Bollettino
Unione Matematica Italiana

Sezione A – La Matematica nella Società e nella Cultura

Alessandro Andretta

I teoremi di assolutezza in teoria degli insiemi: prima parte

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **6-A**—*La Matematica nella Società e nella Cultura* (2003), n.1, p. 57–84.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2003_8_6A_1_57_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2003.

Bollettino U. M. I.
La Matematica nella Società e nella Cultura
Serie VIII, Vol. VI-A, Aprile 2003, 57-84

I teoremi di assolutezza in teoria degli insiemi: prima parte.

ALESSANDRO ANDRETTA

Sommario. – *Questa è la prima parte di una articolo espositivo dedicato ai teoremi di assolutezza, un argomento che sta assumendo un'importanza via via più grande in teoria degli insiemi. In questa prima parte vedremo come le questioni di teoria dei numeri non siano influenzate da assunzioni insiemistiche quali l'assioma di scelta o l'ipotesi del continuo.*

1. – Introduzione.

La teoria degli insiemi viene considerata in modo curioso dalla maggior parte dei matematici. Da un lato, essa viene comunemente accettata come sistema fondazionale, come linguaggio universale con cui descrivere e costruire i vari enti matematici. Dall'altro le si rimprovera un'eccessiva generalità, per cui i suoi risultati più spettacolari, ottenuti negli ultimi decenni, vengono accolti con molto scetticismo, se non del tutto ignorati. Questa situazione, dovuta — a nostro parere — in parte alla complessità e alla sofisticazione dei metodi della disciplina e in parte ad un insufficiente sforzo di divulgazione da parte degli insiemisti, ingenera nel matematico medio alcuni pregiudizi che ci paiono tanto immotivati quanto duri a morire.

Il primo — e forse più diffuso — tenderebbe a sostenere che dopo il lavoro di Cohen sull'indipendenza dell'ipotesi del continuo non sia successo nulla di veramente significativo per le altre parti della matematica. La disciplina — sempre secondo taluni — sarebbe naufragata in una miriade di *risultati di indipendenza*, vale a dire dimostrazioni del fatto che certe questioni non sono né dimostrabili né confutabili in ZFC, il sistema di assiomi (riportati qui sotto nella sezione 2) comunemente adottato in teoria degli insiemi. E anche la rilevanza in matematica dell'ipotesi del continuo ([1]) (che spesso abbrevieremo con CH) è spesso messa in discussione.

Naturalmente non tutti i matematici la pensano in questo modo. Per esempio C. Dellacherie e P.-A. Meyer in [DM] scrivono:

> We shall see below several very beautiful consequences of the continuum hypothesis (due to Mokobodzki) which lead us to adopt it in this book with the same standing as the axiom of choice.

D'altra parte ci sono principi insiemistici (primo fra tutti il *proper forcing axiom* — vedi [Ba]) che contraddicono CH e che hanno importanti applicazioni in topologia generale, analisi funzionale, teoria della misura, etc. Inoltre i risultati di indipendenza non si limitano a questioni di teoria degli insiemi che potremmo definire «pura», ma coinvolgono problemi ed enti che provengono dalle più disparate aree della matematica: il problema di von Neumann del sollevamento Boreliano in teoria della misura [S], la congettura di Kaplansky sulla continuità automatica per le algebre di Banach [DW], il problema di Whitehead sull'esistenza di gruppi abeliani quasi-liberi [EM], etc. (Vedremo alcuni di questi risultati di indipendenza nella sezione 3.) Dimostrare che una certa congettura in uno specifico settore della matematica è indipendente da ZFC ci sembra importante tanto per la teoria degli insiemi quanto per il settore in questione. Naturalmente non tutte le aree della matematica interagiscono nello stesso modo con la teoria degli insiemi e quindi non sorprende che questo pregiudizio sia particolarmente diffuso là dove le interazioni sono più scarse.

Il secondo pregiudizio è più sottile: un matematico pur riconoscendo l'importanza dell'interazione fra la teoria degli insiemi e taluni problemi in altre aree, potrebbe obiettare che proprio a causa di queste interazioni, questi non sono buoni problemi. Una congettura ritenuta interessante fino al giorno prima cadrebbe

([1]) Per la definizione di CH rimandiamo il lettore alla sezione 2.

in disgrazia non appena si scopre dipendere da qualche questione insiemistica. Per esempio G. Folland in [Fo, p. 17]:

> My own feeling, subject to revision in the event of a major breakthrough in set theory, is that if the answer to one's question turns out to depend on the continuum hypothesis, one should give up and ask a different question.

Lo scopo di questo articolo è illustrare come le *tecniche* che producono i risultati di indipendenza possano essere utilizzate per dimostrare (in ZFC!) dei nuovi teoremi di matematica. In altre parole: le dimostrazioni di indipendenza e, più in generale, lo studio dei modelli di ZFC, lungi dall'aver fatto naufragare la teoria degli insiemi in una miriade di rivoli indipendenti, ci forniscono dei nuovi metodi di dimostrazione (oltre che una maggiore comprensione dell'universo insiemistico). Quindi anche il matematico con scarse simpatie per le questioni fondazionali dovrebbe riconoscere che questo tipo di ricerche ha una sua utilità per la matematica assoluta, vale a dire quella parte della matematica che è immune da fenomeni di indipendenza.

Tanto per dare un'idea al lettore del tipo di risultati di cui vogliamo parlare, consideriamo un sistema di assiomi T come ZFC o ZF (vale a dire ZFC meno l'assioma di scelta) e un'ipotesi aggiuntiva σ. Supponiamo che il teorema τ sia deducibile da $\mathsf{T} + \sigma$, in simboli $\mathsf{T} + \sigma \vdash \tau$. I teoremi di assolutezza ci garantiscono che se σ e τ sono sufficientemente semplici, allora $\mathsf{T} \vdash \tau$. Un'applicazione riguarderà il caso in cui T sia ZFC e σ sia CH, l'ipotesi del continuo, quando τ è un enunciato che «parla solo di numeri reali.» Un'altra applicazione riguarda AC, l'assioma di scelta. È ben noto che AC è estremamente utile in molte parti della matematica contemporanea (algebra, analisi funzionale, etc.), ma allo stesso tempo ha molte conseguenze bizzarre, per esempio l'esistenza di insiemi non misurabili secondo Lebesgue, o il paradosso di Banach-Tarski (2) Queste applicazioni ri-

(2) Il paradosso di Banach-Tarski dice che una sfera piena può essere suddivisa in un numero finito di pezzi che possono essere ricomposti per formare due sfere uguali alla sfera di partenza — si veda [Wa] e la sezione 6 nella Parte II di questo articolo.

guardano oggetti in qualche modo astratti (sottoinsiemi arbitrari di $\mathbb{R}^n$) e sorge quindi naturale la domanda: è necessario usare AC per dimostrare teoremi sugli oggetti più concreti del mondo matematico, i numeri naturali? Per esempio: è possibile dimostrare l'ultimo teorema di Fermat *senza* usare l'assioma di scelta? La dimostrazione di Wiles e Taylor coinvolge una gran quantità di risultati di matematica che utilizzano il Lemma di Zorn in maniera esplicita, o che si basano su risultati che a loro volta dipendono da AC. Quindi, anche conoscendo a fondo questa difficile dimostrazione, non potremmo facilmente verificare se la risposta alla nostra domanda sia affermativa. Tuttavia la risposta è affermativa, poiché se un enunciato σ che menziona solo numeri naturali è dimostrabile in ZFC allora è dimostrabile in ZF. Questo è un esempio di teorema di assolutezza — in questo caso una semplice applicazione di L, l'universo costruibile, che vedremo nella sezione 4.

Esistono ulteriori usi delle tecniche insiemistiche che ci paiono anche più interessanti. In [T], per esempio, si ottengono nuovi importanti risultati sugli insiemi compatti di funzioni di classe di Baire 1; questi sono comunemente noti come compatti di Rosenthal e rivestono un'importanza fondamentale nello studio della geometria degli spazi di Banach. Più che i risultati in sé (ottenuti in ZFC) ci affascina l'uso del *forcing* e dell'assolutezza. Scrive S. Todorčević in [T, p. 1183]:

> ..., while the really new idea is the use of forcing which is not only crucially employed in some of the proofs (especially of Theorem 1), but was also the guiding force behind the discovery of these results.

Un'altra interessante applicazione dell'assolutezza alla teoria delle successioni uniformemente distribuite si trova in [G].

