

CAPITOLO 9

[indice](#)

GENERARE I TEOREMI DI UNA QUALUNQUE TEORIA

1. Altre regole di inferenza

Nel capitolo precedente abbiamo definito la nozione di sistema inferenziale corretto cioè un sistema A di assiomi ed un sistema di regole di inferenza per cui valga l'implicazione

$$T \vdash \alpha \Rightarrow T \vDash \alpha$$

Tale implicazione afferma che se si è provato α allora α risulta vera in tutti i modelli di T . Inoltre abbiamo proposto un sistema inferenziale che si è dimostrato adeguato per teorie particolarmente semplici: i programmi. In questo capitolo ci proponiamo obiettivi più ambiziosi perché vogliamo definire sistemi inferenziali che si applichino a tutti i tipi di teorie e che siano "adeguatamente potenti" cioè tali che sia verificata l'altra implicazione

$$T \vDash \alpha \Rightarrow T \vdash \alpha.^1$$

Naturalmente per fare in modo che tale implicazione sia valida dobbiamo fornire il nostro sistema inferenziale di un numero sufficiente di regole di inferenza e di assiomi logici².

Cominciamo con l'esplorare alcune possibili regole di inferenza. Molte si possono ottenere a partire da ovvie equivalenze logiche. Ad esempio le seguenti due regole derivano dalla legge della doppia negazione

$$\frac{\alpha}{\neg(\neg(\alpha))} \quad (\text{regola di } \neg\text{-introduzione}) \qquad \frac{\neg(\neg(\alpha))}{\alpha} \quad (\text{regola di } \neg\text{-eliminazione})$$

Le seguenti esprimono la proprietà commutativa della congiunzione e della disgiunzione

$$\frac{\alpha \wedge \beta}{\beta \wedge \alpha} \quad (\wedge\text{-commutativa}) \qquad \frac{\alpha \vee \beta}{\beta \vee \alpha} \quad (\vee\text{-commutativa})$$

Queste sono relative alla disgiunzione.

$$\frac{\neg\alpha ; \alpha \vee \beta}{\beta} \quad (\vee\text{-eliminazione}) \qquad \frac{\alpha}{\alpha \vee \beta} \quad (\vee\text{-introduzione})$$

Da notare che se si è provato α ed $\alpha \rightarrow \beta$, cioè $(\neg\alpha) \vee \beta$, allora possiamo asserire anche $\neg\neg\alpha$ e $(\neg\alpha) \vee \beta$ e quindi per la regola di \vee -eliminazione, possiamo asserire β . In altre parole la regola di \vee -eliminazione permette anche di definire MP e quindi questa regola di inferenza può

¹ Da notare che non è affatto scontato che questo avvenga. Infatti a sinistra dell'implicazione viene coinvolto l'universo, enorme, di tutti i possibili modelli. A destra ci si riferisce alla applicazione di un numero finito di regole di inferenza ed ad semplice sistema di formule logicamente vere.

² In queste note non cercherò di ridurre al minimo il numero di regole ed assiomi. Invece abonderò in regole di inferenza. Questo perché vorrei arrivare a definire una nozione di dimostrazione che sia non troppo lontana da quello che viene fatto dai matematici i quali usano continuamente regole di inferenza e modi di "riscrivere" le formule già dimostrate. Da questo punto di vista la nozione di dimostrazione viene messa sullo stesso piano dei sistemi di riscrittura che abbiamo proposto nei capitoli precedenti per la riduzione a forma normale.

essere considerata una regola derivata.

Accettiamo anche un paio di regole relative a \wedge .

$$\frac{\alpha; \beta}{\alpha \wedge \beta} \text{ (regola della } \wedge\text{-introduzione)} \quad \frac{\alpha \wedge \beta}{\alpha} \text{ (regola di } \wedge\text{-eliminazione)}$$

Da notare che tali regole permettono facilmente di provare che

$$T \vdash \alpha \wedge \beta \Leftrightarrow T \vdash \alpha \text{ e } T \vdash \beta.$$

Esistono anche regole relative ai quantificatori. La principale è la regola di generalizzazione che abbiamo già citato a cui affianchiamo una regola di particolarizzazione. Chiameremo queste regole di \forall -introduzione e \forall -eliminazione, rispettivamente

$$\frac{\alpha}{\forall x(\alpha)} \text{ (regola di } \forall\text{-introduzione)} \quad \frac{\forall x(\alpha)}{\alpha(t)} \text{ (regola di } \forall\text{-eliminazione)}$$

dove t è un termine chiuso. Infine accettiamo una regola di introduzione di \exists

$$\frac{\alpha(t)}{\exists x(\alpha)} \text{ (regola di } \exists\text{-introduzione)}$$

Altre regole che spesso vengono usate si basano sul fatto che per i matematici il "simbolo" con cui viene indicata una variabile quantificata non ha importanza. Ad esempio la formula $\forall x_1 \forall x_2 (x_1 + x_2 = x_2 + x_1)$ ha lo stesso significato della formula $\forall x_3 \forall x_2 (x_3 + x_2 = x_2 + x_3)$ (nel senso che sono logicamente equivalenti ed entrambe esprimono la proprietà commutativa. E' possibile precisare questo fatto al modo seguente. Chiamiamo *simili* due formule $\alpha(x_i)$ e $\alpha(x_j)$ se la prima formula contiene occorrenze libere di x_i esattamente in quei posti in cui la seconda possiede occorrenze libere di x_j . Ad esempio sono simili le formule $\alpha(x_3) = \forall x_2 (x_3 + x_2 = x_2 + x_3)$ e $\alpha(x_1) = \forall x_2 (x_1 + x_2 = x_2 + x_1)$ perché nella prima formula la variabile x_3 compare in tutti e soli i posti in cui compare x_1 nella seconda. Introduciamo allora le seguenti regole di inferenza che prende il nome di "rinonima delle variabili" e che si applica a coppie di formule simili $\alpha(x_i)$ e $\alpha(x_j)$:

$$\frac{\forall x_i \alpha(x_i)}{\forall x_j \alpha(x_j)} \quad \frac{\exists x_i \alpha(x_i)}{\exists x_j \alpha(x_j)} \text{ (regola di rinonima delle variabili)}$$

Una coppia di regole utili sono le seguenti che sono legate alla riduzione di una formula a forma normale prenessa.

$$\frac{\forall x(\alpha \rightarrow \gamma)}{\alpha \rightarrow \forall x(\gamma)} \quad \frac{\alpha \rightarrow \forall x(\gamma)}{\forall x(\alpha \rightarrow \gamma)} \text{ (regole della forma normale prenessa)}$$

dove viene supposto che α sia una formula chiusa. Infine si ammette che l'insieme degli assiomi logici $A1$ contenga almeno tutti gli esempi di tautologie³ anche se poi di fatto ne

³ Ricordiamo che un esempio di tautologia è una formula α^* della logica del primo ordine che si ottiene considerando una tautologia α del calcolo proposizionale classico e sostituendo a ciascuna variabile proposizionale una opportuna formula.

useremo solo poche. Nel seguito decideremo quali ulteriori formule conviene mettere in Al^4 .

Possiamo ora ricavare il seguente fondamentale teorema.

Teorema 1.1. (Teorema di Deduzione). Consideriamo un sistema inferenziale corretto le cui regole di inferenza sono quelle elencate in questo paragrafo. Allora per ogni teoria T e per ogni formula chiusa α risulta

$$T \cup \{ \alpha \} \vdash \beta \Rightarrow T \vdash \alpha \rightarrow \beta.$$

Dim. Dobbiamo dimostrare che:

esiste una dimostrazione π di β sotto ipotesi $T \cup \{ \alpha \}$

\Rightarrow esiste una dimostrazione π^* di $\alpha \rightarrow \beta$ sotto ipotesi T .

Procediamo per induzione sulla lunghezza n di π . Se la lunghezza della dimostrazione è 1 allora sono possibili i seguenti due casi:

1. β è un assioma logico oppure appartiene a T . In tale caso, tenendo conto che per la regola di \vee -introduzione da β è possibile dedurre $\neg\alpha \vee \beta$, abbiamo che $T \vdash \alpha \rightarrow \beta$ e la proposizione è dimostrata.

2. β coincide con α . In tale caso $\alpha \rightarrow \beta$ coinciderebbe con la formula $\alpha \rightarrow \alpha$ che, essendo un esempio di tautologia, è sicuramente un teorema di T .

