La Matematica nella Società e nella Cultura

Rivista dell'Unione Matematica Italiana

Alberto Marcone

Equivalenze tra teoremi: il programma di ricerca della reverse mathematics

La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Serie 1, Vol. **2** (2009), n.1, p. 101–126.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=RIUMI_2009_1_2_1_101_0>

La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Unione Matematica Italiana, 2009.

La Matematica nella Società e nella Cultura
Rivista dell'Unione Matematica Italiana
Serie I, Vol. II, Aprile 2009, 101-126

Equivalenze tra teoremi: il programma di ricerca della reverse mathematics

ALBERTO MARCONE

Spesso i matematici fanno affermazioni del tipo «i teoremi A e B sono equivalenti», oppure «il teorema A è più forte del teorema B». Dato che A e B sono entrambi dimostrabili, e quindi equivalenti, se prendiamo alla lettera le due affermazioni la prima è banalmente vera e la seconda banalmente falsa. Chiaramente però si intende comunicare qualcosa di diverso. Per fissare le idee consideriamo un'affermazione del secondo tipo: essa usualmente significa che dedurre B da A è facile (assumendo certe competenze in una certa parte di matematica), mentre non si sa come dimostrare facilmente A a partire da B. L'affermazione è certamente influenzata dal momento storico in cui è fatta (una nuova dimostrazione può essere trovata, e ciò che è considerato difficile oggi potrebbe essere un esercizio di routine tra un secolo). Sembrerebbe dunque che un'affermazione della forma considerata non sia suscettibile di un'analisi matematicamente rigorosa.

La logica matematica ha però sviluppato negli ultimi decenni strumenti in grado di rendere precise affermazioni come le precedenti. In particolare ci riferiamo alle ricerche sulla forza assiomatica di molti risultati in diversi settori della matematica (altri filoni di ricerca esaminano ad esempio la lunghezza delle dimostrazioni). Queste ricerche hanno dato origine ad un programma di ricerca noto con il nome di *reverse mathematics*.

Nel presente articolo evidenziamo gli «antenati» della *reverse mathematics*, descriviamo lo stato attuale della ricerca, e illustriamo il significato della *reverse mathematics* per i fondamenti della matematica.

1. – Equivalenze tra enunciati

Già Aristotele aveva notato che l'equivalenza è un fenomeno abbastanza diffuso in varie parti della matematica:

> *la suddetta conversione [tra conclusione e premesse] si verifica più frequentemente nelle scienze matematiche [che nelle discussioni dialettiche].*
>
> (Secondi Analitici, 78a10)

Probabilmente Aristotele ha qui in mente equivalenze come «un triangolo ha due lati congruenti se e solo se ha due angoli congruenti». A noi invece interessano principalmente equivalenze tra enunciati, come quelle che citiamo qui di seguito, che possono essere espresse solamente all'interno di un contesto assiomatico moderno.

I. Le equivalenze tra diversi assiomi sono un argomento classico della geometria piana e trovano ampio spazio in libri di testo come [16]. Ad esempio:
   a. In una geometria di incidenza le seguenti asserzioni sono equivalenti:
      (i) l'assioma di Pasch: se una retta interseca un lato di un triangolo in un punto diverso dai vertici allora interseca anche un altro lato;
      (ii) l'assioma di separazione del piano: ogni retta r divide il piano in due insiemi convessi e tali che ogni segmento con un estremo in ognuno dei due insiemi interseca r.

      Aggiungendo agli assiomi della geometria di incidenza una di queste asserzioni si ottiene la geometria di Pasch.
   b. In una geometria di Pasch sono equivalenti:
      (i) il criterio di congruenza tra triangoli lato-angolo-lato;
      (ii) il criterio di congruenza tra triangoli angolo-lato-angolo.

      Aggiungendo agli assiomi della geometria di Pasch uno di questi criteri si ottiene la geometria neutrale.
   c. In una geometria neutrale le seguenti asserzioni sono equivalenti:
      (i) il quinto postulato di Euclide;
      (ii) esiste un'unica parallela ad una retta data per un punto dato;

(iii) la somma degli angoli interni di un triangolo è congruente a due retti;
(iv) esiste un rettangolo (cioè un quadrilatero con quattro angoli retti);
(v) due rette parallele sono equidistanti.

Aggiungendo agli assiomi della geometria neutrale una di queste asserzioni si ottiene la geometria euclidea.

d. In una geometria neutrale le seguenti asserzioni sono equivalenti:
(i) la negazione del quinto postulato di Euclide;
(ii) esiste più di una parallela ad una retta data per un punto dato;
(iii) la somma degli angoli interni di un triangolo è minore di due retti;
(iv) non esiste nessun rettangolo;
(v) esistono rette parallele asintotiche;
(vi) il criterio di congruenza tra triangoli angolo-angolo-angolo.

Aggiungendo agli assiomi della geometria neutrale una di queste asserzioni si ottiene la geometria iperbolica.

II. In logica l'equivalenza tra diversi principi non costruttivi è ben nota. Ad esempio sulla base della logica intuizionistica i seguenti principi sono equivalenti (si veda ad esempio [14]):
(i) il principio del terzo escluso $F \vee \neg F$;
(ii) la legge della doppia negazione $\neg\neg F \rightarrow F$.

L'aggiunta alla logica intuizionistica di uno di questi principi conduce alla logica classica.

III. Le equivalenze tra assiomi rappresentano uno dei tratti distintivi della teoria degli insiemi. Interi libri sono dedicati all'assioma della scelta e alle sue varianti (ad esempio [11] classifica 383 forme dell'assioma della scelta e per ognuna di esse elenca parecchi enunciati equivalenti). Inoltre la ricerca moderna sui grandi cardinali ha prodotto moltissimi risultati di equivalenza o di equiconsistenza (si veda [13] per una panoramica). In particolare ricordiamo i risultati di Harvey Friedman sull'equivalenza tra enunciati che riguardano oggetti finiti e la consistenza dell'esistenza di grandi cardinali ([6, 7]). Ci limitiamo a citare alcuni risultati classici ed alcuni esempi più recenti che stabiliscono legami con varie parti della matematica:

a. In ZF le seguenti asserzioni sono equivalenti:
 (i) l'assioma della scelta;
 (ii) il teorema del buon ordinamento: ogni insieme può essere ben ordinato;
 (iii) il teorema del buon ordinamento ristretto ad insiemi potenza;
 (iv) due numeri cardinali sono sempre confrontabili;
 (v) il lemma di Zorn;
 (vi) il teorema di Tychonoff: il prodotto di spazi topologici compatti è compatto;
 (vii) ogni anello commutativo con identità ha un ideale massimale;
 (viii) ogni insieme che genera uno spazio vettoriale contiene una base;
 (ix) la sfera unitaria del duale di uno spazio vettoriale normato su $\mathbb{R}$ contiene un punto estremo (cioè un punto che non è nell'interno di nessun segmento contenuto nella sfera).

 Aggiungendo agli assiomi di ZF una qualunque di queste asserzioni si ottiene ZFC.

b. In ZF le seguenti asserzioni sono equivalenti:
 (i) l'assioma della scelta per insiemi numerabili;
 (ii) l'unione di un insieme numerabile di insiemi a due a due disgiunti ha un sottoinsieme numerabile;
 (iii) ogni spazio topologico σ-compatto (cioè che è unione numerabile di compatti) è Lindelöf (ogni ricoprimento aperto ha un sottoricoprimento numerabile);
 (iv) ogni funzione a valori reali su uno spazio metrico che sia sequenzialmente continua è continua.

c. In ZFC le seguenti asserzioni sono equivalenti:
 (i) l'ipotesi del continuo (ogni sottoinsieme più che numerabile di $\mathbb{R}$ è in biiezione con $\mathbb{R}$);
 (ii) esiste un insieme $A \subseteq \mathbb{R}^2$ tale che per ogni $a \in \mathbb{R}$ ambedue

gli insiemi $\{x \in \mathbb{R} | (x, a) \in A\}$ e $\{y \in \mathbb{R} | (a, y) \notin A\}$ sono numerabili.

