Bollettino
Unione Matematica Italiana

Sezione A – La Matematica nella Società e nella Cultura

Carlo Toffalori, Stefano Leonesi, Sonia L'Innocente

Teoria dei Modelli, Cultura (e Società?)

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **8-A**—*La Matematica nella Società e nella Cultura* (2005), n.1, p. 149–178.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2005_8_8A_1_149_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2005.

Bollettino U. M. I.
La Matematica nella Società e nella Cultura
Serie VIII, Vol. VIII-A, Aprile 2005, 149-178

Teoria dei Modelli, Cultura (e Società?).

Carlo Toffalori - Stefano Leonesi
Sonia L'Innocente

1. – Introduzione 1 (dove si tenta di volare alto).

Questo articolo è il seguito di [4], dove abbiamo avuto modo di introdurre quella parte della (Logica) Matematica che si chiama Teoria dei Modelli e descriverne l'evoluzione dagli albori di cinquanta anni fa fino quasi ai giorni nostri. Lo scopo primario di questo secondo lavoro è quello di approfondire, appunto, gli sviluppi più recenti del settore e sottolinearne le numerose applicazioni ad altre aree della Matematica, e non solo della Matematica. La tesi che cercheremo di sostenere e possibilmente dimostrare è, ovviamente, quella che la Teoria dei Modelli è settore vitale e contribuisce proficuamente allo sviluppo della cultura matematica: val dunque la pena di sentirne parlare almeno una volta (esperienza che il lettore ha in realtà già compiuto se ha avuto la ventura e la bontà di sorbirsi [4]). Ma, visto che «due è meglio di uno», eccoci tornare sull'argomento, ad illustrarne, appunto, gli ultimi sviluppi. C'è un'ovvia obiezione che si potrebbe fare a questa nostra insistenza, e cioè: «ammettiamo pure che questa Teoria dei Modelli, di cui così convintamente celebrate i fasti, interessi in qualche modo la nostra cultura di matematici; ma, quando parliamo di Matematica, Cultura e Società, e specificamente di Matematica e Società, ebbene, quale traccia, quale rilevanza ha la Teoria dei Modelli in queste prospettive? Passi per la Cultura... ma dov'è la Società?» Obiezione, come si vede, rispettabile e, quel che è peggio, fondata e motivata: infatti, se è vero che basta scorrere le liste dei convegni annuali di Matematica, anche negli ambienti più selettivi, oppure gli indici dei giornali di Matematica, anche di quelli più illustri, per vedere ogni tanto affacciarsi qualche titolo che si collega alla Teoria dei Modelli, pur tuttavia il numero di questi esempi resta largamente minoritario. Del resto, quanti potranno esse-

re a questo mondo quelli che si interessano di mestiere alla nostra disciplina? Vogliamo dire cinquecento? Mille? Ma, anche a dire mille, sbaglieremmo forse per eccesso e tuttavia ci arresteremmo ad una cifra assolutamente trascurabile. Eppure, una qualche pur timida risposta a queste obiezioni può essere abbozzata, certamente applicabile ad ogni settore scientifico di qualche vitalità e dunque, proprio per questo, anche in particolare alla nostra Teoria dei Modelli. Il discorso è: quando persone di varia estrazione e nazionalità, mille o più di mille, si riuniscono tra loro e si infervorano per qualche giorno in convegno a comunicarsi le loro ricerche, le loro scoperte, i loro dubbi; quando giovani laureati e laureandi si aprono e si appassionano a questi argomenti e vi dedicano il loro studio e il loro entusiasmo; quando queste ricerche hanno impatto, applicazioni, collegamenti con altri settori matematici e non; ebbene, quando tutto questo accade, all'origine non possiamo non riconoscere una spinta, un'anima, una comunanza di sensibilità e di obiettivi che, pur nelle sue piccole dimensioni, costituisce pur sempre «società». Follia, forse, ma con qualche metodo; meritevole dunque di una minima, benevola curiosità. Scopo sommesso di queste note, mai esplicito nelle righe che seguiranno eppure presente nella intenzione di chi le scrive, è, allora, anche quello di testimoniare di questa comune passione «sociale».

2. – Introduzione 2 (dove si resta più terra terra).

Torniamo comunque ai dettagli tecnici. In [4] ci capitò di sottolineare il ruolo fondamentale che nella Teoria dei Modelli ha il concetto di *insieme definibile* (in una data struttura, o in una classe di strutture). Si tratta di nozione astratta che racchiude in sè esempi importanti in Algebra e Geometria. Ricordiamo infatti che gli insiemi definibili più semplici sono quelli che potremmo chiamare *costruibili* per analogia col caso dei campi algebricamente chiusi: le varietà algebriche, cioè gli insiemi di soluzioni di equazioni, e poi le loro combinazioni Booleane, dunque gli insiemi formati con le usuali operazioni di unione, intersezione e complementazione. Nuovi definibili si ottengono alternando due usuali procedimenti per gli insiemi: le proiezioni e, appunto, le combinazioni Booleane. Talora questo

processo si perde in un meandro di crescenti complicazioni: è quanto avviene, ad esempio, per i naturali con l'addizione e la moltiplicazione. Ma in altri casi il meccanismo si stabilizza dopo pochi passi iniziali, ed i definibili si riducono ai costruibili o alle loro proiezioni, e vanno a coincidere con rilevanti nozioni di Algebra e Geometria. Vari esempi hanno illustrato questa possibilità in [4]. Vogliamo allora capire i fondamenti teorici che permettono queste situazioni «docili» (quelle in cui, appunto, i definibili coincidono con i costruibili o con le loro proiezioni). Questi approfondimenti ci consentiranno di illustrare gli insiemi definibili in altre importanti classi di strutture (come i campi differenzialmente chiusi, o l'esponenziazione reale $\boldsymbol{R}_{exp}$) e ribadiranno l'importanza di uno studio astratto e generale del concetto di definibile. Cercheremo allora di presentare i primi passi fondamentali di questo studio, le sue prospettive, i suoi sviluppi, le sue difficoltà. Ne descriveremo anche alcune applicazioni ad altri rami della Matematica e, in particolare la più celebrata tra di esse: daremo infatti un breve resoconto della soluzione ottenuta da Hrushovski di una classica congettura di Geometria Diofantea (quella di Mordell-Lang) con l'uso di strumenti di Teoria dei Modelli.

Prima di addentrarci in questa analisi è tuttavia opportuno che stabiliamo in maggior dettaglio il contesto in cui lavoriamo, e che dunque delimitiamo con precisione quali classe di strutture intendiamo considerare. La nostra opzione per la Logica del Primo Ordine (lungamente discussa in [4]) ci porta a trattare classi *elementari* di strutture, cioè classi assiomatizzabili nel linguaggio del primo ordine che le riguarda: questa assunzione ci assicura, del resto, una certa flessibilità e potenti strumenti di analisi. Un'altra restrizione che deriva da queste premesse è la seguente. Nell'ambito appena delineato, c'è un'ovvia distinzione tra strutture che, pur corrispondendo allo stesso linguaggio L, soddisfano differenti enunciati del primo ordine in L. Ad esempio, all'interno della classe di tutti i gruppi è ragionevole separare i gruppi abeliani da quelli non abeliani, cioè i gruppi in cui l'operazione è commutativa da quelli in cui non lo è: la commutatività è facilmente esprimibile al primo ordine. La scelta, che conseguentemente operiamo, è di concentrarci su strutture che soddisfano gli stessi enunciati. Una tale classe si dice *com-*

pleta e l'insieme degli enunciati veri nella classe in questione (cioè veri in tutte le strutture che la costituiscono) si dice *teoria completa*. Queste classi e queste teorie sono l'ambito in cui spesso svilupperemo il nostro studio.

3. – La eliminazione dei quantificatori.

Il caso più favorevole nella identificazione degli insiemi definibili si manifesta quando essi si restringono a quelli costruibili, dunque agli insiemi di soluzioni di equazioni e alle loro combinazioni Booleane: le proiezioni non aggiungono «nuovi» esempi. Domandiamoci allora quali ipotesi teoriche garantiscono questa situazione. La condizione di appartenenza di un elemento a ad un insieme X che è proiezione di X' (ad esempio sulla prima coordinata) si esprime dicendo: esiste un qualche b tale che la sequenza (a, b) appartiene a X'; coinvolge dunque quantificatori, $\exists$ nello specifico; ovviamente procedere con successive combinazioni Booleane, in particolare negare la appartenenza ad X, richiede in linea di principio anche l'uso di $\forall$. Se dunque vogliamo evitare il contributo di proiezioni e successive complicazioni nella classificazione degli insiemi definibili, abbiamo bisogno che le formule prive di quantificatori siano già capaci di definire tutto quanto è possibile: ci serve una proprietà di *eliminazione dei quantificatori*, nel senso che ora cerchiamo di illustrare in dettaglio.