In questo articolo, che si divide in due parti strettamente collegate, ma che possono essere lette indipendentemente, cercheremo di illustrare alcuni risultati di assolutezza e le loro applicazioni, evitando gli aspetti tecnici e le dimostrazioni. In questa prima parte, dopo aver richiamato le nozioni di base in sezione 2, vedremo qualche esempio di risultato di indipendenza proveniente da altre aree della matematica. Nelle sezioni 4 e 5 daremo qualche cenno sull'universo costruibile e sul metodo del *forcing* e vedremo come gli enunciati della teoria dei numeri non siano influenzati da assunzioni quali AC o CH. Nella seconda parte (sezioni 6-9) vedremo come estendere questi risultati agli enunciati dell'analisi: dopo aver introdotto le nozioni di base della teoria descrittiva degli insiemi nella sezione 6, enunceremo il teorema di assolutezza di Shoenfield nella sezione 7, mentre nell'ultime due sezioni vedremo come i teoremi di assolutezza siano strettamente connessi alla teoria dei grandi cardinali, una delle aree più vitali della teoria degli insiemi.

Da parte del lettore non presupponiamo nessuna particolare conoscenza tecnica di logica o teoria degli insiemi, se non una generica buona disposizione per le astrazioni. La trattazione è fortemente condizionata dalla scelta degli argomenti, per cui molte aree centrali della teoria degli insiemi non sono neppure menzionate. Anche i riferimenti storici sono ridotti al minimo — il lettore può consultare [M] per i risultati classici e [Ka] per la storia più recente. Per chi volesse approfondire gli argomenti qui trattati consigliamo [Ku], [J], [DW] e [EM] per le sezioni 2-5, [Ke] per la sezione 6 e [Ka] per le sezioni 7-8.

2. – L'universo V degli insiemi.

Nella trattazione rigorosa della teoria degli insiemi, a differenza di quanto si fa nella trattazione intuitiva, non ci sono elementi che non siano insiemi, cioè ogni elemento di un insieme è un insieme. Per esempio un numero reale è una sezione di Dedekind, cioè un sottoinsieme di $\mathbb{Q}$; un razionale è una classe di equivalenza di coppie di interi; e così via. L'insieme più semplice è $\emptyset$, l'insieme vuoto. Ogni altro insieme è generato da esso mediante le operazioni dell'insieme potenza

$$\wp(x) := \{y \mid y \subseteq x\}$$

e di unione generalizzata: dato un insieme x, poiché i suoi elementi sono a loro volta insiemi, esso può essere considerato una famiglia di insiemi $x = \{z \mid z \in x\}$ e quindi $\bigcup x = \bigcup_{z \in x} z$ è l'unione di tutti gli insiemi z che appartengono ad x, vale a dire

$$\bigcup x := \{y \mid \exists z \in x (y \in z)\}.$$

Consideriamo gli insiemi:

$$\begin{aligned}
V_0 &= \emptyset \\
V_1 &= \wp(V_0) = \{\emptyset\} \\
V_2 &= \wp(V_1) = \{\emptyset, \{\emptyset\}\} \\
V_3 &= \wp(V_2) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\} \\
&\vdots
\end{aligned}$$

Quindi $V_{n+1} = \wp(V_n)$ è la collezione di tutti i 2^n insiemi ottenibili da $\emptyset$ con al più n livelli di parentesi graffe. I numeri naturali sono definiti induttivamente come

$$0 = \emptyset \quad \text{e} \quad n + 1 = n \cup \{n\},$$

così che $n = \{0, 1, \dots, n-1\}$ ed $n < m$ se e solo se $n \in m$. Dato che non c'è motivo per fermarsi a questo punto, possiamo definire

$$\omega = \{0, 1, \dots, n, \dots\}$$

l'insieme dei numeri naturali e

$$V_\omega = \bigcup_{n \in \omega} V_n$$

l'insieme di tutti gli insiemi ottenibili a partire da $\emptyset$ con un numero finito di parentesi graffe. Ripetendo la costruzione di prima otteniamo una generalizzazione dei numeri naturali

$$\omega + 1, \quad \omega + 2, \ \dots \quad \omega + \omega = \bigcup_{n \in \omega} \omega + n, \quad \omega + \omega + 1, \dots$$

dove $\alpha + 1 := \alpha \cup \{\alpha\}$. Questi oggetti si chiamano *ordinali* e sono generati mediante le operazioni di successore ($\alpha \mapsto \alpha + 1$) e di unione generalizzata. Le lettere greche minuscole (α, β, γ, etc.) variano sugli ordinali, con l'avvertenza che la lettera ω denota un ordinale ben preciso, l'insieme dei numeri naturali. L'ordinamento sugli ordinali è dato dalla relazione di appartenenza, cioè

$$\alpha < \beta \Leftrightarrow \alpha \in \beta$$

e questo ordinamento è un buon ordine. Infatti ogni insieme bene ordinato è isomorfo ad uno ed un solo ordinale. Quelli della forma $\alpha + 1$ si dicono *ordinali successori*, gli altri, se diversi da 0, si dicono *ordinali limite.*

Alcuni ordinali sono in biezione con ordinali più piccoli: per esempio $\omega + 1$ è in biezione con ω mediante $n \mapsto n + 1$ e $\omega \mapsto 0$. Più generalmente, se $\alpha \geqslant \omega$ allora $\alpha + 1$ è in biezione con α. Gli ordinali che non possono essere messi in biezione con ordinali più piccoli si dicono *cardinali.* Essi sono perciò dei particolari numeri ordinali. I numeri naturali ed ω sono chiaramente dei cardinali e non è difficile convincersi che dato un ordinale α si può sempre trovare un cardinale $\kappa > \alpha$. La funzione che enumera tutti i cardinali infiniti è denotata con la lettera $\aleph$. Quindi $\aleph_0$ è ω, il primo cardinale infinito, $\aleph_1$ è il più piccolo cardinale più che numerabile, $\aleph_2$ è il cardinale immediatamente più grande, ..., $\aleph_\omega$ è l'estremo superiore degli $\aleph_n$. In generale

$$\begin{aligned} \aleph_0 &= \omega \\ \aleph_{\alpha+1} &= \text{il più piccolo cardinale } \kappa > \aleph_\alpha \\ \aleph_\lambda &= \sup\{\aleph_\alpha \mid \alpha < \lambda\} \quad (\lambda \text{ limite.}) \end{aligned} \tag{1}$$

Senza troppo sforzo di fantasia, i cardinali della forma $\aleph_{\alpha+1}$ si dicono cardinali successori, quelli della forma $\aleph_\lambda$ con λ limite, si dicono cardinali limite.

La successione dei V_α è data da

$$\begin{aligned} V_0 &= \emptyset \\ V_{\alpha+1} &= \wp(V_\alpha) \\ V_\lambda &= \bigcup_{\alpha<\lambda} V_\alpha \quad (\lambda \text{ limite}) \end{aligned} \tag{2}$$

ed è tale che $V_\alpha \subset V_\beta$ e $V_\alpha \in V_\beta$, se $\alpha < \beta$. L'universo degli insiemi è la collezione di tutti gli insiemi che appartengono a qualche V_α,

$$V = \bigcup_\alpha V_\alpha,$$

dove α varia sulla famiglia degli ordinali.

Come lo spazio $\mathbb{R}^3$ è assiomatizzato dalla geometria Euclidea, così l'universo degli insiemi V è assiomatizzato dal sistema ZF, introdotto da E. Zermelo e A. Fraenkel. Gli assiomi di ZF sono formulati nel linguaggio $\mathcal{L}$ contenente solo il simbolo primitivo di appartenenza «$\in$,» le variabili e gli usuali simboli logici: $=$, $\neg$, $\vee$, $\&$, $\Rightarrow$, $\Leftrightarrow$, $\exists$ e $\forall$. Per non appesantire l'esposizione enunceremo gli assiomi di ZF nel linguaggio informale comunemente usato in matematica, limitandoci a formalizzare in $\mathcal{L}$ qualcuno di essi. Il lettore può facilmente formalizzare gli altri oppure consultare un qualsiasi testo, per esempio [J] o [Ku].

Estensionalità: due insiemi x e y coincidono se hanno gli stessi elementi. La sua traduzione in $\mathcal{L}$ è

$$\forall x \forall y (x = y \Leftrightarrow \forall z (z \in x \Leftrightarrow z \in y)).$$

Coppia: dati due insiemi x e y c'è un insieme z che li contiene entrambi come unici elementi.

Unione: per ogni insieme x c'è un insieme $y = \bigcup x$.

Potenza: per ogni insieme x c'è un insieme $y = \wp(x) = \{w \mid w \subseteq x\}$.

Fondazione: la relazione di appartenenza è ben fondata (3) su ogni insieme non vuoto x, cioè se $x \neq \emptyset$ c'è un $y \in x$ tale che $y \cap x = \emptyset$.

Quest'assioma garantisce che non esistono $\in$-catene discendenti infinite $\ldots x_3 \in x_2 \in x_1 \in x_0$, né $\in$-cicli $x_0 \in x_n \in x_{n-1} \in \ldots \in x_1 \in x_0$. In particolare non esistono insiemi che appartengano a se stessi e quindi $x \notin x$ per ogni x. In presenza degli altri assiomi, la fondazione garantisce che ogni insieme appartiene ad un qualche V_α, cioè $V = \bigcup_{\alpha \in \mathrm{Ord}} V_\alpha$.

