfa un certo enunciato $A(x, \alpha)$. Ma allora b è il solo oggetto che soddisfa $B(y, \alpha) : \forall z(z \in y \iff \exists u(u \in a \wedge z \in u))$. Dunque b è il solo oggetto che soddisfa l'enunciato $\exists x[A(x, \alpha) \wedge B(y, x)]$ che ha per unico parametro l'ordinale α. Ne segue che b è definibile in termini di ordinali per il Lemma 6.2.2.

assioma dell'insieme delle parti: Siano a un insieme della collezione HDO e b l'insieme delle parti di a che sono in HDO. Ogni elemento di b è ereditariamente definibile in termini di ordinali, dunque è sufficiente dimostrare che b è definibile in termini di ordinali. Se $A(x, \alpha)$ è una definizione di a in termini di ordinali, allora b è l'unico oggetto che soddisfa l'enunciato $B(x, a) : \forall z[z \in y \iff HDO(z) \wedge z \subseteq a]$, dunque anche l'enunciato $\exists x[A(x, \alpha) \wedge B(y, x)]$. Abbiamo già osservato che HDO è definita da un enunciato senza parametri, ciò dimostra che b è definibile in termini di ordinali.

schema di rimpiazzamento: Si consideri un enunciato $R(x, y, a_1, ..., a_k)$ a due variabili libere, a parametri in HDO e che in HDO definisce una relazione funzionale. Tale relazione funzionale è definita nell'universo

$\mathscr{U}$ dall'enunciato seguente che noteremo $S(x, y, a_1, ..., a_k)$: $x\varepsilon HDO \wedge y\varepsilon HDO \wedge R^{HDO}(x, y, a_1, ..., a_k)$. Siano a un oggetto di HDO, e b l'insieme delle immagini degli elementi di a tramite questa relazione funzionale. Ogni elemento di b è in HDO ed è sufficiente dimostrare che b è in DO. Siano $A(x, \alpha), A(x_1, \alpha_1), ..., A(x_k, \alpha_k)$ definizioni di $a, a_1, ..., a_k$ (rispettivamente) in termini di ordinali. Allora b è l'unico insieme che soddisfa $B(y, a, a_1, ..., a_k)$:

$$\forall z[z \in y \iff \exists t(t \in a \wedge S(t, z, a_1, ..., a_k))]$$

dunque anche l'enunciato:

$$\exists x, x_1, ..., x_k[A(x, \alpha) \wedge A(x_1, \alpha_1) \wedge ... \wedge A(x_k, \alpha_k) \wedge B(y, x, x_1, ..., x_k)]$$

i cui unici parametri sono gli ordinali $\alpha, \alpha_1, ..., \alpha_k$. Si ha, dunque, che b è definibile in termini di ordinali.

assioma di scelta: Dimostriamo che HDO soddisfa il teorema di Zermelo, dunque l'assioma di scelta. Possiamo definire una relazione funzionale $\alpha = \Theta(\varphi)$, a valori in On, definita da un enunciato senza parametri, iniettiva, il cui dominio è la collezione delle formule ad una variabile libera: alla formula $\varphi = \psi(x, \alpha_1, ..., \alpha_r)$ si associa prima la coppia di ordinali (n, β) dove n è l'intero associato alla formula senza parametri $\psi(x, x_1, ..., x_r)$ tramite la biiezione K; e β è l'ordinale associato alla successione di ordinali $(\alpha_1, ..., \alpha_r)$ tramite la biiezione J. Si associa poi un ordinale α alla coppia (n, β) tramite l'isomorfismo J.
Per come è stata definita, Θ è iniettiva in quanto: date due formule distinte $\psi(x, \alpha_1, ..., \alpha_r)$,$\phi(y, \beta_1, ..., \beta_k)$, allora o $\psi(x, x_1, ..., x_r) \neq \phi(y, y_1, ..., y_k)$ e in tal caso gli interi che K associa alle due formule sono distinti; oppure $\psi(x, x_1, ..., x_r) = \phi(y, y_1, ..., y_k)$ ma $(\alpha_1, ..., \alpha_r) \neq (\beta_1, ..., \beta_k)$, in tal caso gli interi che J associa alle due successioni sono distinti.
Si definisce, allora, una relazione funzionale $\beta = D(x)$ di dominio DO e a valori in On tramite l'enunciato: *β è il più piccolo ordinale che rappresenta la coppia (α, γ) tale che γ è l'ordinale associato da Θ a una formula φ ad una variabile libera e a parametri nell'ordinale α e tale che l'unico insieme di V_α che soddifa l'enunciato corrispondente alla formula*

