Teorie Assiomatiche
I Numeri Naturali

Alberto Zanardo

16 settembre 2005

Indice

0 Avvertenza

In queste dispense verranno presentati risultati generalmente esposti in testi di logica matematica, ma si è cercato di rendere il lavoro comprensibile anche a chi non abbia seguito un corso su tale argomento. Conseguenza inevitabile e prevedibile di questo tentativo è stata la mancanza, in alcuni punti, del rigore formale proprio della logica matematica. Si è volutamente evitata, per esempio, la definizione rigorosa di linguaggio formale, anche se viene considerata la distinzione tra assiomi del primo ordine e assiomi del secondo ordine. Strettamente connesso a questa carenza è anche il fatto che non viene considerata la distinzione tra formula e proposizione - viene generalmente usato il secondo termine - anche se si è cercato di evidenziare la distinzione tra aspetto sintattico e aspetto semantico di una teoria assiomatica.

1 Introduzione

Il *metodo assiomatico* consiste nello sviluppare una teoria scientifica $\mathcal{T}$, che diciamo appunto *teoria assiomatica*, fissando un insieme di proposizioni, gli *assiomi* o *postulati* di $\mathcal{T}$, che poniamo alla base della teoria stessa, e deducendo logicamente da queste altre proposizioni: i *teoremi* di $\mathcal{T}$. Ciò significa in particolare che, per dimostrare una data proposizione in una teoria assiomatica $\mathcal{T}$, possiamo far ricorso esclusivamente a leggi logiche ed agli assiomi di $\mathcal{T}$.[1] Se $\mathcal{T}$ è una teoria fisica, per esempio, le osservazioni sperimentali sono ovviamente di importanza cruciale nella scelta degli assiomi e successivamente nella conferma della teoria stessa, ma, una volta fissati gli assiomi, tali osservazioni non possono avere alcun ruolo nelle dimostrazioni.

Osservazione 1.1 Il significato di espressioni quali 'deducibile logicamente' e 'legge logica' potrebbe essere precisato sulla base di una teoria logica rigorosa, ma non è indispensabile farlo in queste dispense. Le nozioni elementari di logica classica[2] che si trovano all'inizio di molti testi di matematica

[1] Poiché una legge logica banale è che una proposizione segue da sé stessa, tra i teoremi di $\mathcal{T}$ abbiamo in particolare gli assiomi di $\mathcal{T}$.

[2] Potremmo anche considerare una nozione di deduzione logica basata sulla logica intuizionista, e in effetti è possibile sviluppare una matematica intuizionista. Quando si parla di 'matematica' senza ulteriori precisazioni, tuttavia, si intende una matematica basata sulla logica classica.

sono sufficienti per capire le pagine seguenti. Ci sono però due aspetti delle deduzioni logiche che è importante ricordare:

(a) se una proposizione A è logicamente deducibile da un insieme $\mathcal{A}$ di proposizioni, e una struttura matematica $\mathcal{S}$ verifica tutte le proposizioni in $\mathcal{A}$, allora anche A è verificata in $\mathcal{S}$;

(b) una dimostrazione consiste di un numero *finito* di passaggi e quindi, anche se una teoria assiomatica ha infiniti assiomi, ogni dimostrazione in tale teoria coinvolge un numero finito dei suoi assiomi.

Scriveremo $\mathcal{T} \vdash A$ (A è teorema di $\mathcal{T}$) intendendo che la proposizione A è logicamente deducibile nella teoria assiomatica $\mathcal{T}$. Con questa notazione l'asserzione (b) vista sopra implica che, se $\mathcal{T} \vdash A$ allora esiste un teoria $\mathcal{T}'$ con un numero finito di assiomi scelti tra gli assiomi di $\mathcal{T}$, tale che $\mathcal{T}' \vdash A$. L'espressione $\mathcal{T} \nvdash A$ esprime invece il fatto che la formula A non è logicamente deducibile dagli assiomi di $\mathcal{T}$.

Gli *Elementi di Euclide* sono l'esempio più antico di teoria assiomatica, e la lunga storia del quinto postulato mostra quanto i matematici che si sono occupati della sua indipendenza fossero consapevoli della natura assiomatica degli Elementi, anche se tale nozione non era stata ancora precisata rigorosamente. Nella matematica moderna, dopo un allontanamento dalla tradizione euclidea nei secoli XVII e XVIII, il metodo assiomatico è penetrato in ogni campo con influenza sempre crescente. Attualmente possiamo dire che praticamente tutte le branche della matematica sono sviluppate secondo questo metodo.

Consideriamo come primo esempio la teoria dei gruppi. Un gruppo può essere definito come una terna $\langle G, *, u\rangle$ in cui G è un insieme non vuoto, $*$ è un'operazione binaria su G, e u è un elemento di G (l'*elemento neutro*), tali che:

(G1) $\forall xyz,\ x * (y * z) = (x * y) * z$

(G2) $\forall x,\ x * u = u * x = x$

(G3) $\forall x, \exists x' :\ x * x' = x' * x = u$

dove si intende che i quantificatori $\forall x$ e $\exists x$ varino sull'insieme G. In generale, quando formule sono riferite ad una certa struttura basata su un dato insieme, si intende sempre che i quantificatori agiscano su quell'insieme.

Le formule sono G1-G3 sono gli assiomi della teoria dei gruppi; possiamo quindi dire che i teoremi di questa teoria sono le proposizioni logicamente deducibili da G1-G3.

Questa caratterizzazione della teoria dei gruppi è senz'altro corretta ed è effettivamente quella che si trova nei testi di algebra. Poiché l'argomento principale di queste dispense sono le teorie assiomatiche, tuttavia, è opportuno essere più precisi. Bisogna osservare che la definizione di gruppo coinvolge la nozione di insieme (e la nozione di operazione, che comunque è riconducibile a quella di insieme). Affinché la teoria dei gruppi abbia effettivamente carattere assiomatico, bisogna quindi che anche l'uso della nozione di insieme in tale teoria sia regolato da assiomi, gli assiomi appunto della *Teoria degli Insiemi*. Dire che una data proposizione A è un teorema della teoria dei gruppi vuol dire dunque che A è logicamente deducibile da G1-G3 e dagli assiomi della (o meglio, di una) teoria degli insiemi.

Per essere più precisi, quindi, potremmo parlare degli *assiomi propri* di una teoria assiomatica come quelli che la caratterizzano e non sono comuni, come gli assiomi per gli insiemi, a tutte le teorie. Nel caso dei gruppi, gli assiomi propri sono G1-G3. Nel seguito, continueremo comunque a chiamare semplicemente assiomi anche gli assiomi propri, usando l'aggettivo quando sarà importante distinguerli dagli altri.