Abbiamo già sottolineato in [4] come due differenti formule $\phi(\vec{v})$ e $\phi'(\vec{v})$ di un linguaggio L possano ammettere lo stesso significato in una data struttura $\mathcal{A}$ di L, o in una classe di strutture di L. Ad esempio, nel campo ordinato dei reali, e perfino in ogni campo reale chiuso, la formula

$$\phi(v) : v \geqslant 0$$

(che definisce gli elementi non negativi) equivale all'altra formula

$$\phi'(v) : \exists v_1 \ (v = v_1^2)$$

(che determina invece i quadrati). Si noti che la seconda formula coinvolge quantificatori, e la prima no.

La nozione dell'eliminazione dei quantificatori emerge in modo naturale in questo ambito. Infatti diciamo che una classe $\mathcal{K}$ di strutture di L ha, appunto, la eliminazione dei quantificatori quando ogni formula di L risulta equivalente rispetto a $\mathcal{K}$ ad una formula priva di quantificatori. Si verifica facilmente che ogni classe $\mathcal{K}$ di strutture di L raggiunge questa proprietà in un opportuno linguaggio che estende L. La cosa fu osservata già all'inizio del secolo scorso prima da Löwenheim e poi da Skolem, il quale propose un procedimento effettivo per ridurre una formula arbitraria in un'altra equivalente e senza quantificatori. L'algoritmo di Skolem viene ancora oggi utilizzato per applicazioni legate all'informatica, in particolare nell'ambito del *Problema della Soddisfacibilità* e dunque del collaudo di nuovi programmi. Tuttavia, si tratta di una procedura astratta, che assicura l'eliminazione non direttamente nel linguaggio L, ma in sue estensioni artificiali opportunamente costruite e spesso assi distanti dalla natura algebrica delle strutture della classe $\mathcal{K}$. A noi invece interessa una eliminazione in L, oppure in sue semplici estensioni suggerite dalle proprietà algebriche di $\mathcal{K}$.

Va osservato che, da un punto di vista storico, le maggiori applicazioni (e motivazioni) della eliminazione dei quantificatori riguardano la *decidibilità.* In effetti, i primi e più famosi risultati di eliminazione sono collegati al tema della decisione. Vediamo perché. Abbiamo una classe $\mathcal{K}$ di strutture (il singolo campo complesso, o quello reale, o la classe di tutti i campi algebricamente chiusi, o quella dei campi reali chiusi) e vogliamo un algoritmo capace di determinare in un numero finito di passi, per ogni enunciato α del linguaggio di L di $\mathcal{K}$, se α è o no vero in ogni struttura di $\mathcal{K}$. Ammettiamo a questo punto di sapere che $\mathcal{K}$ elimina i quantificatori ed anzi di disporre di un procedimento effettivo che riduce ogni enunciato di L in una forma equivalente che non ha bisogno di quantificatori. Allora l'algoritmo di decisione che cerchiamo per $\mathcal{K}$ può essere trovato purché si ottenga un analogo procedimento nel contesto ridotto degli enunciati di L privi di quantificatori.

L'interesse per la decidibilità è comunque oggi parzialmente superato. In effetti, negli anni trenta e quaranta dello scorso secolo, quando i primi e principali risultati di eliminazione dei quantificatori

vennero ottenuti, la sensibilità era diversa dalla nostra: sotto l'influsso dei *Teoremi di Incompletezza* (e di indecidibilità) di Gödel, ed in un'epoca che ancora non conosceva gli attuali calcolatori ma solo certi loro modelli astratti *ante litteram*, si era forzatamente portati a dare molta enfasi a risultati astratti di decidibilità, che magari provavano la sola esistenza di algoritmi di decisione senza fornirne alcun esempio esplicito, oppure producevano tali algoritmi senza preoccuparsi della loro efficacia. Oggi, invece, si dà anche importanza all'efficienza di un simile procedimento (di decisione, di risoluzione, di ottimizzazione, di ricerca) e dunque alla sua rapidità, se conveniamo di privilegiare il criterio del tempo per misurare la complessità degli algoritmi.

L'eliminazione dei quantificatori è utile, poi, anche per verificare l'eventuale completezza di una classe $\mathcal{K}$: in effetti, la verifica che le strutture di $\mathcal{K}$ soddisfano gli stessi enunciati si può limitare al più semplice caso di enunciati privi di quantificatori.

Ma la applicazione della eliminazione dei quantificatori che più ci interessa riguarda, come detto, la *definibilità*. Infatti, se una classe $\mathcal{K}$ elimina i quantificatori in un linguaggio L, allora gli insiemi definibili in una struttura $\mathcal{A}$ di $\mathcal{K}$ si riducono a quelli della forma $\phi(\mathcal{A}^n, \vec{b})$ dove i parametri $\vec{b}$ stanno in A e ϕ è, appunto, senza quantificatori, in altre parole agli insiemi costruibili. Questo è quanto abbiamo osservato in [4] a proposito del campo complesso, del campo reale, degli ordini lineari densi e discreti. In tutti questi casi, dietro il risultato di caratterizzazione dei definibili, sta un teorema di eliminazione dei quantificatori.

I primi risultati di eliminazione risalgono alla fine degli anni venti, riguardano ordini lineari densi o discreti e furono ottenuti da Langford; i più recenti includono certe espansioni del campo reale tramite funzioni analitiche e l'esponenziazione exp, con importanti applicazioni all'Analisi Reale (li tratteremo tra breve). I più classici e famosi teoremi di eliminazione dei quantificatori sono comunque quelli relativi al campo complesso e al campo ordinato reale e sono dovuti ad Alfred Tarski. Una impostazione comune, che spesso ricorre in queste dimostrazioni, è la seguente.

Abbiamo una formula $\phi(\vec{v})$ nel nostro linguaggio L e cerchiamo

una formula equivalente $\phi'(\vec{v})$ equivalente e priva di quantificatori. Dapprima si usano argomenti elementari e generali di logica, che prescindono dal particolare contesto algebrico e ci permettono di ridurre l'analisi a formule $\phi(\vec{v})$ del tipo $\exists w \bigwedge_{i \leq r} \alpha_i(\vec{v}, w)$ dove ogni α_i è una formula atomica o la sua negazione e dunque $\bigwedge_{i \leq r} \alpha_i(\vec{v}, w)$ si presenta come un sistema finito di equazioni e disequazioni di L: ci riconduciamo in questo modo a cercare condizioni sui parametri $\vec{v}$ del sistema che si possano esprimere senza usare quantificatori e garantiscano l'esistenza di una radice w del sistema stesso. Questo è il secondo passo della dimostrazione e, in verità, il nocciolo della questione. Ovviamente, vi intervengono l'algebra e comunque le proprietà intrinseche delle strutture considerate (ordini, campi, campi ordinati); si perde, forzatamente, generalità e si va a condurre un'analisi caso per caso per ottenere l'obiettivo desiderato.

Come detto, vi sono risultati di eliminazione dei quantificatori anche recenti; ma l'intero argomento dell'eliminazione dei quantificatori è assai classico, e la sua origine risale a quasi un secolo fa. Come già osservato, un aspetto che a quei tempi era parzialmente trascurato e che invece ha assunto oggi maggiore rilevanza riguarda l'efficienza (la rapidità) dei procedimenti di eliminazione: in effetti, la nascita dei moderni calcolatori e l'avvio della loro scienza ha ispirato questo interesse prevalente per algoritmi che lavorano in tempi veloci. Così, in Informatica Teorica la Teoria della Complessità ha introdotto

- la classe P dei problemi che ammettono una procedura rapida che *determina* le soluzioni,

- la classe NP dei problemi che hanno una procedura rapida che *verifica* le soluzioni (e cioè controlla se una data soluzione funziona).

Accogliendo una proposta di Edmonds-Cook-Karp, la Complessità definisce poi una procedura «*rapida*» se essa lavora al più in tempo polinomiale rispetto alla lunghezza dell'input. Per realizzare la differenza tra trovare e verificare soluzioni, consideriamo ad esempio il *Problema della Primalità*, la questione cioè di riconoscere se

un dato intero $\geqslant 2$ è primo o composto (problema celebrato anche da Gauss nelle sue Disquisitiones Arithmeticae del 1801 come «*importante ed utile, … elegante e famoso*»). Algoritmi capaci di distinguere gli uni dagli altri e, se è per questo, anche di decomporre ogni intero composto nel prodotto dei suoi fattori primi erano noti sin dall'antichità ma si basavano su pazienti e prolungate verifiche. Quelle che dunque si imponevano, ed anche Gauss sollecitava, erano procedure più brillanti e veloci. Ma si è dovuto attendere il 2002 per avere finalmente una risposta positiva al problema, grazie all'algoritmo polinomiale di primalità proposto qualche mese fa dai 3 ricercatori indiani Agrawal, Kayal e Saxena (e già battezzato AKS dalle loro iniziali) [1]. Ma, a prescindere da questi recentissimi sviluppi, non è difficile riconoscere che stabilire che un numero è composto (per veloce che sia il tempo richiesto) può essere talora significativamente più lento che verificare che un numero composto è, appunto, tale. Per citare un esempio famoso, ricordiamo che F. Cole annunciò nel 1903, durante un convegno dell'American Mathematical Society, che il numero di Mersenne $2^{67} - 1$ non è primo. Questo non è facile da provare, e certamente non lo era nel 1903, quando mancavano i moderni calcolatori. Pur tuttavia la dimostrazione di Cole è brevissima da scrivere (ed anche da verificare), visto che richiede un solo rigo $2^{67} - 1 = 193797721 \times 761838257287$.