(iii) esiste una partizione numerabile di $\mathbb{R}^2$ tale che nessun elemento della partizione contiene i vertici di un triangolo rettangolo.

Per i primi due gruppi di equivalenze si vedano [15, 18, 11], per l'ultimo [4, 5].

A partire dagli anni '70 del secolo scorso il termine *reverse mathematics* si è affermato per descrivere risultati di equivalenza di questo genere. L'espressione *reverse mathematics* ha però anche un significato più specifico, e indica il programma di ricerca che ha sviluppato (in un certo contesto assiomatico) la ricerca sistematica di equivalenze e a partire da essa la scoperta di fenomeni imprevisti e interessanti.

Per giustificare la terminologia di «matematica al contrario» prendiamo come paradigma l'equivalenza citata in precedenza tra l'assioma della scelta e il teorema di Tychonoff. L'equivalenza è stabilita attraverso tre passi:

(1) fissiamo la teoria ZF in cui né l'assioma della scelta né il teorema di Tychonoff siano dimostrabili;

(2) dimostriamo, in ZF più l'assioma della scelta, il teorema di Tychonoff (questa dimostrazione in ZFC si trova in qualunque libro di topologia generale);

(3) ragionando in ZF , dimostriamo l'assioma della scelta a partire dal teorema di Tychonoff (questa dimostrazione si trova spesso nei libri di teoria degli insiemi, ma più raramente nei testi di topologia).

La teoria fissata nel punto (1) è detta *teoria di base*, la dimostrazione del punto (2) stabilisce la direzione «in avanti» dell'equivalenza, mentre la dimostrazione del punto (3) stabilisce la direzione «all'indietro» o, in inglese, *reversal*. Il punto (3) è peculiare di questo genere di risultati. Se il punto (2) rappresenta la matematica «usuale» in cui i teoremi sono dedotti dagli assiomi, il punto (3) consiste nell'inversione di questo procedimento ed è quindi «matematica al contrario».

2. – Il programma di ricerca della reverse mathematics

Oggi con «*reverse mathematics*» si intende soprattutto un programma di ricerca, iniziato da Harvey Friedman negli anni immediatamente precedenti al 1970 (si veda la ricostruzione storica in [8]) e sviluppato soprattutto da Steve Simpson e dai suoi studenti. Scopo della *reverse mathematics* è stabilire la «forza assiomatica» delle affermazioni matematiche. Per raggiungere questo obiettivo occorre innanzitutto:

(i) fissare un linguaggio formale $\mathcal{L}$ in cui tradurre le affermazioni;
(ii) fissare una teoria di base T in $\mathcal{L}$.

Una volta fatte queste scelte definiamo una relazione d'equivalenza ponendo:

$$\varphi \equiv \psi \quad \text{se e solo se} \quad \mathsf{T} \text{ dimostra } \varphi \leftrightarrow \psi.$$

(Qui φ e ψ sono enunciati di $\mathcal{L}$ e $\varphi \leftrightarrow \psi$ è la formula che esprime la loro equivalenza.) Notiamo che se $\varphi \equiv \psi$ allora φ e ψ sono dimostrabili nelle stesse teorie che estendono T e possiamo affermare che (sulla base di T) i due enunciati hanno la stessa forza assiomatica.

Lo stadio attuale della *reverse mathematics* è ampiamente documentato in [22] e [23] e utilizza le seguenti scelte:

(i) il linguaggio è quello dell'aritmetica del second'ordine, indicato da $\mathcal{L}_2$ (1);
(ii) la teoria di base è la teoria RCA_0 che corrisponde alla cosiddetta «matematica computabile» (2). In prima approssimazione pos-

(1) $\mathcal{L}_2$ ha variabili per i numeri naturali e variabili per gli insiemi di numeri naturali, simboli di costante 0 e 1, simboli di funzione binari per somma e prodotto di numeri naturali, simboli per l'uguaglianza e la relazione d'ordine tra numeri naturali e l'appartenenza tra un numero naturale e un insieme. In $\mathcal{L}_2$ possono quindi venir espresse direttamente proprietà dei numeri naturali (da cui «aritmetica») e degli insiemi di numeri naturali (da cui «del second'ordine»).

L'idea che in $\mathcal{L}_2$, attraverso opportune codifiche, sia possibile esprimere una parte assai significativa della matematica risale almeno ai lavori di Hilbert e Bernays ([9, 10], si veda in particolare il supplemento IV) sui fondamenti della matematica. In realtà già Hermann Weyl ([25]) aveva usato una teoria simile al sistema ACA_0^+ che menzioneremo brevemente più avanti.

(2) RCA_0 consiste degli usuali assiomi che asseriscono che $(\mathbb{N}, 0, 1, +, \cdot, <)$ è un semianello commutativo ordinato con identità, dello schema di induzione per formule di

siamo dire che se RCA_0 dimostra l'esistenza di un insieme X, allora esiste un algoritmo che risponde a domande del tipo «$n \in X$?».

Non è possibile esprimere tutte le affermazioni fatte in matematica nel linguaggio $\mathcal{L}_2$: la linea di confine tra ciò che è esprimibile in $\mathcal{L}_2$ e ciò che non lo è divide la matematica «numerabile» dalla matematica «più che numerabile». In questo contesto «numerabile» va inteso in un senso piuttosto ampio: rientra infatti nella matematica numerabile anche lo studio di oggetti più che numerabili, la cui struttura sia però determinata da una collezione numerabile di oggetti. Ad esempio l'analisi delle funzioni continue di variabili reale studia funzioni definite su un insieme (quello dei reali) che è più che numerabile, ma le cui strutture metrica e d'ordine sono determinate dal suo essere completamento dell'insieme numerabile dei razionali. Pertanto l'analisi delle funzioni continue di variabili reale fa parte a pieno titolo della matematica numerabile.

Le affermazioni relative a strutture numerabili sono esprimibili facilmente in $\mathcal{L}_2$: ciò permette di formulare direttamente in $\mathcal{L}_2$ risultati di teoria dei numeri, algebra numerabile, combinatorica numerabile, logica matematica relativa a linguaggi numerabili. Le affermazioni che parlano di strutture più che numerabili che fanno parte della matematica numerabile hanno bisogno di una codifica per poter essere espressi in $\mathcal{L}_2$ (3). In questo modo si esprimono in $\mathcal{L}_2$ risultati di geo-

una certa (piuttosto bassa) complessità, ed infine di uno schema di assiomi che asseriscono l'esistenza degli insiemi di numeri naturali la cui funzione caratteristica è algoritmicamente calcolabile. Quest'ultimo schema (formulato precisamente in $\mathcal{L}_2$) è chiamato *recursive comprehension axiom*, da cui il nome del sistema.

(3) Descriviamo brevemente le idee delle codifiche per i concetti di numero reale e di funzione continua da $\mathbb{R}$ in $\mathbb{R}$, rimandando a [22] per i dettagli.