Supponiamo ora che $n \neq 1$ e che il teorema sia vero per tutte le dimostrazioni di lunghezza minore di n . Poiché abbiamo già esaminato il caso in cui β possa essere un assioma logico oppure appartenere a T , supporremo che β sia stato ottenuto tramite una regola di inferenza. E' necessario allora esaminare tanti casi quante sono le regole di inferenza.

- β è stato ottenuto per \vee -eliminazione dalle formule $\neg\gamma$ e $\gamma \vee \beta$. Allora poiché tali formule sono state dimostrate con dimostrazioni di lunghezza minore di n per ipotesi di induzione risulterà che $T \vdash \alpha \rightarrow \neg\gamma$ e $T \vdash \alpha \rightarrow (\gamma \vee \beta)$. Pertanto esistono due dimostrazioni π_1 e π_2 di tali formule. Ne segue che per provare $T \vdash \alpha \rightarrow \beta$ è sufficiente osservare che la formula $(\alpha \rightarrow \neg\gamma) \rightarrow ((\alpha \rightarrow (\gamma \vee \beta)) \rightarrow (\alpha \rightarrow \beta))$ è un esempio di tautologia e quindi un assioma logico.

- β è stato ottenuto per generalizzazione da una formula γ in π e quindi $\beta = \forall x(\gamma)$. Allora per ipotesi di induzione sappiamo che $T \vdash \alpha \rightarrow \gamma$ e quindi per generalizzazione $T \vdash \forall x(\alpha \rightarrow \gamma)$. L'applicazione della prima regola della forma normale prenessa permette allora di dimostrare che $T \vdash \alpha \rightarrow \forall x(\gamma)$.

Per le altre regole di inferenza si prosegue in modo analogo.

2. Una condizione perché un sistema deduttivo sia sufficientemente potente

Per potere definire una semplice condizione perché un sistema deduttivo sia sufficientemente potente, introduciamo la nozione di consistenza.

Definizione 2.1. Diremo che una teoria T è *contraddittoria* o *inconsistente* se esiste $\alpha \in \mathcal{L}$ tale che

$$T \vdash \alpha \quad \text{e} \quad T \vdash \neg\alpha.$$

⁴ Si osservi che se mettiamo tutti gli esempi di tautologia in Al allora potremmo ridurci ad accettare MP come unica regola di inferenza. Ad esempio tramite l'esempio di tautologia $\alpha \rightarrow \beta \rightarrow (\alpha \wedge \beta)$ ed una doppia applicazione di MP possiamo ottenere tutte le asserzioni che si ottengono tramite la regola di \wedge -introduzione. Invece tutte le asserzioni che si possono ottenere tramite le regole di eliminazione possono essere anche ottenute tramite MP e gli esempi di tautologia $\alpha \wedge \beta \rightarrow \alpha$ e $\alpha \wedge \beta \rightarrow \beta$.

Una teoria non contraddittoria si dirà *consistente*.

Le teorie inconsistenti creano un collasso dell'apparato deduttivo nel senso che a partire da una teoria inconsistente tutte le asserzioni sono dimostrabili.

Teorema 2.2. Le seguenti proposizioni sono equivalenti.

- a) T è contraddittoria
- b) ogni formula può essere dimostrata in T
- c) esiste una formula α tale che $T \vdash \alpha \wedge \neg \alpha$.

Dim. a) \Rightarrow b) Supponiamo che esista una formula α tale che $T \vdash \alpha$ e $T \vdash \neg \alpha$ e siano π_1 e π_2 due dimostrazioni di α e di $\neg \alpha$, rispettivamente. Allora, detta β una qualunque formula, essendo $\alpha \rightarrow (\neg \alpha \rightarrow \beta)$ una tautologia, mettendo una dopo l'altra π_1 e π_2 ed applicando due volte MP abbiamo che $T \vdash \beta$.

b) \Rightarrow c) Ovvio.

c) \Rightarrow a) Se $T \vdash \alpha \wedge \neg \alpha$ allora per le regole di \wedge -eliminazione risulta che $T \vdash \alpha$ e $T \vdash \neg \alpha$. \square

Il teorema di deduzione consente di dimostrare che le nozioni di deducibilità e quella di inconsistenza sono una riconducibile all'altra.

Teorema 2.3. Data una teoria consistente T ed una formula chiusa α ,

$$T \cup \{\neg \alpha\} \text{ inconsistente} \Leftrightarrow T \vdash \alpha.$$

Dim. Se $T \cup \{\neg \alpha\}$ è inconsistente allora ogni formula può essere provata in tale teoria e pertanto $T \cup \{\neg \alpha\} \vdash \alpha$. Essendo α chiusa, per il teorema di deduzione sarà anche $T \vdash \neg \alpha \rightarrow \alpha$. D'altra parte la formula $(\neg \alpha \rightarrow \alpha) \rightarrow \alpha$ è un esempio di tautologia, pertanto per MP possiamo concludere che $T \vdash \alpha$.

E' evidente che se $T \vdash \alpha$ allora $T \cup \{\neg \alpha\} \vdash \alpha$ e $T \cup \{\neg \alpha\} \vdash \neg \alpha$ e quindi che $T \cup \{\neg \alpha\}$ è inconsistente. \square

Da notare che per provare le due proposizioni ora esposte non è necessario che in Al ci siano tutti gli esempi di tautologie ma solo quelli utilizzati nel corso della dimostrazione. Pertanto è sufficiente supporre che Al contenga tutte le formule del tipo:

$$\alpha \rightarrow (\neg \alpha \rightarrow \beta).$$

$$\alpha \rightarrow \alpha$$

$$(\alpha \rightarrow \gamma) \rightarrow ((\alpha \rightarrow (\gamma \rightarrow \beta)) \rightarrow (\alpha \rightarrow \beta))$$

$$(\neg \alpha \rightarrow \alpha) \rightarrow \alpha$$

Non proseguiremo oltre in tale tipo di osservazione ma è chiaro che ogni volta che proviamo un teorema che riguarda il nostro sistema inferenziale possiamo allungare l'elenco degli esempi di tautologie che ci servono. In questo modo possiamo evitare di considerare tutti i possibili esempi di tautologie.

Torniamo al problema fondamentale da cui siamo partiti, cioè di fare in modo che il nostro sistema inferenziale sia corretto e completo. Tale problema si può ricondurre ad un altro che appare più semplice. Ricordiamo che una teoria si dice *soddisfacibile* se ammette almeno un modello.

Teorema 2.4. Supponiamo che un sistema inferenziale sia tale che, per ogni teoria T ,

$$T \text{ consistente} \Leftrightarrow T \text{ soddisfacibile.}$$

Allora tale sistema è corretto e completo.

Dim. Sia \underline{T} una qualunque teoria ed osserviamo che invece di provare l'equivalenza

$$\underline{T} \vdash \alpha \Leftrightarrow \underline{T} \vDash \alpha$$

possiamo provare l'equivalenza

$$\text{non } \underline{T} \vdash \alpha \Leftrightarrow \text{non } \underline{T} \vDash \alpha \Leftrightarrow \text{esiste un modello di } \underline{T} \text{ in cui } \alpha \text{ è falsa.}$$

D'altra parte,

$$\text{non } \underline{T} \vdash \alpha \Leftrightarrow \underline{T} \cup \{\neg \alpha\} \text{ consistente}$$

e quindi dobbiamo provare

$$\underline{T} \cup \{\neg \alpha\} \text{ consistente} \Leftrightarrow \underline{T} \cup \{\neg \alpha\} \text{ ammette un modello.}$$

Ma tale equivalenza abbiamo supposto che valga per ogni teoria T e quindi anche per la teoria $T = \underline{T} \cup \{\neg \alpha\}$.

Ne segue che ora il nostro compito è trovare un sistema inferenziale in cui sia possibile provare l'equivalenza

$$T \text{ consistente} \Leftrightarrow T \text{ ammette un modello.}$$

Per un lato di tale equivalenza non ci sono problemi.

Proposizione 2.5. Ogni teoria T che ammette un modello è consistente.

Dim. Supponiamo che T ammetta un modello I , e supponiamo, per assurdo, che le formule α e $\neg \alpha$ siano dimostrabili in T . D'altra parte, poiché il nostro sistema inferenziale è corretto, ciò comporterebbe che $T \vDash \alpha$ e $T \vDash \neg \alpha$. Poiché I è un modello di T , ne seguirebbe che $I \vDash \alpha$ e $I \vDash \neg \alpha$, e ciò è assurdo poiché una formula non può essere falsa e vera nello stesso modello.

