

CAPITOLO 5 LA MATEMATICA COME SISTEMA FORMALE

1. Hilbert contro l'infinito: la matematica come calcolo di simboli.

Abbiamo visto che il problema della non contraddizione di un dato sistema di assiomi è centrale per la concezione ipotetico-deduttiva di Hilbert. Ora tale problema si risolve usualmente mostrando un modello del dato sistema di assiomi. Ad esempio la consistenza della geometria non euclidea veniva provata dal modello di Klein o da uno dei tanti modelli di cui abbiamo già parlato. In realtà tutti i modelli di geometria non euclidea vengono costruiti a partire dal modello euclideo e quindi, ad esempio, la dimostrazione di non contraddittorietà delle geometrie non euclidee è valida a patto che la geometria euclidea sia affidabile. In breve,

noi riusciamo a provare che la teoria delle geometrie non euclidee è consistente solo ammettendo che il sistema di assiomi per la geometria euclidea è consistente.

D'altra parte, si direbbe, è facile provare tale consistenza costruendone un modello tramite i numeri reali. Ma come giustificare i numeri reali? Coerentemente con il metodo assiomatico, dobbiamo fornire un sistema di assiomi per i numeri reali (ricordiamo che la nozione di campo completo archimedeo fornisce un tale sistema di assiomi) e ciò porta alla necessità di provare che tale sistema è consistente. D'altra parte abbiamo visto come sia possibile costruire il campo dei numeri reali a partire dagli interi; purtroppo però dobbiamo servirci della teoria degli insiemi. In definitiva, se ci potessimo fidare della teoria degli insiemi, avremmo risolto tutti i problemi e ci potremmo fermare:

riusciamo a provare la consistenza della teoria dei numeri reali solo se la teoria degli insiemi è consistente.

Purtroppo la scoperta dei paradossi mostra che la nozione di insieme è alquanto inaffidabile e che quindi si deve procedere ad una assiomatizzazione della teoria degli insiemi. Ora è vero che esistono diverse teorie assiomatiche degli insiemi che permettono di evitare tutti i paradossi fino ad ora noti, ma chi ci assicura che un giorno non vengano scoperti paradossi anche per tali nuove teorie? Il problema appare senza soluzioni.

Ora Hilbert pensò che tutte le difficoltà nascessero dalla considerazione dell'infinito attuale (cioè degli insiemi infiniti) che già tanta diffidenza aveva suscitato da Pitagora in poi. Infatti, come abbiamo già osservato, nessuno dubita della consistenza della teoria dei gruppi perché non è difficile fornire "concretamente" esempi di gruppi finiti. Esaminiamo in proposito un passo dall'articolo di Hilbert *Sull'infinito* apparso nel 1925. In questo passo viene fatto riferimento alla definizione di limite che aveva permesso di eliminare ogni riferimento alle grandezze infinitamente piccole ed a quelle infinitamente grandi.

Proprio come le operazioni sull'infinitamente piccolo sono state sostituite da operazioni sul finito che danno luogo esattamente agli stessi risultati e alle stesse eleganti relazioni formali, così in generale i metodi deduttivi basati sull'infinito devono essere sostituiti con procedimenti finiti che diano gli stessi risultati, che cioè rendano possibili le stesse catene di dimostrazioni e gli stessi metodi per ottenere formule e teoremi.

Questo è lo scopo della mia teoria, essa si propone di dare definitivamente sicurezza al metodo matematico . . .

Hilbert vede nella chiarificazione del concetto di infinito una questione fondamentale il cui interesse non è solo matematico.

Le considerazioni precedenti intendono solo affermare che la chiarificazione definitiva della natura dell'infinito non riguarda esclusivamente l'ambito degli interessi scientifici specializzati ma è necessaria per la dignità stessa dell'intelletto umano.

D'altra parte l'esistenza dei paradossi della teoria degli insiemi sembra spingere al rifiuto dell'infinito attuale. C'è tuttavia un modo soddisfacente per evitare i paradossi senza tradire la nostra scienza. Il punto di vista utile per la scoperta di tale modo e il desiderio che ci mostra la via da prendere sono:

1. *Se c'è la più piccola speranza, esamineremo accuratamente tutte le definizioni e i metodi deduttivi fecondi, li cureremo, li potenzieremo e li renderemo utili. Nessuno potrà cacciarci dal paradiso che Cantor ha creato per noi.*
2. *Dobbiamo estendere a tutta la matematica quella sicurezza dei metodi dimostrativi che è propria della teoria elementare dei numeri, di cui nessuno dubita e in cui contraddizioni e paradossi sorgono solo per negligenza.*

Il punto di vista di Hilbert è chiaro. Per prima cosa il rigore in matematica non si deve ottenere semplicemente eliminando quella parte della matematica e quei metodi che, pur essendosi rivelati fondamentali, non risultano avere basi sicure. Pertanto, nonostante i paradossi Nessuno potrà cacciarci dal paradiso che Cantor ha creato per noi. L'atteggiamento di Hilbert è pragmatico, se certi metodi si sono rivelati fecondi allora devono essere accettati.

In effetti il successo è essenziale perché, in matematica come altrove, esso costituisce la corte suprema di fronte a cui tutti si inchinano.

D'altro lato è indiscutibile che il rigore e la sicurezza si possono ottenere solo facendo riferimento ai metodi finitari propri dei numeri interi. Come fare per conciliare le due cose apparentemente contraddittorie? Hilbert suggerisce di esaminare il concetto di "punto all'infinito" elaborato dalla geometria proiettiva. Come è noto, il piano proiettivo viene definito aggiungendo all'insieme dei punti del piano euclideo dei punti ideali, detti punti all'infinito in modo che si possa dire che due rette parallele abbiano un punto all'infinito in comune. Tecnicamente ciò si ottiene al modo seguente.