Prima di tutto in RCA_0 è possibile definire una bijezione tra $\mathbb{N} \times \mathbb{N}$ e $\mathbb{N}$ e quindi si possono definire i numeri interi ed i numeri razionali come rappresentanti canonici delle classi di equivalenza di coppie di numeri naturali secondo opportune relazioni di equivalenza. Si può anche definire la distanza tra due razionali. Un numero reale è codificato da una successione di razionali che converge ad una velocità prestabilita ($|q_n - q_{n+i}| \leq 2^{-n}$). Ci sono ragioni tecniche (discusse in [8, §4]) per cui questa scelta è migliore di quella delle successioni di Cauchy di razionali o di quella dei tagli di Dedekind.

metria, analisi classica, analisi reale e complessa, topologia degli spazi metrici completi separabili e teoria descrittiva degli insiemi. Recentemente è stata introdotta anche una codifica per una classe di spazi topologici che comprende anche significativi esempi di spazi non metrizzabili ([17]).

Non si possono invece formalizzare in $\mathcal{L}_2$ affermazioni relative alla matematica più che numerabile, che comprende la topologia generale, l'analisi funzionale astratta, l'algebra più che numerabile, la combinatorica più che numerabile, la teoria degli insiemi. In effetti queste importanti parti della matematica moderna sarebbero inconcepibili senza la rivoluzione insiemistica avviata da Cantor, e non è quindi sorprendente che affermazioni relative ad esse richiedano un linguaggio insiemistico più espressivo di quello di $\mathcal{L}_2$.

Consideriamo ora la relazione d'equivalenza definita in precedenza nel nostro caso particolare (ovviamente φ e ψ sono enunciati di $\mathcal{L}_2$):

$$\varphi \equiv \psi \quad \text{se e solo se} \quad \mathsf{RCA}_0 \text{ dimostra } \varphi \leftrightarrow \psi.$$

Se consideriamo enunciati arbitrari di $\mathcal{L}_2$ è facile mostrare che ci sono infinite classi d'equivalenza di $\equiv$. La *reverse mathematics* restringe la sua attenzione al comportamento di $\equiv$ relativamente alle traduzioni in $\mathcal{L}_2$ di enunciati che sono stati dimostrati dai matematici per il loro interesse intrinseco. D'ora in poi faremo riferimento ad enunciati di questo tipo come «teoremi della matematica numerabile». Ci si può forse aspettare che la $\equiv$-equivalenza tra traduzioni di teoremi della matematica numerabile sia un evento piuttosto raro, e che in questo contesto ristretto le classi d'equivalenza contengano pochi elementi e siano molto numerose. La «scoperta» della *reverse mathematics* consiste nell'aver evidenziato, attraverso una collezione ormai assai vasta di esempi, che la situazione è invece ben diversa. In particolare sono stati osservati i seguenti fatti:

(A) il numero di classi d'equivalenza di $\equiv$ che contengono traduzioni

Una funzione continua $f:\mathbb{R}\to\mathbb{R}$ è codificata da una successione di coppie di intervalli aperti a estremi razionali che soddisfa certe condizioni: la successione enumera le coppie di intervalli $((q_1,q_2),(r_1,r_2))$ tali che l'immagine di (q_1,q_2) secondo f è inclusa in (r_1,r_2).

di teoremi della matematica numerabile è piccolo: ci sono cinque classi principali (in cui ricadono le traduzioni di quasi tutti i teoremi studiati durante il tradizionale corso di laurea in matematica), e sei altre classi più piccole; i casi intermedi sono rarissimi;

(B) ognuna delle cinque classi d'equivalenza principali contiene un enunciato che asserisce l'esistenza di insiemi di numeri naturali di una certa complessità; è naturale considerare questo enunciato il rappresentante canonico della classe d'equivalenza.

Questi fenomeni empirici, rilevati sperimentalmente attraverso l'analisi di parti diverse della matematica numerabile in decine di pubblicazioni scientifiche, permettono di tracciare un quadro piuttosto ampio che classifica centinaia di teoremi in una gerarchia con pochi gradini. Questa classificazione stabilisce legami insospettati tra teoremi provenienti da aree molto diverse della matematica: accade sistematicamente che un teorema di analisi ed uno di algebra siano equivalenti.

Il fatto **(B)** implica che quando mostriamo che la traduzione τ di un teorema della matematica numerabile appartiene ad una delle undici classi d'equivalenza abbiamo raggiunto l'obiettivo di determinare la sua forza assiomatica. Abbiamo infatti individuato il più debole assioma che, aggiunto a RCA_0, dimostra τ. Data una traduzione τ di un teorema della matematica numerabile il fatto **(A)** ci permette inoltre di avere una strategia per raggiungere questo obiettivo: confrontiamo τ con la ricca collezione di traduzioni di teoremi che sono già stati classificati, cercando di trovarne uno che risulti essere equivalente, nel senso di $\equiv$, a τ.

Si noti inoltre la differenza tra la situazione descritta da **(A)** e quella cui si è accennato nella §1 relativamente all'assioma delle scelta. In quel caso (in cui il linguaggio è quello della teoria degli insiemi e la teoria di base ZF) le classi di equivalenza che contengono enunciati matematici sono molte (come già ricordato, [11] considera 383 forme dell'assioma della scelta, indicando i molti casi in cui è noto che essi non sono equivalenti in ZF e quando invece il problema della loro indipendenza è aperto).

3. – Un esempio di dimostrazione

In questa sezione forniamo un esempio di dimostrazione di equivalenza tra la traduzione di un teorema della matematica numerabile ed un assioma. Indichiamo con BW la traduzione in $\mathcal{L}_2$ del teorema di Bolzano-Weierstrass: ogni successione limitata di numeri reali ha una sottosuccessione convergente. Dimostreremo che BW è equivalente (nel senso di $\equiv$) all'assioma di comprensione aritmetica che asserisce l'esistenza di insiemi definiti da formule aritmetiche, cioè prive di quantificatori su insiemi di numeri.

Direzione in avanti: Dobbiamo dimostrare nella teoria ACA_0 (che consiste di RCA_0 più la comprensione aritmetica) BW. Data la successione limitata $\{x_n | n \in \mathbb{N}\}$ assumiamo per semplicità che essa sia contenuta nell'intervallo $[0, 1]$. Vogliamo trovare una sottosuccessione che converge al limite superiore della $\{x_n | n \in \mathbb{N}\}$, anche se prima della dimostrazione non possiamo affermare che questo limite esiste. Consideriamo l'insieme

$$A = \{(k, i) | \forall m\, \exists n > m(i \cdot 2^{-k} \leq x_n)\}.$$

La definizione di A è lecita per l'assioma di comprensione aritmetica (nella formula usata non compaiono quantificatori su insiemi). L'idea che conduce alla definizione di A è la seguente: per ogni k consideriamo gli estremi della divisione di $[0, 1]$ in 2^k intervalli di uguale lunghezza, e tra di essi selezioniamo quelli che sono minori o uguali di infiniti elementi di $\{x_n | n \in \mathbb{N}\}$. È immediato che $(k, 0) \in A$ per ogni k e che $(k, i) \in A$ implica $i \leq 2^k$. Sia $f : \mathbb{N} \to \mathbb{N}$ definita da $f(k) = \max\{i | (k, i) \in A\}$: la successione di razionali $x = \{f(k) \cdot 2^{-k} | k \in \mathbb{N}\}$ rappresenta un numero reale secondo la codifica descritta nella nota 3 (x è il limite superiore della successione, anche se in questa sede non è necessario dimostrarlo). Se definiamo $g : \mathbb{N} \to \mathbb{N}$ per ricorsione ponendo $g(0) = 0$ e

$$g(k + 1) = \min \{n > g(k) | f(k) \cdot 2^{-k} \leq x_n \leq (f(k) + 1) \cdot 2^{-k}\}$$

è facile verificare che la sottosuccessione $\{x_{g(k)} | k \in \mathbb{N}\}$ converge a x.