Infinito: c'è un insieme x contenente $\emptyset$ chiuso sotto l'operazione $y \mapsto y \cup \{y\}$ (e quindi tale che $\omega \subseteq x$). Vale a dire

$$\exists x (\emptyset \in x \ \& \ \forall y \in x (y \cup \{y\} \in x)).$$

Ad essere pignoli, questa non è una formula del nostro linguaggio,

(3) Ricordiamo che una relazione R è ben fondata su un insieme X se ogni $Y \subseteq X$ non vuoto ammette un elemento R-minimale.

poiché contiene simboli come $\emptyset$ e $y \cup \{y\}$, ma è facilmente traducibile in una formula ufficiale di $\mathcal{L}$, dato che $z = \emptyset \Leftrightarrow \neg \exists t(t \in z)$ e $w = y \cup \{y\} \Leftrightarrow \forall u(u \in w \Leftrightarrow u \in y \vee u = y)$.

Separazione: data una proprietà di insiemi P, per ogni insieme x c'è un insieme y formato da tutti gli z in x che soddisfano P. Per esempio, se $x = \mathbb{C}$ e $P(z)$ è la proprietà «essere radice del polinomio f,» l'assioma di separazione ci garantisce che $y = \{z \in \mathbb{C} \,|\, f(z) = 0\}$ è un insieme. In generale, le proprietà P vengono individuate mediante una formula $\varphi(z, x, p)$ e l'assioma di separazione diventa

$$\forall p \forall x \exists y \forall z(z \in y \Leftrightarrow z \in x \;\&\; \varphi(z, x, p)).$$

(Nell'esempio il parametro p è il polinomio f.)

Rimpiazzamento: se x è un insieme e $P(z, w)$ è una proprietà di coppie di insiemi che definisce una funzione su x, cioè $\forall z \in x \exists ! w$ per cui vale $P(z, w)$, allora c'è un insieme y formato da tutti questi w. Vale a dire: se $\varphi(z, w, x, p)$ è una formula, allora

$$\forall p \forall x \big(\forall z \in x \exists ! w \, \varphi(z, w, x, p) \Rightarrow \\ \exists y \forall w (w \in y \Leftrightarrow \exists z \in x \, \varphi(z, w, x, p))\big).$$

L'espressione «$\exists ! w$» significa «esiste uno ed un solo w» e non è un simbolo ufficiale di $\mathcal{L}$. Tuttavia possiamo ricondurci a $\mathcal{L}$ sostituendo le espressioni del tipo «$\exists ! w \, \psi(w)$» con «$\exists w(\psi(w) \;\&\; \forall w'(\psi(w') \Rightarrow w' = w))$.» L'idea è che l'immagine di un insieme mediante una funzione definita da una proprietà è un insieme.

Questi sono gli assiomi di ZF. La separazione (4) ed il rimpiazzamento sono in realtà degli *schemi di assiomi*, uno per ogni formula e quindi ZF ha infiniti assiomi. Se a questa lista aggiungiamo l'assioma di scelta, AC, otteniamo la teoria ZFC. Per formulare l'assioma di scelta dobbiamo introdurre il concetto di funzione e quindi di coppia ordinata: dati due insiemi a e b la *coppia ordinata* (a, b) è l'insieme

$$(a, b) := \{\{a\}, \{a, b\}\}.$$

(4) Il lettore più attento avrà notato che tanto nella separazione quanto nel rimpiazzamento si deve richiedere che y non occorra libera in φ.

Questa definizione può apparire un po' bizzarra, ma assolve il suo scopo, dato che $(a, b) = (a', b')$ se e solo se $a = a'$ e $b = b'$. Siamo ora in grado di enunciare l'assioma di

Scelta: se x è una famiglia di insiemi non vuoti, allora c'è una funzione f tale che $f(y) \in y$ per tutti gli $y \in x$.

Nella trattazione intuitiva la cardinalità di un insieme X è definita come la classe degli Y equipotenti ad X. Tuttavia se $X \neq \emptyset$, quest'ultima è una classe propria e non un insieme. Definiamo invece la *cardinalità* di X come

$$|X| = \text{il più piccolo ordinale in biezione con } X\,.$$

Questa definizione è ben data poiché l'assioma di scelta implica che ogni insieme è bene-ordinabile e quindi in biezione con qualche ordinale, ed è facile verificare che $|X|$ è un cardinale. Se κ, λ sono cardinali

$$^{\lambda}\kappa = \{f | f : \lambda \to \kappa\}$$

è l'insieme delle funzioni da λ in κ e

$$\kappa^{\lambda} = |{}^{\lambda}\kappa| \tag{3}$$

è la cardinalità dell'insieme delle funzioni da λ in κ. (Usiamo simboli tipografici diversi per distinguere l'insieme delle funzioni dall'ordinale che ne misura la cardinalità.) Identificando i sottoinsiemi con le funzioni caratteristiche vediamo che $2^{\kappa} = |\wp(\kappa)|$ e quindi

$$2^{\aleph_0} = |{}^{\omega}2| = |\wp(\omega)| = |\mathbb{R}|\,.$$

L'*ipotesi del continuo*, CH, è

$$2^{\aleph_0} = \aleph_1,$$

l'*ipotesi generalizzata del continuo*, GCH, è

$$\forall\alpha \in \mathrm{Ord}\,(2^{\aleph_\alpha} = \aleph_{\alpha+1})\,.$$

Sottolineiamo che $\aleph_1$ è un ordinale (anzi: un cardinale) ben preciso, definito indipendentemente dalla cardinalità di $\mathbb{R}$: è il più piccolo ordinale infinito non in biezione con ω. Per (3) $2^{\aleph_0}$ è l'unico cardinale in biezione con ${}^{\omega}2$ e quindi con $\mathbb{R}$. Per il teorema di Cantor $2^{\aleph_0} \geqslant \aleph_1$.

L'ipotesi del continuo dice che $2^{\aleph_0}$ assume il più piccolo valore consentito.

Notiamo infine che, sebbene in ZF (o in ZFC) ufficialmente si parli solo di insiemi, in pratica ci si imbatte spesso in collezioni quali V, l'universo degli insiemi, oppure Ord, la classe degli ordinali, che sono troppo grandi per essere insiemi. Sono quegli oggetti che poco sopra chiamavamo proprietà, ma che sono noti comunemente come *classi proprie.* Poiché una classe propria è della forma $\{x \mid \varphi(x, p)\}$ essa è completamente identificata dalla formula φ e dall'insieme p.

3. – Qualche risultato di indipendenza.

Ricordiamo che una formula di $\mathcal{L}$ è un enunciato se non contiene variabili libere, cioè ogni occorrenza di variabile è vincolata da un quantificatore. Per esempio, la formula $\varphi(f, x)$ che asserisce «la funzione $f : \mathbb{R} \to \mathbb{R}$ è continua nel punto x» non è un enunciato, dato che f ed x sono libere di variare, mentre $\exists f \forall x\, \varphi(f, x)$ è l'enunciato che esiste una funzione continua reale di variabile reale. Gli assiomi di ZFC sono degli enunciati. Per il Primo Teorema di Incompletezza di Gödel, esistono enunciati σ che sono *indipendenti da* ZFC, il che vuol dire che non sono né dimostrabili né confutabili in ZFC. Per i risultati di K. Gödel (1938) e P. J. Cohen (1963) CH e GCH sono esempi di enunciati indipendenti. Quindi ZFC non caratterizza completamente V. Ovviamente lo stesso si può dire di ZF e in questo caso possiamo prendere AC come enunciato indipendente σ. In questa sezione illustreremo il fenomeno dell'indipendenza da ZFC con qualche esempio proveniente da varie parti della matematica.

Analisi reale. Un insieme $X \subseteq \mathbb{R}$ si dice di *misura fortemente nulla* se per ogni successione di reali positivi $\varepsilon_n \to 0$ è possibile trovare intervalli aperti I_n tali che $X \subseteq \bigcup_n I_n$ e la lunghezza di I_n è $< \varepsilon_n$. Ogni insieme di misura fortemente nulla è di misura (di Lebesgue) nulla, dato che nell'usuale definizione di insieme di misura nulla gli I_n possono essere presi unioni finite di intervalli aperti. Le due nozioni non coincidono dato che l'insieme ternario di Cantor è un insieme di misura nulla che non è di misura fortemente nulla. Ogni insieme numerabile è di misura fortemente nulla ed Emile Borel congetturò l'implicazione inversa; cioè la *congettura di Borel*, per brevità BC, è l'affermazione

$$\forall X \subseteq \mathbb{R} (X \text{ è di misura fortemente nulla } \Rightarrow |X| \leqslant \aleph_0).$$

Tuttavia mediante l'ipotesi del continuo è possibile costruire un sottoinsieme $X \subseteq \mathbb{R}$ più che numerabile di misura fortemente nulla, cioè

$$\mathsf{CH} \Rightarrow \neg \mathsf{BC}.$$

La possibilità di eliminare CH da questa costruzione o la possibilità di dimostrare l'implicazione inversa (cioè che BC $\Leftrightarrow$ ¬ CH) rimasero aperte fino all'introduzione del *forcing*. Sin dalle prime applicazioni del *forcing* si osservò che ¬ BC è compatibile con ¬ CH e nel 1976 R. Laver dimostrò che la coerenza della congettura di Borel, provando così che BC è indipendente da ZFC.