La teoria degli insiemi sta alla base di quasi tutta la matematica moderna. Nella pratica matematica usuale, tuttavia, il riferimento esplicito agli assiomi della teoria degli insiemi viene spesso omesso, non per mancanza di rigore formale, ma semplicemente perché i concetti insiemistici coinvolti nelle dimostrazione sono molto semplici e, in tale ambito, la nozione intuitiva di insieme non è meno affidabile di quella rigorosa basata su un ben precisato insieme di assiomi. Da un punto di vista didattico, sarebbe molto discutibile presentare e discutere tutti gli assiomi di una teoria degli insiemi per poi usare solo le nozioni di unione, intersezione e funzione. Va comunque tenuto presente che, qualora se ne manifestasse la necessità, le nozioni insiemistiche che usiamo intuitivamente possono sempre essere precisate internamente ad una teoria assiomatica.

Nello studio delle teorie assiomatiche possiamo distinguere due aspetti principali. Il primo riguarda ovviamente la deduzione di teoremi: data una teoria $\mathcal{T}$, siamo interessati alle conseguenze logiche dei suoi assiomi. Un secondo aspetto, non meno importante, riguarda la ricerca dei *modelli* di $\mathcal{T}$, cioè delle strutture matematiche in cui gli assiomi di $\mathcal{T}$ sono verificati. Come

conseguenza del punto (a) dell'Osservazione 1.1 abbiamo che tutti i teoremi di $\mathcal{T}$ sono verificati in ogni suo modello. Tornando all'esempio della teoria dei gruppi, la dimostrazione che l'elemento neutro è unico riguarda il primo tipo di indagine: dall'assunzione che u e u' siano entrambi elementi neutri, e che quindi l'assioma G2 valga anche per u', usando appunto questo assioma arriviamo facilmente alla conclusione $u = u'$. La verifica che la struttura $\langle \mathbb{Z}, +, 0 \rangle$ è un gruppo riguarda invece il secondo tipo di indagine. Dire che $\langle \mathbb{Z}, +, 0 \rangle$ è un gruppo equivale a dire che questa struttura è un modello della teoria dei gruppi, cioè che gli assiomi G1-3 sono verificati interpretando G, $*$ e u rispettivamente come l'insieme dei numeri interi, l'operazione di somma e lo zero.

La dimostrazione dei teoremi di una teoria assiomatica partendo dagli assiomi e sulla base di regole logiche ben precisate, può essere vista, in ultima analisi, come una manipolazione di simboli, indipendente dal loro significato. Per questo motivo, il primo aspetto dell'indagine sulle teorie assiomatiche viene spesso chiamato aspetto *sintattico*. Quando invece ci occupiamo dei modelli di una data teoria, diamo un significato ai simboli che compaiono negli assiomi. Il secondo aspetto dell'indagine sulle teorie assiomatiche viene quindi spesso chiamato aspetto *semantico*.

Nella pratica matematica usuale, questi due aspetti sono spesso considerati contemporaneamente senza sottolinearne la distinzione. Non c'è niente di male in questo modo di procedere, nel caso in cui si vogliano presentare particolari teorie assiomatiche, come quella dei gruppi. Dal punto di vista di uno studio generale di tali teorie, tuttavia, diventa importante (a volte essenziale) distinguere i due aspetti e stabilirne le connessioni.[3] Un primo legame banale tra sintassi e semantica è che, come osservato sopra, in ogni modello di una teoria assiomatica sono verificati tutti i teoremi di quella teoria. Molto meno banale e ricco di interessanti conseguenze è invece il problema opposto: se una proposizione è vera in ogni modello di una teoria, è vero che tale proposizione è dimostrabile?

[3] A rigore, la distinzione tra aspetto sintattico e aspetto semantico dovrebbe trasparire anche a livello terminologico. In logica matematica, si parla di *formule* per indicare sequenze di simboli non ancora interpretati, e quindi a livello sintattico, mentre si parla di *proposizioni* per indicare formule interpretate, e quindi a livello semantico. L'assioma G1 della teoria dei gruppi è una formula, mentre l'asserzione (comunque formulata) che l'operazione di somma tra interi è associativa è la proposizione corrispondente all'interpretazione di G1 in $\langle \mathbb{Z}, +, 0 \rangle$.

2 Coerenza. Decidibilità degli assiomi

Un requisito minimo che una teoria assiomatica $\mathcal{T}$ deve soddisfare perché abbia senso studiarla, è quello della *coerenza* o *non contradditorietà*. Vogliamo cioè che la teoria non permetta di dedurre una proposizione e al tempo stesso la sua negazione. Usando la notazione introdotta nel paragrafo precedente, diciamo che una teoria $\mathcal{T}$ è coerente se non esiste nessuna formula A tale che $\mathcal{T} \vdash A$ e $\mathcal{T} \vdash \neg A$. Poiché inoltre una teoria dimostra due formule A e B se e solo se ne dimostra la congiunzione $A \wedge B$, possiamo dire che $\mathcal{T}$ è coerente se e solo se, per nessuna formula A si ha $\mathcal{T} \vdash A \wedge \neg A$. Le formule del tipo $A \wedge \neg A$ vengono chiamate *contraddizioni* (e sono equivalenti a negazioni di *tautologie*). Possiamo dunque dire che una teoria è coerente se non dimostra contraddizioni.

Il motivo per cui si richiede che una teoria sia coerente è ovvio: se $\mathcal{T}$ dimostra una proposizione e la sua negazione, allora non esiste nessuna struttura matematica della quale $\mathcal{T}$ descrive le proprietà. Ogni accettabile definizione di verità (di una formula in una struttura), infatti, non può consentire che siano contemporaneamente verificate in una struttura due proposizioni che si contraddicono. Oltre a questo, abbiamo che una teoria non coerente dimostra ogni proposizione,[4] per cui possiamo dire che $\mathcal{T}$ è coerente se esiste una proposizione A tale che $\mathcal{T} \nvdash A$. Chiaramente non c'è alcun interesse nello studiare teorie in cui tutto è dimostrabile.

Un esempio di teoria incoerente è la teoria $\mathcal{T}$ ottenuta aggiungendo agli assiomi per i numeri reali, cioè alla teoria $\mathcal{T}_{\mathbb{R}}$ dei campi ordinati completi, la proposizione $\forall x, \exists y(y^2 = x)$ (ogni elemento è un quadrato). Poiché dagli assiomi per i reali segue che l'equazione $y^2 = x$ (nell'incognita y) non ha soluzioni se x è negativo, abbiamo che $\mathcal{T}$ non è coerente. Ovviamente, ciò non significa che la proposizione $\forall x, \exists y(y^2 = x)$ sia in sé stessa contraddittoria; i numeri complessi, per esempio, verificano tale proposizione (ma, a differenza dei reali, non sono ordinabili).