REVERSAL: Per dimostrare l'assioma di comprensione aritmetica è sufficiente mostrare che per ogni formula algoritmicamente calcolabile $\varphi(k,m)$ esiste l'insieme dei k tali che $\exists m\, \varphi(k,m)$ (l'esistenza di insiemi definiti da formule aritmetiche più complesse viene poi dimostrata induttivamente). Usando BW troveremo una condizione equivalente a $\exists m\, \varphi(k,m)$ che ci permetterà di verificare in un numero finito di passi se k appartiene o meno all'insieme $\{k|\exists m\, \varphi(k,m)\}$ (ciò non può essere fatto direttamente perché per mostrare che k non appartiene all'insieme dobbiamo esaminare infiniti m).

Fissiamo dunque φ e poniamo

$$x_n = \sum\{2^{-k}|k < n, \exists m < n\, \varphi(k,m)\}$$

per ogni n. L'esistenza della successione $\{x_n|n \in \mathbb{N}\}$ è dimostrabile in RCA_0: per calcolare ogni x_n è necessario controllare solo per un numero finito di k e m se $\varphi(k,m)$ vale, e ciò può essere fatto algoritmicamente. La successione $\{x_n|n \in \mathbb{N}\}$ è contenuta in $[0,2]$ ed è quindi limitata. Per BW essa ha una sottosuccessione convergente a un limite x (che in realtà è il limite dell'intera successione). Si può verificare che per ogni k vale l'equivalenza

$$\exists m\, \varphi(k,m) \iff \forall n(|x - x_n| < 2^{-k} \Rightarrow \exists m < n\, \varphi(k,m)).$$

Consideriamo il seguente algoritmo che, dato k, stabilisce se $\exists m\, \varphi(k,m)$: l'algoritmo esamina uno dopo l'altro i numeri naturali fino a che trova un m tale che $\varphi(k,m)$ oppure trova un n tale che $|x - x_n| < 2^{-k}$ e $\forall m < n\, \neg\varphi(k,m)$. Per l'equivalenza una (e una sola) di queste possibilità deve accadere: se si tratta della prima abbiamo ovviamente $\exists m\, \varphi(k,m)$, altrimenti siamo certi che per nessun m vale $\varphi(k,m)$. Questo algoritmo mostra in RCA_0 l'esistenza dell'insieme $\{k|\exists m\, \varphi(k,m)\}$ e completa la dimostrazione.

4. – I sistemi della reverse mathematics

Il fatto **(B)** permette di ottenere per ognuna delle undici classi d'equivalenza un assioma. Aggiungendo questo assioma a RCA_0 si ottiene un sistema, ed è a questi sistemi che viene usualmente fatto riferimento nei lavori di *reverse mathematics*. In alcuni casi questi assiomi sono stati studiati ben prima che le ricerche della *reverse mathematics* ne evidenziassero l'importanza nel proprio contesto. In teoria della dimostrazione sono stati studiati molti altri assiomi da aggiungere a RCA_0: essi non sono significativi dal punto di vista dello studio della forza assiomatica di traduzioni di teoremi della matematica numerabile, pur conservando evidentemente il loro interesse da altri punti di vista.

Gli undici sistemi corrispondenti alle classi d'equivalenza menzionate in **(A)** sono RCA_0, WWKL_0, WKL_0, RCA_0 +«ω^ω è ben ordinato», ACA_0, ACA_0', ACA_0^+, ATR_0, Π^1_1-CA_0, Π^1_1-TR_0 e Π^1_2-CA_0. Essi sono disposti in una gerarchia lineare: ogni sistema è più debole di quelli che lo seguono nell'elenco. Salvo che per RCA_0 +«ω^ω è ben ordinato», ciò significa che la teoria più forte dimostra l'assioma della teoria più debole, ma il contrario non avviene. Quindi gli enunciati dimostrabili nella teoria più debole sono un sottoinsieme proprio di quelli dimostrabili nella teoria più forte. Nel caso di RCA_0 +«ω^ω è ben ordinato» la posizione nella gerarchia è determinata dal fatto che esso dimostra la consistenza di WKL_0 e ACA_0 dimostra che «ω^ω è ben ordinato» (i teoremi di RCA_0 +«ω^ω è ben ordinato» non contengono né sono contenuti in quelli di WWKL_0 e WKL_0). Il primo teorema equivalente a Π^1_2-CA_0 è stato scoperto recentemente ([17]).

D'ora in poi concentreremo la nostra attenzione sui cinque sistemi principali, i cosiddetti *«big five»* della *reverse mathematics*, ovvero RCA_0, WKL_0, ACA_0 , ATR_0 e Π^1_1-CA_0.

I seguenti teoremi raccolgono alcuni risultati esemplificativi della *reverse mathematics*. La lista di risultati è lunga e a prima vista può essere sconcertante. Essa ha un duplice scopo. Innanzitutto si vuole dare un'idea dell'ampiezza del progetto di ricerca della *reverse mathematics* e di come esso ha studiato e classificato una grande varietà di teoremi della matematica numerabile. Inoltre si spera che ogni lettore possa trovare nella lista, insieme a qualche enunciato poco familiare, anche qualche teorema che lo interessa particolarmente.

TEOREMA 1. – *In* RCA_0, WKL_0 *è equivalente ad ognuna delle seguenti asserzioni:*

(i) *Il teorema di Heine-Borel: ogni ricoprimento dell'intervallo* $[0,1]$ *per mezzo di intervalli aperti ha un sottoricoprimento finito.*

(ii) *Ogni funzione continua da* $[0,1]$ *in* $\mathbb{R}$ *è limitata.*

(iii) *Ogni funzione continua da* $[0,1]$ *in* $\mathbb{R}$ *ha un massimo.*

(iv) *Ogni funzione continua da* $[0,1]$ *in* $\mathbb{R}$ *è uniformemente continua.*

(v) *Ogni funzione continua da* $[0,1]$ *in* $\mathbb{R}$ *è integrabile secondo Riemann.*

(vi) *Il teorema di Cauchy-Peano per l'esistenza locale di soluzioni di un'equazione differenziale.*

(vii) *Il teorema di punto fisso di Brouwer: ogni funzione continua da* $[0,1]^n$ *a* $[0,1]^n$ *ha un punto fisso.*

(viii) *Il teorema di Hahn-Banach per spazi di Banach separabili: ogni funzionale limitato* f *su un sottospazio di uno spazio di Banach separabile con* $\|f\| \leq 1$ *ha un'estensione* F *all'intero spazio con* $\|F\| \leq 1$.

(ix) *Il teorema di Banach per spazi di Banach separabili: se* A *e* B *sono sottoinsiemi aperti convessi e disgiunti di uno spazio di Banach separabile, allora esiste un iperpiano chiuso rispetto a cui* A *e* B *sono su lati opposti.*

(x) *Ogni anello commutativo con identità numerabile ha un ideale primo.*

(xi) *Ogni campo numerabile ha un'unica chiusura algebrica.*

(xii) *Ogni campo numerabile formalmente reale è ordinabile.*

(xiii) *Ogni campo numerabile formalmente reale ha un'unica chiusura reale.*

(xiv) *Il teorema di Levi: ogni gruppo numerabile abeliano privo di torsione è ordinabile.*

(xv) *Il prodotto numerabile di gruppi numerabili ordinabili è ordinabile.*

(xvi) *Il teorema di completezza di Gödel per insiemi numerabili di formule: ogni insieme numerabile e consistente di formule del prim'ordine ha un modello numerabile.*

(xvii) *Ogni grafo numerabile bipartito k-regolare ammette un matching perfetto* (4).