Teoria della misura. Sia X uno spazio di Hausdorff e $\boldsymbol{B}(X)$ la σ-algebra dei Boreliani. Una misura $\mu : \boldsymbol{B}(X) \to [0, +\infty]$ si dice

regolare se per ogni $B \in \boldsymbol{B}(X)$

$$\begin{aligned} \mu(B) &= \inf\{\mu(U) \mid U \text{ aperto e } B \subseteq U\} \\ &= \inf\{\mu(K) \mid K \text{ compatto e } K \subseteq B\}; \end{aligned}$$

di Radon se ogni punto ha un intorno di misura finita, cioè

$$\forall x \in X \, \exists U (U \text{ aperto}, \ x \in U \text{ e } \mu(U) < \infty);$$

σ-finita se c'è una partizione $\{X_n\}_n$ dello spazio X tale che gli X_n sono Borel e $\mu(X_n) < \infty$.

Un problema più volte considerato in teoria della misura è se ogni misura di Radon regolare sia necessariamente σ-finita. R. Gardner e W. Pfeffer (1979) hanno dimostrato che la risposta è negativa se si assume CH: usando l'ipotesi del continuo è possibile costruire uno spazio X ed una misura regolare di Radon su X che non è σ-finita. D'altro canto S. Todorčević ha dimostrato che è consistente assumere che tutte le misure di Radon regolari sono σ-finite. Quindi l'enunciato «Tutte le misure di Radon regolari sono σ-finite» è indipendente da ZFC.

Algebre di Banach. Sia K uno spazio compatto di Hausdorff e sia $C(K, \mathbb{C})$ l'algebra delle funzioni continue su K a valori complessi dotato della topologia della convergenza uniforme, cioè indotta dalla norma uniforme

$$\|f\|_\infty = \sup \{ |f(x)| \mid x \in K \} .$$

La *congettura di Kaplansky* (1948), KC per brevità, asserisce che la struttura topologica è completamente determinata dalla struttura algebrica: Ogni norma su $C(K, \mathbb{C})$ è equivalente alla norma uniforme, cioè è compatibile con la topologia di $C(K, \mathbb{C})$.

Questa congettura è equivalente al seguente problema della *continuità automatica*: ogni omomorfismo algebrico tra due algebre di Banach commutative è necessariamante continuo. G. Dales e, indipendentemente, J. Esterle dimostrarono nel 1976 che, assumendo CH, è possibile costruire per ogni K una norma su $C(K, \mathbb{C})$ non equivalente alla norma uniforme, cioè $\mathsf{CH} \Rightarrow \neg\, \mathsf{KC}$. Viceversa R. Solovay, basandosi su una costruzione di W. H. Woodin, dimostrò, sempre nel 1976, che KC è consistente. Inoltre, come nel caso della congettura di Borel, KC non è equivalente alla negazione di CH, dato che Woodin ha dimostrato che $\neg\, \mathsf{KC} + \neg\, \mathsf{CH}$ è consistente.

Analisi complessa. Consideriamo il problema di classificare i domini (cioè aperti connessi) di $\mathbb{C}$ a meno di biolomorfismo. Data una famiglia $\mathcal{F}$ di domini, vorremmo trovare degli invarianti per $\mathcal{F}$, cioé delle funzioni $\Phi : \mathcal{F} \to I$ tali che se $D_1, D_2 \in \mathcal{F}$ sono biolomorfi, in simboli $D_1 \sim D_2$, allora $\Phi(D_1) = \Phi(D_2)$. Un invariante è completo se vale anche il viceversa, cioè se $\Phi(D_1) = \Phi(D_2)$ implica che $D_1 \sim D_2$. Un invariante completo esiste sempre: basta prendere $I = \mathcal{F}/\sim$ e Φ la proiezione canonica. Tuttavia lo scopo di trovare degli invarianti (possibilmente completi) è proprio quello di analizzare meglio la struttura — in genere assai complessa — di $\mathcal{F}/\sim$, per cui si richiede che l'insieme I sia ragionevolmente concreto e che la funzione Φ sia semplice. Più precisamente chiederemo che I sia uno spazio Polacco [5] e che Φ sia definibile nel linguaggio $\mathcal{L}$. Poiché dati due spazi

[5] Uno spazio Polacco è uno spazio separabile metrico completo. Rimandiamo il lettore a [Ke] o alla sezione 6 della parte II per maggiori dettagli.

Polacchi più che numerabili c'è sempre una biezione definibile tra di loro, possiamo supporre che $I = \mathbb{C}$ oppure $I = \prod_n \mathbb{C}$.

In alcuni casi è facile trovare un invariante completo, per esempio se $\mathscr{F}$ è l'insieme dei domini semplicemente connessi (il teorema di Riemann) o se $\mathscr{F}$ è l'insieme delle regioni anulari (il rapporto tra i raggi). Altri invarianti non sono completi, per esempio la funzione che conta il numero di «buchi» del dominio. J. Becker, W. Henson e L. Rubel hanno dimostrato in [BHR] che l'esistenza di un invariante completo per

$$\mathscr{F} = \{\mathbb{C} \setminus S \mid S \subseteq \mathbb{Z}\}$$

è indipendente da ZFC e da CH. Vale a dire né CH né la sua negazione implicano o refutano l'esistenza di un invariante completo per $\mathscr{F}$. Questo risultato è stato generalizzato al caso di più variabili complesse da [LR].

Operatori compatti. Consideriamo l'algebra $L(H)$ degli operatori limitati su H, spazio di Hilbert separabile di dimensione infinita, e sia K l'ideale degli operatori compatti. In [BPS] è stato posto il seguente problema: è possibile che

($\star$) K è somma di due ideali propri di $L\ (H)$ Ø

Andreas Blass e Gary Weiss hanno dimostrato in [BlW] che la risposta è affermativa se si assume l'ipotesi del continuo, cioè CH $\Rightarrow$ ($\star$). Viceversa Blass in [Bl], usando dei risultati di S. Shelah sugli ultrafiltri, ha dimostrato che $\neg(\star)$ è consistente con ZFC.

Gruppi abeliani infiniti. In questo esempio «gruppo» significa «gruppo abeliano infinito.» Un gruppo A si dice libero se ammette una base $X \subseteq A$, cioè un insieme di generatori linearmente indipendenti su $\mathbb{Q}$. Equivalentemente, A è libero se e solo se $A \cong \bigoplus_{i \in X} \mathbb{Z}$. Le basi $X \subseteq A$ possono essere caratterizzate così: per ogni omomorfismo suriettivo $f : B \to A$ ed ogni funzione $g : X \to B$ tale che $f(g(x)) = x$ per tutti gli $x \in X$, è possibile trovare un omomorfismo iniettivo $\widehat{g} : A \to B$ che estende g e tale che $f(\widehat{g}(a)) = a$ per tutti gli $a \in A$. Un gruppo A è di Whitehead se per ogni omomorfismo suriettivo $f : B \to A$ con $\ker(f) = \mathbb{Z}$ c'è un omomorfismo iniettivo $g : A \to B$ tale che $f(g(a)) = a$ per tutti gli $a \in A$. Quindi tutti i gruppi liberi sono di Whitehead e si dimostra che tutti i gruppi di Whitehead numerabili sono liberi. Il problema seguente, formulato da J. H. C. Whitehead nel 1955, dice:

È vero che ogni gruppo di Whitehead è libero?

S. Shelah ha dimostrato nel 1973 che la risposta a questo problema è indipendente da ZFC. Ma, a differenza dagli esempi precedenti, CH non è sufficiente per decidere questo problema.

Topologia generale. Consideriamo un insieme linearmente ordinato $(X, <)$ senza primo né ultimo elemento che sia connesso nella topologia generata dagli intervalli aperti. M. Suslin dimostrò (1920) che se X è separabile, cioè se contiene un insieme denso e numerabile, allora X è isomorfo come insieme linearmente ordinato (e quindi omeomorfo come spazio topologico) ad $\mathbb{R}$. Suslin si domandò se l'ipotesi di separabilità può essere indebolita richiedendo soltanto che ogni famiglia di aperti disgiunti sia al più numerabile. Una retta di Suslin è un ordine lineare $(X, <)$ senza primo né ultimo elemento, connesso non isomorfo ad $\mathbb{R}$ e tale che ogni famiglia di aperti a due a due disgiunti sia al più numerabile. L'ipotesi di Suslin (SH) è l'affermazione che le rette di Suslin non esistono. I risultati di T. Jech, R. Jensen, D.A. Martin e R. Solovay alla fine degli anni '60 dimostrarono che SH è indipendente da ZFC e, come nel caso del problema di Whitehead, pure da $\mathsf{ZFC} + \mathsf{CH}$.

