Bollettino U. M. I.
(4) **12** (1975), pp. 252-261

Metodi algebrici in teoria della dimostrazione.

ROBERTO MAGARI (Siena) (*)

Introduzione.

La teoria della dimostrazione (la cui fondazione, almeno come programma, si deve a Hilbert) studia, direbbero alcuni filosofi, il « grado di evidenza » dei processi (dimostrazioni) con i quali si riconosce in matematica la « validità logica ». Poichè ogni tentativo di precisare questa oscura definizione dipende da concezioni generali relative allo status della matematica e della metamatematica, in questa sede me ne asterrò, limitandomi ad osservare che la precisazione del « grado di evidenza » può essere intesa come classificazione ricorsiva di relazioni, problemi e teorie o come confronto col punto di vista intuizionistico o col punto di vista finistico etc...

Un importante settore di ricerche è stato inaugurato da Gentzen, che ha dimostrato, usando il principio di induzione transfinita fino a ε_0, la consistenza dell'aritmetica peaniana. Per notizie su questo settore e sui moderni sviluppi dell'intuizionismo si veda ad esempio G. KREISEL [11], [12], D. PRÄWITZ [21].

Un altro importante settore si rifà alla memoria di GÖDEL [8] ed è stato in un primo tempo sviluppato soprattutto da FEFERMAN [4, 5, 6] che ha ripreso anche talune idee di TURING [24]. Queste ricerche analizzano a fondo la situazione che sorge per l'aritmetica e per le teorie cui essa è riducibile in vista del lemma di diagonalizzazione e delle speciali proprietà del predicato Theor.

I metodi classici di algebrizzazione della logica che hanno portato allo studio delle algebre cilindriche e poliadiche non sono in grado di solito di render conto dell'aspetto *parzialmente autologo* delle teorie cui l'aritmetica è riducibile, nè permettono quindi lo studio e la classificazione delle teorie T che, come appunto l'aritme-

(*) Conferenza tenuta a Cagliari il 25 settembre 1975 in occasione del X Congresso U.M.I.

tica peaniana, « esprimono » il predicato « essere un teorema di T ».

Argomento di questa relazione sarà lo stato dei lavori nello studio di certe algebre che invece rendono conto di questi aspetti.

1. – Richiami elementari.

D'ora in poi con $\mathcal{T}$ si indicherà l'aritmetica peaniana al primo ordine e con T l'insieme dei suoi teoremi. « $\vdash p$ » starà per « $p \in T$ » e « $\models p$ » per « p è valida in ω » (insieme dei naturali munito delle ordinarie operazioni e relazioni elementari).

Come è ben noto si possono fissare:

(a) una iniezione computabile γ da ω all'insieme dei termini di $\mathcal{T}$: se $x \in \omega$ allora γx, che si indicherà anche con $\overline{x}$, si dice il « numerale di x e gli elementi di $\mathcal{C}\gamma$ si diranno « numerali »;

(b) una iniezione computabile δ dall'insieme E delle formule ben formate di $\mathcal{T}$ a ω (si scriverà $\ulcorner\alpha\urcorner$ per $\delta\alpha$ e $\ulcorner\alpha\urcorner$ si dirà il « gödeliano » di α: si scriverà talvolta $\bar{\alpha}$ per $\overline{\ulcorner\alpha\urcorner}$).

Ciò, insieme ad altre possibilità di contorno che non stiamo a richiamare, dà luogo a una situazione parzialmente autologa. Ricordiamo ancora che:

(c) *una* $\alpha(x_1, x_2, \dots, x_n) \in E$ *(con le n variabili libere $x_1, x_2, \dots, x_n$)* numera *una* $R \subseteq \omega^n$ *se si ha*:

$$\langle x_1, x_2, \dots, x_n \rangle \in R \text{ se e solo se } \vdash \alpha(\overline{x}_1, \overline{x}_2, \dots, \overline{x}_n) \qquad (x_i \in \omega)$$

e la binumera *se inoltre* $\neg\alpha$ *numera* $\omega^n \setminus R$.