TEOREMA 2. – *In* RCA_0, ACA_0 *è equivalente ad ognuna delle seguenti asserzioni:*

(i) *Ogni successione limitata di numeri reali ha un estremo superiore.*

(ii) *Il teorema di Bolzano-Weierstrass: ogni successione limitata di numeri reali ha una sottosuccessione convergente.*

(iii) *Il lemma di Ascoli-Arzelà: ogni successione limitata ed equicontinua di funzioni da un intervallo limitato in* $\mathbb{R}$ *ha una sottosuccessione uniformemente convergente.*

(iv) *Ogni* $C \subseteq S^1$ *chiuso e numerabile è un insieme di unicità, cioè l'unica serie trigonometrica nulla sul complemento di* C *è quella con tutti i coefficienti nulli.*

(v) *Ogni sottoinsieme aperto di* $\mathbb{R}$ *è Lebesgue misurabile.*

(vi) *Il teorema di convergenza dominata di Lebesgue per la misura di Lebesgue su* $[0,1]$.

(vii) *Il teorema di rappresentazione di Riesz per funzionali lineari positivi su* $[0,1]$.

(viii) *Ogni anello commutativo con identità numerabile ha un ideale massimale.*

(ix) *Ogni spazio vettoriale numerabile su un campo numerabile ha una base.*

(x) *Ogni campo numerabile ha una base di trascendenza.*

(xi) *Ogni gruppo numerabile e abeliano ha un'unica chiusura divisibile.*

(xii) *Il teorema di Hahn: ogni gruppo abeliano ordinato è immergibile in un prodotto di copie di* $(\mathbb{R}, +)$.

(xiii) *Se* α *e* β *sono buoni ordini numerabili allora* α^β *è bene ordinato.*

(4) Un grafo $G = (V, E)$ è bipartito se $V = V_1 \cup V_2$ con $V_1 \cap V_2 = \emptyset$ e ogni lato di G (cioè ogni elemento di E) collega un elemento di V_1 a un elemento di V_2. G è k-regolare se da ogni vertice escono esattamente k lati. $M \subseteq E$ è un matching di V se lati distinti di M non hanno vertici in comune, ed è perfetto se inoltre contiene lati uscenti da ogni vertice.

(xiv) *Il lemma di König: ogni albero infinito e finitamente generato ha un cammino infinito.*

(xv) *Il teorema di Ramsey per* $[\mathbb{N}]^k$ *con* $k \geq 3$*: per ogni* $P \subseteq [\mathbb{N}]^k$ *esiste* $X \subseteq \mathbb{N}$ *infinito con* $[X]^k \subseteq P$ *oppure* $[X]^k \cap P = \emptyset$ (5).

Teorema 3. – *In* RCA_0, ATR_0 *è equivalente ad ognuna delle seguenti asserzioni:*

(i) *Il teorema dell'insieme perfetto: ogni sottoinsieme chiuso e più che numerabile di* $\mathbb{R}$ *ha un sottoinsieme perfetto (chiuso e privo di punti isolati) non vuoto.*

(ii) *Il teorema di separazione di Lusin: due sottoinsiemi analitici di* $\mathbb{R}$ *disgiunti sono separati da un Boreliano.*

(iii) *Il dominio di un sottoinsieme Boreliano di* $\mathbb{R}^2$ *con al più un valore per ogni elemento è Boreliano.*

(iv) *Il teorema di Ulm: due p-gruppi abeliani ridotti numerabili che hanno gli stessi invarianti di Ulm sono isomorfi.*

(v) *Dati due buoni ordini numerabili uno di essi è immergibile nell'altro.*

(vi) *Il teorema di forma normale di Cantor per buoni ordini numerabili.*

(vii) *Ogni successione numerabile ben ordinata di buoni ordini numerabili ha estremo superiore.*

(viii) *La disuguaglianza di Sherman: se* α, β *e* γ *sono buoni ordini numerabili allora* $(\alpha+\beta)\gamma \leq \alpha\gamma+\beta\gamma$.

(ix) *I giochi relativi ad aperti sono determinati* (6).

(x) *Gli insiemi aperti hanno la proprietà di Ramsey* (7).

(5) $[X]^k$ è l'insieme dei sottoinsiemi di X con esattamente k elementi.

(6) Una partita nel gioco relativo a $X \subseteq \mathbb{N}^{\mathbb{N}}$ ($\mathbb{N}^{\mathbb{N}}$ è lo spazio delle funzioni da $\mathbb{N}$ in $\mathbb{N}$, fornito della topologia prodotto ottenuta a partire dalla topologia discreta di $\mathbb{N}$) si svolge tra due giocatori *I* e *II* che giocano a turno numeri naturali; al termine della partita si è ottenuto $x \in \mathbb{N}^{\mathbb{N}}$ e il giocatore *I* vince se $x \in X$, mentre se $x \notin X$ vince *II*. Il gioco è determinato se uno dei giocatori ha una strategia vincente (la strategia determina ogni mossa sulla base delle mosse precedenti).

(7) Un insieme X di sottoinsiemi infiniti di $\mathbb{N}$ ha la proprietà di Ramsey se esiste $A \subseteq \mathbb{N}$ infinito tale che tutti i sottoinsiemi infiniti di A sono in X oppure nessun sottoinsieme infinito di A appartiene a X. Ogni sottoinsieme infinito di $\mathbb{N}$ è identificato

TEOREMA 4. – *In* RCA_0, Π^1_1-CA_0 *è equivalente ad ognuna delle seguenti asserzioni:*

(i) *Il teorema di Cantor-Bendixson: ogni sottoinsieme chiuso di* $\mathbb{R}$ *è unione di un insieme numerabile e di un insieme perfetto.*

(ii) *Il teorema di Silver: ogni relazione di equivalenza Boreliana su* $\mathbb{R}$ *che ha una quantità più che numerabile di classi di equivalenza ha un insieme perfetto di elementi non-equivalenti.*

(iii) *Ogni sottoinsieme numerabile del duale di uno spazio di Banach separabile ha un più piccolo sottospazio chiuso nella topologia* $*$*debole che lo contiene* ([8]).

(iv) *Ogni sottospazio di* $\ell_1 = c_0^*$ *chiuso rispetto alla norma ha una chiusura nella topologia* $*$*debole.*

(v) *Ogni gruppo abeliano numerabile è la somma diretta di un gruppo divisibile e di un gruppo ridotto.*

(vi) *Il teorema di Mal'tsev: ogni gruppo numerabile ordinato ha tipo d'ordine* $\mathbb{Z}^a\mathbb{Q}^\varepsilon$ *dove* a *è un ordinale numerabile e* $\varepsilon \in \{0,1\}$.

(vii) *I giochi relativi a insiemi che sono unione di un aperto e di un chiuso sono determinati (si veda la nota* 6 *per le definizioni).*

(viii) *Gli insiemi* G_δ *(intersezioni numerabili di aperti) hanno la proprietà di Ramsey (si veda la nota* 7 *per le definizioni).*

In alcuni casi (ad esempio punto (v) del Teorema 3 e punti (iii) e (iv) del Teorema 4) questi risultati mostrano che fatti quasi banali (e che difficilmente vengono etichettati come teoremi in un testo matematico in cui vengono enunciati) sono piuttosto forti da un punto di vista assiomatico.

La tabella 1 (una versione adattata ed estesa della tabella I.3 di [22]) riassume i teoremi precedenti indicando per alcuni degli argomenti più importanti della matematica numerabile quali dei cinque sistemi risultano equivalenti a teoremi celebri di quella parte della matematica.

con l'elemento di $\mathbb{N}^\mathbb{N}$ che lo enumera in ordine crescente: la topologia dello spazio dei sottoinsiemi infiniti di $\mathbb{N}$ è quella indotta da $\mathbb{N}^\mathbb{N}$ attraverso questa identificazione.