Definizione. Chiamiamo *punto all'infinito* del piano euclideo ogni fascio completo di rette parallele. Diciamo che un punto all'infinito P appartiene ad una retta r se r appartiene al fascio P .

L'introduzione dei punti all'infinito permette di semplificare e rendere simmetrici gli assiomi della geometria. Ad esempio due rette si incontrano sempre in un punto (che è finito se le rette non sono parallele ed infinito se le rette sono parallele). Inoltre in tale modo si ottiene un potente ed elegante strumento per la trattazione delle curve algebriche. A tale proposito è

importante osservare che non si pretende che i punti all'infinito siano realmente esistenti, essi sono strumenti linguistici, enti ideali la cui introduzione è utile per ottenere risultati e per avere una trattazione più efficace della geometria. Discorso analogo vale per l'introduzione dell'unità immaginaria i . La proposta di Hilbert è pertanto di considerare l'infinito un ente ideale, per meglio dire un oggetto linguistico da manipolare secondo certe regole, regole non solo di carattere algebrico ma anche di natura logica. In altre parole si tratta di spostare il ruolo del linguaggio che da strumento di indagine del mondo degli enti matematici diviene esso stesso oggetto di investigazione. Oggetto di studio dovranno essere i "segni concreti" che rimangono comunque oggetti finiti da maneggiare con un numero finito di regole.

Questa è la filosofia che ritengo necessaria non solo per la matematica ma per ogni pensiero, per ogni comprensione e per ogni comunicazione che rientrano nell'ambito della scienza. In base ad essa, in particolare, oggetto della nostra considerazione matematica sono gli stessi segni concreti la cui forma, in virtù del nostro approccio, è immediatamente chiara e riconoscibile.

Fino a qui non esistono, come lo stesso Hilbert sottolinea, grandi differenze con la tradizione algebrica. Anche la semplice risoluzione di una equazione di primo grado consiste in una manipolazione di equazioni (oggetti linguistici) secondo certe regole che permettono di passare da una equazione ad un'altra. Lo stesso si può dire anche di un semplice calcolo. La grossa novità nasce dal fatto che per "segni concreti" Hilbert intendeva non solo equazioni ma anche espressioni linguistiche molto più complicate che coinvolgevano i quantificatori, i connettivi logici (ad esempio la negazione, la congiunzione, la disgiunzione). Arriviamo pertanto al punto fondamentale: il calcolo logico.

Certo questo fu sviluppato in origine per motivi del tutto differenti. I suoi segni furono introdotti originariamente solo per scopi di comunicazione. Tuttavia è coerente col nostro punto di vista non attribuire alcun significato ai segni logici, così come non se ne è attribuito alcuno ai segni matematici, e dichiarare che anche le formule del calcolo logico sono elementi ideali che di per sé non significano niente. Col calcolo logico abbiamo un linguaggio simbolico che permette di tradurre in formule le asserzioni matematiche e di esprimere le deduzioni logiche mediante processi formali.

In definitiva non bastava ridurre la matematica a linguaggio, ma era anche necessario formalizzare la logica che permetteva la manipolazione di tale linguaggio. Più precisamente una particolare teoria matematica veniva vista come un insieme finito di espressioni linguistiche (gli assiomi propri della teoria) da aggiungere ad un insieme fissato di espressioni (gli assiomi logici) il tutto da manipolare tramite determinate regole (le regole di inferenza) in modo da produrre altre espressioni (i teoremi). In tale modo qualunque teoria (anche quelle che parlano di oggetti infiniti) diviene un oggetto finito e quindi passibile di essere esaminato nella sua interezza. Il problema della consistenza diviene allora quello di esaminare tale oggetto finito e vedere se tra le sue proprietà vi è anche quella della consistenza.

2. La logica matematica: il linguaggio.

Abbiamo visto che per Hilbert la matematica si riduce ad un linguaggio a cui siano state aggiunte delle regole per la manipolazione del linguaggio stesso. Esaminiamo più da vicino come sia possibile dare delle rigorose definizioni in proposito. Un linguaggio formale che vada bene per "parlare di matematica" dovrà contenere nomi per oggetti matematici (come 3 , 13 , π , \emptyset , e), nomi per funzioni ed operazioni (come \log , $+$, sen , x_2) e nomi per relazioni (come $=$, \leq , \geq , \supseteq). Sembra infatti ragionevole poter scrivere una asserzione come " $\log(2+3) \geq 0$ " che si avvale del nome di funzione \log , dei nomi di numeri 2 , 3 e 0 , di un simbolo $+$ per un'operazione binaria e di un simbolo \geq per una relazione binaria. Ancora, in matematica sono di uso frequente le variabili ed i quantificatori (esiste, per ogni) che permettono ad esempio di scrivere proposizioni del tipo "esiste una soluzione dell'equazione $x^2-1=0$ ", in breve " $\exists x(x^2-1=0)$ ". Infine sono usati connettivi logici come "non", "e", "oppure", "implica" che consentono di costruire asserzioni (composte) a partire da altre asserzioni. Ciò suggerisce le seguenti definizioni. Chiamiamo alfabeto di un linguaggio del primo ordine un alfabeto A costituito da:

- un insieme di simboli per denotare variabili, ad esempio x, y, z, \dots ;
- i *connettivi proposizionali* $\{\wedge, \vee, \rightarrow, \sim\}$;
- il quantificatore esistenziale \exists ;
- la parentesi (e la parentesi) ;
- un insieme finito o numerabile C di elementi detti *costanti* ;
- per ogni intero n un insieme finito o vuoto O_n (nomi di operazioni n -arie) ;
- per ogni intero n un insieme finito o vuoto R_n (nomi di relazioni n -arie).