I derivati di « numerare » e « binumerare » si usano in modo ovvio. Si ha come è noto:

PROPOSIZIONE 1. – *Sono numerabili tutte e sole le relazioni ricorsivamente enumerabili e binumerabili tutte e sole le relazioni ricorsive.*

Ricordiamo ancora che, con un procedimento sostanzialmente dovuto a Gödel, si dimostra che:

PROPOSIZIONE 2 (LEMMA DI DIAGONALIZZAZIONE). – *Per ogni* $\alpha(x) \in E$ *con una variabile libera* x *esiste una* $p \in E$ *chiusa tale che*:

$$\vdash p \leftrightarrow \alpha(\overline{p}) .$$

In questa forma il lemma è dovuto a Feferman: per alcuni rafforzamenti successivi vedi MONTAGUE, PAGLI [20].

Infine ricordiamo che T ammette una particolare numerante $\dot{T}(x)$ per cui (¹):

$$\left.\begin{array}{l} \vdash \dot{T}(\overline{p}) \text{ se e solo se } p \in T \\ \vdash \dot{T}(\overline{p \wedge q}) \leftrightarrow \dot{T}(\overline{p}) \wedge \dot{T}(\overline{q}) \\ \vdash \dot{T}(\overline{p}) \to \dot{T}(\overline{\dot{T}(\overline{p})}) \\ \vdash \dot{T}(\overline{p \to q}) \to (\dot{T}(\overline{p}) \to \dot{T}(\overline{q})) \\ \text{se } \vdash \dot{T}(\overline{p}) \to p \text{ allora } \vdash p \text{ (teorema di Löb)} \end{array}\right| \begin{array}{l} p, q \in E \\ p, q \text{ chiuse} \end{array}$$

Sulla base di questi pochi risultati è agevole arrivare ai due noti teoremi di Gödel sull'incompletezza dell'aritmetica e sul fatto che la consistenza di $\mathcal{T}$ (nella sua espressione « canonica » in $\mathcal{T}$) non è un teorema di $\mathcal{T}$ (sempre che $\mathcal{T}$ sia consistente).

2. – Passando all'algebra di Lindenbaum di $\mathcal{T}$ (sulle proposizioni chiuse) si ottiene un'algebra di Boole $\langle A, +, \cdot, \nu, 0, 1 \rangle$ in cui, tenuto conto delle proprietà di $\dot{T}$, è possibile definire un'ulteriore operazione unaria τ ponendo, con ovvio simbolismo:

$$\tau[p] = [\dot{T}(\overline{p})] .$$

Siamo spinti così a considerare delle strutture algebriche $\langle A, +, \cdot, \nu, 0, 1, \tau \rangle$ in cui:

$$\begin{array}{l} \langle A, +, \cdot, \nu, 0, 1 \rangle \text{ è un'algebra di Boole} \\ \tau 1 = 1 \\ \tau(a \cdot b) = \tau a \cdot \tau b \\ \tau(a \to b) \leqslant \tau a \to \tau b \\ \tau a \leqslant \tau\tau a \end{array}$$

Allo scopo di ritrovare in queste strutture anche un analogo del lemma di diagonalizzazione si può poi arricchirne il tipo e l'insieme delle identità considerando per ogni polinomio $f(x, y_1, y_2, \dots, y_n)$ in cui la x occorra solo sotto l'azione di τ una nuova operazione g_f e l'identità

$$g_f(y_1, y_2, \dots, y_n) = f(g_f(y_1, y_2, \dots, y_n), y_1, y_2, \dots, y_n) .$$

(¹) Si mostra che la $\dot{T}(x)$ che di solito si costruisce numera T sotto l'ipotesi che $\mathcal{T}$ sia ω-coerente.

P. Pagli dimostra in [20], generalizzando il lemma di diagonalizzazione, che $\mathfrak{T}$ dà effettivamente luogo a un'algebra di questa classe.