([8]) La topologia $*$debole sul duale X^* di uno spazio di Banach è quella generata dalle funzioni del tipo $x^* \mapsto x^*(x)$ per $x \in X$.

TABELLA 1. – I teoremi dimostrati dai vari sistemi.

	RCA_0	WKL_0	ACA_0	ATR_0	Π^1_1-CA_0
analisi e topologia					
chiusi e aperti	✓	✓		✓✓	✓
completezza	✓	✓	✓		
funzioni continue	✓✓	✓✓	✓		
compattezza	✓	✓	✓		
equazioni differenziali	✓	✓			
spazi di Banach	✓	✓✓			✓
misura secondo Lebesgue	✓		✓		
Boreliani e analitici	✓			✓✓	✓✓
algebra numerabile					
campi	✓	✓✓	✓		
anelli commutativi	✓	✓	✓		
spazi vettoriali	✓		✓		
gruppi abeliani	✓		✓	✓	✓
gruppi ordinabili	✓	✓	✓		✓
logica matematica	✓	✓			
buoni ordini numerabili	✓		✓	✓✓	
grafi bipartiti		✓	✓	✓	
teoremi di Ramsey			✓	✓	✓
giochi e determinatezza			✓	✓	✓

La presenza di un doppio simbolo ✓ indica che i teoremi in quel campo della matematica che risultano essere equivalenti a quel sistema sono particolarmente importanti e numerosi.

5. – Alcuni risultati esemplari

I teoremi della sezione precedente contengono solo una parte dei risultati della *reverse mathematics*, ma testimoniano l'ampiezza delle ricerche svolte negli ultimi decenni. Esamineremo ora più in dettaglio cinque esempi che illustrano alcuni possibili significati dei risultati di *reverse mathematics*.

5.1 – *Nozioni di compattezza*

Per spazi metrici completi esistono diverse definizioni di compattezza: la compattezza di Heine-Borel (da ogni ricoprimento aperto è possibile estrarre un sottoricoprimento finito), la compattezza sequenziale (da ogni successione è possibile estrarre una sottosuccessione convergente) e la totale limitatezza (per ogni $\varepsilon > 0$ esiste un insieme finito di punti tali che ogni altro punto dista meno di ε da uno di essi).

Le indagini della *reverse mathematics* hanno stabilito le relazioni che intercorrono tra queste nozioni nel caso degli spazi metrici completi separabili (si veda [3] per una panoramica). Limitandoci per semplicità al caso dell'intervallo $[0,1]$, risulta che la sua totale limitatezza è dimostrabile nella teoria base RCA_0. La compattezza di Heine-Borel di $[0,1]$ (cioè il teorema di Heine-Borel) è invece equivalente a WKL_0, e quindi non dimostrabile in RCA_0. Come visto nella sezione 3, la compattezza sequenziale di $[0,1]$ (cioè il teorema di Bolzano-Weierstrass) risulta invece equivalente ad ACA_0, ed è quindi propriamente più forte degli altri tipi di compattezza.

Ciò che questi risultati ci dicono è che le differenti nozioni di compattezza rappresentano aspetti diversi della nozione intuitiva di compattezza. Il fatto che in un sistema forte essi siano tutti equivalenti è certamente importante, ma sistemi più deboli ci fanno apprezzare le loro differenze e ci permettono di classificarli.

5.2 – *Il teorema di Cauchy-Peano*

La dimostrazione usuale del teorema di esistenza locale di soluzioni alle equazioni differenziali ordinarie di Cauchy-Peano utilizza il lemma di Ascoli-Arzelà: questa era anche la dimostrazione originale di Peano. I risultati di *reverse mathematics* mostrano che, mentre il teorema di Cauchy-Peano può essere dimostrato in WKL_0, il lemma di Ascoli-Arzelà necessita del più forte sistema ACA_0. In effetti WKL_0 è sufficiente per avere una buona teoria della continuità (e quindi affrontare il problema delle equazioni differenziali), mentre ACA_0 è necessario per avere una buona teoria della convergenza (ed il lemma di Ascoli-Arzelà è un risultato di convergenza). Quindi il lemma di Ascoli-Arzelà è propriamente più forte del teorema nella cui dimostrazione viene applicato, ed esiste una dimostrazione del teorema di Cauchy-Peano che evita il ricorso al lemma di Ascoli-Arzelà. Questa dimostrazione è dovuta a Simpson ([19]) ed è più «costruttiva» di quella usuale, proprio perché utilizza solo WKL_0.

Questi risultati certamente non suggeriscono la necessità (e neppure l'opportunità) di sostituire la dimostrazione classica del teorema di Cauchy-Peano con un'altra, tecnicamente più complessa. Ci forniscono però un'informazione interessante dal punto di vista fondazionale sul rapporto tra questi teoremi: in un senso ben preciso, il lemma di Ascoli-Arzelà è più forte del teorema di Cauchy-Peano.

5.3 – *Gli ideali di un anello*

Una situazione analoga alla precedente si può ritrovare anche nella teoria degli anelli commutativi con identità. Usualmente si dimostra che ogni anello commutativo con identità ha un ideale primo osservando che ogni ideale massimale è primo e utilizzando il teorema secondo cui ogni anello commutativo con identità ha un ideale massimale (quest'ultimo teorema è una conseguenza del lemma di Zorn).

Nel contesto della *reverse mathematics*, a causa delle limitazioni intrinseche al linguaggio $\mathcal{L}_2$, vengono considerati solo anelli numerabili. I risultati dei Teoremi 1 e 2 mostrano che l'esistenza di ideali massimali richiede ACA_0, mentre l'esistenza di ideali primi è dimostrabile in WKL_0. Perciò la dimostrazione usuale dell'esistenza di ideali primi non è la più «economica» dal punto di vista assiomatico: in un senso ben preciso, il teorema che asserisce l'esistenza di ideali primi è più debole del teorema che asserisce l'esistenza di ideali massimali.

5.4 – *Il teorema di dualità di König*

Intorno al 1930 Denes König dimostrò un'importante teorema sui grafi bipartiti finiti, noto come teorema di dualità di König (KDT).

Oltre alle definizioni riportate nella nota 4, ricordiamo che se $G = (V, E)$ è un grafo, $C \subseteq V$ è un ricoprimento di G se ogni lato di G ha almeno un estremo in C. Un ricoprimento di König di G è una coppia (C, M) in cui C è un ricoprimento di V, M è un matching di V e C contiene esattamente un vertice di ogni elemento di M. König dimostrò che ogni grafo bipartito finito ha un ricoprimento di König.

Il teorema venne esteso a grafi bipartiti numerabili nel 1976 da Podewski e Steffens, e nel 1984 Aharoni dimostrò che esso vale per grafi bipartiti arbitrari. Le tre dimostrazioni (caso finito, numerabile e più che numerabile) sono via via più complesse. In particolare non sembra possibile applicare a KDT un principio di compattezza, che è il modo in cui molto spesso in combinatorica si generalizza un risultato dal caso finito a quello infinito. Dal punto di vista della *reverse mathematics*, un ragionamento che utilizzi la compattezza è usualmente formalizzabile in WKL_0 ([9]).

La maggior parte dei teoremi sui grafi numerabili, KDT incluso, affermano l'esistenza di un oggetto, e le loro dimostrazioni forniscono un limite alla complessità (nel senso della teoria della ricorsività) di questo oggetto: ciò non accade per la dimostrazione di Podewski e Steffens. Dal nostro punto di vista i limiti di complessità spesso conducono facilmente a dimostrare il teorema in ACA_0 o in una teoria più debole di ACA_0.