Tornando a P e NP, è banale osservare che $P \subseteq NP$ perché un algoritmo che produce soluzioni è anche implicitamente capace di confermare queste soluzioni. Un problema fondamentale in Teoria della Complessità (e, più in generale, nell'ampio spazio di ricerca comune a Matematica e Informatica) chiede se addirittura $P = NP$, quindi se, tutte le volte che un problema ammette un procedimento rapido di verifica delle soluzioni, allora può anche disporre di un algoritmo, magari più lento e pur tuttavia ancora polinomiale, per trovare le soluzioni. Come detto, il problema è ancora oggi aperto e dibattuto: [3] ne dà maggiori dettagli e riferimenti.

Entro questi nuovi orizzonti, quello che diventa fondamentale anche nell'ambito dell'eliminazione dei quantificatori (soprattutto in collegamento alla decidibilità) è l'efficienza delle relative procedure. Discutiamo questo punto nel caso del campo ordinato dei reali (e dei

campi reali chiusi). C'è qui infatti un importante risultato di Fischer e Rabin del 1974 che è tanto profondo nella dimostrazione quanto disastroso nelle conseguenze, e dice:

TEOREMA. – Un algoritmo che decide, o anche solo verifica, la verità nel campo reale di un enunciato del linguaggio dei campi ordinati richiede (talora) un tempo di lavoro almeno esponenziale rispetto alla lunghezza dell'input. Lo stesso vale per il campo complesso e il linguaggio dei campi.

(A questo proposito, va aggiunto che non si conosce nessuna classe di strutture infinite che sia decidibile in tempo polinomiale e si sa che, se una tale classe esiste, allora se ne può dedurre $P = NP$). Circa poi la eliminazione dei quantificatori, bisogna ammettere che i procedimenti di Tarski per reali e complessi sono assai lenti e poco efficienti. Recentemente sono stati introdotti per i reali metodi di eliminazione più veloci e potenti: citiamo la procedura di Collins denominata *CAD* (*decomposizione algebrica cilindrica*), che tuttavia lavora nei casi peggiori in tempo doppiamente esponenziale rispetto al numero delle variabili nella formula di input, e anche successive implementazioni di *CAD*.

Ma vogliamo ora trattare brevemente un altro affascinante collegamento tra Teoria dei Modelli (in particolare, eliminazione dei quantificatori) e Teoria della Complessità. In computabilità classica, si conviene che un problema ammette un algoritmo di soluzione quando c'è una macchina di Turing che lo risolve. Questa ipotesi di lavoro, avanzata negli anni trenta e comunemente chiamata Tesi di Church e Turing, sembra per certi versi ancora adeguata ai nuovi sviluppi dell'Informatica; pur tuttavia il modello di Turing ha un carattere essenzialmente *discreto*, e la sua applicazione a contesti *continui* come quello reale e complesso sembra travagliata e poco naturale. In effetti, se rappresentiamo un reale nella forma decimale (con un allineamento decimale eventualmente infinito dopo la virgola), anche la sola verifica che due reali sono uguali pare, dal punto di vista di Turing, proibitiva: una macchina potrà controllare che i due input coincidono fino alla milionesima, o alla miliardesima cifra deci-

male, ma non dedurne la definitiva uguaglianza. Conseguentemente sono stati proposti di recente nuovi modelli di computazione, capaci di accettare numeri reali o complessi come possibili input, e di lavorare addirittura con strutture arbitrarie. Il più famoso di questi modelli è denotato *BSS* (dalle iniziali di chi l'ha introdotto: Blum, Shub, Smale [2]). Esso allarga il punto di vista di Turing (ed in effetti la classica computabilità secondo Turing corrisponde, in questa nuova prospettiva, alla computabilità sull'anello $(\boldsymbol{Z}, +, \cdot)$ degli interi); pur tuttavia consente, come detto, una computabilità su ogni struttura $\mathcal{A}$. In particolare, per ogni $\mathcal{A}$ si possono considerare le classi P e NP (riferite ad $\mathcal{A}$), confrontare queste classi e controllare se $P = NP$ su $\mathcal{A}$. Introdurre questi argomenti in dettaglio richiederebbe un tempo troppo lungo, possiamo comunque sottolineare il seguente risultato, che collega la nostra Teoria dei Modelli, e l'eliminazione dei quantificatori, alla Complessità.

TEOREMA. – Se $P = NP$ su $\mathcal{A}$, allora $\mathcal{A}$ elimina i quantificatori (ed anzi ha un algoritmo rapido di eliminazione).

È relativamente semplice convincersi del perché. Riferiamoci ancora all'esempio di Cole riferito poco fa: in quell'ambito, provare che $2^{67} - 1$ è composto richiede di garantire un qualche divisore non banale e dunque, in definitiva, ottenere una qualche coppia di testimoni all'enunciato esistenziale $\exists w \exists w' (2^{67} - 1 = w \cdot w' \wedge w, w' \neq 1)$; ma, dopo Cole, noi dobbiamo semplicemente verificare l'equazione $2^{67} - 1 = 193797721 \times 761838257287$. Dunque la situazione configura proprio un procedimento di eliminazione dei quantificatori.

Come conseguenza del precedente teorema, si ottengono vari esempi di strutture $\mathcal{A}$ su cui $P \neq NP$: è questo il caso dei razionali (come campo e come campo ordinato) o dei reali (come campo, senza la relazione di ordine), si sa infatti che le relative strutture non eliminano i quantificatori. D'altra parte esistono modelli che hanno l'eliminazione dei quantificatori e che pur tuttavia devono condividere la negativa conclusione $P \neq NP$: un esempio riguarda ancora i reali, intesi stavolta come gruppo rispetto alla sola addizione. Non è invece chiaro se $P = NP$ per il campo ordinato dei reali, o per il campo

dei complessi. Val la pena di riferire che, in quest'ultimo caso, un problema chiave («*NP-completo*») verso la soluzione della questione riguarda un classico teorema di algebra, quel *Teorema degli Zeri di Hilbert* che, come vedremo nel prossimo paragrafo, ha altri profondi collegamenti con la Teoria dei Modelli. Una possibile formulazione del teorema afferma quanto abbiamo già avuto modo di sottolineare nel paragrafo sulla definibilità, e cioè che

> nel campo complesso (e, se è per questo, in ogni campo algebricamente chiuso) qualunque sistema finito di equazioni, che abbia soluzione in qualche estensione, ha già qualche radice.

Ebbene, Blum, Shub e Smale provano che $P = NP$ vale sul campo complesso se e solo se si riesce a trovare un procedimento rapido per controllare la risolubilità di un qualunque sistema di polinomi a coefficienti complessi.

4. – La model completezza.

Se non c'è eliminazione dei quantificatori e dunque nella gerarchia dei definibili si ha bisogno anche di coinvolgere le proiezioni, il caso più favorevole si ha quando la prima applicazione di queste ultime esaurisce già tutto il procedimento. È facile convincersi che questo fenomeno si manifesta quando nelle strutture in esame ogni formula $\varphi(\vec{v})$ equivale ad una formula («*esistenziale*») $\exists \vec{w} \varphi^*(\vec{v}, \vec{w})$ con φ^* priva di quantificatori. Una classe $\mathcal{K}$ di strutture con questa proprietà si dice *model-completa*. Dunque, in una classe model-completa si ha

$$definibile = proiezione\ \ di\ \ costruibile.$$

L'aggettivo model-completo è una pessima traduzione italiana, ormai invalsa nell'uso (degli interessati), dell'inglese *model complete*, che forse avrebbe meritato un migliore adattamento alla nostra lingua.

Il concetto di model-completezza venne elaborato alla fine degli anni cinquanta da Abraham Robinson, ed è ispirato dall'Algebra. In effetti, un modo equivalente di introdurlo è il seguente: una classe

elementare $\mathcal{K}$ di strutture di un linguaggio L è model-completa se e solo se ogni struttura $\mathcal{A}$ che ne fa parte soddisfa qualunque sistema finito di equazioni e disequazioni che ha parametri in A e soluzioni in qualche estensione di $\mathcal{A}$ in $\mathcal{K}$: una situazione che richiama il Teorema degli Zeri di Hilbert enunciato alla fine del precedente paragrafo (e, in effetti, la classe dei campi algebricamente chiusi è model-completa).