Nel seguito converrà spesso identificare una teoria con l'insieme dei suoi assiomi. Scriveremo quindi $\{A_0, \ldots, A_n\} \vdash A$ intendendo che A è teorema della teoria assiomatica avente $A_0, \ldots, A_n$ come assiomi. Un insieme $\{A_0, \ldots, A_n\}$ di proposizioni sarà dunque coerente se è tale la teoria assioma-

[4] Date due formule A e B, l'implicazione $A \wedge \neg A \to B$ (avendo l'antecedente sempre falso) è una verità della logica classica (una tautologia) ed è dimostrabile in ogni teoria assiomatica. Se una teoria $\mathcal{T}$ quindi dimostra la contraddizione $A \wedge \neg A$, allora, per *Modus Ponens*, $\mathcal{T}$ dimostra anche B per ogni formula B.

tica che ha quelle proposizioni come assiomi, ossia se esiste una formula A tale che $\{A_0, \ldots, A_n\} \nvdash A$

Teorema 2.1 (T. di Compattezza Sintattica). *Un insieme di proposizioni è coerente se e solo se ogni suo sottoinsieme finito è coerente.*

Dim. Per (b) nell'Osservazione 1.1, ogni dimostrazione in una teoria assiomatica coinvolge un numero finito di assiomi e quindi, se possiamo dedurre $A \wedge \neg A$ da un dato insieme di proposizioni, possiamo dedurre la stessa contraddizione anche da un suo sottoinsieme finito. ∎

Si osservi che, asserendo che una data teoria $\mathcal{T}$ è coerente, implicitamente consideriamo tutte le (infinite) possibili deduzioni logiche basate sugli assiomi di $\mathcal{T}$, e asseriamo che nessuna di queste deduzioni si conclude con una contraddizione. Considerare tutte le possibili deduzioni in una data teoria è nella maggioranza dei casi molto difficile, ma, fortunatamente, per dimostrare che una teoria assiomatica è coerente possiamo usare anche altre tecniche. La più usata è mostrare che la teoria in esame ha un modello. Abbiamo già osservato infatti che (1) se gli assiomi di una teoria $\mathcal{T}$ sono verificati in una struttura, allora in tale struttura sono verificati anche tutti i teoremi di $\mathcal{T}$, e (2) in una struttura non possono essere contemporaneamente vere una proposizione e la sua negazione. Da questo segue che se gli assiomi di una teoria sono verificati in una struttura, allora tale teoria non può dimostrare una contraddizione, cioè è coerente.

Il fatto che gli assiomi G1-G3 siano verificati in $\langle \mathbb{Z}, +, 0 \rangle$ dimostra che la teoria dei gruppi è coerente. Si può raggiungere lo stesso risultato anche considerando modelli molto più semplici. Consideriamo infatti la struttura $\langle \{a\}, \cdot, a \rangle$ in cui a è un arbitrario oggetto (per esempio, l'insieme vuoto) e $\cdot$ è l'operazione su $\{a\}$ definita da $a \cdot a = a$. È immediato verificare che in questa struttura molto semplice gli assiomi G1-G3 sono veri e ciò implica la coerenza della teoria dei gruppi.

La ricerca di un modello non è comunque l'unico modo per ricavare risultati di coerenza. Possiamo per esempio cercare di dimostrare che se la teoria in considerazione non fosse coerente allora non lo sarebbe neanche un'altra della quale abbiamo precedentemente dimostrato la coerenza. In alcuni casi possono anche esserci dimostrazioni dirette, in cui di fatto si considerano tutte le possibili dimostrazioni: con metodi puramente sintattici si mostra che le trasformazioni di simboli che costituiscono le dimostrazioni della data

teoria non permettono di dedurre contraddizioni. È importante osservare che dimostrazioni di questo tipo richiedono una definizione rigorosa di deduzione.

Osservazione 2.2 Per il Teorema di Compattezza Sintattica, per dimostrare che una teoria assiomatica $\mathcal{T}$ con infiniti assiomi è coerente è sufficiente dimostrare che ogni insieme finito dei suoi assiomi è coerente. Può succedere in particolare che vengano esibiti vari modelli per i vari insiemi finiti di assiomi, ma che ciascuno di questi modelli non sia modello di tutta la teoria. Nei paragrafi 3.4 e 5 vedremo due esempi di questa situazione.

Osservazione 2.3 Abbiamo visto che per dimostrare la coerenza di una teoria possiamo dimostrare che esiste una struttura insiemistica in cui gli assiomi di tale teoria sono verificati. La dimostrazione rigorosa dell'esistenza di tale struttura deve ovviamente avvenire internamente alla teoria assiomatica degli insiemi e quindi sorge inevitabilmente il problema della coerenza di questa teoria. Questo è un problema molto delicato e per esporre quanto è attualmente noto al riguardo sarebbero necessarie nozioni e risultati molto sofisticati di logica matematica e teoria degli insiemi. Ci limitiamo a ricordare il risultato principale, cioè che non è possibile dare una dimostrazione della coerenza di questa teoria internamente alla teoria stessa. Per il *Teorema di Incompletezza di Gödel*, infatti, se la teoria degli insiemi fosse in grado di dimostrare la propria coerenza (per esempio dimostrando l'esistenza di un suo modello), allora sarebbe contraddittoria! Se poi teniamo presente che la teoria degli insiemi viene posta alla base della matematica, il Teorema di Incompletezza di Gödel implica che la coerenza della teoria degli insiemi non è dimostrabile.

Nella pratica matematica, la non contradditorietà della teoria degli insiemi viene presupposta, basandosi essenzialmente sull'evidenza intuitiva dei suoi assiomi, anche se non possiamo escludere che prima o dopo qualcuno trovi una contraddizione.

Le teorie assiomatiche che incontriamo in matematica sono generalmente presentate elencandone gli assiomi, se questi sono in numero finito, oppure elencando degli 'schemi d'assiomi', cioè dicendo che tutte le proposizioni aventi una data struttura sono assiomi della teoria. Ci sono molti modi tuttavia per definire un insieme (di proposizioni, nel nostro caso) e non tutti gli insiemi possono essere descritti elencandone in qualche modo gli elementi.

Diventa quindi sensato chiederci se un qualsiasi insieme coerente di proposizioni, comunque definito, possa essere visto come l'insieme degli assiomi di una teoria assiomatica. Ci possiamo chiedere, per esempio, se possiamo considerare la teoria assiomatica $\mathcal{T}_{\mathbf{N}}$ i cui assiomi sono *tutte le formule scritte con i simboli* $0,\ 1,\ +,\ \times,\ =$ *(oltre ai simboli logici) vere nella struttura dei numeri naturali*[5]. La risposta è no. C'è un altro requisito infatti, meno ovvio e meno noto della coerenza, che le teorie assiomatiche devono soddisfare: quello della *decidibilità degli assiomi*. Ciò significa che dobbiamo essere in grado di decidere per mezzo di una procedura effettiva se una data proposizione sia un assioma oppure no[6]. Il senso di questo requisito è che una teoria assiomatica non deve lasciare alcun dubbio sul fatto che una data successione di passaggi sia una dimostrazione e, affinché questo succeda, deve essere ben determinato l'insieme degli assiomi che possono essere usati nelle dimostrazioni.

Come abbiamo osservato, per molte teorie assiomatiche la procedura effettiva per stabilire se una data proposizione è un assioma si riduce al verificare se quella proposizione compare in un dato elenco, oppure se ha una data struttura. La teoria $\mathcal{T}_{\mathbf{N}}$ vista sopra, invece, potrebbe essere considerata una teoria assiomatica solo se esistesse una procedura effettiva che permetta di verificare se una arbitraria formula scritta con i simboli $0,\ 1,\ +,\ \times,\ =$ sia vera nella struttura dei numeri naturali. Il teorema di Incompletezza di Gödel ci dice che una tale procedura non esiste.