Da notare che nel linguaggio comune si parla di predicati per indicare le relazioni 1-arie mentre si preferisce parlare di relazioni solo nel caso $n \neq 1$. In generale inoltre si considerano solo operazioni e relazioni unarie o binarie. Naturalmente esistono tanti alfabeti, e quindi tanti linguaggi del primo ordine, quanti sono i modi di specificare le costanti, i nomi delle relazioni e delle operazioni. Avremo ad esempio un linguaggio adeguato alla teoria dei gruppi, uno per la teoria degli anelli, uno per le strutture ordinate, e così via. In generale vengono presi in considerazione solo un numero finito di relazioni e di funzioni e quindi gli R_n e O_n sono vuoti tranne che per un numero finito di indici. Non si esclude la possibilità che gli insiemi C , O_n , possano essere tutti vuoti, cioè che non vi siano costanti e operazioni n -arie. L'unica cosa che si richiede è che vi sia almeno il simbolo per l'identità " $=$ ". Per poter definire il linguaggio del primo ordine corrispondente ad un dato alfabeto dobbiamo prima definire il linguaggio dei termini al modo seguente:

- a) ogni variabile o costante è un termine
- b) se $f \in O_n$ e t_1, \dots, t_n sono termini allora $f(t_1, \dots, t_n)$ è un termine.

Intuitivamente i termini sono tutte le "descrizioni di funzioni" che si possono costruire a partire dalle variabili, dalle costanti e dai nomi di funzioni di un dato linguaggio.

Esempio. Ad esempio se tra i nomi di funzioni abbiamo \log , sen , allora sono termini $\log(\text{sen}(x))$, $\log(\text{sen}(x))$, $\text{sen}(\log(y))$, $\log(\log(x))$,

Nota 1. Nella pratica matematica quasi sempre si utilizzano operazioni binarie che consentono un modo diverso di costruire i termini. Infatti se f è un nome di operazione binaria allora si preferisce scrivere $t_1 f t_2$ al posto di $f(t_1, t_2)$. Così scriveremo $x+y$ e non $+(x,y)$ e $(x+y)+z$ al posto di $+(+(x,y),z)$. Una scrittura del tipo $f(t_1, t_2)$ viene detta *prefissa*, una del tipo $t_1 f t_2$ viene detta

infissa. Se si preferisce utilizzare la notazione infissa allora la condizione b) deve essere data come segue.

b) se $f \in O_2$ e se t_1 e t_2 sono termini allora $(t_1)f(t_2)$ è un termine.

Ad esempio l'espressione $x \log(y+x)$ coinvolge la notazione infissa per + e - e quella prefissa per \log . Esistono anche notazioni "post-fisse" per le operazioni unarie, ad esempio per la funzione fattoriale $x!$ e notazioni "esponenziali" come la funzione inverso x^{-1} . Nel seguito ci atterremo all'uso comune ed utilizzeremo anche questi tipi di notazione.

Problema. Scrivere cinque termini di un linguaggio il cui alfabeto contiene $\{\log, x, y, sen, +, 1\}$.

Un linguaggio del primo ordine è l'insieme \mathcal{L} delle parole su di un alfabeto del primo ordine definito dalle seguenti regole di formazione:

a) se r è il nome di una relazione ad n posti e t_1, \dots, t_n sono termini allora $r(t_1, \dots, t_n)$ è un elemento di \mathcal{L} (che viene detto *formula atomica*);

b) se α e $\beta \in \mathcal{L}$ allora $\alpha \wedge \beta$, $\alpha \vee \beta$, $\alpha \rightarrow \beta$ e $\neg \alpha$ appartengono a \mathcal{L} ;

d) se x è una variabile ed $\alpha \in \mathcal{L}$ allora $\exists x(\alpha) \in \mathcal{L}$.

Gli elementi di \mathcal{L} vengono chiamati *formule ben formate* o, più semplicemente, *formule*. I seguenti sono alcuni esempi di linguaggi del primo ordine utilizzati in matematica.

Esempi. Linguaggio usato per le strutture ordinate. È un linguaggio che contiene i soli simboli \leq e $=$ di relazioni binarie. Pertanto nell'alfabeto non vi sono costanti o nomi per funzioni, e quindi $O_n = \emptyset$ per ogni intero n , mentre $R_2 = \{\leq, =\}$ e $R_n = \emptyset$ per $n \neq 2$. A volte si aggiunge anche una costante 0 (da interpretare come minimo elemento) e una costante 1 (da interpretare come massimo elemento) e pertanto $C = \{0, 1\}$. Poiché non ci sono nomi di operazioni, gli unici termini sono le variabili e le costanti. Sono esempi di formule

$$\forall x(x \geq 0) ; \forall x \exists y(x \geq y) ; \forall x(x \leq x) ; \forall x(\forall y((x \leq y) \wedge (y \leq z) \Rightarrow x \leq z)).$$

Linguaggio usato per la teoria dei gruppi. È costituito da "." per rappresentare l'operazione binaria, da "inv" per rappresentare l'operazione che associa ad ogni x il suo inverso e la costante 1 per rappresentare l'elemento neutro. L'unica relazione è l'identità. Pertanto $C = \{1\}$, $O_1 = \{1\}$, $O_2 = \{\cdot\}$, $R_2 = \{=\}$ mentre i rimanenti insiemi di nomi R_n e O_n sono vuoti. In generale si preferisce la notazione esponenziale x^{-1} al posto di $inv(x)$. I termini sono le espressioni del tipo $(x \cdot y) \cdot x^{-1}$, $((1 \cdot x)^{-1} \cdot y)^{-1}$. Sono esempi di formule:

$$\forall x(x \cdot y = y \cdot x) ; x \cdot 1 = x ; \forall x(x = 1 \Rightarrow x \cdot x = 1).$$

Ma naturalmente è possibile utilizzare anche linguaggi diversi per trattare lo stesso tipo di strutture matematiche. Ad esempio per la teoria dei gruppi si usa spesso la notazione additiva invece di quella moltiplicativa che abbiamo indicato. In questo caso $C = \{0\}$, $O_2 = \{+\}$, $O_1 = \{-\}$, $R_2 = \{=\}$.