E' invece molto più complicato provare il viceversa, cioè che ogni teoria consistente ammette un modello. Esporremo tale dimostrazione nei prossimi paragrafi.

3. Modelli di Herbrand associati ad una data teoria

Abbiamo visto che il nostro compito è, data una teoria consistente T , costruire in qualche modo un modello di T . Una via ragionevole sembra quella suggerita dalla programmazione logica in cui sono coinvolti i modelli di Herbrand⁵. Più precisamente abbiamo visto T è un programma per costruire il minimo modello di Herbrand di T è sufficiente considerare il modello determinato dall'insieme dei fatti che sono dimostrabili a partire da T . Allora appare naturale considerare la seguente definizione.

Definizione 3.1. Sia T una teoria, allora chiamiamo *interpretazione di Herbrand associata a T* l'interpretazione di Herbrand definita dall'insieme S di fatti deducibili da T :

$$S = \{r(t_1, \dots, t_n) \in B_{\mathcal{L}} \mid T \vdash r(t_1, \dots, t_n)\}.$$

Indichiamo con I_T una tale interpretazione.

⁵ D'altra parte abbiamo già provato che se una teoria ammette un modello allora ammette anche un modello di Herbrand (in una estensione opportuna del linguaggio). Quindi il fatto di concentrarci sui modelli di Herbrand non è restrittivo.

Purtroppo, a differenza del caso in cui T è un programma positivo, in generale non è detto che I_T sia un modello di T . Ad esempio consideriamo la teoria

$$T = \{r(a), r(b), \exists x(\neg r(x))\},$$

allora I_T non è un modello di T . Infatti l'universo di Herbrand si riduce a $\{a, b\}$ e, essendo $T \vdash r(a)$ e $T \vdash r(b)$, necessariamente $I_T(r) = \{a, b\}$ e quindi $\exists x(\neg r(x))$ è falsa. Ciò è conseguenza del fatto che, in un senso che preciseremo, la nostra teoria "non ha sufficienti nomi". Infatti se al linguaggio si aggiunge una terza costante c allora $(\{a, b, c\}, I_T)$ è un modello di Herbrand di T . Questa osservazione suggerisce la seguente definizione.

Definizione 3.2. Diremo che una teoria T ha *sufficienti nomi* nel linguaggio \mathcal{L} se risulta, per ogni formula α ,

$$T \vdash \exists x \alpha(x) \Rightarrow \text{esiste un termine chiuso } t \text{ tale che } T \vdash \alpha(t).$$

Diremo che T è *sintatticamente completa*⁶ se ogni formula o è dimostrabile o è confutabile in T .

In altri termini, T ha sufficienti nomi se ogni volta che può essere dimostrato in T che esiste un elemento per cui vale la proprietà α , allora nel linguaggio esiste un "nome" per tale elemento (cioè un termine chiuso che lo denota). Se si accetta questa proprietà allora si spera che nell'universo di Herbrand esista abbastanza materiale per costruire un modello di T . Da notare che poiché l'implicazione inversa si ottiene tramite una applicazione della regola di \exists -introduzione, l'implicazione presente nella definizione 2.2 in realtà è una equivalenza

$$T \vdash \exists x \alpha(x) \Leftrightarrow \text{esiste un termine chiuso } t \text{ tale che } T \vdash \alpha(t).$$

Da osservare che nel capitolo 8 abbiamo già dimostrato che se I è un modello di Herbrand allora vale l'equivalenza

$$I \models \exists x_i \alpha(x_i) \Leftrightarrow \text{esiste un termine } t \in U(\mathcal{L}) \text{ tale che } I \models \alpha(x_i/t).$$

che invece di coinvolgere una teoria T e la relazione sintattica \vdash coinvolge il modello I e la relazione semantica \models .

Proposizione 3.3. Se T è una teoria completa allora

$$T \vdash \beta \vee \gamma \Leftrightarrow T \vdash \beta \text{ oppure } T \vdash \gamma$$

Proof. Supponiamo che $T \vdash \beta \vee \gamma$ e che β non sia un teorema di T . Allora, poiché T è completa deve essere un teorema di T la formula $\neg \beta$. Applicando la regola di \vee -eliminazione alle formule $\beta \vee \gamma$ e $\neg \beta$, otteniamo che γ è un teorema di T .

Supponiamo che $T \vdash \beta$ oppure $T \vdash \gamma$ allora per le regole di \vee -introduzione ed eventualmente le regole relative alla commutatività di \vee , otteniamo che $T \vdash \beta \vee \gamma$.

Proposizione 3.4. Sia T una teoria con sufficienti nomi, consistente e completa e sia I_T il modello di Herbrand ad essa associato. Allora per ogni formula chiusa α

$$I_T \models \alpha \Leftrightarrow T \vdash \alpha \tag{3.1}$$

Pertanto I_T è un modello di T .

Dim. Dimostriamo (3.1) per induzione sulla complessità di α .

⁶ Ricordiamo che abbiamo definito già la nozione analoga di *semanticamente completa* che si riferisce alla relazione semantica \models e non a quella sintattica \vdash . Poiché si dimostrerà, con il teorema di completezza, che tali relazioni coincidono, la nozione di semanticamente completa e sintatticamente completa di fatto coincidono.

Sia α uguale alla formula atomica $r(t_1, \dots, t_n)$, allora, per il modo come è stata definita $I_T(r)$,

$$I_T \vDash r(t_1, \dots, t_n) \Leftrightarrow (t_1, \dots, t_n) \in I_T(r) \Leftrightarrow T \vdash r(t_1, \dots, t_n).$$

Sia α del tipo $\beta \wedge \gamma$ e supponiamo che (3.1) sia vera per β e γ . Inoltre osserviamo che per le regole di \wedge -introduzione e di \wedge -eliminazione risulta che $T \vdash \beta \wedge \gamma$ se e solo se $T \vdash \beta$ e $T \vdash \gamma$. Allora, risulta che

$$I_T \vDash \beta \wedge \gamma \Leftrightarrow I_T \vDash \beta \text{ e } I_T \vDash \gamma \Leftrightarrow T \vdash \beta \text{ e } T \vdash \gamma \Leftrightarrow T \vdash \beta \wedge \gamma.$$

Sia α del tipo $\beta \vee \gamma$, e supponiamo che (3.1) valga per β e γ . Allora, essendo T completa,

$$T \vdash \beta \vee \gamma \Leftrightarrow T \vdash \beta \text{ oppure } T \vdash \gamma \Leftrightarrow T \vDash \beta \text{ oppure } T \vDash \gamma \Leftrightarrow T \vDash \beta \vee \gamma$$

Inoltre,

$$I_T \vDash \beta \vee \gamma \Leftrightarrow I_T \vDash \beta \text{ oppure } I_T \vDash \gamma \Leftrightarrow T \vdash \beta \text{ oppure } T \vdash \gamma \Rightarrow T \vdash \beta \vee \gamma.$$

Sia α uguale a $\neg\beta$, allora abbiamo che

$$T \vdash \neg\beta \Leftrightarrow \text{non è vero che } T \vdash \beta.$$

Infatti, per l'ipotesi di consistenza per T risulta che da $T \vdash \neg\beta$ segue che non $T \vdash \beta$, per l'ipotesi di completezza abbiamo che da non $T \vdash \beta$ segue che $T \vdash \neg\beta$. Utilizzando allora l'ipotesi di induzione per β , risulta che

$$I_T \vDash \neg\beta \Leftrightarrow \text{non è vero che } I_T \vDash \beta \Leftrightarrow \text{non è vero che } T \vdash \beta \Leftrightarrow T \vdash \neg\beta.$$

Infine sia α la formula $\exists x\beta(x)$, allora, poiché T è con sufficienti nomi,

$$\begin{aligned} I_T \vDash \exists x\beta(x) &\Leftrightarrow I_T \vDash \beta(t) \text{ per un opportuno termine chiuso } t \\ &\Leftrightarrow T \vdash \beta(t) \text{ per un opportuno termine chiuso } t \\ &\Leftrightarrow T \vdash \exists x\beta(x). \end{aligned}$$

Dove la prima equivalenza vale per la proposizione 4.6 del Capitolo 8, la seconda per ipotesi di induzione, la terza per l'ipotesi per cui T ha sufficienti nomi. Abbiamo pertanto provato (3.1).