3 Proprietà delle teorie assiomatiche

Prima di considerare alcune caratteristiche delle teorie assiomatiche che sono generalmente oggetto di indagine, conviene accennare, come ulteriore esempio, alla presentazione assiomatica dei numeri reali. In tale presentazione i numeri reali vengono visti come una struttura $\langle R, +, \cdot, 0, 1, \leq\rangle$ in cui R è un insieme, $+$ e $\cdot$ sono operazioni su R, 0 e 1 sono elementi di R e $\leq$ è una relazione su R, che verificano gli assiomi dei *campi ordinati completi*,

[5]Si osservi che queste formule, essendo verificate in una data struttura matematica, costituiscono un insieme coerente.

[6]Si potrebbe dare una definizione rigorosa di decidibilità e di procedura effettiva, ma, ancora una volta, non è il caso di farlo. Possiamo dire che una procedura effettiva è un insieme di operazioni e di verifiche eseguibili (in linea di principio) da un calcolatore opportunamente programmato.

o assiomi dei reali, che possiamo trovare in molti testi di analisi (o nella dispensa *Sistemi Numerici*)[7]. Indicheremo con $\mathcal{T}_{\mathbb{R}}$ la corrispondente teoria assiomatica. Tra gli assiomi di $\mathcal{T}_{\mathbb{R}}$ ricordiamo l'*Assioma di Completezza*, che verrà discusso più avanti:

$$\begin{aligned}\forall XY\,[X \neq \emptyset \wedge Y \neq \emptyset \wedge \forall x \in X, \forall y \in Y\,(x \leq y) \rightarrow \\ \rightarrow \exists z\,(\forall x \in X, \forall y \in Y\,(x \leq z \leq y))]\end{aligned} \tag{3.1}$$

dove X e Y indicano variabili per insiemi e quindi $\forall X$ è una quantificazione sull'insieme $\mathbf{P}(R)$ di tutti i sottoinsiemi di R.[8]

La costruzione di un modello per i reali, e quindi la dimostrazione della non contraddittorietà di $\mathcal{T}_{\mathbb{R}}$, può essere quella considerata nella nota *Dai numeri naturali ai numeri reali* (e che pure troviamo in molti testi analisi): partendo dai naturali (che possiamo costruire internamente alla teoria degli insiemi), costruiamo gli interi e poi i razionali, e quindi mostriamo che le *classi di equivalenza di successioni di Cauchy* (o i *tagli di Dedekind*) sui razionali, con le operazioni di somma e prodotto e la relazione d'ordine opportunamente definite, verificano gli assiomi dei campi ordinati completi.

3.1 Categoricità

Definizione 3.1 *Siano* $\mathbf{X} = \langle X, f_1 \ldots, f_N, R_1, \ldots, R_M, c_1, \ldots, c_K\rangle$ *e* $\mathbf{X}' = \langle X',\ f'_1 \ldots, f'_N, R'_1, \ldots, R'_M, c'_1, \ldots, c'_K\rangle$ *strutture in cui le* f_i *e* f'_i *sono funzioni, le* R_i *e* R'_i *sono relazioni, e le* c_i *e* c'_i *sono costanti. Si supponga inoltre che le* f_i *e* R_i *abbiano arietà uguali alle corrispondenti* f'_i *e* R'_i.

La funzione φ *da* X *su* X' *è un* isomorfismo *da* $\mathbf{X}$ *su* $\mathbf{X}'$ *se è una funzione biunivoca tale che* (1) $\varphi(c_i) = c'_i$, (2) $\varphi(f_i(x_1, \ldots, x_{n_i})) = f'_i(\varphi(x_1), \ldots, \varphi(x_{n_i}))$, *e* (3) $R_i(x_1, \ldots, x_{m_i})$ *se e solo se* $R'_i(\varphi(x_1), \ldots, \varphi(x_{m_i}))$, *dove* n_i *e* m_i *indicano rispettivamente l'arietà di* f_i *e* R_i.

Diciamo che le strutture $\mathbf{X}$ *e* $\mathbf{X}'$ *sono* isomorfe *se esiste un isomorfismo da* $\mathbf{X}$ *su* $\mathbf{X}'$.

---

[7] Per evitare inutili e noiose precisazioni, usiamo qui i simboli $+, \cdot, \ldots$ che corrispondono alla effettiva interpretazione degli assiomi nel campo dei reali. Volendo procedere come abbiamo fatto per i gruppi, avremmo dovuto parlare di una struttura $\langle X, *_1, *_2, u_1, u_2, \rho\rangle$ in cui X è un insieme, $*_1$ e $*_2$ sono operazioni binarie su X, u_1 e u_2 sono elementi di X e ρ è una relazione binaria su X.

[8] La versione (equivalente a (3.1)) dell'Assioma di Completezza presentata in molti testi di analisi è che *ogni insieme superiormente limitato ha estremo superiore.*

Gli isomorfismi sono quindi le funzioni biunivoche che *conservano le costanti, le operazioni e le relazioni.*

Osservazione 3.2 Il fatto che una data funzione sia o meno un isomorfismo dipende in generale dalle particolari relazioni e funzioni che vengono considerate nelle strutture. Per esempio, la funzione $\varphi : n \mapsto 2n$ è un isomorfismo dalla struttura $\langle N, \leq \rangle$ dei numeri naturali con la relazione d'ordine nella struttura $\langle 2N, \leq \rangle$ dei naturali pari, pure con la relazione d'ordine. La funzione φ è infatti biiettiva e inoltre vale $n \leq m$ se e solo se vale $2n \leq 2m$, cioè $\varphi(n) \leq \varphi(m)$. Oltre alla relazione d'ordine possiamo anche considerare l'operazione (cioè la funzione binaria) di somma, ottenendo così le strutture $\langle N, \leq, + \rangle$ e $\langle 2N, \leq, + \rangle$. Anche in questo caso la funzione φ è un isomorfismo; infatti, $\varphi(n+m) = 2(n+m) = 2n+2m = \varphi(n)+\varphi(m)$. Se consideriamo anche il prodotto, abbiamo invece che φ non è più un isomorfismo; l'uguaglianza $2(n \cdot m) = 2n \cdot 2m$ ha infatti controesempi nell'insieme dei naturali. Questo risultato tuttavia non è sufficiente per dire che le strutture $\langle N, \leq, +, \cdot \rangle$ e $\langle 2N, \leq, +, \cdot \rangle$ non sono isomorfe: non possiamo a priori escludere che esistano isomorfismi diversi dalla funzione φ. Non è difficile dimostrare però che tale φ è l'unico isomorfismo da $\langle N, \leq, + \rangle$ su $\langle 2N, \leq, + \rangle$ e quindi le due strutture con il prodotto sono di fatto non isomorfe.