Tra i simboli di relazione binaria il simbolo "=" riveste particolare importanza, tanto che usualmente si suppone che ogni linguaggio lo contenga.

3. L'apparato deduttivo: una macchina per produrre teoremi.

In accordo con il punto di vista di Hilbert, dobbiamo vedere le dimostrazioni che usualmente si effettuano in matematica come un procedimento meccanico con cui produrre, a partire da un dato sistema di formule (gli assiomi), nuove formule (i teoremi). Esaminiamo quali sono le regole che usualmente si usano per "produrre teoremi".

Il Modus Ponens. La regola più usata è il "*modus ponens*", cioè la regola per cui se ho dimostrato (a partire dagli assiomi T) la formula $\alpha \rightarrow \beta$ ed ho dimostrato α allora posso affermare anche β .

La generalizzazione. Un'altra regola è quella per cui se ho dimostrato (a partire da T) che vale $\alpha(x)$, allora posso affermare anche $\forall x(\alpha)$. Tale regola viene detta di "*generalizzazione*" e si giustifica col fatto che se ho dimostrato $\alpha(x)$ allora, essendo x una variabile, non ho mai utilizzato nessuna particolare proprietà dell'oggetto denotato da x . In altri termini, durante la dimostrazione x ha sempre denotato un generico elemento del dominio. Pertanto, di fatto, si è dimostrato $\forall x(\alpha)$.

$$\frac{\alpha, \alpha \rightarrow \beta}{\beta} \quad (\text{Modus Ponens}) \qquad \frac{\alpha}{\forall x(\alpha)} \quad (\text{Generalizzazione})$$

Vi sono poi delle formule di cui ci si può servire durante la dimostrazione perché sono vere sempre, qualunque siano le cose di cui si sta parlando. In altre parole si possono utilizzare delle formule logicamente vere del tipo $\alpha \rightarrow \alpha$ o $\alpha \wedge \beta \rightarrow \alpha$ o $\alpha(t) \rightarrow \exists x \alpha$. Chiamiamo *assiomi logici* un opportuno insieme A_l di tali formule che non mi preoccupa di specificare. Usualmente in A_l si mettono anche formule del tipo

$$p \rightarrow p, \neg(\neg(\alpha)) \rightarrow \alpha, (\forall x \alpha(x)) \rightarrow \alpha(t), \exists x(\alpha) \rightarrow \neg \forall x(\neg(\alpha)).$$

Inoltre si aggiungono assiomi relativi all'uguaglianza

$$\begin{aligned} U_1 & \quad \forall x(x=x) && \text{(riflessività)} ; \\ U_2 & \quad \forall x \forall y((x=y) \rightarrow (y=x)) && \text{(simmetria)} ; \\ U_3 & \quad \forall x \forall y \forall z((x=y) \wedge (y=z)) \rightarrow (x=z) && \text{(transitività)} ; \\ U_4 & \quad x = y \rightarrow (r(z_1, \dots, x, \dots, z_n) \Leftrightarrow r(z_1, \dots, y, \dots, z_n)) ; \\ U_5 & \quad x = y \rightarrow f(z_1, \dots, x, \dots, z_n) = f(z_1, \dots, y, \dots, z_n) \end{aligned}$$

dove U_4 e U_5 vanno intesi estesi a tutti i nomi di relazione r ed a tutti i nomi di funzione f e dove $r(z_1, \dots, y, \dots, z_n)$ è la formula atomica ottenuta da $r(z_1, \dots, x, \dots, z_n)$ sostituendo una occorrenza della variabile x con y e $f(z_1, \dots, y, \dots, z_n)$ è il termine ottenuto da $f(z_1, \dots, x, \dots, z_n)$ rimpiazzando una occorrenza di x con y .

Dato un insieme T di formule, che chiameremo *sistema di assiomi*, chiameremo *dimostrazione di α sotto ipotesi T* una successione di formule $\alpha_1, \dots, \alpha_n$ con $\alpha_n = \alpha$ e tale che per ogni formula α_i si verifichi almeno uno dei seguenti casi:

- α_i è un assioma logico
- α_i è una ipotesi, cioè $\alpha_i \in X$
- α_i è stata ottenuta da formule precedenti per modus ponens o per generalizzazione.

Indicheremo con $D(T)$ l'insieme delle formule che ammettono una dimostrazione sotto ipotesi T . Possiamo visualizzare il sistema deduttivo di una logica del primo ordine come una macchina che produce teoremi. La macchina può utilizzare in ogni istante un assioma logico oppure una formula in T . Utilizzando le regole di inferenza a partire da tale materiale produce teoremi.

Diremo che T è *contraddittorio* se esiste una formula α tale che $\alpha \in D(T)$ e $\neg\alpha \in D(T)$, cioè se la macchina deduttiva non produce una "stringa" del tipo $\neg\alpha$ ed allo stesso tempo una stringa di tipo α . Un sistema di assiomi non contraddittorio si dirà *consistente*. Diremo che T è *completo* se per ogni formula α risulta $\alpha \in D(T)$ oppure $\neg\alpha \in D(T)$, in altri termini ogni formula può essere provata o confutata da T .