Concludiamo osservando che per ogni $\alpha \in T$ risulta che $T \vdash \alpha$ e quindi, per quanto dimostrato, $I_T \vDash \alpha$. Questo prova che I_T è un modello di T . □

4. Il teorema di completezza di Gödel

Una volta che abbiamo provato che ogni teoria T con sufficienti nomi, consistente e completa ammette un modello, non resta che cercare di ridurre una qualunque teoria a tali condizioni.

Proposizione 4.1. Se $(T_n)_{n \in \mathbb{N}}$ è una successione crescente di teorie consistenti, allora la teoria $T = \cup_{n \in \mathbb{N}} T_n$ è consistente. Inoltre ogni teoria consistente T si può estendere ad una teoria consistente e completa.

Dim. Per provare che $T = \cup_{n \in \mathbb{N}} T_n$ è consistente supponiamo, per assurdo, che $T \vdash \alpha \wedge \neg\alpha$. Allora dovrebbe esistere una dimostrazione π di $\alpha \wedge \neg\alpha$ che utilizzi gli assiomi di T , e quindi, detto F l'insieme delle formule in T utilizzate in π , F sarebbe un insieme finito tale che $F \vdash \alpha \wedge \neg\alpha$. Ma allora, per il Lemma 3 del secondo paragrafo del Capitolo 3, F sarebbe contenuto in una delle teorie T_n e quindi $T_n \vdash \alpha \wedge \neg\alpha$ in contrasto con l'ipotesi di consistenza per T_n .

Sia ora $\alpha_1, \alpha_2, \dots$ una enumerazione di tutte le formule chiuse e definiamo una successione $T_1, T_2, \dots, T_n, \dots$ di teorie per ricorsione ponendo $T_1 = T$, e (una volta che si sia definita T_n)

$$T_{n+1} = \begin{cases} T_n \cup \{\alpha_n\} & \text{se } \alpha_n \text{ è consistente con } T_n \\ T_n & \text{altrimenti.} \end{cases}$$

Per costruzione ognuna di tali teorie è consistente, pertanto per quanto ora dimostrato la teoria

$$T' = \bigcup_{n \in \mathbb{N}} T_n,$$

è una estensione consistente di T . Per provare la completezza di T' consideriamo una qualunque formula chiusa α e supponiamo che $\alpha = \alpha_n$, allora i casi possibili sono due:

- la teoria $T_n \cup \{\alpha_n\}$ è consistente; allora α_n appartiene a T_{n+1} e quindi a T'
- la teoria $T_n \cup \{\alpha_n\}$ non è consistente, allora, per la proposizione 2.3, $T_n \vdash \neg \alpha_n$ e quindi in T' è possibile provare la formula $\neg \alpha_n$. \square

Il seguente lemma prova che se la costante c non è presente in una teoria T ed è stata provata la formula $\alpha(c)$ sotto ipotesi T , allora la proprietà α vale per qualunque elemento. Questo perché a tutti gli effetti la costante c ha assunto il ruolo di variabile.

Lemma 4.2. Sia c una costante, T una teoria nelle cui formule non compare c ed $\alpha(x)$ una formula con una variabile libera x in cui non compare c . Allora se $T \vdash \alpha(c)$ sarà anche $T \vdash \forall x \alpha(x)$.

Dim. Sia π una dimostrazione della formula $\alpha(c)$ sotto le ipotesi T . Nelle formule di tale dimostrazione c non può essere presente in una ipotesi. Pertanto può comparire solo in un assioma logico o come conseguente nell'applicazione di una regola di inferenza. Sia y una variabile che non compare in π , allora se sostituiamo in π ad ogni occorrenza di c la variabile y , π si trasforma in una dimostrazione, sotto le ipotesi T , della formula $\alpha(y)$ che si ottiene sostituendo y a c . Applicando la regola di generalizzazione abbiamo quindi che $T \vdash \forall y \alpha(y)$. Naturalmente, essendo $\forall y \alpha(y)$ simile a $\forall x \alpha(x)$, abbiamo anche che $T \vdash \forall x \alpha(x)$. \square

Proposizione 4.3. Data una teoria consistente T nel linguaggio \mathcal{L} è sempre possibile ampliare \mathcal{L} con opportune costanti in modo che T si possa estendere in una teoria completa consistente e con sufficienti nomi.

Dim. Quello che vogliamo fare è ampliare il linguaggio \mathcal{L} e la teoria T in modo che, data una proprietà α , non appena sia possibile dimostrare che esiste un elemento per cui vale α , allora ci sia un "nome" t per cui sia possibile provare $\alpha(t)$. Ciò si ottiene non solo aggiungendo opportuni nomi (cioè costanti) ma anche legando opportunamente tali nomi alle proprietà esprimibili nel nuovo linguaggio. Il "trucco" che vogliamo applicare è quello di associare ad ogni formula $\alpha(x)$ con una variabile libera x una "nuova" costante c e di aggiungere alla teoria T la formula $\exists x \alpha(x) \rightarrow \alpha(c)$. In tale modo se dovesse risultare che $\exists x \alpha(x)$ è un teorema allora, per MP, sarebbe possibile dimostrare anche $\alpha(c)$. Possiamo vedere questa attività come creazione di nuovi nomi di oggetti man mano che si scopre l'esistenza di tali oggetti. Naturalmente si deve essere attenti al fatto che i nomi siano veramente nuovi e che quindi non compaiano già nel discorso già fatto.

Più precisamente procediamo al modo seguente.

Aggiungiamo ad \mathcal{L} un nuovo insieme numerabile di costanti Q e chiamiamo \mathcal{L}^* il linguaggio così ottenuto.

Indichiamo con $\alpha_1(x_1), \alpha_2(x_2), \dots$ una enumerazione di tutte le formule di \mathcal{L}^* che hanno al più una variabile libera (abbiamo indicato con x_i la variabile libera di α_i se tale variabile esiste).

Costruiamo una successione c_1, c_2, \dots di costanti distinte, scelte in Q , in modo che:

- la costante c_1 non appartenga alla formula α_1
- la costante c_2 non appartenga alle formule α_1, α_2
- ...
- la costante c_n non appartenga alle formule $\alpha_1, \alpha_2, \dots, \alpha_n$
- ...

Indichiamo con T_n la successione di teorie che si ottiene ponendo

$$T_0 = T \quad \text{e} \quad T_n = T_{n-1} \cup \{ \exists x_n \alpha_n \rightarrow \alpha_n(c_n) \}.$$

Proviamo, per induzione su n , che per ogni n la teoria T_n è consistente. Infatti ciò è vero per ipotesi nel caso $n = 0$. Supponiamo che T_{n-1} sia consistente e, per assurdo, che

$$T_n = T_{n-1} \cup \{ \exists x_n \alpha_n \rightarrow \alpha_n(c_n) \}$$

non lo sia. Allora $T_{n-1} \vdash \neg \{ \exists x_n \alpha_n \rightarrow \alpha_n(c_n) \}$ e quindi per ovvii passaggi $T_{n-1} \vdash (\exists x_n \alpha_n) \wedge \neg \alpha_n(c_n)$ da cui $T_{n-1} \vdash \exists x_n \alpha_n(x_n)$ e $T_{n-1} \vdash \neg \alpha_n(c_n)$. Ora la condizione per cui c_i non appartiene alle formule $\alpha_1, \alpha_2, \dots, \alpha_i$ assicura che c_n è una costante che non compare in T_{n-1} e quindi per il lemma 3.2 che $T_{n-1} \vdash \forall x_n \neg \alpha_n(x_n)$ e pertanto che $T_{n-1} \vdash \neg \exists x_n \alpha_n(x_n)$. Ciò è in contrasto con l'ipotesi di consistenza per T_{n-1} e con il fatto che abbiamo già provato che $T_{n-1} \vdash \exists x_n \alpha_n(x_n)$.

Consideriamo la teoria $T^* = \bigcup_{n \in \mathbb{N}} T_n$. Avendo dimostrato che ogni teoria T_n è consistente, ne segue che anche T^* è consistente⁷.

Sia T^c un completamento di T^* . Non è difficile provare che T^c è consistente, completa e con sufficienti nomi. □

Teorema 4.4. Sia T una teoria, allora vale la seguente equivalenza:

$$T \text{ è consistente} \Leftrightarrow T \text{ è soddisfacibile.}$$

Dim. Sia T consistente e sia T^c una estensione di T consistente completa e con sufficienti nomi. Allora per il corollario 3.6 esiste un modello di Herbrand di T^c e quindi di T e ciò prova che T è soddisfacibile. L'implicazione inversa è ovvia. □

Tale teorema prova che le condizioni espresse dal teorema 2.4 sono verificate e quindi che vale il seguente teorema di completezza⁸.