Alcuni specialisti di teoria dei grafi (ed in particolare Aharoni stesso) iniziarono a chiedersi la ragione dello «strano» comportamento di KDT. La risposta è stata fornita dalla *reverse mathematics*. Aharoni, Magidor e Shore ([1]) hanno dimostrato che KDT per grafi numerabili implica ATR_0: non può quindi essere ottenuto attraverso nessuno dei metodi «usuali» di generalizzazione all'infinito (che sono tutti conseguenze di teoremi dimostrabili in ACA_0), né è possibile ottenere gli usuali limiti sulla complessità dell'oggetto la cui esistenza viene dimostrata. Questo risultato stabilisce che KDT è effettivamente, ed in un senso ben preciso, più complicato di altri teoremi della teoria dei grafi.

([9]) Un argomento di compattezza serve a dimostrare in WKL_0 l'enunciato del punto (xvii) del teorema 1.

Inoltre Aharoni, Magidor e Shore dimostrarono KDT per grafi numerabili in Π^1_1-CA_0. Simpson ([21]) ha poi dimostrato KDT in ATR_0, e quindi stabilito la forza assiomatica di questo teorema.

I risultati ottenuti dalla *reverse mathematics* hanno quindi spiegato il fenomeno empirico della difficoltà di una certa dimostrazione, e hanno fornito un significato rigoroso all'affermazione «il teorema di dualità di König è più difficile di altri teoremi sui grafi».

5.5 – *L'invenzione della teoria degli insiemi*

Come è ben noto Georg Cantor iniziò le ricerche che lo portarono a formulare le idee fondamentali della teoria degli insiemi spinto da alcune questioni di analisi armonica, in particolare relative agli insiemi di unicità (cioè i $C \subseteq S^1$ tali che l'unica serie trigonometrica nulla sul complemento di C è quella con tutti i coefficienti nulli). Introducendo il concetto di ordinale transfinito Cantor dimostrò che ogni insieme numerabile chiuso è un insieme di unicità. In [12] Humphreys ha analizzato dal punto di vista della *reverse mathematics* questo risultato di Cantor dimostrando che esso è equivalente a ACA_0.

La teoria ACA_0 è troppo debole per sviluppare una buona teoria dei buoni ordini numerabili e quindi degli ordinali (ad esempio, dal Teorema 3 risulta che ATR_0 è necessaria per dimostrare un fatto fondamentale quale la confrontabilità tra buoni ordini): la dimostrazione in ACA_0 del teorema di Cantor evita infatti il ricorso ad una costruzione transfinita. Si può quindi affermare che Cantor non aveva bisogno di introdurre gli ordinali per dimostrare il suo teorema: per ottenerlo sono sufficienti assiomi che non bastano a sviluppare le basi della teoria degli ordinali.

Humphreys ha anche ottenuto che l'esistenza degli oggetti utilizzati nella dimostrazione originale di Cantor è equivalente ad ATR_0. Quindi possiamo affermare che per quella dimostrazione gli ordinali sono inevitabili.

In questo caso la *reverse mathematics* contribuisce a chiarire alcuni aspetti di una questione storica, sulla necessità o meno di certi sviluppi della storia della matematica.

6. – Il contributo della reverse mathematics ai fondamenti della matematica

I risultati ottenuti in *reverse mathematics* hanno anche un significato per i fondamenti della matematica. Infatti ciascuno dei cinque sistemi più importanti della *reverse mathematics* può venir fatto corrispondere a un programma nello studio dei fondamenti della matematica. La tabella 2 (che è la traduzione della tabella I.1 di [22]) riporta le corrispondenze, con i nomi degli autori che hanno sostenuto (spesso prima della nascita della *reverse mathematics*) i vari programmi.

La *reverse mathematics* permette di stabilire quali parti della matematica siano conservate da ognuno di queste posizioni, e quali teoremi invece non siano dimostrabili sulla base di essa. Emergono così chiaramente le conseguenze matematiche dei programmi sui fondamenti della matematica, ovvero quanta matematica «si perde» o «si guadagna» adottando una certa posizione. Spiegheremo ora le corrispondenze della tabella 2, dedicando più spazio alla seconda riga, in cui il rapporto tra *reverse mathematics* e fondamenti della matematica è particolarmente interessante.

La tabella associa RCA_0 al costruttivismo nello stile di Bishop, che accetta solamente dimostrazioni «costruttive» o «effettive» dei teoremi matematici. RCA_0 non è una teoria costruttiva (ad esempio perché usa ragionamenti per assurdo) ma in pratica nella maggior parte dei casi le dimostrazioni in RCA_0 di traduzioni di teoremi della matematica

Tabella 2. – I sistemi della *reverse mathematics* e i fondamenti della matematica.

sistema	programma	autori
RCA_0	costruttivismo	Bishop
WKL_0	riduzionismo finitista	Hilbert
ACA_0	predicativismo	Weyl, Feferman
ATR_0	riduzionismo predicativista	Friedman, Simpson
Π^1_1-CA_0	impredicativismo	Feferman, Buchholz, Pohlers, Sieg

numerabile sono costruttivamente accettabili. Viceversa, molte dimostrazioni in RCA_0 provengono direttamente dalla tradizione costruttivista (data una dimostrazione costruttiva è sufficiente verificare che non venga usata più induzione di quella disponibile in RCA_0: nelle teorie costruttive si assume l'induzione sui naturali per tutte le formule del linguaggio).

Come è ben noto il programma di Hilbert aveva come obiettivo la riduzione di tutta la matematica alla matematica finitistica (il «riduzionismo finitista» che è associato a WKL_0 nella tabella 2). Hilbert proponeva di raggiungere questo obiettivo attraverso la dimostrazione della consistenza di ogni teoria matematica per mezzo di strumenti finitistici. Il successo del programma di Hilbert avrebbe fondato tutta la matematica sulla solida base di alcuni assiomi estremamente intuitivi (quelli che stabiliscono le relazioni fondamentali tra oggetti finiti) e avrebbe definitivamente fugato i dubbi sulla solidità dell'edificio matematico sorti in seguito alla cosiddetta «crisi dei fondamenti» avvenuta nel periodo a cavallo tra XIX e XX secolo.

I teoremi di incompletezza di Gödel mostrano che il programma di Hilbert non può essere realizzato, perché la consistenza di ogni sistema assiomatico sufficientemente potente non può essere dimostrata nel sistema stesso, e quindi meno che mai in un sistema più debole, che usi soltanto principi finitistici. I teoremi di incompletezza di Gödel non escludono però che il programma di Hilbert ammetta realizzazioni parziali, cioè che frammenti significativi della matematica possano venir ridotti alla matematica finitistica attraverso dimostrazioni di consistenza. Vedremo ora il ruolo di WKL_0 in una realizzazione parziale del programma di Hilbert (ulteriori dettagli si trovano in [20], ma si veda anche [2], che tratta questi argomenti a partire da un punto di vista lievemente diverso).

Una rappresentazione ragionevolmente fedele della matematica finitistica così come probabilmente la intendeva Hilbert è rappresentata dal sistema PRA dell'aritmetica primitiva ricorsiva (10): si

(10) Il linguaggio di PRA ha variabili per i soli numeri naturali e simboli per tutte le funzioni primitive ricorsive (quelle che si ottengono per composizione e ricorsione a

veda ad esempio Tait ([24]) ([11]). Friedman ([22, §IX.3]) ha mostrato che PRA e WKL_0 dimostrano esattamente gli stessi enunciati di una certa complessità. Sieg ha mostrato che il risultato di Friedman può venir dimostrato in PRA. Ciò implica che in PRA è possibile dimostrare che PRA e WKL_0 sono equiconsistenti (se WKL_0 dimostra $0 = 1$ allora PRA è sufficiente a derivare questa contraddizione). Quindi nella matematica finitistica rappresentata da PRA e assumendo la consistenza di PRA stesso (che è certamente accettabile da un punto di vista finitistico) si dimostra la consistenza di WKL_0. Pertanto WKL_0, e di conseguenza anche RCA_0 e $WWKL_0$ che sono più deboli ([12]), sono stati ridotti alla matematica finitistica in un senso che Hilbert avrebbe probabilmente accettato.