Ad esempio un sistema di assiomi per la teoria dei gruppi è costituito dalle formule

$$\forall x(\forall y((x \cdot y) \cdot z = x \cdot (y \cdot z))) ; \forall x(x \cdot 1 = 1) ; \forall x(1 \cdot x = 1) ; \forall x(x \cdot x^{-1} = 1) ; \forall x(x^{-1} \cdot x = 1).$$

4. Teoremi limitativi.

Esistono notevoli limiti alla logica matematica che sono stati posti in rilievo dal logico Gödel nel 1930.

Proposizione 1 (Primo teorema di Gödel) Se T è una teoria consistente "contenente la teoria dei numeri interi" allora esiste una formula ϕ indecidibile in T , cioè ϕ non può essere né provata né confutata da T .

Dim. Non esporremo una dimostrazione rigorosa limitandoci a fornire l'idea che è alla base di tale dimostrazione. Partiamo dalla famosa antinomia che si ottiene considerando l'asserzione

$$\gamma \equiv \text{"io sono una proposizione falsa"}.$$

Allora

$$\gamma \text{ vera} \Rightarrow \gamma \text{ falsa} ; \gamma \text{ falsa} \Rightarrow \gamma \text{ vera}$$

e pertanto γ non può essere né vera né falsa. Alla base di tale antinomia è il fatto che γ è una proposizione che parla di se stessa, cioè si manifesta quello che viene chiamato un "autoriferimento". Ora una prima "rozza" dimostrazione del primo teorema di Gödel si ottiene partendo dall'asserzione

$$\gamma = \text{"io sono una formula che non è un teorema di } T\text{"}.$$

Allora, ammesso che γ sia una formula del linguaggio \mathcal{L} ,

$T \vdash \gamma$ allora γ non è un teorema di T ; se non $T \vdash \gamma$ allora γ è un teorema di T

e pertanto né γ né la sua negata $\neg\gamma$ possono essere teoremi di T .

Per potere formalizzare quanto sopra detto, è necessario che sia possibile il fenomeno dell'autoriferimento, abbiamo cioè bisogno di far vedere come T possa "parlare di se stesso". In particolare, perché quel termine "io" abbia senso deve essere dato un nome all'interno del linguaggio \mathcal{L} per ciascuna delle formule di \mathcal{L} . Inoltre deve essere definita una formula in \mathcal{L} che significhi "essere teorema". Per fare ciò cominciamo con il mettere in rilievo che

1. ogni numero naturale ha un "nome" corrispondente in \mathcal{L} .

Infatti abbiamo ipotizzato che la teoria che stiamo considerando contiene la teoria dei numeri interi. Inoltre

2. è possibile codificare le formule di \mathcal{L} .

Cioè è possibile associare ad ogni formula ϕ un numero intero detto *numero di codice* di ϕ . Ciò può essere fatto in vari modi, ad esempio ricordiamo che ogni formula è una parola sull'alfabeto finito A di \mathcal{L} . Si può associare allora in un modo qualunque ad ogni lettera $l \in A$ un numero $g(l)$ e

poi ad ogni parola $a(1)...a(j)$ in tale alfabeto il numero $p(1)^{g(a(1))} \dots p(j)^{g(a(j))}$ essendo $p(1), p(2), \dots$ la successione dei numeri primi. Poiché una formula è anche una parola, in tale modo ad ogni formula viene assegnata un numero. Se viceversa si ha un numero m lo si può "decodificare" in una formula procedendo ad una sua scomposizione $m = p(1)^{n(1)} \dots p(n)^{n(j)}$ in prodotto di successivi numeri primi. Se $n(1), \dots, n(j)$ sono codici di lettere in A , cioè se esistono $a(1), \dots, a(j)$ in A tali che $g(a(1)) = n(1), \dots, g(a(j)) = n(j)$, e se la parola $a_1 \dots a_n$ è una formula di \mathcal{L} , allora assumeremo tale formula come decodifica di m . Altrimenti assumiamo per convenzione che m sia decodificato (ad esempio) in una formula che si è fissato.

3. Ad ogni formula ϕ di \mathcal{L} può essere assegnato un "nome" $c(\phi)$ in \mathcal{L} .

Ciò si ottiene considerando il termine chiuso $c(\phi)$ che rappresenta il numero di codice di ϕ .

4. Si può dare un numero di codice ad ogni dimostrazione π in T .

La cosa non è difficile poiché una dimostrazione può essere vista come una sequenza di formule $\alpha_1, \alpha_2, \dots, \alpha_n$ e tale sequenza è una parola nell'alfabeto che si ottiene aggiungendo ad A il simbolo ", ". Si può pertanto procedere allo stesso modo di quanto si è fatto per la codifica delle formule.

5. Ad ogni dimostrazione π può essere assegnato un "nome" $c(\pi)$,

Come nel caso delle formule basta considerare il termine chiuso che rappresenta il numero di codice di π .