Teorema 4.5. (Teorema di Completezza) Per ogni teoria T ed ogni formula chiusa α risulta:

$$T \models \alpha \Leftrightarrow T \vdash \alpha.$$

Il teorema di completezza fornisce un significato semantico alla relazione \vdash di deducibilità e quindi permette di trovare esempi di teorie consistenti, teorie inconsistenti, teorie complete e teorie incomplete. Ad esempio sia T_1 la teoria dei gruppi e sia $T_2 = T_1 \cup \{ \alpha_1 \}$ dove α_1 è la formula $\exists x_1 \exists x_2 \neg (x_1 + x_2 = x_2 + x_1)$ (α_1 esprime il fatto che non vale la proprietà commutativa). La teoria T_2 è consistente poiché esistono gruppi non commutativi. Un esempio è il gruppo $G(S)$ delle permutazioni su di un dato insieme S (gruppo simmetrico). La teoria T_2 non è

⁷ Tale teoria si ottiene aggiungendo a T la successione di formule $\exists x_n \alpha_n \rightarrow \alpha_n(c_n)$ e quindi contiene, per ogni formula α_i , anche l'informazione " c_i è un elemento per cui vale α_i (se un tale elemento esiste)".

⁸ Tale teorema, che è uno dei primi e più importanti teoremi di logica matematica, è stato dimostrato nel 1929 da Kurt Gödel nella sua tesi di dottorato.

completa, infatti indichiamo con $\text{magg}(n)$ la formula

$$\exists x_1 \exists x_2 \dots \exists x_n ((x_1 \neq x_2) \wedge \dots \wedge (x_j \neq x_i) \wedge \dots)$$

esprime l'esistenza di un numero di elementi maggiore di n , allora è immediato che sia $T_2 \cup \{\text{magg}(1000)\}$ che $T_2 \cup \{\neg \text{magg}(1000)\}$ sono consistenti in quanto esiste sia un modello della prima teoria che uno della seconda. Infine consideriamo la teoria $T_2 \cup \{\neg \text{magg}(4)\}$ che è la teoria dei gruppi non commutativi con meno di quattro elementi. Tale teoria è inconsistente poiché in essa è possibile provare sia che non vale la proprietà commutativa (per l'assioma α_1) sia che in essa vale la proprietà commutativa (ricordiamo che tutti i gruppi con un numero primo di elementi sono ciclici e quindi commutativi).

5. Alcune conseguenze del teorema di completezza.

Una prima conseguenza immediata del teorema di completezza è il seguente teorema che mostra come ogni teoria che ammetta un modello ne ammette anche uno finito o numerabile.

Teorema 5.1. Consideriamo un linguaggio del primo ordine con identità il cui alfabeto sia finito o numerabile, allora ogni teoria consistente ammette un modello normale finito o numerabile.

Dim. Sia T consistente, allora esiste modello di Herbrand $(U(\mathcal{L}), I)$ di T . Poiché $U(\mathcal{L})$ è numerabile, il quoziente normale di $(U(\mathcal{L}), I)$ è un modello di T che ha dominio finito o numerabile. \square

Ricordiamo che il sistema di assiomi che si usa in generale per la teoria dei numeri reali comprende anche l'assioma di completezza che non è del primo ordine. Infatti tale assioma, nell'affermare che ogni sottoinsieme inferiormente limitato ammette estremo inferiore, "quantifica" sui sottoinsiemi e non sugli elementi. Si pone allora il problema se sia possibile proporre un altro sistema di assiomi che sia del primo ordine. Il seguente corollario dice che la risposta è negativa e che ogni sistema di assiomi che si possa proporre ammette anche un modello non isomorfo al campo dei numeri reali.

Teorema 5.2. Non esiste una teoria del primo ordine capace di caratterizzare una struttura matematica che abbia la potenza del continuo. In particolare non è possibile assiomatizzare nella logica del primo ordine il campo ordinato dei numeri reali o la geometria euclidea.

Dim. Data una struttura (D, I) non esiste una teoria del primo ordine T che abbia (D, I) come unico modello (a meno di isomorfismi). Infatti, essendo T soddisfacibile è anche consistente e quindi deve ammettere un modello finito o numerabile. Tale modello non può essere isomorfo a (D, I) . \square

Abbiamo già provato il teorema di compattezza passando per la teoria degli ultraprodotti. Il teorema di compattezza si può provare anche come immediata conseguenza del teorema di completezza.

Teorema 5.3. (Teorema di compattezza). Sia T una teoria, allora

$$T \text{ ammette un modello} \Leftrightarrow \text{ogni parte finita di } T \text{ ammette un modello.}$$

Dim. Poiché la nozione di soddisfacibilità coincide con quella di consistenza, possiamo

provare tale equivalenza per la consistenza. Supponiamo che ogni parte finita di T sia consistente, allora non può accadere che esista α tale che $T \vdash \alpha \wedge \neg \alpha$. Infatti in tale caso esisterebbe una dimostrazione π sotto ipotesi T di $\alpha \wedge \neg \alpha$. Detto F l'insieme di ipotesi coinvolte in π , F sarebbe un sottoinsieme finito di T tale che $F \vdash \alpha \wedge \neg \alpha$. \square

Teorema 5.4. Esiste un campo ordinato non archimedeo.

Dim. Consideriamo la teoria T dei campi ordinati, aggiungiamo al relativo linguaggio la costante i ed in tale linguaggio consideriamo la teoria T^* che si ottiene aggiungendo a T l'insieme infinito di assiomi del tipo

$i > 1$

$i > 1 + 1$

$i > (1 + 1) + 1$

...

che indichiamo in breve con $i > 1, i > 2, i > 3, \dots$. Allora ogni parte finita Fin di T^* ammette un modello. Infatti sia n il più grande n tale che $i > n$ sia in Fin . Allora il campo dei numeri reali in cui i sia interpretato con un numero maggiore di n fornisce un modello di $T \cup Z$.

Dal teorema di compattezza segue il seguente teorema.

Teorema 5.5. Sia T una teoria e supponiamo che per ogni naturale m , T ammetta modelli di cardinalità maggiore o uguale ad n , allora T ammette anche un modello di cardinalità infinita.

Dim. Per ogni intero n esiste una formula che asserisce che esistono almeno n elementi diversi tra loro. Infatti basta considerare la formula

$$a_n = \exists x_1 \dots \exists x_n (\neg(x_1 = x_2) \wedge \neg(x_1 = x_3) \wedge \dots \wedge \neg(x_2 = x_3) \wedge \neg(x_2 = x_4) \wedge \dots).$$

Sia T^* la teoria che si ottiene aggiungendo a T questo insieme infinito di formule. Allora, data una parte finita Fin di T^* esisterà un valore massimo m tra le formule a_n presenti in Fin . E' chiaro che ogni modello di T con un numero di elementi maggiore di m sarà un modello di Fin e quindi Fin è soddisfacibile. Ma poiché soddisfacibile implica consistente possiamo ricavare che Fin è consistente. Ma allora ogni parte finita di T^* è consistente e quindi T^* è consistente. In conclusione T^* ammette un modello che ovviamente sarà infinito.

Proposizione 5.6. Esiste un anello infinito che possiede divisori dello zero.

Dim. Sia T la teoria che si ottiene aggiungendo alla teoria degli anelli l'assioma $\exists x \exists y (x \neq 0 \wedge y \neq 0 \wedge x \cdot y = 0)$. Allora tutti gli interi modulo m con m non primo sono modelli di tale teoria. Pertanto per il teorema ora dimostrato esiste un modello infinito di T .

6. Il sistema di assiomi di Peano per l'aritmetica.

Con il teorema di completezza abbiamo visto che esiste un processo meccanico che permette di produrre tutte e sole le conseguenze logiche di un dato sistema di assiomi. E questo un punto a favore della logica matematica che permette, in un certo senso, una meccanizzazione del processo inferenziale. Tuttavia esistono notevoli limiti alla logica matematica che sono stati posti in rilievo dal logico Kurt Gödel nel 1930. Per esaminare tali limiti riferiamoci ad una teoria molto elementare, la teoria dei numeri interi. Il primo sistema di assiomi per i numeri naturali fu proposto da Dedekind nel 1901 ed è noto sotto la denominazione di

Sistema di postulati di Peano perché proposto anche da Peano qualche anno dopo ed indipendentemente. Si considerano strutture nel cui dominio D è definita una operazione unaria $s : D \rightarrow D$ detta *successore* ed in cui esiste un particolare elemento, detto *zero*, denotato da 0. Si postula che

P_1 $0 \neq s(x)$ (zero non è successore di un numero naturale)

P_2 $s(x) = s(y) \rightarrow x = y$ (numeri che hanno lo stesso successore coincidono)

P_3 per ogni sottoinsieme X , se $0 \in X$ e " $x \in X$ implica $s(x) \in X$ " allora $X = D$.