φ relativizzato a V_α è x. Si osservi che: dato un insieme $x \varepsilon DO$ possono esserci più formule soddisfatte solo da x inoltre, per una stessa formula soddisfatta solo da x, possiamo avere più di un ordinale α che contenga i parametri di una tale formula e tale che $x \in V_\alpha$. Dunque α e γ variano per uno stesso insieme x, per questo diciamo che β è "il più piccolo ordinale" associato alla coppia (α, γ). L'enunciato $\beta = D(x)$ è senza parametri; è chiaro che $x \neq x' \Rightarrow D(x) \neq D(x')$ (perché la collezione delle formule soddisfatte *solo* da x è disgiunta dalla collezione delle formule soddisfatte solo da x' se $x \neq x'$). Ne consegue che la relazione $R(x, y)$ definita dall'enunciato senza parametri $DO(x) \wedge DO(y) \wedge D(x) \leq D(y)$ è una relazione di buon ordine sulla collezione DO : ogni insieme X a elementi in DO ha un minimo, infatti $\{\alpha = D(x); x \in X\}$ è un insieme (è l'immagine di X che è un insieme, dunque è un insieme per rimpiazzamento). Poiché si tratta di un insieme di ordinali ha un minimo γ. Supponiamo $\gamma = D(y)$ per un $y \in X$, abbiamo visto che y è unico, dunque y è il minimo di X.

Sia allora a un insieme di HDO. La restrizione di questo buon ordine a a è l'insieme $b = \{(x, y) \in a^2; D(x) \leq D(y)\}$. Poiché gli elementi di b sono in HDO, è sufficiente dimostrare che b è in DO. In effetti b è il solo insieme che soddisfa l'enunciato: $B(y, a) : \forall z[z \in y \iff \exists u \exists v(u \in a \wedge v \in a \wedge z = (u, v) \wedge D(u) \leq D(v))]$ (l'unicità è una conseguenza dell'assioma di estensionalità). Dunque se $A(x, \alpha)$ è una definizione di a in termini di ordinali, allora b è definito in termini di ordinali dall'enunciato $\exists x[A(x, \alpha) \wedge B(y, x)]$. Ciò dimostra che b è in HDO. b è un buon ordine su a in $\mathscr{U}$, dunque anche in HDO : perché ogni sottoinsieme non vuoto di a, in particolare quelli che sono in HDO, hanno un più piccolo elemento (mod b). Abbiamo dimostrato che HDO soddisfa il teorema di Zermelo.

Il teorema appena dimostrato inferisce la *consistenza* dell'assioma di scelta: se ZF ammette un modello allora esiste un modello anche di $ZF + AF + AC$. Per mostrare l'*indipendenza* dell'assioma di scelta dovremmo dimostrare il seguente teorema:

Teorema 6.4.2 *Se ZF ha un modello, allora $ZF + AF + \neg AC$ ammette un modello.*

Questo risultato è stato dimostrato da Cohen nel 1963. La dimostrazione di Cohen si basa sulla costruzione di un modello in cui tutti gli assiomi di ZF sono veri e l'assioma della scelta è falso, che si costruisce mediante la tecnica del forcing.

Ci siamo limitati a dimostrare rigorosamente la consistenza dell'assioma di scelta. Quanto è stato trattato, tuttavia, ci fornisce gli strumenti necessari per uno studio più dettagliato della dimostrazione di Cohen. Il lettore, dunque, se interessato, potrà misurarsi con la prova della consistenza della negazione senza problemi.