Detto questo si dimostra (ma noi non lo dimostriamo) che in \mathcal{L} esiste una formula $Pr(x,y)$ il cui significato è che x è (un numero di codice di) una dimostrazione di y (della formula codificata da y). Più precisamente si assume che Pr verifica la seguente proprietà

$$"T \vdash \phi \text{ se e solo se esiste un termine chiuso } t \text{ tale che } T \vdash Pr(t, c(\phi))".$$

Infine si prova l'esistenza di una formula γ tale che

$$T \vdash \gamma \leftrightarrow (\neg \exists x Pr(x, c(\gamma))).$$

La formula γ asserisce proprio quello che volevamo, cioè che "io sono una formula che non è un teorema di T ". Supponiamo ora che γ sia dimostrabile, allora sarebbe dimostrabile anche $\neg \exists x Pr(x, c(\gamma))$ e quindi non potrebbe esistere una dimostrazione di γ in T . Supponiamo invece che $\neg \gamma$ sia dimostrabile, allora sarà dimostrabile in T anche $\exists x Pr(x, c(\gamma))$. Ciò comporta che esiste un termine chiuso t per cui $Pr(t, c(\gamma))$ e pertanto che esiste una dimostrazione di γ . Ciò è in contrasto con l'ipotesi di consistenza per T .

Corollario. Esiste una asserzione dell'aritmetica che pur essendo vera non può essere dimostrata; in altre parole T non è abbastanza potente da permettere di provare tutte le proposizioni vere dell'aritmetica.

Dim. Detta ϕ la formula indecidibile, se si ammette il modello naturale dell'aritmetica, allora in tale modello sarà vera ϕ oppure $\neg \phi$. Nel primo caso ϕ è una proposizione vera che non può essere dimostrata, nel secondo caso la stessa cosa si può dire per $\neg \phi$.

Secondo teorema di Gödel. La formula $\neg \exists x Pr(x, \gamma \wedge \neg \gamma)$ che asserisce la consistenza di T non si può provare in T .

Pertanto anche per il secondo teorema la possibilità di autoriferimento è essenziale. Il teorema afferma che la consistenza di una teoria T non può essere provata all'interno della stessa teoria T . In altri termini per provare la consistenza di T dobbiamo necessariamente utilizzare strumenti più potenti di T stesso. Tale teorema mostra che non è possibile, come sperava Hilbert, provare la consistenza di teorie "forti" che coinvolgono l'infinito attuale tramite metodi finitisti.

6. La matematica come sistema di riscrittura: (Mathematica, Derive).

Dato un linguaggio L spesso viene introdotta una relazione di equivalenza che, detto in termini intuitivi, rappresenta l'idea che due espressioni in L "dicono la stessa cosa". Ad esempio nel calcolo proposizionale abbiamo già definito la relazione di equivalenza logica. Nel calcolo dei predicati si definisce una analoga relazione di equivalenza logica. Nell'aritmetica consideriamo equivalenti due espressioni del tipo $3+4$ e $4+3$, $3 \times (3+4)$ e $3 \times 3 + 3 \times 4$ e così via. Appare allora naturale porsi il problema di come si possa trasformare una espressione di L in una più semplice che sia equivalente, cioè che rappresenti la stessa cosa. Questo viene fatto tramite opportune "regole di trasformazioni" che consentano, appunto, di partire da una data parola e di arrivare, dopo un certo numero di passi alla parola equivalente più semplice possibile (forma normale).

Esempio. Nell'insieme delle espressioni aritmetiche, cioè espressioni del tipo $(3+5) \cdot 37 + 1$ possiamo chiamare forma normale la forma decimale in cui un intero è rappresentato da una somma di potenze di dieci. Allora quando si esegue una operazione, ad esempio il prodotto, il problema consiste nel passare dalla forma normale di due numeri x ed y alla forma normale di $x \cdot y$. Ad esempio, il prodotto di 234 per 11 viene visto come riduzione a forma normale dell'espressione $(2 \cdot (10 \cdot 10) + 3 \cdot 10 + 4) \cdot (10 + 1)$ riduzione che porta alla espressione $2 \cdot (10 \cdot 10) + 5 \cdot 10 + 7$. Lo stesso "calcolo delle espressioni" che si studia a scuola non è altro che una riduzione di una espressione a forma normale.

Anche tutti i sistemi di "calcolo simbolico" come Derive o Mathematica consistono nel considerare un insieme L di espressioni e di applicare a tale insieme di espressioni degli opportuni processi di trasformazione fino a giungere alla relativa forma canonica.

La teoria generale che tratta tali tipi di problematiche prende il nome teoria dei "sistemi di riduzione" detti anche sistemi di *trasformazione* o di *riscrittura*. I sistemi di trasformazione permettono di rappresentare anche i più svariati problemi. Infatti spesso risolvere un problema consiste nel fare una serie di "azioni" che facciano passare da uno stato iniziale ad uno stato che si possa considerare soluzione del problema. Naturalmente non tutte le azioni sono da considerare possibili, allora nell'insieme S degli stati è definita una relazione binaria $\rightarrow \subseteq S \times S$ tale che $x \rightarrow y$ se e solo se è possibile passare dallo stato x allo stato y .

Esempio. Ad esempio consideriamo un qualunque solitario di carte, chiamiamo *stato* una qualunque possibile distribuzione di carte sul tavolo ed indichiamo con S l'insieme degli stati. Le regole del solitario si possono rappresentare da una relazione binaria \rightarrow in S in modo che $s \rightarrow s'$ significa che esiste una mossa (corretta in base al regolamento del gioco) con cui è lecito passare dallo stato s allo stato s' . Risolvere il solitario significa trovare una successione s_1, s_2, \dots, s_n di stati tali che

- i) s_1 sia lo stato iniziale (in generale scelto in modo casuale)
- ii) $s_i \rightarrow s_{i+1}$ cioè è lecito passare da s_i a s_{i+1} per ogni $i = 1, \dots, n-1$
- iii) s_n sia uno stato considerato vincente.