Questo ultimo assioma è noto come "*principio di induzione*" e spesso viene espresso in termini di "proprietà definite in D " piuttosto che per sottoinsiemi X di D . In tale caso si enuncia dicendo che data una proprietà P definita in D , se

- P vale per 0

e

- dal fatto che P valga per n si può dedurre che P vale anche per $s(n+1)$,

allora è possibile asserire che $P(n)$ vale per tutti i possibili n .

Spesso i modelli del sistema P_1, P_2, P_3 di assiomi vengono anche chiamati "*terne di Peano*".

Possiamo vedere una terna di Peano anche come una struttura algebrica $(S, s, 0)$ con una operazione unaria s e un elemento "designato" 0 tale che siano verificati gli assiomi P_1, P_2 e l'assioma

P_3^* 0 è un generatore della struttura $(S, s, 0)$

Infatti la condizione P_3 significa appunto che se X è una sottostruttura generata da 0 allora coincide con S . Questo modo di interpretare una terna di Peano permette di dimostrare il seguente teorema che, se si accetta la teoria degli insiemi, la teoria delle terne di Peano è soddisfacibile e quindi consistente.

Teorema 6.1. Il sistema P_1, P_2, P_3 di assiomi ammette un modello se e solo se esiste un insieme infinito.

Dim. Per prima cosa ricordiamo che un insieme S è infinito se e solo se è equipotente ad una sua parte propria, cioè se e solo se esiste una funzione iniettiva $f : S \rightarrow S$ che non è suriettiva. Supponiamo ora che la struttura $(D, s, 0)$ sia una terna di Peano, allora da P_2 si ricava che s è una funzione iniettiva, da P_1 che s non è suriettiva. Pertanto D è un insieme infinito.

Viceversa, sia S un insieme infinito, $f : S \rightarrow S$ una funzione iniettiva non suriettiva ed x_0 un elemento di S che non appartiene a $f(S)$. Allora la struttura algebrica (S, f, x_0) , pur verificando P_1 e P_2 , non è detto che sia una terna di Peano cioè che verifichi anche la condizione P_3 . Tuttavia se consideriamo la sottostruttura algebrica $(\langle x_0 \rangle, f, x_0)$ di (S, f, x_0) generata da x_0 l'assioma P_3^* è verificato in modo ovvio. \square

Si noti che poiché abbiamo una tecnica di tipo punto-fisso per trovare la sottostruttura algebrica generata da un dato sottoinsieme, possiamo applicare tale tecnica per definire in modo più diretto una terna di Peano. Definiamo infatti l'operatore algebrico H ponendo

$$H(X) = X \cup f(X).$$

Allora $\langle x_0 \rangle$ il minimo punto fisso di H contenente $\{x_0\}$ e risulterà $N = \bigcup_{n \in \mathbb{N}} H^n(\{x_0\})$. D'altra parte

$$H^1(\{x_0\}) = \{x_0, f(x_0)\}, H^2(\{x_0\}) = \{x_0, f(x_0), f(f(x_0))\}, \dots$$

pertanto N è costituito dagli elementi $x_0, f(x_0), f(f(x_0)), f(f(f(x_0))) \dots$

In ogni terna di Peano è possibile "fare dell'aritmetica" al solito modo. Ad esempio possiamo definire un'operazione di addizione tramite le equazioni

$$x+0 = x \quad ; \quad x+s(y) = s(x+y).$$

ed una operazione di prodotto tramite

$$x \cdot 0 = 0 \quad ; \quad x \cdot s(y) = x \cdot y + x.$$

Teorema 6.2. La teoria (del secondo ordine) delle terne di Peano è categorica, cioè tutte le terne di Peano sono isomorfe tra loro.

Dim. Siano (S, s, z_0) e (S', s', z_0') due terne di Peano, allora possiamo definire per ricorsione la funzione $f: S \rightarrow S'$ ponendo

$$f(z_0) = z_0' \quad ; \quad f(s(x)) = s'(f(x)).$$

Tale funzione, che per il principio di induzione si prova essere ovunque definita, è per definizione un omomorfismo. Non è difficile provare poi che f è un isomorfismo, cioè che è iniettiva e suriettiva.

Volendo formalizzare la nozione di terna di Peano nella logica del primo ordine, dobbiamo considerare un linguaggio \mathcal{L} il cui alfabeto finito A consiste di

- una costante 0 (per denotare lo zero),
- un nome s per denotare il successore
- un nome $+$ per la somma
- un nome \cdot per il prodotto.

Gli assiomi sono i seguenti.

$$A1 \quad 0 \neq s(x)$$

(zero non è successore di un numero naturale)

$$A2 \quad s(x) = s(y) \rightarrow x = y \quad (\text{numeri che hanno lo stesso successore coincidono})$$

Inoltre, per ogni formula α in \mathcal{L}

$$A3 \quad \alpha(0) \wedge \forall x (\alpha(x) \rightarrow \alpha(s(x))) \rightarrow \forall x \alpha(x) \quad (\text{principio di induzione}).$$

Si noti che A3 in realtà è uno "schema di assiomi" e rappresenta infiniti assiomi che si ottengono considerando tutte le possibili formule α . Invece P3 è un unico assioma del secondo ordine. E' importante d'altra parte sottolineare la grande differenza tra il principio di induzione come è espresso da A3 e quello come è espresso da P3. Infatti P3 è ovviamente più potente poiché si riferisce a tutti i possibili sottoinsiemi di N (che sono in quantità maggiore del numerabile) mentre A3 si riferisce solo a quegli insiemi che siano rappresentabili da formule in \mathcal{L} (che sono in quantità numerabile). Ne segue che ogni modello di P1-P3 è un modello di A1-A3 ma, come vedremo, il viceversa non vale.

Proposizione 6.3. Nessuna teoria del primo ordine che ammetta una terna di Peano come modello è categorica. In altre parole la nozione di numero intero non è caratterizzabile al primo ordine. In particolare ogni modello di P1-P3 è un modello di A1-A3 ma il viceversa non vale.

Dim. Si procede in modo simile a quanto fatto per dimostrare che esistono campi ordinati non archimedei. Sia T una teoria del primo ordine che abbia come modello una terna di

Peano, aggiungiamo al linguaggio di T la costante i ed in tale linguaggio consideriamo la teoria T^* che si ottiene aggiungendo a T l'insieme infinito di assiomi del tipo

$$i > 1$$

$$i > 1+1$$

$$i > (1+1)+1$$

...

che indichiamo in breve con $i>1, i>2, i>3, \dots$. Allora ogni parte finita Fin di T^* ammette un modello. Infatti sia m il più grande n tale che $i > n$ sia in Fin e consideriamo un'interpretazione che si ottiene a partire da una terna di Peano interpretando i con un numero maggiore di m . E' subito visto che tale interpretazione è un modello di Fin .

Nel seguito indicheremo con S il sistema di assiomi A1-A3 più gli assiomi per l'identità. Naturalmente se si ammette la costruzione insiemistica presente nella dimostrazione della proposizione 6.1 allora si ottiene un modello di S e ciò prova che S è consistente. Ma il punto di vista di Hilbert è proprio di fare a meno della teoria degli insiemi e, più in generale, della semantica. Infatti Hilbert vuole presentare tutta la matematica come un sistema di manipolazione del materiale linguistico e quindi si pone come fondamentale il problema di provare, con metodi finitistici, la consistenza di S . Un altro problema, ovviamente, è quello della completezza. Ogni asserzione riguardante l'aritmetica può essere sempre provata o confutata nella teoria S ?

7. Il fallimento del programma di Hilbert: i teoremi limitativi di Gödel.

Nel 1930 il matematico Kurt Gödel dimostrò che il programma proposto da Hilbert non poteva essere realizzato nemmeno per una teoria semplice come S è ciò a causa di due teoremi, che rappresentano una tappa fondamentale per la matematica. Tali teoremi pongono in questione proprio i due punti sopra indicati della consistenza e della completezza.