Definizione 3.3 *Una teoria assiomatica è* categorica *se tutti i suoi modelli sono isomorfi (cioè se ha un solo modello, a meno di isomorfismi).*

La categoricità è molto importante quando, come nel caso dei numeri reali, una teoria assiomatica ha lo scopo di precisare formalmente proprietà di una particolare struttura, come la retta reale, della quale abbiamo un'intuizione abbastanza precisa. In questo caso possiamo dire che gli assiomi *catturano* tutte le proprietà essenziali di quella struttura, nel senso che non esistono strutture diverse (non isomorfe) in cui tali assiomi sono verificati. Come viene dimostrato in molti testi di analisi, la teoria assiomatica dei numeri reali è categorica. Inversamente, non è difficile rendersi conto che la teoria dei gruppi non è categorica. La struttura $\langle \mathbb{Z}, +, 0 \rangle$ e la struttura $\langle \{a\}, \cdot, a \rangle$ considerata a pagina 7 sono entrambe modelli della teoria dei gruppi, ma ovviamente non sono isomorfe[9].

[9]La teoria dei gruppi e la teoria dei numeri reali sono in effetti esempi di due atteggiamenti contrapposti (o meglio, complementari) che possiamo intravedere nell'attività matematica. Per i numeri reali abbiamo già osservato che la ricerca degli assiomi cor-

Si potrebbe pensare che questa differenza tra teoria dei gruppi e teoria dei reali sia dovuta semplicemente al fatto che la prima ha meno assiomi della seconda. È effettivamente vero che aumentando gli assiomi in generale diminuiscono i modelli di una teoria perché tali modelli devono verificare più proposizioni, ma la differenza tra le due teorie è molto più sostanziale: la prima è una *teoria del primo ordine* mentre la seconda è una *teoria del secondo ordine*. La teoria dei gruppi è del primo ordine perché, nei suoi assiomi propri G1-G3, i quantificatori $\forall$ e $\exists$ agiscono su *elementi* (dell'insieme G). Anche la teoria dei campi ordinati è del primo ordine, mentre la teoria dei reali (campi ordinati completi) è del secondo ordine perché nell'Assioma di Completezza (3.1) compaiono quantificatori ($\forall XY$) che agiscono su *insiemi*. Le teorie del primo ordine sono quindi quelle in cui, negli assiomi propri, nessun quantificatore agisce su insiemi.

Le teorie del primo ordine hanno proprietà molto interessanti che verranno descritte nel seguito. D'altra parte, la possibilità di quantificare su insiemi dà alle teorie del secondo ordine una notevole capacità espressiva, nel senso che riescono a descrivere meglio i loro modelli. Come conseguenza del prossimo teorema, per esempio, l'unicità del modello degli assiomi dei reali viene a cadere se sostituiamo l'Assioma di Completezza con un qualsiasi insieme, anche infinito, di proposizioni del primo ordine.

Teorema 3.4 (T. di Löwenheim-Skolem). *Se un insieme di proposizioni del primo ordine ha un modello infinito, allora tale insieme ha modelli di qualsiasi cardinalità infinita.*

Questo teorema risolve, negativamente, il problema della categoricità di molte teorie: nessuna teoria del primo ordine con un modello infinito può essere categorica. Ciò segue dal fatto che due modelli di cardinalità diversa non possono essere isomorfi.

Il seguente corollario usa il Teorema di Löwenheim-Skolem per stabilire la non eliminabilità della quantificazione al secondo ordine nella teoria dei numeri reali. Anche senza sollevare pur legittime questioni di predicatività, non c'è dubbio che la quantificazione su insiemi sia più problematica, o

risponde all'esigenza di precisare il più possibile le proprietà di una data struttura, fino a caratterizzarla completamente. Per quanto riguarda la teoria dei gruppi, invece, l'idea sottostante è quella di *isolare* particolari caratteristiche comuni a diverse strutture, quali la presenza di un'operazione associativa e di un elemento neutro, in modo di individuare le proprietà di quelle strutture che dipendono da quelle caratteristiche.

almeno più complicata, della quantificazione su individui. Diventa quindi sensato vedere se il primo tipo di quantificazione non sia eliminabile, cioè sostituibile con quantificazioni del secondo tipo. Per quanto riguarda l'Assioma di Completezza nella teoria dei Campi Ordinati Completi, la risposta è negativa.

Corollario 3.5 *Nella teoria dei Campi Ordinati Completi, l'Assioma di Completezza non può essere sostituito da nessun insieme di proposizioni del primo ordine.*

Dim. Indichiamo con $\mathcal{T}'_{\mathbb{R}}$ la teoria ottenuta sostituendo l'Assioma di Completezza in $\mathcal{T}_{\mathbb{R}}$ con un insieme $\mathcal{A}$ di proposizioni del primo ordine. Vogliamo dimostrare che nessun insieme $\mathcal{A}$ rende $\mathcal{T}_{\mathbb{R}}$ e $\mathcal{T}'_{\mathbb{R}}$ equivalenti. Assumiamo per assurdo che, per un dato $\mathcal{A}$, $\mathcal{T}_{\mathbb{R}}$ e $\mathcal{T}'_{\mathbb{R}}$ siano equivalenti; da ciò segue in particolare che ogni modello di $\mathcal{T}_{\mathbb{R}}$ è anche modello di $\mathcal{T}'_{\mathbb{R}}$, e viceversa.

L'Assioma di Completezza è l'unica proposizione del secondo ordine negli assiomi dei reali e quindi $\mathcal{T}'_{\mathbb{R}}$ è una teoria del primo ordine che ha un modello infinito essendo equivalente a $\mathcal{T}_{\mathbb{R}}$. Per il Teorema di Löwenheim-Skolem, $\mathcal{T}'_{\mathbb{R}}$ ha modelli di cardinalità arbitraria, ma ciò è assurdo perchè $\mathcal{T}_{\mathbb{R}}$ ha solo modelli di cardinalità $2^{\aleph_0}$. ∎

Un altro corollario del Teorema di Löwenheim-Skolem è che condizione necessaria affinché una teoria del primo ordine $\mathcal{T}$ sia categorica è che essa abbia solo modelli finiti. Per tutte le teorie del primo ordine con modelli infiniti il Teorema di Löwenheim-Skolem dà una risposta negativa al problema della categoricità. Per queste teorie, diventa invece interessante chiedersi, per esempio, se tutti i modelli numerabili siano isomorfi, oppure se siano isomorfi tutti i modelli con la cardinalità del continuo. In questo caso il Teorema di Löwenheim-Skolem non chiude la questione. In generale, dato un numero cardinale α, diciamo che una teoria è α-categorica se tutti i suoi modelli di cardinalità α sono isomorfi, per cui i problemi di categoricità effettivamente interessanti (ed effettivamente studiati) per teorie del primo ordine sono problemi di α-categoricità.