Abraham Robinson provò l'equivalenza tra la model-completezza così come è stata precedentemente definita e la caratterizzazione algebrica che abbiamo appena dato; diede altri significativi criteri necessari e sufficienti per provarla; applicò questi criteri a varie specifiche classi. In particolare, mostrò che la classe dei campi algebricamente chiusi è model-completa (come abbiamo appena sottolineato), e che lo stesso vale per la classe dei campi reali chiusi: una coppia di risultati già impliciti nei precedenti lavori di Tarski (perché l'eliminazione dei quantificatori è ovvia condizione sufficiente per la model-completezza) ma ribaditi in altra via, atta a sottolineare le non marginali connotazioni algebriche. Nei casi specifici ora ricordati, Abraham Robinson dedusse poi dal suo approccio alcune rilevanti applicazioni algebriche e, tra queste, una chiara ed elegante dimostrazione del citato Teorema degli Zeri di Hilbert, o anche della soluzione di Artin-Schreier del XVII problema dello stesso Hilbert (quello che afferma che ogni funzione razionale $f(\vec{x})$ a coefficienti reali e valori ovunque non negativi deve essere una somma di quadrati in $\boldsymbol{R}(\vec{x})$).

Fig. 1. – Emil Artin.

Come già sottolineato, ogni struttura $\mathcal{A}$ di una classe model-completa $\mathcal{K}$ è capace di soddisfare qualunque sistema di equazioni e disequazioni a coefficienti in A che sia già risolubile in qualche estensione di $\mathcal{A}$. In una classe che non è model-completa, invece, esiste qualche struttura che non rispetta più questa proprietà di chiusura; può tuttavia capitare che qualche altra struttura di $\mathcal{K}$ riesca ancora a soddisfarla; può addirittura succedere che queste ultime strutture siano sufficientemente dense in $\mathcal{K}$, al punto da estendere ogni possibile altro modello di $\mathcal{K}$. Ci sono ambienti familiari dell'algebra in cui riconosciamo questa situazione. Ad esempio, la classe di tutti i campi non è model-completa, ci sono tuttavia campi che hanno la proprietà di chiusura sopra descritta: il teorema degli zeri di Hilbert li identifica come i campi algebricamente chiusi, e sappiamo che ogni campo si estende ad un ampliamento algebricamente chiuso, ed anzi ad un minimo ampliamento algebricamente chiuso (la sua *chiusura algebrica*). La stessa situazione si riscontra fra i campi ordinati. La loro classe non è model-completa, ma ci sono campi ordinati $\mathcal{A}$ capaci di soddisfare ogni sistema di equazioni e disequazioni con coefficienti in A e soluzione in qualche estensione (ordinata) di $\mathcal{A}$: essi coincidono con i campi reali chiusi. Di nuovo, apprendiamo dai manuali di Algebra che ogni campo ordinato ha qualche estensione reale chiusa, ed anzi un minimo ampliamento reale chiuso (la sua *chiusura reale*). Il discorso si può ovviamente generalizzare ad una qualunque classe elementare $\mathcal{K}$ in un linguaggio L. Sulla base dei due ultimi esempi ci chiediamo se possiamo individuare una sottoclasse di strutture di $\mathcal{K}$ che siano

a) abbastanza ricche da risolvere ogni ragionevole sistema di equazioni e disequazioni che possa proporsi in L a loro riguardo,

b) abbastanza frequenti in $\mathcal{K}$ da estendervi ogni possibile struttura

e che dunque si comportino come i campi algebricamente chiusi tra i campi e come i campi reali chiusi tra i campi ordinati. È naturale chiamare queste strutture, se pur esistono, *algebricamente chiuse*, o anche *esistenzialmente chiuse*, in riferimento alla prima condizione che le definisce, quella relativa all'«esistenza» di soluzioni.

Si mostra che l'esistenza della nostra sottoclasse è vincolata -non sorprendentemente- dalla natura di $\mathcal{K}$, meglio ancora dalla sua assiomatizzazione, che deve coinvolgere enunciati dela forma $\forall \vec{v} \exists \vec{w} \alpha(\vec{v}, \vec{w})$ con $\alpha(\vec{v}, \vec{w})$ formula senza quantificatori -in particolare enunciati universali o esistenziali- ma niente di più complicato (come è facile controllare nel caso dei due esempi proposti); del resto molte classi di strutture algebriche (i gruppi, gli anelli, gli ordini, i grafi) soddisfano questa condizione. Ma a questo punto si può osservare che i campi esistenzialmente chiusi -cioè i campi algebricamente chiusi- e i campi ordinati esistenzialmente chiusi -cioè i campi reali chiusi- formano anch'essi classi elementari e conseguentemente ci si può chiedere: è vero che per ogni classe elementare $\mathcal{K}$ la classe delle strutture esistenzialmente chiuse in $\mathcal{K}$ è anch'essa elementare? A questo proposito si possono incontrare delle sorprese, perché la risposta può essere negativa: questo è quanto capita, ad esempio, per gruppi, o anelli commutativi unitari. In questi casi, ci sono certamente

– gruppi esistenzialmente chiusi
– anelli commutativi unitari esistenzialmente chiusi

ma ci sono gruppi, anelli commutativi unitari rispettivamente che *non* sono più esistenzialmente chiusi, eppure condividono gli stessi enunciati. Coloro che osservarono queste anomalie furono Eklof e Sabbagh nel caso dei gruppi e Cherlin nel caso degli anelli; ambedue le dimostrazioni coinvolgono (prevedibilmente) il Teorema di Compattezza. Chi invece sviluppò l'intera teoria astratta delle strutture esistenzialmente chiuse fu Abraham Robinson.

Maggiori dettagli su tutto l'argomento e sulla sua storia possono trovarsi in [5].

5. – Ancora insiemi definibili.

È ormai tempo di aggiungere alla lista di esempi di insiemi definibili, che ha allietato il paragrafo 4 di [4], nuovi importanti casi. Il motivo per cui abbiamo ritardato a trattarli è il fatto che essi richiedono una minima familiarità con i concetti di classe model-completa

e di struttura esistenzialmente chiusa appena proposti. Del resto, la loro analisi in Teoria dei Modelli risale talora a pochissimi anni fa. Inoltre, i nuovi casi hanno un'altra caratteristica da non trascurare: per ciascuno di essi, la Teoria dei Modelli ha significativamente preceduto e illuminato la ricerca algebrica, come adesso cercheremo di spiegare. Tratteremo nell'ordine:

1. i campi differenzialmente chiusi,
2. l'esponenziazione reale.

1. L'*algebra differenziale* nacque sin dagli anni trenta principalmente su impulso di Ritt. Il suo interesse si concentra su insiemi K di funzioni che si possono sommare e moltiplicare in modo da formare un campo, oppure più semplicemente un anello commutativo, ed in più ammettono un'ulteriore operazione 1-aria D che soddisfa le usuali regole di derivazione:

$$D(a+b) = Da + Db, \quad D(a\cdot b) = a\cdot Db + b\cdot Da$$

per ogni scelta di due funzioni $a, b \in K$. La struttura che così si ottiene si chiama *campo* (o *anello*) *differenziale*. Notiamo che qualunque campo K diviene un campo differenziale se poniamo $D = 0$ uniformemente; ma questo esempio è poco interessante. Ne esistono altri più rilevanti, come:

- $\left(\mathcal{K}(x), \frac{d}{dx}\right)$ dove $\mathcal{K}$ è un campo, $\mathcal{K}(x)$ è il campo delle funzioni razionali in x a coefficienti in $\mathcal{K}$ e $\frac{d}{dx}$ è l'usuale operazione di derivata (quella che associa ad ogni $f \in K(x)$ la sua funzione derivata).

L'Algebra differenziale studia queste strutture, elaborando gli opportuni strumenti di analisi. Ad esempio, invece di polinomi (algebrici) $f(x) \in \mathcal{K}[x]$, si considerano polinomi differenziali in x: si tratta di polinomi nelle indeterminate $x, Dx, \ldots, D^n x, \ldots$ per n naturale. Ai gradi di un tale polinomio $f(x) \neq 0$ (rispetto alle sue numerose variabili) si accompagna il concetto di *ordine* di $f(x)$: il massimo naturale n tale che $D^n x$ occorre significativamente in $f(x)$ se un tale n esiste, e -1 se $f(x)$ è costante.

Da un punto di vista logico i campi differenziali possono essere vi-

sti come strutture del linguaggio L che amplia quello dei campi tramite un simbolo D di operazione 1-aria (per la derivazione). In questo ambito, le formule atomiche corrispondono ad equazioni differenziali riguardanti i polinomi differenziali $f(x)$ appena introdotti.