Capitolo 7

Conclusioni

La teoria degli insiemi ha un taglio algebrico: abbiamo visto nel Capitolo 1 che è nata con l'intento di emancipare le teorie e i concetti matematici dall'intuizione, e dalla geometria. Enunciando la teoria e sviluppandone i principali teoremi abbiamo creato la base per una comprensione più approfondita di questa sua caratteristica. Riflettiamo, infatti, sugli assiomi di ZF: le operazioni di base, quelle a cui si riferiscono gli assiomi, sono la grande unione, l'insieme delle parti e, se si vuole, l'intersezione. Nessuna di queste riflette il modo in cui noi, intuitivamente, *pensiamo* agli insiemi, e altre funzioni sono, forse, quelle più utili in matematica nonché le più intuitive: mi riferisco alle operazioni sui cardinali. Tali operazioni sono: il prodotto cartesiano, l'unione disgiunta e la funzione esponenziale, e sono quelle che la teoria degli insiemi ha più difficoltà a descrivere. Il carattere geometrico del prodotto cartesiano, probabilmente, è evidente a tutti, ma è meno scontato per l'unione disgiunta ed è con questa operazione che le difficoltà della teoria degli insiemi risultano maggiori. Quando pensiamo all'unione disgiunta di due insiemi lo facciamo in modo geometrico: pensiamo a due insiemi disgiunti e ne immaginiamo l'unione "facendo attenzione alle ripetizioni". Questo fare attenzione alle ripetizioni è una procedura per noi semplice, invece in teoria degli insiemi è necessario rinominare gli elementi tramite il prodotto cartesiano con il singoletto 0 e il singoletto 1 [1]. Così facendo, procediamo in modo inverso rispetto al nostro modo naturale di approcciarci a questo oggetto matematico: *ri*nominiamo. La teoria degli insiemi, nata dal tentativo di liberarsi della geometria ha non pochi punti di debolezza. Laddove sorgono dei problemi, quali il risultato discusso in questo contesto, si è costretti ad aggiungere degli assiomi: poiché ci troviamo nell'impossibilità di dimostrare o negare l'esistenza di una funzione di scelta siamo costretti a farne un assioma e così per l'hipotesi del continuo. Nulla di sbagliato in ciò ma noi non sentiamo come assiomatici questi principi ne vorremmo una dimostrazione dagli altri assiomi perché, a differenza degli altri, non ci sembrano poi così evidenti. Anche dell'assioma dell'infinito, in realtà, potremmo dire lo stesso. In quanto l'esistenza di un insieme infinito è un assioma, non possiamo costruirlo in alcun modo. D'altra parte, abbiamo già discusso del finitismo, e questo ci suggerisce che l'assunzione che un tale insieme esista non è pacifica come la teoria vorrebbe farci credere. Per tutte queste ragioni, la dimostrazione dell'indipendenza dell'assioma di scelta, ampiamente usato in matematica da essere ritenuto indispensabile, deve farci riflettere e deve essere uno stimolo per la creazione di qualcosa di nuovo. Non dimentichiamo che questi risultati sono legati ad una particolare formalizzazione: nulla vieta che una diversa formulazione della teoria ci conduca a risultati diversi più vicini alla concezione intuitiva degli insiemi. Dunque, posto che il risultato di indipendenza dell'assioma di scelta non tolga nulla alla sua validità, alla possibilità cioè di farne uso, fintanto che ne facciamo un'assioma, quanto è appropriata questa teoria degli insiemi? L'assioma di scelta non è per noi, eventualmente, una conseguenza, piuttosto che un'assunto di base? Se ne facciamo un assioma viene meno il motivo stesso della teoria: fondare la matematica su degli assiomi in quanto proposizioni condivise. Dunque chiediamoci: che motivo c'è di conservare una teoria in cui è tanto difficile definire le nozioni e le operazioni più intuitive (abbiamo visto il prodotto cartesiano e l'unione disgiunta) se oggi ha perso la sua funzione fondazionale? Perché non restituirle quella dimensione geometrica, che le era stata sottratta nel XIX sec.?

[1] Dati due insiemi a e b si definisce *unione disgiunta* di a e b (e si scrive $a \biguplus b$) l'insieme $a \times \{0\} \cup b \times \{1\}$

Nel caso in cui questa domanda dovesse venire accolta, allora, il problema sarebbe: in una tale nuova teoria l'assioma di scelta sarebbe vero o falso? Si troverà un nuovo assioma che ci permetta di dimostrare o refutare l'assioma di scelta? Forse però questa chimera dell'intuizione è un pò troppo ambiziosa. Volendo fondare la matematica sull'intuizione ci troviamo comunque di fronte a un problema. Una dimostrazione, infatti, è qualcosa che lega le premesse alle conclusioni. Spesso però siamo più sicuri delle conclusioni che non delle premesse. L'assioma di scelta, ad esempio, implica il paradosso di Banach-Tarski: ciòè è possibile operare su una sfera in modo da ottenerne due che hanno le stesse dimensioni dell'originale. In base al criterio dell'intuizione allora dovremmo scartarlo. D'altra parte l'esperienza matematica sembra darci ragione del fatto che l'assioma di scelta è vero. Perché infatti non riconoscere che una partizione in classi di equivalenza ammette un insieme di rappresentanti? Dunque ci troviamo a decidere tra certe intuizioni e altre intuizioni incompatibili tra di loro. Allora una delle possibilità è che uno dei due gruppi di intuizioni non sia poi così intuitivo come credevamo. Potrebbe darsi ad esempio che il paradosso di Banach-Tarski nasconda delle ipotesi implicite discutibili, oppure che poter ben ordinare tutti gli insiemi sia una pretesa un pò troppo ambiziosa. Come decidere tra le due ipotesi?
Probabilmente un giorno, la teoria degli insiemi di Zermelo-Fraenkel sarà soppiantata da una nuova assiomatizzazione. Avrà ancora quel taglio algebrico che è la debolezza ma, allo stesso tempo, l'apetto più affascinante dell'attuale teoria degli insiemi?