4. – Gli insiemi costruibili.

Consideriamo ora la seguente situazione, abbastanza frequente in matematica: si parte da una struttura specifica (nel nostro caso V), per analizzarla si introduce un sistema di assiomi (ZF), e poi si scopre che ci sono molte altre strutture che soddisfano gli assiomi introdotti. Nel nostro caso queste strutture sono i *modelli* di ZF. Un modello di ZF — o più in generale, di una collezione T di enunciati di $\mathcal{L}$ — è un insieme non vuoto M ed una relazione binaria $E \subseteq M \times M$ tale che tutti gli enunciati di T sono veri in M quando la relazione di appartenenza viene re-interpretata come la relazione E. Più precisamente, se φ è una formula di $\mathcal{L}$, allora $\varphi^{M,E}$ (o semplicemente φ^M se E è chiaro dal contesto) è la formula che si ottiene sostituendo tutte le occorrenze del simbolo «$\in$» con «E» e poi tutti i quantificatori «$\forall x$» ed «$\exists x$» con «$\forall x \in M$» ed «$\exists x \in M$,» rispettivamente. Si dice che $\varphi^{M,E}$ è la relativizzazione di φ ad (M, E) ed asserire $\varphi^{M,E}$ significa dire che φ è vera in (M, E). Per esempio, dire che «l'assioma di estensionalità vale in (M, E)» equivale a dire che

$$\forall x \in M \, \forall y \in M (\forall z \in M (zEx \Leftrightarrow zEy) \Rightarrow x = y).$$

Un modello arbitrario è un oggetto troppo difficile da maneggiare, per cui ci si concentra sui *modelli transitivi*, cioè modelli della forma (M, E) dove M è transitivo ed E è la relazione di appartenenza ristretta ad M, cioè $E = \{(x, y) \in M \times M \mid x \in y\}$. Ricordiamo che una struttura M è transitiva se M è un insieme o una classe propria e $x \in y$ & $y \in M \Rightarrow x \in M$; gli ordinali e i V_α sono insiemi transitivi, mentre, per esempio, l'insieme dei numeri pari non lo è. Vediamo qualche esempio di modello transitivo:

(i) Ogni insieme transitivo è un modello degli assiomi di estensionalità e fondazione.

(ii) V_ω è un modello per $\mathsf{ZFC} - \mathsf{Inf} + \neg\, \mathsf{Inf}$, dove Inf è l'assioma dell'infinito.

(iii) $V_{\alpha+1}$ non soddisfa gli assiomi della coppia, potenza e separazione.

(iv) Se $\lambda \geqslant \omega$, allora tutti gli assiomi di ZFC, con la eventuale eccezione del rimpiazzamento, valgono in V_λ. Se V_λ è un modello di ZFC allora λ è un cardinale più grande di $\aleph_0$, $\aleph_{\aleph_0}$, $\aleph_{\aleph_{\aleph_0}}$, ...

(Per la dimostrazione in (iv) che AC vale in V_λ si deve supporre che AC valga in V, vale a dire bisogna lavorare in ZFC, mentre per dimostrare in (ii) che AC vale in V_ω è sufficiente lavorare in ZF.)

Se M è una classe propria transitiva che soddisfa gli assiomi di ZF (come nel caso di V) o più in generale di una lista T di enunciati di $\mathcal{L}$, diremo che M è un *modello interno* di ZF, ovvero di T. Cominciamo a guardare i modelli interni di ZF e ZFC. Riguardando la costruzione dei V_α nella formula (2) vediamo che allo stadio successore prendiamo *tutti* i sottoinsiemi di V_α per formare $V_{\alpha+1}$. Se invece prendiamo solo quelli definibili otteniamo gli *insiemi costruibili.* Un sottoinsieme x di un insieme transitivo M si dice *definibile in* M *mediante la formula* φ *e i parametri* $p_1, \ldots, p_n \in M$ se x è l'insieme dei $t \in M$ per cui $\varphi(t, \vec{p})$ è vera in M, cioè

$$x = \{t \in M \mid \varphi(t, p_1, \ldots, p_n)^M\}. \tag{4}$$

Def(M) è l'insieme di tutti i sottoinsiemi siffatti, al variare di φ e $\vec{p}$. In altre parole, gli insiemi in Def(M) sono quelli ottenibili da M mediante l'assioma di separazione. (Abbiamo dovuto usare una sequenza finita di parametri invece di un singolo insieme perché M, un insieme transitivo arbitrario, non è necessariamente chiuso per coppie ordinate.) La *gerarchia dei costruibili,* introdotta da Gödel nel 1938, è così definita:

$$\begin{aligned} L_0 &= \emptyset \\ L_{\alpha+1} &= \mathrm{Def}(L_\alpha) \\ L_\lambda &= \bigcup_{\alpha<\lambda} L_\alpha \quad (\lambda \text{ limite}) \\ L &= \bigcup_{\alpha \in \mathrm{Ord}} L_\alpha. \end{aligned} \tag{5}$$

Un risultato fondamentale è il seguente: si dimostra in ZF (senza alcun uso dell'assioma di scelta) che L è un modello interno per ZFC. Come corollario immediato si ha che se ZF è consistente [6], allora anche ZFC lo è: se ZFC dimostrasse un assurdo, allora questa dimostrazione dovrebbe valere in L e quindi avremmo una contraddizione in ZF. Per il secondo Teorema di Gödel, ogni teoria sufficientemente potente (per esempio ZF) non può dimostrare la propria coerenza: quindi non possiamo sperare di dimostrare (in ZF) la non contraddittorietà dell'assioma di scelta con gli altri assiomi di ZF. L'argomento qui sopra dimostra soltanto che *se* ZF è consistente *allora* anche ZFC è consistente e la dimostrazione di tutto questo avviene in (una sottoteoria molto debole di) ZF. In un certo senso, la dimostrazione di consistenza di ZFC re-

[6] Una teoria T si dice consistente se da T non è possibile dedurre una contraddizione da T.

lativa a ZF è analoga alla dimostrazione della consistenza della geometria iperbolica relativa alla geometria Euclidea, dove il piano di Poincaré gioca il ruolo analogo ad L.

Gli L_α formano una catena ascendente di insiemi transitivi,

$$L_0 \subset L_1 \subset \ldots \subset L_\alpha \subset \ldots ,$$

e si dimostra che

$$\alpha = L_\alpha \cap \mathrm{Ord} = V_\alpha \cap \mathrm{Ord}$$

e $L_\alpha \subseteq V_\alpha$. Se $\alpha \leqslant \omega$, allora $L_\alpha = V_\alpha$, ma $L_{\omega+1} \neq V_{\omega+1}$: poiché ci sono solo $\aleph_0$ formule e parametri in $L_\omega = V_\omega$, allora $L_{\omega+1}$ è numerabile, mentre $V_{\omega+1}$ ha la potenza del continuo. Anche se gli L_α crescono più lentamente dei V_α, potrebbe tuttavia accadere che per α arbitrariamente grandi $V_\alpha = L_\alpha$ e quindi $V = L$. Questa affermazione è tuttavia indipendente da ZFC: gli abitanti di L ritengono che tutti gli insiemi siano costruibili, cioè $(V = L)^L$, mentre gli abitanti dei modelli ottenuti mediante il metodo del *forcing* (vedi sezione 5) ritengono che $V \neq L$.

Riprendendo l'esempio della sezione 1, supponiamo che σ sia un enunciato riguardante i numeri naturali, cioè un enunciato in cui i quantificatori sono applicati ad oggetti che variano, diciamo, su V_ω. Più precisamente diremo che σ è un enunciato *aritmetico* se è della forma φ^{V_ω}, cioè se σ è la relativizzazione di un enunciato φ di $\mathcal{L}$ a V_ω. Se $\mathsf{ZFC} \vdash \sigma$ allora, ragionando come nel paragrafo precedente, questa dimostrazione deve valere in L e quindi $\mathsf{ZF} \vdash \sigma^L$. Ma dato che i quantificatori di σ variano su $V_\omega = L_\omega \subset L$, ne segue che σ^L è σ. In altre parole

$$\mathsf{ZFC} \vdash \sigma \Rightarrow \mathsf{ZF} \vdash \sigma .$$

L'enunciato dell'ultimo teorema di Fermat

$$\forall x, y, z, n \in \omega (x, y, z > 0 \ \ \& \ \ n > 2 \Rightarrow x^n + y^n \neq z^n),$$

una volta opportunamente tradotto nel linguaggio $\mathcal{L}$, è aritmetico e quindi è dimostrabile in ZF. L'unica difficoltà consiste nel descrivere le operazioni aritmetiche mediante insiemi in V_ω: per esempio, la formula «$n + m = k$» è equivalente a dire che esiste una funzione $s \in V_\omega$ tale che $(n, m) \in \mathrm{dom}(s)$, $s(n, m) = k$ e s è definita induttivamente come l'addizione.