Uno sguardo all'assiomatizzazione dei campi differenziali assicura che ha senso considerare campi differenziali esistenzialmente chiusi, dunque oggetti matematici che soddisfano la proporzione

$$\textit{campo} : \textit{campo algebricamente chiuso} =$$
$$\textit{campo ordinato} : \textit{campo ordinato reale chiuso} =$$
$$\textit{campo differenziale} : ???$$

Ci chiediamo quale ne sia la natura e se sia possibile assiomatizzarli al primo ordine.

Per affrontare la questione, conviene lavorare in caratteristica 0 (se la caratteristica è un numero primo, la trattazione si può fare ma diventa un po' più complicata). Sotto questa ipotesi Abraham Robinson (1959) e Lenore Blum (1968) risolsero la questione. Più precisamente, A. Robinson fu il primo a provare che la classe di campi differenziali esistenzialmente chiusi è elementare; ma solo Lenore Blum riuscì a darne una semplice ed elegante assiomatizzazione al primo ordine. Eccone la descrizione.

Un campo differenziale $(\mathcal{K}, D)$ si chiama *differenzialmente chiuso* se, per ogni scelta di polinomi differenziali $f(x)$ e $g(x)$ a coefficienti in K tali che l'ordine di $f(x)$ è maggiore di quello di $g(x)$, esiste $a \in K$ per cui $f(a) = 0$ ma $g(a) \neq 0$.

Lenore Blum provò che i campi differenzialmente chiusi sono appunto i campi differenziali esistenzialmente chiusi (in caratteristica 0). In particolare, ogni campo differenziale $(\mathcal{K}, D)$ si estende ad un campo differenzialmente chiuso. In più, si prova che c'è un minimo ampliamento di tal forma (come ogni campo ha un minimo ampliamento algebricamente chiuso – la sua *chiusura algebrica* – ed ogni campo ordinato ha un minimo ampliamento reale chiuso – la sua *chiusura reale* –): questa estensione si chiama, in analogia con gli altri casi citati, la *chiusura differenziale* di $(\mathcal{K}, D)$. La sua esistenza e unicità furono dimostrate da Lenore Blum come conseguenza del suo studio sui campi differenzialmente chiusi e come applicazione di

risultati astratti generali di Teoria dei Modelli (certamente trascendenti l'ambito differenziale) dovuti a Morley e Shelah. È da sottolineare che esistenza e unicità della chiusura differenziale, così come lo stesso concetto di campo differenzialmente chiuso, sono questioni essenzialmente algebriche; e pur tuttavia la loro prima, e finora unica, introduzione è quella, ottenuta con metodi di Teoria dei Modelli, di Lenore Blum. Anzi, allo stato attuale, nel 2004, non si conosce ancora in Algebra alcun esempio esplicito di campo differenzialmente chiuso, qualcosa, insomma, che illustri ed incarni la nozione, come il campo complesso fa tra i campi algebricamente chiusi, e il campo reale fa tra quelli reali chiusi.

Concludiamo la trattazione dei campi differenzialmente chiusi descrivendo quali sono gli insiemi definibili in queste strutture.

Dai risultati di Lenore Blum si deduce la classe dei campi differenzialmente chiusi $(\mathcal{K}, D)$ (di caratteristica 0) ha l'eliminazione dei quantificatori nel suo linguaggio. In particolare, sono definibili tutti e soli gli insiemi di soluzioni di polinomi differenziali, insieme alle loro combinazioni Booleane finite. Tali insiemi sono usualmente chiamati *insiemi costruibili secondo Kolchin*, in riferimento all'analogo concetto di insieme costruibile elaborato per i campi, e al nome di Kolchin, un matematico che molti contributi (ed un intero libro) ha dedicato allo studio degli anelli differenziali. In altre parole, gli insiemi di soluzioni di polinomi differenziali e le semplici operazioni Booleane tra insiemi bastano a produrre tutto quanto è definibile in $(\mathcal{K}, D)$, senza neppure bisogno di scomodare le proiezioni:

$$definibile = costruibile \ \ secondo \ \ Kolchin.$$

Nuovamente, la definibilità ha una caratterizzazione assai elementare, anche se per $n = 1$ si incontrano insiemi definibili di assai maggiore complicazione rispetto ai finiti e ai loro complementari (come invece avviene tra i campi algebricamente chiusi).

2. Adesso consideriamo l'espansione – usualmente denotata $\boldsymbol{R}_{exp}$ – del campo reale tramite la funzione esponenziale $exp : x \mapsto e^x$ per ogni $x \in \boldsymbol{R}$. Questa struttura rappresenta il contesto di una classica *Congettura di Tarski*, che chiede un algoritmo di decisione per riconoscere gli enunciati che vi sono veri: si tratta di capire quali siano i

fondamenti algebrici della esponenziazione reale. Il problema di Tarski è ancora aperto, ed anzi recenti risultati ne sottolineano le profonde difficoltà, collegandolo a questioni classiche, quali l'indipendenza algebrica di π ed e. Pur tuttavia la struttura $\boldsymbol{R}_{exp}$ è, adesso, abbastanza ben conosciuta dal punto di vista della Teoria dei Modelli. Chiamiamo infatti *esponenziale* un sottoinsieme E di $\boldsymbol{R}^n$ costituito dalle soluzioni di un'equazione esponenziale

$$f(x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}) = 0$$

con f polinomio a coefficienti reali. È ovvio che ogni insieme esponenziale è definibile in $\boldsymbol{R}_{exp}$; si può poi osservare che gli insiemi esponenziali sono chiusi per unioni e intersezioni finite, ma non per complementazione. Gli insiemi esponenziali e le loro combinazioni Booleane non bastano comunque ad esaurire la classe di tutti gli insiemi definibili in $\boldsymbol{R}_{exp}$ (e nelle strutture elementarmente equivalenti), come notato da Van den Dries sin nel 1982: la relativa teoria non ha l'eliminazione dei quantificatori. Dobbiamo allora considerare le proiezioni di insiemi esponenziali (abitualmente chiamate *insiemi subesponenziali*): tuttavia, nel 1991, Wilkie dimostrò che l'itinerario di ricerca degli insiemi definibili finisce qui, perché in $\boldsymbol{R}_{exp}$

$$definibile = subesponenziale.$$

In altre parole, la classe delle strutture elementarmente equivalenti a $\boldsymbol{R}_{exp}$ è model-completa.

Wilkie dedusse anche per $n = 1$

$$definibile = unione\ finita\ di\ intervalli,$$

come già accade per il campo ordinato dei reali, o anche per l'ordine dei reali senza ulteriore struttura algebrica. Maggiori dettagli sull'argomento si trovano in [7].

6. – Indipendenza e dimensione.

Dopo aver illustrato nelle pagine precedenti alcune tecniche atte ad identificare, nei casi favorevoli, gli insiemi definibili ed aver proposto alcuni esempi rilevanti in cui queste tecniche sono applicate con successo, arriviamo finalmente in questo paragrafo al punto cru-

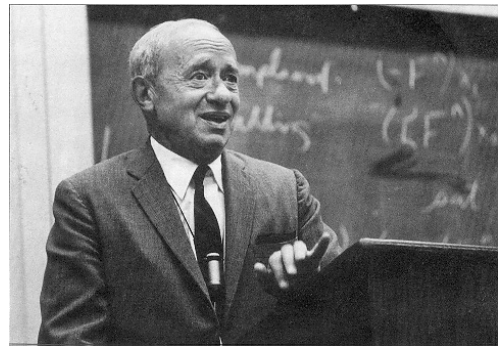

Fig. 2. – Alfred Tarski al Tarski Symposium nel 1971.

ciale della moderna Teoria dei Modelli, e cioè: come sviluppare l'analisi astratta degli insiemi definibili in strutture arbitrarie. Cerchiamo di fissare i termini della questione. Abbiamo una classe $\mathcal{K}$ di strutture, che supponiamo *elementare* (cioè assiomatizzabile al primo ordine), e magari anche *completa* (questo significa che tutti i modelli di $\mathcal{K}$ soddisfano gli stessi enunciati del loro linguaggio); assumiamo poi che le strutture di $\mathcal{K}$ siano infinite. Il nostro obiettivo è misurare la complessità degli insiemi definibili all'interno di $\mathcal{K}$, assegnando a ciascuno di loro un'appropriata *dimensione*, definita in modo astratto ma (possibilmente) corrispondente alle usuali nozioni di Algebra e Geometria nei casi classici di varietà e spazi vettoriali.

Ma, prima di iniziare l'analisi, c'è un'ulteriore cautela che dobbiamo prendere, come il seguente esempio ci mostra.