Quanto appena descritto ha una notevole rilevanza perché WKL_0 e PRA, pur essendo finitisticamente equivalenti, hanno ben diversa capacità dimostrativa. Come le ricerche di *reverse mathematics* hanno ampiamente dimostrato (e come la tabella 1 e il teorema 1 documentano) WKL_0 è in grado di dimostrare molte traduzioni di teoremi della matematica numerabile che non sono affatto finitistici. Per questi teoremi si è ottenuta una riduzione al finitismo nello spirito di Hilbert.

Questa parziale realizzazione del programma di Hilbert ci permette quindi di concludere che parti significative dell'analisi classica (inclusi i teoremi fondamentali sulle funzioni continue e gran parte dello studio delle equazioni differenziali), dell'algebra numerabile, della logica matematica, ecc., ammettono una validazione finitistica del tipo immaginato da Hilbert.

Il predicativismo (associato a ACA_0 nella tabella 2) si pone il seguente problema: quando definiamo l'insieme $X = \{n \in \mathbb{N} \mid \forall Y\, \varphi(n, Y)\}$, per sapere se un certo n appartiene a X dobbiamo esaminare tutti gli insiemi Y, incluso X stesso. In una visione in cui gli insiemi non sono dati in

partire da 0, successore e proiezioni). Gli assiomi di PRA sono le definizioni delle funzioni primitive ricorsive e l'induzione ristretta a formule prive di quantificatori.

([11]) La proposta di Tait è stata criticata sostenendo l'insufficienza di PRA allo sviluppo di tutta la matematica finitistica. Il ragionamento che svilupperemo rimane valido anche qualora si accettino queste critiche.

([12]) $WWKL_0$ è equivalente a diversi teoremi fondamentali in teoria della misura.

partenza ma vengono prodotti in successione, ciò appare inaccettabilmente circolare. Restringere la comprensione alle formule in cui non compaiono quantificatori su insiemi (ciò che viene fatto in ACA_0) evita questo problema.

La corrispondenza tra ATR_0 e il riduzionismo predicativista è giustificata da risultati analoghi a quelli che collegano WKL_0 a PRA: ATR_0 dimostra gli stessi enunciati aritmetici di una teoria predicativa nota come IR (sistema per l'analisi predicativa di Feferman). Perciò ATR_0, pur non essendo predicativa, è equiconsistente ad una teoria predicativa: quindi i teoremi dimostrati in ATR_0 hanno una validazione predicativa, almeno in termini di non contraddittorietà.

Π^1_1-CA_0 ammette esplicitamente la comprensione per formule con quantificatori su insiemi ed è quindi dichiaratamente impredicativa. I teoremi equivalenti a Π^1_1-CA_0 sono certamente non dimostrabili predicativamente.

Sono riconoscente ai relatori anonimi per i loro numerosi suggerimenti che hanno sensibilmente migliorato la leggibilità di questo lavoro.

RIFERIMENTI BIBLIOGRAFICI

[1] RON AHARONI - MENACHEM MAGIDOR - RICHARD A. SHORE, *On the strength of König's duality theorem for infinite bipartite graphs*, J . Combin. Theory Ser. B, **54**, n. 2 (1992), 257–290.

[2] JEREMY AVIGAD , *Number theory and elementary arithmetic*, Philos. Math. (3), **11** (2003), 257–284.

[3] DOUGLAS K. BROWN, *Notions of compactness in weak subsystems of second order arithmetic*, In Simpson [23], 47–66.

[4] KRZYSZTOF CIESIELSKI, *Set theory for the working mathematician*, Cambridge University Press (1997), xii+236.

[5] P. ERDÖS - P. KOMJÁTH, *Countable decompositions of $\boldsymbol{R}^2$ and $\boldsymbol{R}^3$*, Discrete Comput. Geom., **5**, n. 4 (1990), 325–331.

[6] HARVEY FRIEDMAN, *Necessary uses of abstract set theory in finite mathematics*, Adv. in Math., **60**, n. 1 (1986), 92–122.

[7] HARVEY FRIEDMAN, *Finite functions and the necessary use of large cardinals*, Ann. of Math. (2), **148**, n. 3 (1998), 803–893.

[8] Harvey Friedman - Stephen G. Simpson, *Issues and problems in reverse mathematics*, In *Computability theory and its applications (Boulder, CO 1999)*, Amer. Math. Soc. (2000), 127–144.

[9] David Hilbert - Paul Bernays, *Grundlagen der Mathematik. I*, Springer-Verlag, Berlin (1968), xv+473.

[10] David Hilbert - Paul Bernays, *Grundlagen der Mathematik. II*, Springer-Verlag, Berlin (1970), xiv+561.

[11] Paul Howard - Jean E. Rubin, *Consequences of the axiom of choice*, American Mathematical Society, Providence RI (1998), viii+432.

[12] A. James Humphreys, *Did Cantor need set theory?*, In Simpson [23], 244–270.

[13] Akihiro Kanamori, *The higher infinite*, Springer-Verlag, Berlin (1994), xxiv+536.

[14] Stephen Cole Kleene, *Introduction to metamathematics*, D. Van Nostrand Co. Inc., NewYork, N.Y. (1952), x+550.

[15] Azriel Lévy, *Basic set theory*, Springer-Verlag, Berlin (1979), xiv+391.

[16] Richard S. Millman - George D. Parker, *Geometry*, Springer-Verlag, New York (1991), xiv+370.

[17] Carl Mummert - Stephen G. Simpson, *Reverse mathematics and Π^1_2 comprehension*, Bull. Symbolic Logic, **11**, n. 4 (2005), 526–533.

[18] Herman Rubin - Jean E. Rubin, *Equivalents of the axiom of choice. II*, *Studies in Logic and the Foundations of Mathematics*, North-Holland Publishing Co., **116** (1985), xxviii+322.

[19] Stephen G. Simpson, *Which set existence axioms are needed to prove the Cauchy/Peano theorem for ordinary differential equations?* J. Symbolic Logic, **49**, n. 3 (1984), 783–802.

[20] Stephen G. Simpson, *Partial realizations of Hilbert's Program*, J. Symbolic Logic, **53**, n. 2 (1988), 349–363.

[21] Stephen G. Simpson, *On the strength of König's duality theorem for countable bipartite graphs*, J. Symbolic Logic, **59**, n. 1 (1994), 113–123.

[22] Stephen G. Simpson, *Subsystems of second order arithmetic*, Springer-Verlag, Berlin (1999), xiv+445.

[23] Stephen G. Simpson editor, *Reverse mathematics 2001*. Lecture Notes in Logic. Association for Symbolic Logic, La Jolla, Ca, 2005.

[24] William W. Tait, *Finitism*, J. Philos., 78 (1981), 524–546.

[25] Hermann Weyl, *Das Kontinuum: Kritische Untersuchungen über die Grundlagen der Analysis*, Veit, Leipzig (1918).

Alberto Marcone, Dipartimento di Matematica e Informatica,
Università di Udine, viale delle Scienze 206, 33100 Udine, Italy
e-mail: marcone@dimi.uniud.it