Per le algebre di questa classe (algebre diagonalizzate) è facile dimostrare (l'analogo algebrico di) il teorema di Löb:

$$\text{se } \tau p \leqslant p \text{ allora } p = 1$$

e della sua formalizzazione:

$$\tau(\tau p \to p) \leqslant \tau p$$

e inoltre gli analoghi algebrici dei due teoremi di Gödel ricordati, ossia:

1° Teorema di Gödel. – *Se A è un'algebra diagonalizzata non banale (in cui cioè $\tau x = 1$ per ogni $x \in A$) allora A ha più di due elementi.*

2° Teorema di Gödel. – *Se A è un'algebra diagonalizzata non degenere allora $\tau 0 > 0$.*

3. – Algebre diagonalizzabili.

Un teorema dovuto a C. Bernardi [1], di cui si parlerà più oltre, ha permesso di concentrare lo studio sulle cosiddette algebre diagonalizzabili, cioè su quei sistemi $\langle A, +, \cdot, \nu, 0, 1, \tau\rangle$ in cui:

$(\tau\, 0)$ $\quad \langle A, +, \cdot, \nu, 0, 1\rangle$ è un'algebra di Boole

$$\begin{array}{ll} (\tau\,1) & \tau 1 = 1 \\ (\tau\,2) & \tau(xy) = \tau x \cdot \tau y \\ (\tau\,3) & \tau(\tau x \to x) \leqslant \tau x \end{array} \quad \left.\begin{array}{l} \\ \\ \\ \end{array}\right\} (x, y \in A)$$

In [17] si dimostra che queste identità sono sufficienti a provare anche che:

$$\left.\begin{array}{ll} (\tau\,4) & \text{se } x \leqslant y \text{ allora } \tau x \leqslant \tau y \\ (\tau\,5) & \tau(x \to y) \leqslant \tau x \to \tau y \\ (\tau\,6) & \tau x \leqslant \tau^2 x \\ (\tau\,7) & \tau x + \tau y \leqslant \tau(x + y) \\ (\tau\,8) & \tau 0 \leqslant \tau x \\ (\tau\,9) & \tau(\tau x \to x) = \tau x \\ (\tau\,10) & \tau \nu \tau^n x = \tau 0 \\ (\tau\,11) & \text{se } \tau x \leqslant x \text{ allora } x = 1 \end{array}\right| \quad (x, y \in A,\ n > 0)$$

Inoltre $(\tau\, 2)$, $(\tau\, 6)$, $(\tau\, 11)$ implicano $(\tau\, 3)$. Si ha:

Teorema 1 (C. Bernardi [1, 3]). – *Per ogni polinomio $f(x)$ in una variabile (sotto τ) e per ogni algebra diagonalizzabile A esiste uno e un sol $a \in A$ per cui: $a = f(a)$.*

Questo teorema mostra che una forte versione algebrica del lemma di diagonalizzazione si ottiene già come conseguenza delle $(\tau\, 1)$, $(\tau\, 2)$, $(\tau\, 3)$.

4. – Aspetti algebrici elementari e universali.

Anzitutto le τ-algebre ammettono una buona teoria degli ideali nel senso di A. Ursini [25]. Sono 1-ideali i filtri booleani τ-chiusi o τ-filtri.

Si ha poi:

Teorema 2. – *La varietà delle algebre diagonalizzabili è ideale.* (R. Franci [7]).

Dette banali le algebre in cui vale l'identità $\tau x = 1$ si trova che

Teorema 3. – *L'algebra banale 2 di due elementi è l'unica algebra semplice di V.*

Teorema 4. – *Ogni τ-filtro proprio è estendibile a un τ-filtro massimale e ogni τ-filtro massimale è un ultrafiltro booleano.*

Teorema 5. – *Il radicale (= intersezione dei τ-filtri massimali) di un'algebra di V è il filtro booleano generato da $\tau 0$.*

Corollario 1. – *Le algebre semisemplici di V sono precisamente le algebre banali e formano una sottovarietà.*