Esempi di teorie α-categoriche sono la teoria dei gruppi, che è p-categorica per ogni numero primo p. Tale teoria invece non è $\aleph_0$-categorica. Per dimostrarlo consideriamo i gruppi $\langle \mathbb{Z}, +, 0\rangle$ e $\langle \mathbb{Q}^+, \cdot, 1\rangle$, dove $\mathbb{Q}^+$ è l'insieme dei razionali positivi. Entrambe queste strutture sono numerabili, ma non sono isomorfe. Supponiamo infatti per assurdo che f sia un isomorfismo tra le due

strutture e che $f(1)$ sia il razionale positivo a. In quanto isomorfismo la funzione f deve verificare l'uguaglianza $f(n+m) = f(n) \cdot f(m)$ da cui segue che, per k positivo, $f(k) = f(\underbrace{1+1+\ \ldots\ +1}_{k}) = \underbrace{f(1)\cdot\ \ldots\ \cdot f(1)}_{k} = a^k$. Poiché f deve essere iniettiva, abbiamo in particolare $a \neq 1$. Dalle uguaglianze $1 = f(0) = f(m-m) = f(m) \cdot f(-m)$ segue che $f(-m) = \dfrac{1}{f(m)}$, per cui abbiamo $f(k) = a^k$ anche per $k \leq 0$. La funzione f è quindi strettamente crescente o strettamente decrescente a seconda che a sia maggiore o minore di 1; dunque, per ogni k, nessun razionale strettamente compreso tra a^k e a^{k+1} appartiene all'immagine di f. Ciò significa in particolare che f non è suriettiva e quindi non è un isomorfismo.

3.2 Un esempio di teoria del I ordine $\aleph_0$-categorica

Consideriamo la teoria assiomatica, relativa a strutture $\langle L, \leq \rangle$ in cui $\leq$ è una relazione binaria su L, avente come assiomi:

O1	$\forall x(x \leq x)$	(riflessività)
O2	$\forall x, y, z(x \leq y \wedge y \leq z \rightarrow x \leq z)$	(transitività)
O3	$\forall x, y(x \leq y \wedge y \leq x \rightarrow x = y)$	(antisimmetria)
O4	$\forall x, y(x \leq y \vee y \leq x)$	(linearità o totalità)
O5	$\forall x, y[x < y \rightarrow \exists z(x < z < y)]$	(densità)
O6	$\forall x \exists y(x < y)$	(assenza di massimo)
O7	$\forall x \exists y(y < x)$	(assenza di minimo)

dove $x < y$ è un'abbreviazione di $x \leq y \wedge x \neq y$.

Gli assiomi O1-3 sono gli assiomi degli *insiemi ordinati*. Aggiungendo O4, otteniamo gli assiomi per gli *ordini lineari* (o *totali*). Quasi tutte le strutture numeriche che siamo abituati ad usare sono ordini lineari: i naturali, gli interi, i razionali, i reali.

I rimanenti assiomi O5-7 descrivono ulteriori proprietà degli ordini lineari che siamo abituati a considerare. I numeri razionali e i numeri reali sono esempi di ordini lineari densi senza massimo e senza minimo. I numeri interi non hanno massimo né minimo, ma non sono densi. I numeri naturali infine non sono densi e hanno minimo.

Indichiamo con $\mathcal{T}_{OLDN}$ (teoria degli Ordini Lineari, Densi, Non limitati) la teoria avente O1-7 come assiomi. Tale teoria non può essere categorica.

Possiamo infatti osservare che i reali e i razionali sono modelli di $\mathcal{T}_{OLDN}$, ma non possono essere isomorfi perché hanno cardinalità diversa. Avremmo anche potuto considerare uno solo di questi insiemi, che sono infiniti, ed usare il Teorema di Löwenheim-Skolem osservando che gli assiomi O1-7 sono proposizioni del primo ordine.

La teoria $\mathcal{T}_{OLDN}$ è però $\aleph_0$-categorica. Vale cioè il seguente teorema.

Teorema 3.6 *Se le strutture $\langle L, \leq\rangle$ e $\langle L', \leq'\rangle$ sono modelli numerabili di $\mathcal{T}_{OLDN}$, allora $\langle L, \leq\rangle$ e $\langle L', \leq'\rangle$ sono isomorfe.*

La dimostrazione di questo teorema, che verrà brevemente abbozzata, è un esempio della tecnica del *back-and-forth*, nel senso che definiamo un isomorfismo f da $\langle L, \leq\rangle$ su tutto $\langle L', \leq'\rangle$ andando *avanti e indietro* tra le due strutture.

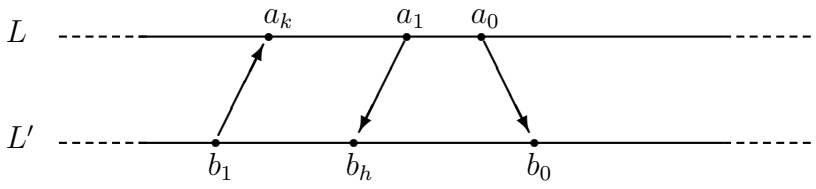
Dalla numerabilità di L e L' segue che possiamo scrivere questi insiemi come:

$$L = \{a_0, a_1, \ldots, a_n, \ldots\} \qquad L' = \{b_0, b_1, \ldots, b_n, \ldots\}$$

Cominciamo ora a definire la funzione f ponendo $f(a_0) = b_0$. Passiamo quindi a b_1; a seconda che sia $b_0 < b_1$ o $b_1 < b_0$, possiamo scegliere un elemento a_k di L che sia rispettivamente in relazione $>$ o $<$ con a_0 (ciò è sempre possibile perché $\langle L, \leq\rangle$ non ha massimo né minimo). Poniamo $f(a_k) = b_1$ e cancelliamo a_k dalla enumerazione di L. Consideriamo ora a_1 (o a_2 se a_k è a_1). Qualunque sia la posizione di questo elemento relativamente ad a_0 e a_k, poiché $\langle L', \leq'\rangle$ non ha massimo né minimo ed è denso, esiste sempre un elemento b_h di L' che si trova in una posizione analoga relativamente a b_0 e b_1. Poniamo $f(a_1) = b_h$ ed eliminiamo b_h dalla enumerazione di L'. A questo punto si passa a considerare b_2 (o b_3 se b_h è b_2), e procediamo analogamente.

È chiaro che il procedimento puè essere iterato, che ad ogni elemento di L viene associato un elemento di L' e che, viceversa, ogni elemento di L' è l'immagine di un elemento di L. Viene così definita f come funzione biiettiva da L su L' che conserva l'ordine.
Come conseguenza del Teorema 3.6 abbiamo che tutti gli ordini lineari densi, senza massimo e minimo, e numerabili sono isomorfi, come insiemi ordinati, ai numeri razionali[10].

[10] È opportuno ricordare qui l'Osservazione 3.2. Se infatti, oltre alla relazione d'ordine consideriamo altre relazioni o operazioni, non è detto che ogni struttura di questo tipo continui ad essere isomorfa ai razionali. I reali algebrici, per esempio, costituiscono un



3.3 Completezza Semantica

Una teoria è *semanticamente completa* se è in grado di dimostrare tutte le proposizioni vere in tutti i suoi modelli. L'importanza di questa nozione è evidente: se in qualche modo stabiliamo che una data proposizione è verificata in tutti i modelli di una teoria semanticamente completa $\mathcal{T}$, allora possiamo concludere che esiste una dimostrazione di quella proposizione partendo dagli assiomi di $\mathcal{T}$.