Nel linguaggio $\{\leqslant\}$ consideriamo l'ordine discreto con primo ma non ultimo elemento $(\boldsymbol{N}, \leqslant)$. Come abbiamo visto nella prima parte del lavoro, i sottoinsiemi di $\boldsymbol{N}$ definibili in questa struttura si riducono alle unioni finite di intervalli e, quindi, viste le proprietà dell'ordine dei naturali, sono finiti o cofiniti. L'intero dominio, definito ad esempio dalla formula $v = v$, è quello che si chiama un insieme *minimale*: è infinito, ma non si può ripartire in alcun modo come unione disgiunta di due sottoinsiemi definibili entrambi infiniti. D'altra parte, nella classe dei modelli degli stessi enunciati di $(\boldsymbol{N}, \leqslant)$ – che, per l'appunto, coincidono proprio con gli ordini discreti con primo e non ultimo elemento – possiamo costruire, magari con il Teorema di

Compattezza, altre strutture più complicate; ad esempio si vede che l'ordine costituito dai naturali $(\boldsymbol{N}, \leqslant)$ seguiti da una o più copie degli interi $(\boldsymbol{Z}, \leqslant)$ condivide le stesse proprietà del primo ordine di $(\boldsymbol{N}, \leqslant)$. In questo ambiente esteso ci sono tutti i parametri naturali e dunque si incontrano tutte le potenzialità di definizione che c'erano in $(\boldsymbol{N}, \leqslant)$, ed altre ancora, derivanti dai nuovi elementi. Ma questa maggiore definibilità cambia sostanzialmente la situazione. Ad esempio possiamo adesso certamente immaginare intervalli infiniti il cui complementare è pure infinito, e dunque l'intero dominio (definito ancora dalla stessa formula $v = v$) non è più minimale e assume maggiore complessità rispetto a quel che sembrava quando ci limitavamo a guardare i naturali. In altre parole, restringere lo sguardo alla struttura dei naturali non ci fa cogliere adeguatamente la esatta natura degli insiemi definibili.

Conviene allora, in generale, allargare l'analisi a strutture di $\mathcal{K}$ che siano abbastanza ricche da garantire un quadro completo di tutta la situazione. Tali strutture si possono formare in ogni classe elementare $\mathcal{K}$, usando un po' di Compattezza e magari scomodando (ma non in modo decisivo) qualche ipotesi di Teoria degli Insiemi, e si chiamano *modelli saturati* di $\mathcal{K}$. A prescindere dai dettagli tecnici della loro costruzione, questi modelli saturati corrispondono ad un'idea già presente nella Geometria Algebrica (sviluppata, ad esempio, da André Weil): quella dei *domini universali*, strutture (nella fattispecie di Weil, campi) talmente ampie e ricche che vi si può immergere ogni altra struttura che possa interessarci. Il riferimento a questi modelli è dunque pienamente giustificato.

A questo punto, chiarito il contesto, puntiamo a definire una *dimensione* per ogni insieme definibile nel dominio universale di $\mathcal{K}$ (che denoteremo con Ω). Ma ogni buona dimensione fa riferimento ad un preliminare concetto di *indipendenza* su cui fondarsi. Così il nostro primo obiettivo è proprio quello di definire una nozione astratta di indipendenza, che generalizzi i casi classici (l'indipendenza lineare negli spazi vettoriali, l'indipendenza algebrica nei campi, e così via). Da un punto di vista formale, l'indipendenza può essere vista come una relazione ternaria che coinvolga

- un elemento a di Ω
- due sottoinsiemi A, B di Ω

e che sia capace di chiarire il significato dell'affermazione «*a è indipendente da B su A*». In questa luce, l'*indipendenza* può essere introdotta assiomaticamente specificando quali proprietà le possono essere ragionevolmente richieste. Così l'esame degli esempi più classici di indipendenza suggerisce alcune trasparenti condizioni quali

- la *simmetria*: se a dipende da b su A, allora b dipende da a su A;
- la *transitività*: per $A \subseteq B \subseteq C$, a è indipendente da C su A se e solo se lo è da C su B e da B su A.

Ci sono poi altre proprietà meno evidenti ed immediate, ma tuttavia ancora pienamente giustificate dal riferimento agli esempi, e dunque inseribili nella nostra lista di assiomi.

Ma il punto cruciale in ogni assiomatizzazione non è tanto quello di accumulare proposizioni più o meno evidenti, quanto di cogliere i caratteri fondamentali del concetto che si sta studiando: esercizio, questo, che si ammetterà assai complicato quando si vuol trattare l'indipendenza in forma assolutamente astratta.

Il primo che si cimentò nell'impresa (in Teoria dei Modelli) fu S. Shelah negli anni '70-'80. In realtà, l'intento principale di Shelah era un po' diverso, e comunque assai ambizioso. Il suo programma era, infatti, quello di elencare le proprietà chiave atte a garantire che le strutture della nostra classe $\mathcal{K}$ siano classificabili, si possano cioè «etichettare» con invarianti quali numeri cardinali, o sequenze ordinate di cardinali, e così via, che ne determinino perfettamente il tipo di isomorfismo (allo stesso modo in cui, per riferirci a casi tutto sommato semplici e comuni, la dimensione di uno spazio vettoriale o il grado di trascendenza di un campo algebricamente chiuso di fissata caratteristica li caratterizzano a meno di isomorfismo).

Impegno gagliardo, come diceva; tra l'altro si ricorderà che, grazie al teorema di Löwenheim-Skolem di cui abbiamo parlato in [4], $\mathcal{K}$ ha modelli in ogni cardinalità infinita; qualche computazione sui car-

dinali assicura poi che può talora averne fino a 2^{λ} modelli (non isomorfi) in ogni data cardinalità infinita λ.

Non sorprendentemente, Shelah concluse (con argomentazioni serie e fondate) che una tale dovizia di modelli (2^{λ} per ogni possibile λ più che numerabile) fosse un sostanziale ostacolo, quasi un divieto, ad ogni ragionevole speranza di classificare strutture e definibili in $\mathcal{K}$. Elaborò conseguentemente una nozione astratta di indipendenza (da lui chiamata indipendenza del *forking*, in italiano potremmo dire indipendenza di *deviazione*) che soddisfa le trasparenti proprietà sopra elencate ed altre più oscure ma quasi altrettanto cruciali; individuò certe classi $\mathcal{K}$ (da lui battezzate *stabili*) in cui un'indipendenza da forking può essere introdotta, provò che questa indipendenza è l'unica possibile nelle classi stabili; dimostrò che le classi non stabili $\mathcal{K}$ hanno troppi modelli (nel senso sopra precisato) e dunque possono essere trascurate nell'ottica della classificazione.

Esempi di classi stabili sono gli spazi vettoriali, i campi algebricamente chiusi, i campi differenzialmente chiusi (in ogni caratteristica). Pur tuttavia si prova che la nozione di stabilità esclude altre rilevanti strutture e, tra esse, ogni classe di modelli linearmente ordinati (e infiniti): l'indipendenza del forking non le riguarda. Queste eccezioni possono stupire, visto che ci sono varie classi di strutture che espandono ordini lineari e sembrano manifestare un ottimo comportamento sia in Algebra che in Teoria dei Modelli e, soprattutto, buone nozioni di indipendenza e dimensione: ad esempio, i campi reali chiusi, o gli ordini lineari sia densi che discreti, o l'espansione reale $\boldsymbol{R}_{exp}$. Così il sospetto che la nozione di stabilità non sia l'«ultima parola» a proposito di un trattamento astratto dell'indipendenza e la necessità di individuare concetti più vasti e convincenti, tali da includere anche questi ultimi esempi ordinati, hanno condotto in questi ultimi anni, ed addirittura negli ultimi mesi, a nuovi sviluppi ancora in corso, per i quali è ragionevole sperare esiti pieni e convincenti. Il più notevole, che merita se non altro una rapida menzione, è quello di classe semplice di strutture. Ma una sua dettagliata introduzione ci porterebbe assai lontano, e sconfina dall'ambito di queste note. Rimandiamo allora, a suo proposito, ad esempio a [6].

Se comunque rivolgiamo la nostra attenzione a classi stabili $\mathcal{K}$ di

strutture, sappiamo di poter disporre di un'appropriata – ed anzi unica – nozione di indipendenza. Ciò che adesso ci interessa è un corrispondente concetto di *dimensione*, intesa come una funzione d che misura la complessità di tutti gli insiemi definibili, assegnando a ciascun X di loro, se possibile, un valore ordinale $d(X)$ in modo tale da soddisfare convenienti condizioni assiomatiche (ad esempio, $d(X) \leqslant d(Y)$ per $X \subseteq Y$) e soprattutto, da corrispondere alla nozione di indipendenza stabilita in $\mathcal{K}$.