A volte capita di avere più regole diverse che consentono il passaggio da uno stato ad un altro e conviene specificare quale regola si è applicata (cioè *spiegare* come si è giunti alla soluzione. Ad esempio in un qualunque problema di geometria possiamo chiamare *stato* l'insieme dei dati del problema che si conoscono. Una regola che consente di passare da uno stato ad un altro (cioè calcolare nuovi dati) è in generale ottenuta tramite una formula o un teorema (il teorema di Pitagora, la formula per il calcolo di un'area, il teorema di Euclide,...). Se assegniamo un indice ad ogni formula o teorema, allora ciascuna di queste regole è una relazione \rightarrow_i in S .

Possiamo dare allora la seguente definizione:

Definizione 1. Chiamiamo *sistema di riduzione* o *sistema di trasformazioni* su un insieme S una famiglia di $(\rightarrow_i)_{i \in I}$ di relazioni binarie su S . Gli elementi di S vengono chiamati *stati* mentre gli indici $i \in I$ vengono chiamati *regole*. Se la coppia x e y di elementi di S è nella relazione \rightarrow_i allora diremo che y è un *ridotto diretto* di x tramite la regola i e scriveremo $x \rightarrow_i y$.

Esempio. Consideriamo il problema di risolvere le equazioni di primo grado in una incognita. Chiamiamo con S l'insieme di tutte le possibili equazioni di primo grado, ad esempio

$$3x+5=x-3x, x=x-3(x+1), \dots$$

Il problema che si pone è di partire da una data equazione ed arrivare ad una equazione equivalente del tipo $x = c$ dove c è un opportuno numero. Ciò naturalmente non può essere fatto manipolando i simboli a piacere. Bisogna procedere "rispettando le regole", cioè tramite una serie di operazioni che si considerano corrette.

Le operazioni che usualmente si utilizzano sono le seguenti:

1. passare una quantità (che si somma) da un lato all'altro di una equazione facendola diventare una quantità che si sottrae
2. passare una quantità (che si sottrae da un lato all'altro di una equazione facendola diventare una quantità che si somma
3. passare una quantità (che si moltiplica) da un lato all'altro facendola diventare una quantità che divide
4. passare una quantità (che si divide) da un lato all'altro facendola diventare una quantità che moltiplica
5. applicare tutte le leggi dell'aritmetica (proprietà distributiva, proprietà commutativa, ...)
6. effettuare tutti i calcoli che si possono fare.

Ad esempio, partendo da $3x+5=x-3x$ e saltando qualche passaggio, otteniamo

$$3x+5=x-3x \quad (\text{punto di partenza})$$

$$3x+5+3x = x \quad (\text{per la regola 2})$$

$$6x+5 = x \quad (\text{per la regola 6})$$

$$6x = x-5 \quad (\text{per la regola 1})$$

$$6x-x = -5 \quad (\text{per la regola 2})$$

$$5x = -5 \quad (\text{per la regola 6})$$

$$x = -5/5 \quad (\text{per la regola 3})$$

$$x = -1 \quad (\text{soluzione del problema}).$$

Definizione 2. Dato un sistema di riduzione $(S, (\rightarrow_i)_{i \in I})$, indichiamo con \rightarrow la relazione che si ottiene come unione delle relazioni \rightarrow_i . Se x ed y sono nella relazione \rightarrow allora diremo semplicemente che y è il ridotto diretto di x .

In altri termini poniamo risulta che $x \rightarrow y$ se esiste $i \in I$ tale che $x \rightarrow_i y$. Ci riferiamo a \rightarrow quando non interessa sapere quale regola è stata utilizzata per passare dallo stato x allo stato y ma solo che è consentito passare da x ad y .

Definizione 3. Dato un sistema di riduzione $(S, (\rightarrow_i)_{i \in I})$, indichiamo con \longrightarrow la chiusura transitiva di \rightarrow . Inoltre se $x \longrightarrow y$ diremo che y è un ridotto di x . Indichiamo invece con \leftrightarrow la chiusura simmetrica di \rightarrow e con \longleftrightarrow la relazione di equivalenza generata da \rightarrow .

Chiamiamo *successione di riduzioni* una successione a_1, \dots, a_n di elementi di S tale che ogni a_i è il ridotto diretto di a_{i-1} . Allora y è un ridotto di x se esiste una successione di riduzioni a_1, \dots, a_n tale che $a_1 = x$ e $a_n = y$. Per indicare una tale successione scriveremo anche $a_1 \rightarrow a_2 \dots \rightarrow a_{n-1} \rightarrow a_n$. Se $x \longleftrightarrow y$ diremo anche che x ed y sono *convertibili*. Naturalmente, x è convertibile in y se e solo se esiste una successione a_1, \dots, a_n tale che $a_1 \leftrightarrow a_2, a_2 \leftrightarrow a_3, \dots, a_{n-1} \leftrightarrow a_n$.

Definizione 4. Diciamo che un elemento a in S è in *forma normale*, se non ammette ridotti propri, cioè se non esiste $b \in S$ tale che $b \neq a$ e $a \rightarrow b$.

Possiamo interpretare $x \rightarrow y$ dicendo che y è una versione semplificata di x . Allora le forme normali sono stati che non possono essere ulteriormente semplificati. Ad esempio, nel caso delle equazioni di primo grado le forme normali sono le equazioni del tipo $x = c$. Uno dei problemi fondamentali dei sistemi di trasformazione è la riduzione a forma normale, cioè dato uno stato x , trovare uno stato x' che sia equivalente ad x e che sia in forma normale.

Proposizione 5. Supponiamo che non esistano catene infinite. Allora ogni elemento $x \in S$ può essere ridotto a forma normale.