Osservazione 3.7 Il fatto che 'esista' una dimostrazione di una proposizione non implica che siamo in grado di trovarla. Bisogna qui stare attenti a non confondere la decidiblità degli assiomi considerata nel paragrafo 2 con il fatto che siamo sempre in grado di determinare una dimostrazione di una proposizione che sappiamo essere dimostrabile. Dalla decidibilità degli assiomi segue che siamo sempre in grado di stabilire se una data successione di passaggi sia effettivamente una dimostrazione, ma ciò è diverso dal trovare effettivamente una dimostrazione di una data formula.

Anche nel caso della completezza semantica è cruciale il passaggio da teorie del primo ordine a teorie del secondo ordine. Il risultato principale riguardante quelle teorie è il seguente teorema dovuto a Kurt Gödel.

Teorema 3.8 (T. di Completezza I). *Se una proposizione del primo ordine A è vera in tutti i modelli di una teoria del primo ordine $\mathcal{T}$, allora A è dimostrabile in $\mathcal{T}$.*

Osservazione 3.9 È molto importante precisare il senso di questo teorema. Quando parliamo di una proposizione A del primo ordine vera in tutti i modelli di una data teoria $\mathcal{T}$, intendiamo una proposizione che contenga

ordine numerabile, denso, senza massimo e minimo, ma se consideriamo anche le operazioni di somma e prodotto, i reali algebrici non sono isomorfi ai razionali.

solo i simboli di $\mathcal{T}$, cioè i simboli che compaiono negli assiomi propri di tale teoria. In logica, si dice che la proposizione (o meglio, la formula[11]) A deve appartenere al *linguaggio* di $\mathcal{T}$. Nel caso della teoria dei gruppi, per esempio, dovranno comparire nella proposizione solo i simboli $*$, u, e il simbolo di uguaglianza, oltre ovviamente ai quantificatori $\forall x$, $\exists x$ e i simboli logici $\neg$, $\wedge$, $\rightarrow$, ecc. Una proposizione del primo ordine sarà quindi, per esempio, $\forall x[\forall y(x * y = y * x = y) \rightarrow x = u]$, che esprime l'unicità dell'elemento neutro. Quando poi diciamo che questa proposizione è vera in ogni modello, intendiamo che essa risulta vera una volta interpretati $*$ e u nelle corrispondenti operazioni nel modello. Parlando del modello $\langle \mathbb{Z}, +, 0\rangle$, per esempio, intendiamo che la proposizione $\forall x[\forall y(x + y = y + x = y) \rightarrow x = 0]$ è vera negli interi.

Invertendo la prospettiva storica, dimostreremo il Teorema 3.8 basandoci sul seguente risultato, dovuto a Leon Henkin, che verrà usato anche in seguito.

Teorema 3.10 (T. di Completezza II). *Se $\mathcal{A}$ è un insieme coerente di proposizioni del primo ordine, allora $\mathcal{A}$ ha un modello.*

Lemma 3.11 *Se la teoria $\mathcal{T}'$ ottenuta aggiungendo la proposizione $\neg A$ agli assiomi di $\mathcal{T}$ è contraddittoria allora A è teorema di $\mathcal{T}$.*

Dim. Per il *Teorema di Deduzione* (dimostrabile in logica classica), per ogni proposizione B, $\mathcal{T}' \vdash B$ se e solo se $\mathcal{T} \vdash \neg A \rightarrow B$ (possiamo cioè portare la formula $\neg A$ aggiunta a $\mathcal{T}$ a destra del segno di dimotrabilità $\vdash$). Se $\mathcal{T}'$ è contraddittoria quindi, esiste una formula C tale che $\neg A \rightarrow C \wedge \neg C$ è teorema di $\mathcal{T}$, ma questa proposizione è tautologicamente equivalente ad A. Anche A sarà dunque teorema di $\mathcal{T}$. ∎

Dimostrazione del Teorema 3.8. Supponiamo che A non sia dimostrabile in $\mathcal{T}$. Dal lemma precedente segue che la teoria $\mathcal{T}'$ ottenuta aggiungendo $\neg A$ agli assiomi di $\mathcal{T}$ è coerente e quindi, per il Teorema 3.10, $\mathcal{T}'$ ha un modello $\mathbf{M}$ che ovviamente è anche modello di $\mathcal{T}$. Basta quindi osservare che A non è vera in $\mathbf{M}$. ∎

Il Teorema 3.8 è uno dei risultati più importante della logica matematica. Bisogna osservare tuttavia che esso non dà nessuna informazione relativa alle

[11] V. nota 3.

proposizioni del secondo ordine vere in tutti i modelli della teoria. Quando abbandoniamo il primo ordine, infatti, è possible trovarsi di fronte a qualche conseguenza del Teorema di Incompletezza di Gödel. Una di queste è che che la teoria $\mathcal{T}_{\mathbb{R}}$ dei numeri reali è incompleta. Poiché la struttura $\mathbb{R}$ dei reali è l'unico modello (a meno di isomorfismi) di $\mathcal{T}_{\mathbb{R}}$, abbiamo che ci sono proposizioni vere in questa struttura, ma non dimostrabili per mezzo degli assiomi dei reali.

Osservazione 3.12 Si potrebbe pensare di aggirare il problema dell'incompletezza di $\mathcal{T}_{\mathbb{R}}$ aggiungendo a tale teoria tutte le proposizioni vere in $\mathbb{R}$, ma non dimostrabili. Sempre per il Teorema di Incompletezza, tuttavia, la teoria risultante non sarebbe assiomatica perchè l'insieme dei suoi assiomi non è decidibile.

Un'altra conseguenza interessante del Teorema 3.10 è il seguente

Teorema 3.13 (T. di Compattezza Semantica). *Un insieme $\mathcal{A}$ di proposizioni del primo ordine ha modello se e solo se ogni suo sottoinsieme finito ha un modello.*

Dim. Un verso del 'se e solo se' è banale: ogni modello di $\mathcal{A}$ è anche modello di ogni sottoinsieme di $\mathcal{A}$ e in particolare di ogni sottoinsieme finito. Inversamente, se ogni sottoinsieme finito di $\mathcal{A}$ ha modello, allora ogni tale sottoinsieme è coerente e, per il Teorema 2.1, anche $\mathcal{A}$ è coerente. Per il Teorema 3.10, $\mathcal{A}$ ha modello. ∎

Corollario 3.14 *Se una teoria $\mathcal{T}$ del primo ordine ha modelli finiti di cardinalità arbitrariamente grande, allora $\mathcal{T}$ ha un modello infinito.*

Dim. Indichiamo con A_n la proposizione

$$\exists x_1, \ldots, x_n \left(\bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \right)$$

dove l'espressione tra parentesi indica la congiunzione di tutte le formule del tipo $x_i \neq x_j$ con i minore di j e $i, j \in \{1, \ldots, n\}$. La proposizione A_n è quindi vera in una struttura se quella struttura ha almeno n elementi. Indichiamo con $\mathcal{A}$ l'insieme di tutte le A_n e con $\mathcal{A}_{\mathcal{T}}$ l'insieme degli assiomi di $\mathcal{T}$.