Di nuovo, ci aspetta una sorpresa non totalmente gradita: la proprietà di *stabilità*, che pure garantisce un buon concetto di indipendenza, non è tuttavia sufficiente a fornire una corrispondente dimensione (almeno secondo gli assiomi di cui al capoverso precedente). Ad esempio la classe dei campi differenzialmente chiusi di caratteristica prima, che è stabile, non può essere dotata di una soddisfacente dimensione. Così si devono enucleare nuove condizioni teoriche per individuare le classi di strutture stabili che ammettono un buon concetto di dimensione; queste classi di strutture vengono chiamate *superstabili* ed includono vari esempi significativi come insiemi infiniti, spazi vettoriali, campi algebricamente chiusi in ogni caratteristica, campi differenzialmente chiusi di caratteristica 0, il gruppo additivo degli interi, e molti altri ancora, ma escludono, come detto, i campi differenzialmente chiusi di caratteristica prima, ed anche il campo ordinato dei reali, o la sua espansione $\boldsymbol{R}_{exp}$ (che del resto non sono neppure stabili). Shelah, Lascar ed altri identificarono le proprietà chiave atte ad assicurare la superstabilità. Chiarito in questo modo quali classi $\mathcal{K}$ di strutture ammettono una dimensione astratta d, resta da stabilire come d possa essere formalmente introdotta in queste classi. Ovviamente si può fare riferimento alle peculiarità algebriche di $\mathcal{K}$. Ad esempio, tra gli insiemi infiniti (senza ulteriori operazioni e relazioni, e dunque senza complicazioni), la dimensione può benissimo coincidere con la cardinalità; tra gli spazi vettoriali, l'usuale dimensione dell'Algebra Lineare funziona perfettamente; tra i campi algebricamente chiusi, le varietà algebriche e gli insiemi costruibili, la classica dimensione elaborata in Geometria Algebrica è concetto ottimo e collaudato, pienamente corrispondente alle richieste assiomatiche della superstabilità. Ma in Teoria dei

Modelli lavoriamo anche e soprattutto in astratto, e dunque ci interessa un concetto di dimensione ampio e generale, coincidente con gli esempi appena proposti nei casi specifici considerati, ma applicabile a contesti diversi ed ancora inesplorati. La più generale nozione astratta di dimensione, quella che in realtà si applica ad ogni classe superstabile, è chiamata rango U e denotata RU: fu introdotta da Lascar negli anni '80, in pieno accordo con il programma di Shelah. Prima di Lascar, Morley aveva proposto negli anni '60 una nozione di dimensione, detta appunto *rango di Morley* RM, e la aveva utilizzata per la dimostrazione di un suo celebre teorema (che afferma che, se una classe elementare ammette un solo modello a meno di isomorfismi in una cardinalità più che numerabile, allora ha un unico modello a meno di isomorfismi in ogni cardinalità più che numerabile). La fonte di ispirazione di Morley fu la classica analisi di Cantor-Bendixson degli spazi topologici, quella che assegna, se possibile, un numero ordinale ad ogni punto dello spazio considerato: 0 ai punti isolati, 1 ai punti che diventano isolati una volta che quelli di rango 0 sono dimenticati, e così via. In effetti, sappiamo che gli insiemi definibili formano un'algebra di Boole, e in tal modo corrispondono dualmente ad uno spazio topologico Booleano (cioè separato, compatto e totalmente sconnesso). Morley combinò questa strategia già conosciuta all'idea di riferirsi al dominio universale Ω per evitare ogni possibile patologia (come nell'esempio con cui abbiamo aperto il paragrafo).

La definizione di RM (e, se per questo, anche quella di RU) sono abbastanza complicate, ed esulano certamente dai propositi di queste note. Possiamo comunque accennare agli interessati che, non sorprendentemente, gli insiemi definibili di dimensione 0 secondo Morley sono quelli finiti, quelli di dimensione 1 sono gli infiniti che non si possono suddividere in un'infinità di sottoinsiemi definibili a 2 a 2 disgiunti tutti di cardinalità infinita, e così via. Quando il rango di Morley di X è un ordinale α, possiamo assegnare a X un intero positivo d, detto *grado di Morley* di X: si tratta del numero massimo di sottoinsiemi di X del suo stesso rango di Morley in una possibile partizione di X. Va detto che non è affatto immediato provare che questo

massimo esiste; anzi, la dimostrazione richiede profondi argomenti di combinatoria, come il Lemma di König.

Va comunque ammesso che il rango astratto di Morley è insufficiente a garantire una dimensione ad ogni insieme definibile in una classe superstabile di strutture. Ci sono casi in cui il rango resta indefinito (o, se preferite, supera ogni possibile ordinale): il gruppo additivo degli interi (ed i gruppi che ne condividono le proprietà esprimibili al primo ordine) hanno questa spiacevole peculiarità. D'altra parte il rango di Morley, quando è definito, va spesso a coincidere con rilevanti (e precedenti) nozioni algebriche. Ad esempio, tra i campi algebricamenti chiusi, per i quali gli insiemi definibili corrispondono alle combinazioni Booleane finite di varietà algebriche,

- il rango di Morley di una varietà V coincide esattamente con la dimensione di V, come elaborata in Geometria Algebrica,
- il grado di Morley di V coincide con il numero delle componenti irriducibili di dimensione massima in una decomposizione di V.

Lo stesso vale per gli spazi vettoriali W su un campo (contabile) F, per i quali il rango di Morley va sostanzialmente a coincidere con la classica dimensione dell'indipendenza lineare.

7. – Dimensione 1: gli insiemi fortemente minimali.

Il lettore che, scoraggiato dalle complicazioni del precedente paragrafo, ritenesse l'obiettivo di misurare la complessità (= il rango) dei definibili troppo complesso e faticoso potrebbe rivolgere il proprio interesse ad una questione certamente collegata ma, in un qualche senso, trasversale, e cioè: fissato un ordinale α, analizzare le classi di strutture in cui tutti i definibili hanno rango $\leqslant \alpha$. Chi poi volesse iniziare lo studio dai contesti più semplici (escludendo ovviamente il caso di strutture finite) si potrebbe concentrare su classi $\mathcal{K}$ di strutture $\mathcal{A}$ tutte di rango 1 (e magari anche grado 1) secondo Morley: dunque infinite, ma prive di sottoinsiemi definibili $X \subseteq A$ contemporaneamente infiniti e coinfiniti. Una tale classe $\mathcal{K}$ si dice *fortemente minimale*. In [4] abbiamo già avuto modo di incontrare 3 casi di classi fortemente minimali: infatti, accanto a

- gli insiemi infiniti

privi di ulteriori operazioni o relazioni (un esempio, dunque, non sorprendente da incontrare in questo ambito), ci sono anche situazioni di maggiore interesse algebrico, come

- gli spazi vettoriali,
- i campi algebricamente chiusi.

I numeri complessi, visti rispettivamente come semplice insieme, come gruppo abeliano, oppure come campo, forniscono un esempio per ciascuno dei tre casi: infatti, a prescindere dalla crescente complicazione algebrica e dal coinvolgimento progressivo delle operazioni di somma e prodotto, gli unici sottoinsiemi definibili di $\boldsymbol{C}$ si riducono sempre a quelli finiti o cofiniti. Naturalmente la differenza tra i tre casi c'è, e si avverte quando consideriamo i sottoinsiemi definibili di $\boldsymbol{C}^2$, $\boldsymbol{C}^3$, e così via. Nel caso degli insiemi, infatti, possiamo utilizzare soltanto il simbolo $=$ di uguaglianza, il che non permette di definire (neppure nelle potenze cartesiane di $\boldsymbol{C}$) niente di matematicamente rilevante, come potrebbe essere un *gruppo infinito*. Invece, nel caso degli spazi vettoriali, un *gruppo infinito* è esplicitamente presente, e dunque definibile, nella struttura; d'altra parte, come osservato in [4], le potenzialità espressive degli spazi vettoriali impediscono la definibilità di oggetti più complicati, come potrebbe essere un *campo infinito*. Nel terzo caso, invece, abbiamo esattamente un *campo infinito* (a proposito, c'è un teorema bello e famoso di Angus Macintyre del 1971 che prova che un campo infinito fortemente minimale deve essere algebricamente chiuso). Una domanda che è ragionevole porsi a questo punto è se vi sono «altri» esempi di classi fortemente minimali. Non si tratta di questione banale; il primo a porla fu Boris Zilber nel 1983, congetturando una risposta negativa. Occorsero comunque 10 anni per avere la soluzione del problema. Infatti solo nel 1993 Ehud Hrushovski mostrò la falsità della *Congettura di Zilber*, producendo un nuovo esempio di struttura fortemente minimale, non assimilabile a nessuno dei precedenti. La costruzione di Hrushovski ha sapore prevalentemente tecnico e combinatorio, e si basa su classici argomenti di Algebra Universale.

Ancor oggi, a 10 anni di distanza dalla sua proposizione, e nonostante i conseguenti tentativi di approfondirla e di coglierne la reale natura ed origine, resta una «patologia» non ancora completamente afferrata e compresa (anche se recenti lavori di Zilber ne sottolineano intriganti collegamenti con l'analisi complessa e con l'algebra di $(\boldsymbol{C}, +, \cdot, exp)$ – l'esponenziazione complessa –).