Proposizione 7.1 (Primo teorema di Gödel) Se S è una teoria consistente abbastanza potente da rappresentare i numeri interi allora S è incompleta. In altre parole esiste una formula φ che non può essere confutata o provata.

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 sta 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

$$\gamma \equiv \text{"io sono una formula che non è un teorema di } S\text{"}$$

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

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

se $S \vdash \neg \gamma$ allora γ è un teorema di S

e pertanto né γ né la sua negata $\neg \gamma$ possono essere teoremi di S (e ciò comporta anche che γ è vera).

Per potere formalizzare quanto sopra detto, è necessario che sia possibile il fenomeno dell'autoriferimento, abbiamo cioè bisogno di far vedere come S possa "parlare di se stesso". In particolare, perché quel termine "io" abbia senso deve essere dato un nome all'interno del linguaggio \mathcal{L} di tutte le formule di \mathcal{L} . Inoltre deve essere definita una formula in \mathcal{L} che significhi "essere teorema". Per fare ciò cominciamo con l'osservare che

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

Infatti a zero corrisponde il termine 0, ad uno il termine $s(0)$ e così via. 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 $a_1 \dots a_n$ in tale alfabeto il numero $p_1^{g(a_1)} \dots p_n^{g(a_n)}$ 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 $m = p_1^{h(1)} \dots p_n^{h(n)}$ in prodotto di successivi numeri primi. Se $h(1), \dots, h(n)$ sono codici di lettere a_1, \dots, a_n in A , cioè se $g(a_1) = h(1), \dots, g(a_n) = h(n)$, 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) nella formula p_1 .

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

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

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

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

" $S \vdash \varphi$ se e solo se esiste un termine chiuso t tale che $S \vdash Pr(t, c(\varphi))$ ".

Infine si prova l'esistenza di una formula γ tale che $S \vdash \gamma \leftrightarrow (\neg \exists x Pr(x, c(\gamma)))$. La formula γ asserisce proprio quello che volevamo, cioè che

"io sono una formula che non è un teorema di S ".

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 S . Supponiamo invece che $\neg \gamma$ sia dimostrabile, allora sarà dimostrabile in S 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 S .

Corollario. Esiste una asserzione dell'aritmetica che pur essendo vera non può essere dimostrata; in altre parole S non è abbastanza potente da permettere di provare tutte le

proposizioni vere dell'aritmetica.

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

- **Commento al primo teorema.** Naturalmente si potrebbe pensare di ovviare a tale inconveniente aggiungendo ad S opportuni assiomi. In realtà il teorema continua a valere anche se si considerano sistemi più potenti di S . Per essere più precisi chiamiamo sufficientemente potente una teoria che contenga S , cioè in cui siano dimostrabili gli assiomi di S . Sono teorie sufficientemente potenti sia quelle che si ottengono semplicemente aggiungendo ad S nuovi assiomi, sia quelle, come la geometria euclidea e la teoria degli insiemi, al cui interno sia possibile definire, in un certo senso, l'aritmetica. Inoltre chiamiamo "assiomatizzabile" una teoria il cui sistema di assiomi sia decidibile, cioè esiste un procedimento effettivo per decidere se un assioma appartiene o meno al sistema. Ovviamente ogni teoria con un numero finito di assiomi è assiomatizzabile (ad esempio la teoria dei gruppi). La teoria S è un esempio di teoria assiomatizzabile con infiniti assiomi. Allora è possibile provare la seguente versione "più forte" del primo teorema.

Ogni teoria assiomatizzabile che sia sufficientemente potente non è completa, cioè ammette una proposizione φ indecidibile.

Pertanto nessun tentativo di assiomatizzare l'aritmetica può avere un completo successo e, per quanto ricco sia il sistema di assiomi proposto, esisterà sempre una proposizione dell'aritmetica che non è "catturata" da tale sistema.

Nota. Se si toglie l'ipotesi di decidibilità per i sistemi di assiomi considerati, allora il teorema non è più valido. Infatti, se T è l'insieme delle formule vere nel modello naturale dell'aritmetica, allora T è una teoria sufficientemente potente completa.

Il secondo teorema di Il seguente teorema afferma, in un certo senso, che la consistenza di S non può essere provata all'interno della stessa teoria S .

Teorema 7.2. (Secondo teorema di Gödel). Esiste una formula $Cons_S$ che asserisce la consistenza di S tale che, se S è consistente allora S non può provare $Cons_S$.

Non accenneremo alla dimostrazione del secondo teorema, ci limiteremo solo ad osservare che la formula $Cons_S$ di cui si parla coincide con la formula $\neg\exists xPr(x, \gamma \wedge \neg\gamma)$ che asserisce la non esistenza di una dimostrazione della contraddizione $\gamma \wedge \neg\gamma$. Pertanto anche per il secondo teorema la possibilità di autoriferimento è essenziale.

Commento al secondo teorema. Il secondo teorema di Gödel afferma che per provare la consistenza di S dobbiamo necessariamente utilizzare strumenti più potenti di quelli di S . Poiché sembra ragionevole assumere che ogni metodo di carattere finitista sia riproducibile all'interno di S , ciò significa che non è possibile dimostrare la coerenza dell'aritmetica elementare con metodi finitisti.

Anche in questo caso il teorema vale per ogni teoria sufficientemente potente. Si osservi che, di fatto, già prima delle scoperte di Gödel i matematici avevano rimandato la questione della consistenza di una teoria a quella di un'altra teoria più potente. Infatti il metodo classico con cui si provava e si prova la consistenza di una teoria è quello di costruire un modello di tale

teoria utilizzando materiale (cioè modelli) fornito da altre teorie. Ad esempio

- che il sistema di assiomi della geometria euclidea sia consistente si mostra costruendone un modello a partire dall'insieme delle coppie di numeri reali.
 - che la teoria dei numeri reali (cioè la teoria dei campi completi archimedei) sia consistente si prova costruendone un modello a partire dal campo ordinato dei numeri razionali (ad esempio con il metodo delle sezioni) ed utilizzando alcuni strumenti della teoria degli insiemi
 - il campo dei razionali a sua volta può essere costruito tramite gli interi relativi che a loro volta sono definibili in termini di numeri naturali.
 - i numeri naturali, infine, possono essere costruiti all'interno della teoria degli insiemi. In definitiva la consistenza di ogni teoria matematica si può rimandare alla consistenza della teoria degli insiemi.
- Il secondo teorema confuta la speranza di Hilbert di poter provare la consistenza di teorie "forti" che coinvolgono l'infinito attuale tramite l'uso di metodi finitisti.

8. La teoria degli insiemi ed il paradosso di Skolem

In questo paragrafo descriviamo brevemente la più famosa assiomatizzazione della teoria degli insiemi, quella proposta da E. Zermelo e successivamente perfezionata da A. Fraenkel. Il linguaggio del primo ordine che viene usato contiene

- un simbolo di relazione binaria \in (detta "appartenenza"),
- un simbolo di relazione binaria \subseteq (detta "inclusione")
- una costante \emptyset (per l'insieme vuoto),
- un simbolo di funzione s_1 ($s_1(x)$ denota il singoletto $\{x\}$)
- un simbolo di funzione s_2 ($s_2(x,y)$ denota l'insieme $\{x,y\}$)
- un simbolo di funzione \mathcal{P} ($\mathcal{P}(x)$ denota l'insieme delle parti di x)
- un simbolo di funzione \cup ($\cup(x)$ denota l'unione degli elementi di x)

La teoria è costituita poi dai seguenti assiomi.