È facile analizzare la struttura dell'algebra libera sul $\emptyset$, F_0. Essa coincide con l'algebra di Boole liberamente generata dalla catena $0 < \tau 0 < \tau^2 0 < \ldots < \tau^n 0 < \ldots$ onde, posto $\tau^\omega 0 = 1$, gli elementi di F_0 si scrivono nelle forme

$$\sum_{i \in k} \nu \tau^{n_i} 0 \cdot \tau^{m_i} 0$$

$$\prod_{i \in k} (\nu \tau^{m_i} 0 + \tau^{n_i} 0)$$

dove $k \in \omega - \{0\}$ e

$$n_0 < m_0 < n_1 < \ldots < m_{k-1}; \qquad n_i, m_i \in \omega + 1$$

τ opera su questi elementi con le leggi:

$$\tau(\sum \nu\tau^{n_i}0\cdot\tau^{m_i}0)=\tau 0$$

$$\tau(\prod(\nu\tau^{m_i}0+\tau^{n_i}0))=\tau^{n_0+1}0$$

È facile anche vedere che F_0 è atomica e i suoi atomi sono, oltre a $\tau 0$, quelli della forma:

$$\nu\tau^n 0\cdot\tau^{n+1}0\ .$$

Meno agevole è invece chiarire la struttura delle $F_n(n\in\omega,\ n>0)$ e di F_ω.

F. Montagna in [19] ha dimostrato che nessuna F_n è generica per V, C. Bernardi in [2] ha dimostrato che le F_n sono atomiche.

5. – Rappresentazione e teoria della dualità.

Poichè in ogni algebra diagonalizzabile $\sigma=\nu\tau\nu$ è un emimorfismo $(\sigma 0=0,\ \sigma(x+y)=\sigma x+\sigma y)$ si può riprodurre per le algebre diagonalizzabili la teoria della dualità. Come duali delle algebre diagonalizzabili si trovano spazi di Stone S muniti di una relazione binaria, $<$, transitiva e «relativamente fondata» tale cioè che ogni «clopen» (= chiuso o aperto) di S ammette un elemento minimale. In [17] si danno inoltre altri risultati di contorno. Più esplicitamente il risultato può essere enunciato così:

Teorema 6. – *Sia $\langle A, +, \cdot, \nu, 0, 1, \tau\rangle$ un'algebra diagonalizzabile, $\sigma=\nu\tau\nu$, S lo spazio di Stone di $\langle A, +, \cdot, \nu, 0, 1\rangle$, φ il monomorfismo canonico da A a $\mathfrak{P}(S)$ e $<$ la relazione definita in S da:*

$$x<y \text{ se e solo se per ogni } p\in A \text{ da } x\in\varphi p \text{ segue } y\in\varphi\sigma p$$

Allora definito in $\mathfrak{P}(S)$ un σ^* ponendo:

$$\sigma^* X=\{y\colon \text{esiste un } x\in X \text{ con } x<y\}\,,$$

si ha:

$$\varphi\circ\sigma=\sigma^*\circ\varphi$$

6. – Altri risultati.

C. Bernardi dimostra in [2] che:

Teorema 7. – *L'insieme delle identità di V è decidibile.*

Teorema 8. – *La classe delle algebre diagonalizzabili* finite *genera V.*

Un'importante caratteristica di V è la seguente. Cominciamo con l'osservare che, imitando il processo di formalizzazione in $\mathfrak{T}$ di proposizioni metalinguistiche, si ricavano da certe proprietà di V altre proprietà che risultano valide in V. Per esempio «formalizzando» il teorema di Löb: se $\tau p\leqslant p$ allora $p=1$, si ricava l'identità:

$$\tau(\tau p\to p)\leqslant\tau p$$

che è anch'essa valida. Ebbene, sia $\mathcal{T}$ la teoria del primo ordine delle algebre diagonalizzabili arricchita di un'infinità numerabile di variabili proposizionali, fissiamo una biiezione μ dall'insieme delle variabili proposizionali a quello delle variabili individuali (scriviamo x^* per $\mu^{-1}x$, p^* per μp) e definiamo una φ^* dall'insieme delle identità all'insieme delle formule ponendo:

$$\varphi x=x^*$$
$$\varphi\tau t=t\simeq 1$$
$$\varphi\nu t=\neg\varphi t$$
$$\varphi(t_1+t_2)=\varphi t_1\vee\varphi t_2$$
etc.