In modo analogo si vede che molti problemi aperti in teoria dei numeri e in combinatorica finita (la congettura di Goldbach, l'esistenza di infiniti primi gemelli, etc.) sono enunciati aritmetici.

Fino ad ora ci siamo occupati di AC. Si potrebbe obiettare che esso è un assioma comunemente accettato ed usato in matematica e che quindi non c'è motivo per eliminarlo dalle dimostrazioni di teoria dei numeri. Ma che dire di enunciati indipendenti da ZFC quali CH o GCH? È possibile dimostrare un risultato analogo a quanto sopra? La risposta è affermativa e la dimostrazione è la stessa di prima, dato che Gödel ha dimostrato che GCH vale in L. Inoltre l'analisi della struttura fine di L, dovuta principalmente a Ronald B. Jensen negli anni '70, ha consentito di distillare una serie di principi combinatoriali che valgono in L e che sono molto utili nello studio dei gruppi abeliani infiniti, spazi di Banach, teoria della misura, topologia generale, etc. (vedere [EM], [S]). Per esempio, in L tutti i gruppi di Whitehead sono liberi e c'è una retta di Suslin.

Riassumendo: l'universo dei costruibili di Gödel non solo ci consente di stabilire la consistenza relativa di $V = L$ (e quindi la consistenza relativa di tutte le sue conseguenze: AC, GCH, i vari principi combinatoriali, etc.), ma ci fornisce un metodo per dimostrare in ZF nuovi teoremi di teoria dei numeri e combinatorica finita. Vale a dire:

TEOREMA 4.1. – *Se σ è un enunciato aritmetico, allora*

$$\mathsf{ZFC} + V = L \vdash \sigma \quad \Rightarrow \quad \mathsf{ZFC} \vdash \sigma .$$

Sarebbe quindi utile generalizzare i ragionamenti fin qui fatti a classi di enunciati un po' più vaste, che siano in grado di parlare di numeri reali funzioni continue, etc. Una opportuna generalizzazione è possibile, ma richiede l'approccio più sofisticato della teoria descrittiva degli insiemi che vedremo nella sezione 7 nella Parte II. Limitiamoci per ora a vedere perché non è possibile generalizzare in modo ovvio quanto fatto fin qui. Benché in L possiamo fare tutte le costruzioni di ZFC, alcuni oggetti possono essere abbastanza diversi dalla loro controparte in V. Per esempio $\wp(\omega)^L = \{y \in L \mid y \subseteq \omega\}$ è ciò che L ritiene essere l'insieme delle parti di ω, ma è possibile che molti sottoinsiemi di ω non siano definibili in nessun L_α. In particolare è possibile (vale a dire: è consistente) che $\mathbb{R}^L$, l'insieme dei reali in L, non esaurisca tutto $\mathbb{R}$. In questo caso $\mathbb{R}^L$ è un sottocampo denso di $\mathbb{R}$ contenente tutti i reali calcolabili, quali i numeri algebrici, e, π, etc. Ricordiamo che un $x \in \mathbb{R}$ è *calcolabile* se esiste un algoritmo che su input n calcola la n-esima cifra dello sviluppo decimale di x. Non solo è possibile che $\mathbb{R} \neq \mathbb{R}^L$, è addirittura possibile che $\mathbb{R}^L$ sia numerabile in V: in questo caso c'è una biezione $f : \omega \rightarrow \mathbb{R}^L$, ma f non appartiene ad L e quindi gli abitanti di L sono del tutto all'oscuro dell'esistenza di queste biezioni. Un ulteriore esempio è dato dalla funzione $\aleph$ e dal concetto di cardinalità — se $\mathbb{R}^L$ è numerabile, allora anche $(\aleph_1)^L$ lo è. Un oggetto (come $\mathbb{R}$) o una operazione (come $\wp$) che variano a seconda del modello considerato si dicono *non assoluti*. Viceversa alcuni oggetti e costruzioni sono *assoluti* e non solo tra V e L, ma in generale tra modelli interni o modelli transitivi. Per esempio, se M è una struttura transitiva e x, $y \in M$ e $(x \subseteq y)^M$ allora $x \subseteq y$: infatti preso un $t \in x$, poiché M è transitivo, $t \in M$ e dato che per ipotesi $\forall t \in M(t \in x \Rightarrow t \in y)$, allora $t \in y$. Analogamente $x \subseteq y \Rightarrow (x \subseteq y)^M$ e quindi «essere un sottoinsieme» è un predicato assoluto:

$$x \subseteq y \Leftrightarrow (x \subseteq y)^M.$$

Altri esempi di nozioni assolute per strutture transitive M sono: $\emptyset$, ω, V_ω, essere un ordinale cioè $\mathrm{Ord} \cap M = (\mathrm{Ord})^M$, essere una funzione, essere un livello della gerarchia costruibile cioè $L_\alpha = (L_\alpha)^M$. Considerazioni sulla assolutezza/non-assolutezza di vari concetti saranno cruciali nella prossima sezione.

5. – Il metodo del *forcing*.

Nella sezione precedente abbiamo definito in ZF un modello interno di $\mathsf{ZFC} + \mathsf{GCH}$. Se tentiamo una costruzione simile per dimostrare

(6) $\qquad \mathsf{ZFC}$ è consistente $\Rightarrow$ $\mathsf{ZFC} + \neg\,\mathsf{CH}$ è consistente

ci imbattiamo immediatamente nel seguente problema. Supponiamo di aver definito in ZFC una classe propria transitiva M che soddisfa ZFC + $\neg$ CH. Allora il medesimo argomento ripetuto dentro L dovrebbe generare una classe propria M^L, la relativizzazione di M ad L, che soddisfa $\neg$ CH. Ma L è il più piccolo modello interno di ZF, nel senso che è contenuto in tutti i modelli interni di ZF, e quindi $M^L = L$, da cui $(\neg \mathsf{CH})^L$: assurdo.

Il metodo del *forcing*, introdotto da Paul J. Cohen nel 1963, è il seguente. Si parte da un *insieme* transitivo che sia un modello di ZFC e si cerca di costruire un altro modello transitivo $N \supset M$ di ZFC che abbia gli stessi ordinali di M, $\mathrm{Ord} \cap M = \mathrm{Ord} \cap N$, e che soddisfi l'enunciato che vogliamo dimostrare essere consistente, nel nostro caso $\neg$ CH. Dovremo allora aggiungere ad M molti nuovi reali, ma per far questo dobbiamo supporre che $\mathbb{R}^M$ sia piccolo rispetto ad $\mathbb{R}$. Quindi M non deve essere troppo grande. Ma ci sono modelli siffatti? Anzi, ci sono modelli di ZFC? La risposta è un po' problematica, dato che per il Teorema di Completezza di Gödel (sempre lui!) un sistema di assiomi T del linguaggio $\mathcal{L}$ è coerente se e solo se c'è un modello (7) (M, E) per gli assiomi di T, cioè $\varphi^{(M, E)}$ per ogni φ in T. Quindi per via del Secondo Teorema di Incompletezza non possiamo sperare di dimostrare in ZFC l'esistenza di un modello di ZFC, men che meno di un modello transitivo. Se non ci sono modelli di ZFC allora ZFC è inconsistente e quindi (6) vale banalmente. Quindi possiamo supporre che esista un modello di ZFC. Infatti richiediamo l'esistenza di un modello transitivo: sebbene questo non discenda dall'esistenza coerenza di ZFC, è solo un modesto rafforzamento dell'ipotesi «ZFC è consistente» e d'altra parte semplifica enormemente i calcoli. Inoltre, per il teorema di Löwenheim-Skolem [Ku, Teorema 1.11 p.156] se esiste un modello transitivo di una teoria T, allora c'è un modello *numerabile* e transitivo di T. L'esistenza di un modello numerabile M di ZFC può sembrare a prima vista contraddittoria: in V c'è una biezione $f : \omega \to M$ e quindi $f \subseteq M$, ma $f \notin \mathrm{Def}(M)$ e quindi gli abitanti di M non si rendono conto della numerabilità del loro

(7) Si noti: (M, E) deve essere un insieme, non una classe propria.

universo. Pare quindi ragionevole fare la seguente

(7) **Ipotesi:** C'è un modello M numerabile transitivo di ZFC.

Naturalmente nozioni e oggetti quali $\wp$, $\aleph$, etc. non sono assoluti tra V e M. Se $\xi = M \cap \mathrm{Ord}$, allora $\xi < \aleph_1$ e $\forall \alpha < \xi (L_\alpha \in M)$ per l'assolutezza della costruzione $\alpha \mapsto L_\alpha$ e quindi $L_\xi = L^M$. Essendo M un modello di ZFC, anche L_ξ lo è e quindi la nostra ipotesi poteva essere riformulata come: «Esiste un ordinale numerabile ξ tale che L_ξ è un modello di ZFC.» Noi assumeremo (7) per dare un'idea di che cos'è il metodo del *forcing* e alla fine della sezione indicheremo come eliminare quest'assunzione. Per una trattazione rigorosa e completa del *forcing* si rimanda il lettore a [J] e [Ku].