Assioma di estensionalità. Afferma che due insiemi x ed y con gli stessi elementi coincidono.
 $\forall z(z \in x \leftrightarrow z \in y) \rightarrow x=y.$

Assioma dell'insieme vuoto. Specifica che \emptyset denota un insieme che non ha elementi.
 $\forall x(\neg(x \in \emptyset)).$

Assioma della coppia non ordinata. Specifica che $s_2(x,y)$ denota l'insieme $\{x,y\}$.
 $\forall z(z \in s_2(x,y) \leftrightarrow (z=x) \vee (z=y)).$

Assioma dell'unione.
 $(y \in \cup(x)) \leftrightarrow \forall z(\exists z(z \in x \wedge y \in z)).$

Assioma dell'inclusione.
 $x \subseteq y \leftrightarrow \forall z(z \in x \rightarrow z \in y).$

Assioma dell'insieme delle parti.
 $z \in \mathcal{P}(x) \leftrightarrow z \subseteq x.$

Schema di assioma di separazione. Sia α una qualunque formula del linguaggio della teoria

degli insiemi, allora l'assioma di separazione (detto anche assioma di isolamento) afferma che, dato un insieme x , α "isola" all'interno di x il sottoinsieme y degli elementi verificanti α (in altri termini data α ed x , $z = \{y \in x \mid \alpha(x)\}$ è un insieme.

$$\forall x \exists y (\forall z (z \in y \leftrightarrow z \in x \wedge \alpha(x))).$$

Assioma dell'infinito. Tale assioma assicura l'esistenza di un insieme infinito.

$$\exists z (\emptyset \in z \wedge \forall x (x \in z \rightarrow s(x) \in z)).$$

Schema di assioma di rimpiazzamento. Afferma che l'immagine di un insieme tramite una funzione è ancora un insieme. Nel seguito $\alpha(x,y)$ è una formula con variabili libere x ed y . La formula consiste in una implicazione il cui antecedente afferma che α definisce una funzione univoca, il conseguente afferma che se x è un qualunque insieme allora esiste un insieme y che è il codominio di x .

$$\forall x \forall y \forall y' (\alpha(x,y) \wedge \alpha(x,y') \rightarrow y = y') \rightarrow \forall x \exists y \forall z (z \in y \leftrightarrow \exists t (t \in x \wedge \alpha(t,z))).$$

Quanto detto per il sistema S per l'aritmetica elementare vale anche per tale teoria. Infatti l'insieme vuoto e la funzione s permettono di costruire una terna di Peano e ciò significa che anche la teoria di Zermelo-Fraenkel è soggetta ai due teoremi di Gödel. Un altro limite di tale teoria (e per qualunque sistema che si proponga per assiomatizzare la teoria degli insiemi) è noto sotto il nome di *Paradosso di Skolem*.

Teorema 8.1. (Paradosso di Skolem). Se la teoria di Zermelo Fraenkel è consistente allora ammette un modello M numerabile.

Dim. Ricordiamo che ogni teoria del primo ordine ammette un modello di Herbrand e che tale modello è finito o numerabile. □

Il paradosso nasce dal fatto che se z è un insieme infinito (la cui esistenza è assicurata dal relativo assioma), allora è un teorema della teoria di Zermelo-Fraenkel la formula che afferma "non esiste una funzione biettiva tra N e $\mathcal{P}(z)$ ". Pertanto è provabile una formula α che afferma l'esistenza di un insieme c non numerabile. Allora pur essendo M un modello numerabile della teoria degli insiemi, esiste in M un insieme non numerabile; cosa questa alquanto strana. In realtà il paradosso è solo apparente poiché la formula α asserisce solo che all'interno del modello M non esiste uno "strumento" f (cioè una funzione) capace di mettere in corrispondenza biettiva i numeri naturali con c . Ciò non toglie che un "osservatore esterno", quello che utilizzando il linguaggio costruisce il modello di Herbrand M , possa essere in possesso di tale strumento. Un esempio si può ricavare se si confronta il punto di vista costruttivista con quello classico. Infatti nella teoria della decidibilità si prova l'esistenza di sottoinsiemi di N che non sono effettivamente enumerabili (pur essendo numerabili). Allora nell'universo del matematico costruttivista in cui esiste solo N , le parti decidibili di N e le funzioni computabili si può provare che esistono insiemi non (effettivamente) numerabili. D'altra parte, ad un osservatore esterno che utilizza la teoria usuale degli insiemi, in tale universo tutto è finito o numerabile.

La situazione è simile a quella presente nel modello di Klein della geometria Euclidea. In tale modello, interamente contenuto in un cerchio del piano euclideo, un uomo situato all'interno del modello non può raggiungere la frontiera con un numero finito di passi. Infatti i suoi passi divengono sempre più piccoli man mano che si avvicina alla frontiera. In tale senso il modello

non è limitato. Ma, ad un osservatore appartenente al mondo euclideo che guardi dall'esterno il modello di Klein il modello appare ovviamente limitato ed un numero finito di passi "euclidei" permette di uscire dal cerchio.

9. La deduzione come ricerca di un punto fisso.

Abbiamo visto quando abbiamo considerato teorie semplici come i programmi, che la nozione di deduzione si può ricondurre a quella di ricerca di un punto fisso di un opportuno operatore di "conseguenza immediata". In questo paragrafo vogliamo osservare che anche nel caso più generale è possibile fare una cosa simile.

Definizione 9.1. Chiamiamo *operatore di conseguenza immediata* l'operatore $C : \mathcal{P}(\mathcal{L}) \rightarrow \mathcal{P}(\mathcal{L})$ definito ponendo, per ogni insieme di formule X ,

$$C(X) = X \cup \{\beta \mid \alpha \rightarrow \beta \in X, \alpha \in X\} \cup \{\forall x(\alpha) \mid \alpha \in X\} \cup Al.$$

In altre parole $C(X)$ è ottenuto aggiungendo ad X :

- le formule in Al ,
- le formule derivate per modus ponens da due formule in X ,
- le formule ricavate per generalizzazione da una formula di X .

$C(X)$ può essere visto come l'insieme delle conseguenze che si possono ricavare da X "in un solo passo". Osserviamo che un insieme di formule è un punto unito dell'operatore C se e solo se è chiuso rispetto le regole di inferenza e contiene Al .

Proposizione 9.2. C è un operatore algebrico. Pertanto, per ogni insieme X di formule, il minimo punto unito di C contenente X è dato da:

$$D(X) = \bigcup_{n \in \mathbb{N}} C^n(X).$$

Proof. E' immediato che $C(X) \supseteq X$ e che C è monotono. Supponiamo che $\beta \in C(X)$, allora:

- se $\beta \in X$, allora $\beta \in C(X_f)$ con $X_f = \{\beta\}$
- se β è ottenuto per *MP* da $\alpha \rightarrow \beta \in X$ e $\alpha \in X$, allora $\beta \in C(X_f)$ con $X_f = \{\alpha, \alpha \rightarrow \beta\}$
- se $\beta = \forall x(\alpha)$ con $\alpha \in X$, allora $\beta \in C(X_f)$ con $X_f = \{\alpha\}$.

In tutti e tre casi X_f è un sottoinsieme finito di X tale che $\beta \in C(X_f)$. Ciò prova che C è algebrico. \square

Definizione 9.3. Chiameremo *operatore di deduzione* l'operatore D che associa ad ogni insieme T di formule il minimo punto unito $D(T)$ di C contenente T .

Si noti che per definizione $D(T)$ è il più piccolo insieme contenente T ed Al che sia chiuso per *MP* e generalizzazione.

Proposizione 9.4. Per ogni insieme di formule X ,

$$X \vdash \alpha \Leftrightarrow \alpha \in D(X).$$

Dim. Proviamo, per induzione su n , che

$$\alpha \in C^n(X) \Rightarrow \text{esiste una dimostrazione } \pi \text{ di } \alpha \text{ con ipotesi in } X.$$

Per $n = 0$ abbiamo che $\alpha \in X$ e quindi possiamo porre π uguale alla successione che si riduce alla formula α assunta come ipotesi. Supponiamo l'implicazione vera per n e che $\alpha \in C^{n+1}(X) = C(C^n(X))$, allora per la definizione di C sono possibili i seguenti casi.

- $\alpha \in C^n(X)$, allora l'esistenza di π è assicurata dall'ipotesi di induzione
- esiste una formula β tale che $\beta \rightarrow \alpha \in C^n(X)$ e $\beta \in C^n(X)$. In tale caso per ipotesi di induzione esiste una dimostrazione π_1 di $\beta \rightarrow \alpha$ ed una dimostrazione π_2 di β con ipotesi in X . Concatenando π_1 con π_2 ed aggiungendo α otteniamo una dimostrazione di α il cui ultimo passo è giustificato dal modus ponens.
- esiste una formula $\beta \in C^n(X)$ tale che $\alpha = \exists x(\beta)$. Per ipotesi di induzione esiste una dimostrazione π di β con ipotesi in X . Aggiungendo a π la formula $\exists x(\beta)$ otteniamo la dimostrazione cercata.
- $\alpha \in AI$. Allora la formula α assunta come assioma logico, è una dimostrazione di α .
In maniera analoga si prova per induzione su n che
esiste una dimostrazione π di α di lunghezza $n \Rightarrow \alpha \in D(X)$. □