(la φ va dall'insieme dei termini all'insieme delle formule aperte)

$$\varphi^*(t_1\simeq t_2)=\varphi(t_1\leftrightarrow t_2)\ .$$

Si trova in [18] che:

Teorema 9. – *Un'identità è valida se e solo se la sua φ^*-immagine è valida.*

In vista del Teorema 7 ciò porta con sè la decidibilità dell'insieme delle formule aperte. La dimostrazione del Teorema 9 richiede che si estenda l'inversa della φ a *tutte* le formule, il che a sua volta richiede che si arricchisca il linguaggio con i simboli $\bigvee$, $\bigwedge$ e si considerino i completamenti minimali delle algebre di Boole sottostanti alle algebre diagonalizzabili. Noti strumenti topologici (soprattutto il teorema di Baire) permettono di conseguire il risultato.

È notevole il fatto che l'operatore ψ che inverte φ ha a sua volta le proprietà di un τ, cosicchè la stessa teoria delle algebre diagonalizzabili fornisce un esempio di teoria che dà luogo a una algebra diagonalizzabile.

Si può congetturare che essa sia, in senso da precisare, *minimale* fra le teorie di questo tipo.

7. – Problemi aperti e ricerche collaterali.

1) Il principale problema aperto riguarda la genericità dell'algebra diagonalizzabile legata all'aritmetica: è possibile che il Teorema 9 fornisca uno strumento utile a questo riguardo.

2) Non si dispone di una descrizione « comoda » degli atomi di F_n $(n > 0)$. C. BERNARDI in [2] indica un insieme di « parole » ciascuna delle quali è un atomo o lo 0 ma, per quanto esista un procedimento di decisione che permette, per ogni data parola, di decidere se essa è o no un atomo, non si riesce ancora a dominare l'insieme degli atomi abbastanza bene da servirsene in vista del problema 1). È da notare che un successo in questa direzione permetterebbe altresì di conoscere in modo strumentalmente utile la struttura di F_ω.

3) (Si tratta di un tema di ricerca). Si dovrebbe per ogni teoria cui l'aritmetica sia riducibile caratterizzare la corrispondente algebra diagonalizzabile.

Per quanto l'algebrizzazione di T permetta di ritrovare a livello algebrico molte delle proprietà peculiari dell'aritmetica peaniana non è chiaro quanto, per così dire, si perda nel processo di algebrizzazione. Recentemente F. MONTAGNA ha studiato la possibilità di algebrizzare, anzichè l'ordinario $\dot{T}$, un predicato che enumera ancora T ma che è analogo al predicato di Rosser. Conformemente al teorema di Gödel-Rosser, le algebre che si ottengono non si riducono mai a due elementi.

Aldo URSINI sta invece studiando le analoghe delle algebre diagonalizzabili che si ottengono dalla logica intuizionistica.

Ricerche abbastanza vicine a quelle qui esposte sono state compiute da un gruppo di logici olandesi (in particolare DE JONGH) ma il gruppo di Siena ne ha ricevuto scarse e frammentarie notizie.

Sia sotto l'aspetto algebrico che sotto l'aspetto logico resta molto da fare: quello che sembra certo è che quanto meno l'agilità dello strumento algebrico getta una luce insperata su molti fenomeni e permetterà forse uno studio generale degli aspetti più rilevanti delle teorie che raggiungono un certo grado critico di complessità.

BIBLIOGRAFIA SOMMARIA (*)

[1] C. BERNARDI, *The fixed-point theorem for the diagonalizable algebras* (*the algebraisation of the theories which express Theor. III*), in corso di pubblicazione in Studia Logica.