Così anche l'analisi delle classi di minor complessità quanto a dimensione si rileva quasi altrettanto ostica ed intricata del problema generale trattato nel precedente paragrafo: a smentire la apparente semplicità del contesto, vi affiorano nuovi misteri, problemi ed intrighi.

8. – O-minimalità.

Parliamo adesso di strutture ordinate. Come abbiamo già avuto modo di sottolineare, molte di esse (il campo ordinato dei reali, o la sua espansione $\boldsymbol{R}_{exp}$) consentono adeguate nozioni di indipendenza e di dimensione, che pur tuttavia non corrispondono alle richieste assiomatiche accennate nel paragrafo 6; anzi, proprio la presenza di un ordine totale implica l'esistenza di «troppi» modelli e dunque pregiudica, almeno nella prospettiva di Shelah, ogni possibile classificazione. Vale dunque la pena di approfondire la questione, e di analizzare queste classi di strutture ordinate, partendo semmai dai casi più semplici. Ora, in presenza di un ordine $\leqslant$ che va ad assommarsi all'uguaglianza $=$, dobbiamo forzatamente inserire tra gli insiemi definibili tutti gli intervalli; conseguentemente le situazioni meno complicate che possiamo incontrare in questo ambito corrispondono adesso alle strutture $\mathcal{A} = (A, \leqslant, \ldots)$ tali che ogni sottoinsieme definibile $X \subseteq A$ è unione finita di intervalli (eventualmente semirette): una tale struttura $\mathcal{A}$ si dice *o-minimale*. È fatto degno di nota che ipotesi così semplici e ridotte permettano tuttavia vasti e significativi risultati generali, che vanno a classificare, ad esempio, i sottoinsiemi definibili nelle potenze cartesiane $\mathcal{A}^n$ di $\mathcal{A}$ per ogni intero positivo n; è questo il contenuto di un teorema di decomposizione di Pillay, Steinhorn e Julia Knight. Ma è altresì rilevante osservare che le strutture o-minimali, cui questi importanti teoremi astratti si applicano, includono molteplici notevolissimi esempi: il campo dei reali è o-mini-

male (come implicitamente osservato in [4]); la sua espansione $\boldsymbol{R}_{exp}$ tramite la funzione esponenziale è, ugualmente, o-minimale (come accennato alla fine di § 5); e almeno quest'ultima struttura ha genuino interesse per l'Analisi Reale.

Tuttavia, altre semplici espansioni del campo reale legate all'analisi elementare non sono o-minimali. Ad esempio l'espansione di $\boldsymbol{R}$ con la funzione *sen* non può esserlo, perché la formula $sen\, v = 0$ vi definisce l'insieme $\pi\boldsymbol{Z}$ che non si riduce ad una unione finita di intervalli. Se però eliminiamo la condizione di periodicità che la funzione seno soddisfa ed è l'ostacolo sostanziale alla o-minimalità, e restringiamo *sen* all'intervallo $\left]\frac{\pi}{2}, -\frac{\pi}{2}\right[$ (dove *sen* si può addirittura invertire e comunque l'equazione $sen\, v = 0$ ha la sola radice 0), allora otteniamo di nuovo una struttura o-minimale. La cosa si generalizza. Infatti, se noi espandiamo il campo reale con *tutte* le funzioni analitiche reali, osservando l'unica cautela di restringerle, come nel caso della funzione *sen*, ad aperti U abbastanza piccoli, otteniamo una struttura o-minimale $\boldsymbol{R}_{an}$. Se poi aggiungiamo nuovamente a $\boldsymbol{R}_{an}$ la funzione esponenziale (considerata in tutto il suo dominio), quel che risulta è ancora una struttura o-minimale $\boldsymbol{R}_{an,\, exp}$. E la lista non si chiude certamente qui.

Come si vede, questi esempi insinuano collegamenti non marginali con Geometria Differenziale ed Analisi reale: in effetti, questa connessione è largamente studiata negli ultimi anni, con significative reciproche applicazioni.

9. – La congettura di Mordell-Lang.

Prima di concludere questa veloce presentazione delle Teoria dei Modelli del duemila e delle sue applicazioni non possiamo evitare un pur rapido accenno alla più famosa di queste conseguenze, e cioè alla soluzione di Hrushovski di un problema di Geometria Algebrica noto con il nome di *Congettura di Mordell-Lang*, tanto più che abbiamo già avuto modo di incontrare tutti i maggiori ingredienti della relativa dimostrazione. Ma cominciamo col presentare i termini della questione. Nel 1922 Mordell propose il seguente problema.

CONGETTURA DI MORDELL. – Siano F un campo di numeri (e cioè una estensione finita del campo razionale), e X una curva di genere $\geqslant 2$ su F. Allora X ha solo un numero finito di punti F-razionali.

Se già questa formulazione risulta ostica, possiamo aggiungere, per illustrare la congettura, che una sua soluzione positiva implica che la curva (proiettiva) determinata dall'equazione di Fermat

$$x^n + y^n = z^n, \quad n \geqslant 3$$

ha solo un numero finito di radici intere (nel piano proiettivo), e quindi garantisce che il famoso *Ultimo Teorema di Fermat* è almeno «asintoticamente vero» (nel senso, appunto, che per ogni n il numero delle soluzioni è, se non proprio 0, almeno finito).

Oggi sappiamo grazie a Wiles che l'Ultimo Teorema di Fermat è assolutamente vero, e dunque non abbiamo più bisogno di ricorrere alla Congettura di Mordell per trattarlo. Del resto anche la Congettura è stata risolta positivamente: ci riuscì Faltings nel 1983. Ma nel frattempo era stata proposto nel 1968 un suo ampliamento, che si chiama *Congettura di Mordell-Lang* ed usa il linguaggio non accessibilissimo della Geometria Diofantea. Ebbene, nel 1996 Hrushovski ha dato la prima dimostrazione di questa congettura nel caso più generale (su campi di funzioni di qualunque caratteristica), meritandosi così fama, premi, riconoscimenti (e qualche polemica) oltre i confini della Teoria dei Modelli.

Chi, interessato alla problematica e familiare con la Geometria Dio-

Fig. 3. – Pierre Fermat.

fantea, volesse maggiori informazioni sulla dimostrazione di Hrushovski potrebbe trovare nell'articolo espositivo [8] una bella discussione di tutto l'argomento e maggiori dettagli tecnici: in particolare, potrebbe apprezzare il ruolo che nella prova hanno vari concetti di Teoria dei Modelli incontrati in queste pagine, ad esempio il rango di Morley, la Congettura di Zilber, i campi differenzialmente chiusi. Concetti disparati per epoca e paternità vengono così a contribuire ad una dimostrazione profonda ed elegante, testimoniando in tal modo certamente della genialità dell'autore (Hrushovski) ma anche, per altri versi, di quanto fertile e omogeneo sia l'ambito che l'ha originata.

RIFERIMENTI BIBLIOGRAFICI

[1] M. AGRAWAL - N. KAYAL - N. SAXENA, *PRIMES is in P*, preprint (2002).
[2] L. BLUM - F. CUCKER - M. SHUB - S. SMALE, *Complexity and Real Computation*, Springer, New York (1998).
[3] P. CINTIOLI - C. TOFFALORI, *Logica Matematica*, McGraw-Hill, Italia (2000).
[4] S. LEONESI - S. L'INNOCENTE - C. TOFFALORI, *Cinquanta anni di Teoria dei Modelli*, in Boll. Un. Mat. Ital. A, La Matematica nella Società e nella Cultura, Serie VIII, Vol. VII-A (Agosto 2004), 347-381.
[5] A. MACINTYRE, *Model-Completeness*, in Handbook of Mathematical Logic (a cura di J. Barwise), North Holland, Amsterdam (1977), 139-180.
[6] A. MARCJA - C. TOFFALORI, *A guide to classical and modern Model Theory*, Kluwer (2003).
[7] D. MARKER, *Model Theory and exponentiation*, Notices Amer. Mth. Soc., **43** (1996), 753-759.
[8] A. PILLAY, *Model Theory and Diophantine Geometry*, Bull. Amer. Math. Soc., **34** (1997), 405-422.

Carlo Toffalori, Dipartimento di Matematica e Informatica
Università di Camerino, Via Madonna delle Carceri, 62032 Camerino, Italy.
E-mail: carlo.toffalori@unicam.it

Stefano Leonesi, Dipartimento di Matematica e Informatica
Università di Camerino, via Madonna delle Carceri, 62032 Camerino, Italy.
E-mail: stefano.leonesi@unicam.it

Sonia L'Innocente, Dipartimento di Matematica e Informatica
Università di Camerino, via Madonna delle Carceri, 62032 Camerino, Italy.
E-mail: sonia.linnocente@unicam.it