Fissiamo dunque un modello numerabile transitivo M di ZFC e sia $(\boldsymbol{P}, \leqslant) \in M$ un ordine parziale che chiameremo *nozione di forcing* o semplicemente *forcing*. Allora esiste un insieme G, detto $\boldsymbol{P}$-generico su M, ed esiste un modello numerabile transitivo $M[G]$ di ZFC tali che

- $\mathrm{Ord} \cap M = \mathrm{Ord} \cap M[G]$,
- $M \cup \{G\} \subseteq M[G]$,
- $M[G]$ è il più piccolo modello transitivo che contiene $M \cup \{G\}$.

Inoltre se $\boldsymbol{P}$ è non-banale, vale a dire

$$\forall p \in \boldsymbol{P}\, \exists q \leqslant p\, \exists r \leqslant p\, \neg \exists s \ (s \leqslant q \ \& \ s \leqslant r),$$

allora $G \notin M$ e quindi $M \subset M[G]$. Tutti i $\boldsymbol{P}$ che considereremo sono non-banali. Gli elementi di $\boldsymbol{P}$ sono approssimazioni del generico G e, contrariamente a quanto ci si aspetterebbe, $p < q$ significa che p è un'approssimazione *migliore* di q. La costruzione di $M[G]$ a partire da M e G ricorda la l'estensione di un campo k mediante un elemento $\xi \notin k$: si definisce in M una collezione di oggetti detti $\boldsymbol{P}$-nomi (i polinomi di $k[X]$), i quali, grazie a G, generano in V gli elementi di $M[G]$ (nell'analogia: $k[X] \ni p \mapsto p(\xi)$). L'esistenza di generici per $\boldsymbol{P}$ è garantita dalla numerabilità di M, ma la scelta del generico non è unica.

Vediamo qualche esempio.

ESEMPIO 1. – Supponiamo di voler aggiungere ad M un nuovo reale o, equivalentemente, una nuova funzione $G : \omega \to \omega$. Se diamo ad ω la topologia discreta e ad allo spazio di Baire

$$^{\omega}\omega = \{f \mid f\colon \omega \to \omega\} = \prod_{n \in \omega} \omega$$

la topologia prodotto, allora gli intorni di base possono essere presi della forma

$$\boldsymbol{N}_s := \{f \in {}^{\omega}\omega \mid f \supset s\}$$

con $s : n \to \omega$ e $n \in \omega$. Poiché G è completamente individuata dalla successione

$$\boldsymbol{N}_{G|0} \supset \boldsymbol{N}_{G|1} \supset \boldsymbol{N}_{G|2} \supset \dots$$

il problema di trovare la G si riconduce a cercare una successione di funzioni

$$p_0 \subset p_1 \subset p_2 \subset \dots$$

tali che $p_i\colon n_i \to \omega$ per qualche $n_i \in \omega$ e tali che $\bigcup_i p_i\colon \omega \to \omega$ sia l'oggetto generico cercato. Il *forcing per aggiungere un reale di Cohen* è $(\boldsymbol{P}_1, \leqslant)$ dove

$$\boldsymbol{P}_1 = \{p \mid p \text{ è una funzione, } \operatorname{dom}(p) \subset \omega, \ \operatorname{ran}(p) \subset \omega \text{ e } |p| < \omega\}$$

e $p \leqslant q \Leftrightarrow p \supseteq q$. Dato che $\boldsymbol{P}_1 \subseteq V_\omega \subset M$ è immediato che $(\boldsymbol{P}_1, \leqslant) \in M$. Inoltre $\boldsymbol{P}_1$ è non-banale e quindi $G \notin M$ per ogni $\boldsymbol{P}_1$-generico su M. I generici G per il *forcing* $\boldsymbol{P}_1$ si dicono *reali di Cohen su M* e sono tutti e soli gli elementi di ω^ω che appartengono a tutti gli aperti densi di ω^ω della forma $\bigcup_{s \in A} N_s$ con $A \subseteq \boldsymbol{P}$ e $A \in M$. Per la numerabilità di M ci sono solo $\aleph_0$ scelte per gli A e quindi l'insieme dei G è un $\mathbf{G}_\delta$ denso, da cui il termine «generico.»

Notiamo che se M soddisfa $V = L$, cioè $M = L_\alpha$ dove $\alpha = M \cap \mathrm{Ord} = M[G] \cap \mathrm{Ord}$, allora $M[G] \neq L_\alpha$ e quindi $(V \neq L)^{M[G]}$. Questo prova che

$$\mathrm{CON}(\mathsf{ZFC}) \Rightarrow \mathrm{CON}(\mathsf{ZFC} + V \neq L).$$

Tuttavia se M soddisfa CH, anche $M[G]$ soddisfa CH e quindi non siamo ancora riusciti a dimostrare la coerenza di $\neg\,\mathsf{CH}$. Per fare questo occorre aggiungere molti reali di Cohen ad M.

ESEMPIO 2. – Sia κ un cardinale più che numerabile di M, per esempio $\kappa = \aleph_2^M$. Il *forcing* per aggiungere κ reali di Cohen è

$$\boldsymbol{P}_2 = \{p \mid p \text{ è una funzione, } \operatorname{dom}(p) \subset \kappa \times \omega, \ \operatorname{ran}(p) \subset \omega \ \text{e} \ |p| < \omega\}$$

con l'ordinamento $p \leqslant q \Leftrightarrow p \supseteq q$. Per l'assolutezza delle nozioni usate nella definizione di $\boldsymbol{P}_2$ si vede che $(\boldsymbol{P}_2, \leqslant) \in M$. Un $\boldsymbol{P}_2$-generico su M è una funzione $G : \kappa \times \omega \to \omega$ tale che le funzioni $G(\alpha, \cdot)$: $\omega \to \omega$ sono tutte distinte. Quindi $M[G]$ ha κ nuovi elementi di ${}^{\omega}\omega$. Inoltre tutti i cardinali di M continuano ad essere cardinali in $M[G]$, cioè la funzione $\aleph$ è assoluta tra M e $M[G]$. (Questo fatto dipende dalla natura specifica di $\boldsymbol{P}_2$ che stiamo usando e non vale per altri *forcings* — vedi $\boldsymbol{P}_3$ dell'esempio successivo.) Riassumendo, in $M[G]$ vale la seguente affermazione: «Ci sono $\aleph_2$ funzioni distinte da $\omega \to \omega$ e quindi $2^{\aleph_0} \geqslant \aleph_2$.» In particolare questo prova che se ZFC è consistente, allora anche $\mathsf{ZFC} + \neg\,\mathsf{CH}$ lo è.

ESEMPIO 3. – Vogliamo ora dimostrare come il *forcing* possa essere usato per dimostrare la coerenza di CH. Non siamo tanto interessati al risultato in sé che, come sappiamo, è ottenibile usando L, quanto alla tecnica usata. Vogliamo un *forcing* che aggiunga ad M una biezione tra $\aleph_1^M$ e $(2^{\aleph_0})^M$ ma che non aggiunga nuovi reali. Questo *forcing* collasserà $(2^{\aleph_0})^M$ ad $\aleph_1^M$, cioè $(2^{\aleph_0})^M$ sarà un ordinale $\geqslant \aleph_1^M$ equipotente ad $\aleph_1^M$ e quindi se CH non vale in M, $(2^{\aleph_0})^M$ cesserà di essere un cardinale in M. Lo stesso destino tocca a tutti i cardinali di M che si trovano tra $\aleph_1^M$ e $(2^{\aleph_0})^M$. Per questo motivo si dice che $\boldsymbol{P}_3$ «ammazza tutti i i cardinali tra $\aleph_1$ e $2^{\aleph_0}$.» Sia $\boldsymbol{P}_3$ l'insieme delle funzioni $p \in M$ che sono numerabili in M, con dominio contenuto in $\aleph_1^M$ e a valori in $(2^{\aleph_0})^M$, cioè

$$\boldsymbol{P}_3 = (\{p \mid p \text{ è una funzione, } \operatorname{dom}(p) \subset \aleph_1, \ \operatorname{ran}(p) \subset 2^{\aleph_0} \ \text{e} \ |p| \leqslant \omega\})^M$$

e, come al solito, $p \leqslant q \Leftrightarrow p \supseteq q$. Per costruzione $(\boldsymbol{P}_3, \leqslant) \in M$ e se G è $\boldsymbol{P}_3$-generico su M, allora:

(a) $G : \aleph_1^{M[G]} \to (2^{\aleph_0})^M$ è suriettiva;

(b) se $f \in M[G]$ e $f : \omega \to M$ allora $f \in M$. In particolare $({}^\omega\omega)^M = ({}^\omega\omega)^{M[G]}$ e quindi $\mathbb{R}^M = \mathbb{R}^{M[G]}$;

(c) $\aleph_1^M = \aleph_1^{M[G]}$ (questo discende da (b)).