Ringraziamenti

Vorrei, innanzitutto, ringraziare tutti coloro hanno permesso, o in qualche modo incoraggiato, sia la mia carriera scolastica che la stesura di questo elaborato; primo fra tutti, quindi, il professore Lorenzo Tortora De Falco che mi ha supportato in veste di relatore.

I miei più sentiti ringraziamenti vanno, poi, a tutto il dipartimento di filosofia dell'università Sorbonne di Parigi per avermi ospitato per nove mesi, ringrazio, dunque, la professoressa Susana Berestovoy, il professor Jean-Baptiste Joinet, e il professor Jacques Dubucs per avermi trasmesso le loro conoscenze e per avermi guidato durante un percorso difficile ma decisamente formativo. Ringrazio, allora, gli studenti del Master 1 de Logique che mi hanno accompagnato in questa esperienza, accogliendomi tra loro.

Ringrazio il mio correlatore, il professore Vito Michele Abrusci per la chiarezza con cui mi ha spiegato il suo punto di vista sul soggetto della mia tesi e per avermi dato dei preziosi spunti di riflessione. Ringrazio Paolo Di Giamberadino, Giulio Guerrieri, Michele per aver pazientemente ascoltato l'esposizione del mio elaborato.

Nessuno dei miei successi, però, sarebbe stato possibile senza il sostegno della mia famiglia che mi ha supportato e sopportato durante questi lunghi anni di studio. Ai miei genitori, a mia sorella, che è la persona che più stimo al mondo, e a mia nonna rivolgo, pertanto, il mio più grande grazie. Un grosso grazie va, dunque, alla mia amica storica Simona Marini e insieme a lei ringrazio Sara Alfieri, Maurilia Natali, Simone Munaò, Sergio Simonella e Edoardo Saba: amici preziosissimi, con i quali sono cresciuta e ho potuto condividere tante esperienze.

Ringrazio, infine, il mio ragazzo Giulio Manzonetto per aver reso meraviglioso il nostro primo anno passato insieme, che è stato l'anno più intenso della mia vita. Grazie per essere riuscito a rendere bello un anno pieno di difficoltà e di incognite, trascorso lontano dalla mia famiglia e dai miei amici. Grazie per avermi incoraggiato e sostenuto moralmente quando più ne avevo bisogno. Grazie per l'amore, l'attenzione, il rispetto e la pazienza che mi hai riserbato.

A tutti: grazie.

Bibliografia

[Cohen, 1963] Cohen, P. (1963). *The indipendence of the axiom of choice.* (mimeographed, Stanford University).

[Cori and Lascar, 1993] Cori, R. and Lascar, D. (1993). *Logique Mathématique, Tomes I et II.* Masson, Paris.

[Heijenoort, 1977] Heijenoort, J. v. (1977). *From Frege to Gödel.* Harvard University Press, third edition.

[Jech, 1997] Jech, T. (1997). *Set theory.* Springer, second edition.

[Johnstone, 1982] Johnstone, P. T. (1982). *Stone Spaces*, volume 3 of *Cambridge studies in advanced mathematics.* Cambridge University Press.

[Krivine, 1998] Krivine, J.-L. (1998). *Théorie des ensembles.* Cassini, Paris.

[Narici and Beckenstein, 1997] Narici, L. and Beckenstein, E. (1997). The Hahn-Banach theorem: The life and times. *Topology and its Applications*, 77:193–211.

[Piacentini-Cattaneo, 1996] Piacentini-Cattaneo, G. M. (1996). *Algebra-un approccio algoritmico.* Zanichelli, Bologna.

[Sernesi, 1989] Sernesi, E. (1989). *Geometria 1.* Bollati Boringhieri, Torino.

Indice analitico