Dim. Sia $x \in S$, allora se x è in forma normale il teorema è provato. Se x non è in forma normale allora esiste x_1 tale che $x \rightarrow x_1$. Se x_1 è in forma normale il teorema è provato altrimenti esiste x_2 tale che $x_1 \rightarrow x_2$. Procedendo in questo modo, poiché non esistono catene infinite si perverrà ad una catena finita $x \rightarrow x_1 \rightarrow \dots \rightarrow x_n$ tale che x_n è in forma normale.

LETTURE

Registrazione di un pezzo di un colloquio televisivo tra Piergiorgio Odifreddi (un logico matematico) e Giorello (un filosofo).

Odifreddi: Credo che, però, la domanda fosse in qualche modo suggerita all'ascoltatore dal teorema di Gödel, che viene spesse volte frainteso in questo senso. Il teorema di Gödel dimostra

semplicemente che non tutte le verità si possono dimostrare, appunto, dal punto di vista matematico. Dimostra cioè una limitazione della matematica, ma è una limitazione non nel senso del relativismo: cioè che ciò che prima era noto, adesso non possiamo più crederlo. In realtà Gödel ha dimostrato che la matematica può fare certe cose, ma non tutte. È una limitazione del senso di potenza, vivaddio.

Giorello: E non riesce ad autogiustificarsi.

Odifreddi: Ma questo non scalfisce la verità matematica: cioè ciò che i matematici dimostrano, appunto, dipende dagli assiomi, ma una volta fissati gli assiomi, questa è una conseguenza necessaria degli assiomi. Mentre il teorema di Gödel troppo spesso viene riformulato in questa maniera un po' approssimativa che si presta ai fraintendimenti.

Giorello: Sì. E tra l'altro questa presentazione non rende giustizia agli aspetti interessanti e stimolanti del teorema di Gödel, cioè al fatto che getta una luce forte sul fenomeno dell'autoriferimento. L'autoriferimento, ecco un altro bell'esempio di legame tra riflessione matematica e umanesimo. Perché l'autoriferimento è un'esperienza che noi facciamo molto spesso, in molti settori. Studiamo il cosmo, ma siamo una parte di questo cosmo che studiamo, studiamo i viventi, ma siamo anche noi esseri viventi, vogliamo studiare l'intelligenza, ma siamo dei soggetti intelligenti, vogliamo studiare la società, ma facciamo parte della società che studiamo. L'autoriferimento attraversa non poche imprese umane. Si impara a fare i conti con l'autoriferimento fin dai tempi di Epimenide il cretese che dice: "Tutti i cretesi mentono"... Un allettante esempio di autoriferimento che, poi, è l'idea che ritroviamo codificata nella conclusione di Gödel e, poi, nel teorema di Tarski sulla difficoltà di esprimere il concetto di verità in modo formale. Ecco, i grandi teoremi cosiddetti della logica contemporanea, in realtà ci fanno toccare le difficoltà profonde di un grande problema filosofico. Il problema che ci riferiamo necessariamente a noi stessi, mentre cerchiamo di proiettarci sul mondo. Forse, veramente la sfida più difficile è il "conosci te stesso" dell'oracolo di Delfi. La truffa maggiore forse è stata questa.

Odifreddi: A proposito del teorema di Gödel, ho una metafora, per spiegarlo, che si riferisce al potere giudiziario. La verità è l'analogo di quello che i pubblici ministeri, gli accusatori, cercano di scoprire quando fanno le indagini e cercano di capire che cosa effettivamente è successo. Quando, però, si fanno i processi, i processi non possono essere fatti altro che all'interno di una certa legislazione che corrisponde esattamente agli assiomi e alle regole dei sistemi formali matematici. Quindi, anche dal punto di vista giudiziario, c'è una differenza tra ciò che si può dimostrare, che sono appunto i contenuti delle sentenze, e ciò che invece veramente è successo. E questo è l'analogo della dimostrabilità e della verità in matematica. Il teorema di Gödel dice semplicemente che ci sono verità indimostrabili. E questo in tutti i processi di mafia lo fanno vedere. Ci sono cose che si sa benissimo come sono andate, però un conto è sapere qual è la verità e un conto è riuscire a dimostrarla. Il teorema di Gödel dice proprio questo, che tante cose che in matematica sono vere, però poi non si riescono a dimostrare, con i mezzi della matematica. E questo appunto mi sembra una buona metafora.

BIBLIOGRAFIA.

Gli argomenti del programma sono contenuti in appunti che possono essere richiesti al docente. Per un maggiore approfondimento si consigliano i seguenti testi.

Per la storia della matematica

- Morris Kline, La matematica nella cultura occidentale, Feltrinelli.
- L. L. Radice, L'infinito, Editori Riuniti.
- Bottazzini-Freguglia-Rigatelli (1992) Fonti per la storia della matematica, Sansoni.
- Eric T. Bell, I grandi Matematici, Sansoni, 1966.
- B. D'Amore, M. Matteuzzi, Gli interessi matematici, Marsilio.

Per quanto riguarda i fondamenti della geometria si consiglia di leggere direttamente

- D. Hilbert, Fondamenti della geometria, Feltrinelli.

Per le geometrie non euclidee

- E. Agazzi, D. Palladino, Le geometrie non euclidee, Mondadori.

Per chi fosse interessato alla filosofia della matematica.

- E. Casari, La filosofia della matematica del '900, Sansoni.
- L. Geymonat, Storia del pensiero filosofico e scientifico, Garzanti.
- D. R. Hofstadter, Goedel, Escher, Bach: un'eterna Ghirlanda Brillante.
- E. Casari, Questioni di filosofia della matematica, Feltrinelli.
- Rudy Rucker, La mente e l'infinito, Muzzio, 1991.
- Wang Hao, Dalla matematica alla filosofia, Boringhieri, 1984.
- C. Cellucci, La filosofia della matematica, Laterza 1967.