Poiché c'è una biezione $f \in M \subset M[G]$ tra $\mathbb{R}^M = \mathbb{R}^{M[G]}$ e $(2^{\aleph_0})^M$, da (a), (b) e (c) segue che

$$(|\mathbb{R}| \leqslant \aleph_1)^{M[G]},$$

cioè $M[G]$ soddisfa CH.

Dagli esempi 2 e 3 possiamo quindi estendere un modello M in modo da verificare o falsificare CH a nostro piacimento.

Diamo infine qualche cenno su come si elimina l'ipotesi (7) di esistenza di un modello numerabile transitivo di ZFC dalla dimostrazione $\mathrm{CON}(\mathsf{ZFC}) \Rightarrow \mathrm{CON}(\mathsf{ZFC} + \neg\,\mathsf{CH})$ nell'esempio 2. L'argomento è del tutto generale e vale per tutte le altre dimostrazioni che utilizzano il *forcing.* Fissiamo un'enumerazione ([8]) di tutti gli assiomi di ZFC e sia ZFC_n la lista dei primi n assiomi. Un'analisi dettagliata della costruzione di modelli generici mediante il *forcing* dimostra che per ogni n c'è un $m > n$, esplicitamente calcolabile a partire da n, tale che: se M è un modello numerabile e transitivo di ZFC_m e $(\boldsymbol{P}, \leqslant) \in M$ e G è $\boldsymbol{P}$-generico su M, allora $M[G]$ è un modello di ZFC_n.

Se, per assurdo, ZFC dimostrasse CH, allora $\mathsf{ZFC}_n \vdash \mathsf{CH}$ per un certo n. Sia $m > n$ come sopra. Il Principio di Riflessione asserisce che per ogni k

(8) $\quad \mathsf{ZFC} \vdash \exists M(M \text{ modello numerabile transitivo di } \mathsf{ZFC}_k)$

e quindi c'è un modello M numerabile transitivo di ZFC_m. Usando il *forcing* $\boldsymbol{P}_2$, $M[G]$ soddisferebbe $\mathsf{ZFC}_n + \neg\,\mathsf{CH}$: contraddizione.

Un'ulteriore elaborazione ci permette di dimostrare un teorema di assolutezza degli enunciati aritmetici per il *forcing*, analogamente a quanto fatto per L nella sezione 4. Supponiamo φ sia un enunciato la cui coerenza può essere dimostrata mediante un opportuno *for-*

([8]) Ricordiamo che ZFC ha infiniti assiomi.

cing, per esempio $\neg\, \mathsf{CH}$, e sia σ un enunciato aritmetico. Supponiamo che $\mathsf{ZFC} + \varphi \vdash \sigma$ e quindi $\mathsf{ZFC}_n \vdash \varphi \Rightarrow \sigma$, con n sufficientemente grande. Prendiamo un $m > n$ come sopra, che garantisca che ogni estensione mediante *forcing* di un modello di ZFC_m soddisfi ZFC_n. Per il Principio di Riflessione c'è un M numerabile transitivo che soddisfa ZFC_m e quindi, applicando il *forcing* appropriato, $M[G]$ soddisfa $\mathsf{ZFC}_n + \varphi$ e quindi vale $\sigma^{M[G]}$. Ma V_ω è assoluto per $M[G]$ e quindi σ è vera in V. In altre parole, abbiamo verificato che $\mathsf{ZFC} \vdash \sigma$. Riassumendo:

TEOREMA 2. – *Se σ è un enunciato aritmetico e se la coerenza di φ può essere dimostrata mediante il forcing, allora*

$$\mathsf{ZFC} + \varphi \vdash \sigma \;\Rightarrow\; \mathsf{ZFC} \vdash \sigma\,.$$

L'applicabilità in matematica dei teoremi visti fin'ora è fortemente limitata dal fatto che gli enunciati devono essere aritmetici. Nella Parte II vedremo come questi risultati possano essere generalizzati a classi di enunciati più ampie.

Indice dei simboli.

Concludiamo questa prima parte con un elenco delle principali notazioni e simboli usati, con a fianco la sezione in cui sono stati introdotti.

Assiomi e congetture:

AC, l'assioma di scelta, sezione 2.
BC, la congettura di Borel, sezione 3.
CH, l'ipotesi del continuo, sezione 2.
GCH, l'ipotesi generalizzata del continuo, sezione 2.
KC, la congettura di Kaplansky, sezione 3.
SH, l'ipotesi di Suslin, sezione 3.
ZF, la teoria Zermelo-Fraenkel, sezione 2.
$\mathsf{ZFC} = \mathsf{ZF} + \mathsf{AC}$, la teoria Zermelo-Fraenkel con l'assioma di scelta, sezione 2.

Simboli:

$\aleph_\alpha$: l'α-esimo cardinale infinito, sezione 2.
$|X|$: la cardinalità di X, sezione 2.
Def(M): l'insieme dei sottinsiemi definibili di M, sezione 4.
φ^M: la relativizzazione di φ ad M, sezione 4.
${}^\lambda\kappa$: l'insieme delle funzioni da λ in κ, sezione 2.
$\mathscr{L}$: il linguaggio della teoria degli insiemi, sezione 2.
L_α: l'α-esimo livello della gerarchia costruibile, sezione 4.
$L = \bigcup_\alpha L_\alpha$: l'universo costruibile, sezione 4.
$M[G]$: l'estensione del modello M mediante il generico G, sezione 5.
N_s: l'aperto di base di ${}^\omega\omega$ individuato da s, sezione 5.
ω: il primo ordinale limite ovvero l'insieme dei naturali, sezione 2.
$\wp(X)$: l'insieme delle parti di X, sezione 2.
$T \vdash \varphi$: la teoria T dimostra l'enunciato φ, sezione 1.
V_α: l'α-esimo livello della gerarchia degli insiemi, sezione 2.
$V = \bigcup_\alpha V_\alpha$: l'universo degli insiemi, sezione 2.

RIFERIMENTI BIBLIOGRAFICI

[Ba] J. Baumgartner, *Applications of the proper forcing axiom*, in *Handbook of Set Theoretic Topology*, a cura di K. Kunen and Jerry E. Vaughan, North-Holland, Amsterdam (1984), vii+1273.

[BHR] J. Becker - C. W. Henson - L. Rubel, *First order conformal invariants*, Annals of Mathematics, **112** (1980), 123-178.

[Bl] A. Blass, *Near coherence of filters. II. Applications to operator ideals, the Stone-Čech remainder of a half-line, order ideals of sequences, and slenderness of groups*, Transactions of the American Mathematical Society, **300** (1987), 557-581.

[BlW] A. Blass - G. Weiss, *A characterization and sum decomposition for operator ideals*, Transactions of the American Mathematical Society, **246** (1978), 407-417.

[BPS] A. Brown - C. Pearcy - N. Salinas, *Ideals of compact operators on Hilbert space*, Michigan Mathematical Journal, **18** (1971), 373-384.

[DW] H. Dales - W. H. Woodin, *An Introduction to Independence for Analysts*, Cambridge University Press, Cambridge (1987), xiv+241.

[DM] C. Dellacherie - P.-A. Meyer, *Probabilities and Potential*, North-Holland, Amsterdam (1978), viii+189.

[EM] P. Eklof - A. Mekler, *Almost Free Modules. Set-theoretic Methods*, North-Holland, Amsterdam (1990), xvi+481.

[Fo] G. Folland, *Real Analysis. Modern Techniques and their Applications*, John Wiley & Sons, Inc., New York (1999), xvi+386.

[G] M. Goldstern, *An application of Shoenfield's absoluteness theorem to the theory of uniform distribution*, Monatshefte für Mathematik, **116** (1993), 237-243.

[J] T. Jech, *Set Theory*, Academic Press, New York-London (1978), xi+621.

[Ka] A. Kanamori, *The Higher Infinite*, Springer-Verlag, Berlin (1994), xxiv+536.

[Ke] A. S. Kechris, *Classical Descriptive Set Theory*, Springer-Verlag, New York (1995), xviii+402.

[Ku] K. Kunen, *Set Theory. An Introduction to Independence Proofs*, North-Holland Publishing Co., Amsterdam (1983), xvi+313.

[LR] L. Lempert - L. Rubel, *An independence result in several complex variables*, Proceedings of the American Mathematical Society, **113** (1991), 1055-1065.

[M] G. Moore, *Zermelo's Axiom of Choice. Its Origins, Development and Influence*, Springer-Verlag, New York (1982), xiv+410.

[S] S. Shelah, *Lifting problem of the measure algebra*, Israel Journal of Mathematics, **45** (1983), 90-96.

[T] S. Todorčević, *Compact subsets of the first Baire class*, The Journal of the American Mathematical Society, **12** (1999), 1179-1212.

[Wa] S. Wagon, *The Banach-Tarski Paradox*, Cambridge University Press, Cambridge (1985), xvi+251.

Alessandro Andretta, Dipartimento di Matematica, via Carlo Alberto 10
10123 Torino, Italy. E-mail: andretta@dm.unito.it