[2] C. BERNARDI, *On the equational class of diagonalizable algebras* (*the algebraisation of the theories which express Theor. VI*), sottoposto a Studia Logica.

[3] C. BERNARDI, *The uniqueness of the fixed-point in every diagonalizable algebra* (*the algebraisation of the theories which express Theor. VIII*), sottoposto a Studia Logica.

[4] S. FEFERMAN, *Arithmetization of metamathematics in general setting*, Fund. Math., **49** (1960), pp. 38-92.

[5] S. FEFERMAN, *Ordinal logics re-examined*, J. Symbolic Logic, **23** (1958), p. 105.

[6] S. FEFERMAN, *Transfinite recursive progressions of axiomatic theories*, J. Symbolic Logic, **24**, 3 (1962), pp. 259-316.

[7] R. FRANCI, *Idealità di alcune classi di algebre di Boole con operatori*, in corso di pubblicazione nel Boll. Un. Mat. Ital.

[8] K. GÖDEL, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I*, Monatsh. Math. und Ph., **38** (1931), pp. 173-198.

[9] C. F. KENT, *The relation of A to Proof A in the Lindenbaum sentence algebra*, J. Symbolic Logic, **38**, 2 (1973), pp. 295-298.

[10] G. KREISEL, *Mathematical logic*, in Lectures on modern mathematics, vol. III, ed. Saaty, New York, 1965, pp. 95-105.

[11] G. KREISEL, *A survey of proof theory*, J. Symbolic Logic, **33** (1968), pp. 321-388.

[12] G. KREISEL, *A survey of proof theory II*, in Proc. of the Second Scandinavian Logic Symposium, ed. Fenstad, North-Holland, Amsterdam, 1971, pp. 109-170.

[13] M. H. LÖB, *Solution of a problem of Leon Henkin*, J. Symbolic Logic, **20** (1955), pp. 115-118.

[14] R. MAGARI, *Su certe teorie non enumerabili* (*sulle limitazioni dei sistemi formali, I*), Ann. Mat. Pura Appl., (4) **98** (1974), pp. 119-152.

[15] R. MAGARI, *Significato e verità nell'aritmetica peaniana* (*sulle limitazioni dei sistemi formali, II*), Ann. Mat. Pura Appl., (4) **103** (1975), pp. 343-368.

[16] R. MAGARI, *The diagonalizable algebras* (*the algebraisation of the theories*

(*) Chi desiderasse più ampie informazioni può rivolgersi all'Istituto di Matematica dell'Università di Siena e in particolare al dott. Franco MONTAGNA, che cura la diffusione degli appunti e dei preprints del locale seminario di Logica.

which express Theor, II), in corso di pubblicazione sul Boll. Un. Mat. Ital.

[17] R. Magari, *Representation and duality theory for diagonalizable algebras* (*the algebraisation of the theories which express Theor, IV*), in corso di pubblicazione su Studia Logica.

[18] R. Magari, *On the autological character of diagonalizable algebras* (*the algebraisation of the theories which express Theor, VII*), sottoposto a Studia Logica.

[19] F. Montagna, *For every n, the n-fréely generated algebras is not generic in the equational class of diagonalizable algebras* (*the algebraisation of the theories which express Theor, V*), sottoposto a Studia Logica.

[20] P. Pagli, *Su alcune estensioni del lemma di diagonalizzazione nell'aritmetica di Peano* (*the algebraisation of the theories which express Theor, I*), in corso di pubblicazione.

[21] D. Prawitz, *On the idea of a general proof theory*, Boll. Un. Mat. Ital., (4), **9**, suppl. fasc. 2 (1974), pp. 108-121.

[22] D. Prawitz, *Ideas and results in proof theory*, in Proc. of the Second Scandinavian Symposium, ed. Fenstad, North Holland, Amsterdam, 1971, pp. 235-307.

[23] C. Smorynski, *Consistency and related metamathematical properties*, Tech. Report 75-62, Univ. di Amsterdam.

„Monograf" - Bologna - Via Collamarini 5