Ogni sottoinsieme finito $\mathcal{A}'$ di $\mathcal{A} \cup \mathcal{A}_\mathcal{T}$ ha modello. Basta infatti considerare il massimo m tale che A_m appartiene ad $\mathcal{A}'$ e scegliere un modello di $\mathcal{T}$ con più di m elementi. Per il Teorema di Compattezza, anche $\mathcal{A} \cup \mathcal{A}_\mathcal{T}$ ha un modello $\mathbf{M}$, che sarà ovviamente modello di $\mathcal{T}$. Inoltre, tutte le A_n sono vere in $\mathbf{M}$ che dovrà quindi essere infinito. ∎

Un'importante conseguenza di questo risultato è che *la finitezza non è caratterizzabile al primo ordine.*

Proposizione 3.15 *Non esiste nessun insieme $\mathcal{A}$ di formule del primo ordine che sono verificate in una struttura $\mathcal{S}$ se e solo se $\mathcal{S}$ è finita.*

Dim. Supponiamo per assurdo che un tale insieme $\mathcal{A}$ esista. In tal caso la teoria avente come assiomi le formule di $\mathcal{A}$ avrebbe modelli di cardinalità finita arbitrariamente grande e quindi, per il corollario precedente, dovrebbe avere un modello infinito, contro l'ipotesi iniziale su $\mathcal{A}$. ∎

Questa proposizione non esclude ovviamente che siano definibili al primo ordine le strutture con un *dato* numero di elementi, oppure con al più un *dato* numero di elementi. Per esempio, la formula $\exists x_1, x_2(x_1 \neq x_2 \wedge \forall x(x = x_1 \vee x = x_2))$ definisce le strutture aventi esattamente due elementi, mentre la formula $\exists x_1, x_2, x_3 \forall x(x = x_1 \vee x = x_2 \vee x = 3)$ definisce le strutture con al più tre elementi.

3.4 Un esempio di teoria coerente e senza modelli.

L'esempio deve riguardare ovviamente una teoria che non sia del primo ordine perché sappiamo che ogni teoria del primo ordine coerente ha modelli.

Consideriamo le strutture del tipo $\langle X, +, \times, \leq, 0, 1, c\rangle$, dove X è un insieme, $+$ e $\times$ sono operazioni binarie su X, $\leq$ è una relazione binaria su X, e 0, 1, e c sono elementi di X. La teoria $\mathcal{T}$ che consideriamo ha come assiomi gli *Assiomi dei Campi Ordinati Completi* ed inoltre le seguenti proposizioni:

$$1 \leq c$$
$$1 + 1 \leq c$$
$$1 + 1 + 1 \leq c$$
ecc.

Dimostriamo che $\mathcal{T}$ è coerente. Sappiamo che un insieme di proposizioni è coerente se e solo se ogni suo sottoinsieme finito è coerente (vedi Osservazione 2.2). Consideriamo un arbitrario insieme finito $\mathcal{A}$ di assiomi di $\mathcal{T}$ e sia n il massimo numero naturale tale che la disuguaglianza $1 + \cdots + 1 \leq c$, con 1 sommato n volte, appartenga ad $\mathcal{A}$. Consideriamo ora la struttura dei numeri reali e in tale struttura interpretiamo la costante c nel numero n. Le proposizioni in $\mathcal{A}$ che sono assiomi dei campi ordinati completi sono ovviamente verificati nella struttura dei reali e, per l'interpretazione scelta di c, sono anche verificate le proposizioni di $\mathcal{A}$ del tipo $1+\cdots+1 \leq c$. Abbiamo quindi che $\mathcal{A}$ ha un modello e quindi è coerente. Poiché $\mathcal{A}$ è un arbitrario insieme finito di assiomi di $\mathcal{T}$ abbiamo che anche $\mathcal{T}$ è coerente.

Dimostriamo ora che la teoria $\mathcal{T}$ non ha modello. Poiché sono assiomi di $\mathcal{T}$ tutti gli assiomi dei campi ordinati completi, sappiamo che l'unico eventuale modello di $\mathcal{T}$ dovrebbe essere (isomorfo a) l'insieme dei numeri reali. Comunque interpretiamo la costante c in tale modello, tuttavia, abbiamo che infiniti assiomi della forma $1 + \cdots + 1 \leq c$ vengono falsificati.

3.5 Completezza Sintattica

Una teoria è *sintatticamente completa* se, per ogni proposizione scritta nel linguaggio della teoria, tale proposizione oppure la sua negazione sono teoremi della teoria[12]. È chiaro che questa proprietà è molto forte. All'inizio del '900, tuttavia, essa era considerata più forte di quanto effettivamente sia; si pensava infatti che i modelli di una teoria sintatticamente completa dovessero essere isomorfi perchè verificano esattamente le stesse proposizioni. In altri termini, si pensava che la completezza sintattica implicasse la categoricità. Il teorema di Löwenheim-Skolem ed altri risultati ci dicono che ciò non è vero: possono esserci strutture non isomorfe che rendono vere le stesse proposizioni. Per quanto riguarda le teorie del primo ordine è vero invece il seguente risultato opposto.

Proposizione 3.16 *Ogni teoria categorica del primo ordine è sintatticamente completa.*

Dim. Sia $\mathcal{T}$ sia una teoria categorica del primo ordine e supponiamo per assurdo che $\mathcal{T}$ non sia sintatticamente completa; esiste quindi un enunciato

[12]Qui sarebbe stato più appropriato parlare di *enunciato* anziché di proposizione. Gli enunciati sono quelle formule in cui ogni variabile compare nel raggio d'azione del corrispondente quantificatore (si veda anche pagina 33).

A tale che $\mathcal{T} \nvdash A$ e $\mathcal{T} \nvdash \neg A$. Per il Lemma 3.11 abbiamo che entrambe le teorie $\mathcal{T}'$ e $\mathcal{T}''$ ottenute aggiungendo rispettivamente $\neg A$ e A agli assiomi di $\mathcal{T}$ sono coerenti e quindi, per il Teorema 3.10, queste teorie hanno modello. Siano $\mathcal{M}'$ e $\mathcal{M}''$ i rispettivi modelli delle due teorie. Questi modelli devono essere isomorfi in quanto modelli anche di $\mathcal{T}$ (che è categorica), ma ciò è assurdo perché il primo modello verifica $\neg A$ mentre il secondo verifica A. ∎

Aggiungendo un'ulteriore ipotesi questo risultato può essere estero al caso di teorie α-categoriche per qualche α infinito.

Proposizione 3.17 *Se la teoria del primo ordine $\mathcal{T}$ non ha modelli finiti ed è α-categorica per qualche α infinito, allora $\mathcal{T}$ è sintatticamente completa.*

Dim. La dimostrazione è simile a quella precedente. Supponendo che la teoria $\mathcal{T}$ non sia sintatticamente completa concludiamo che esistono due modelli $\mathcal{M}'$ e $\mathcal{M}''$ di $\mathcal{T}$ che non verificano le stesse formule. Dalle ipotesi su $\mathcal{T}$ segue che questi due modelli sono infiniti e quindi, per il Teorema di Löwenheim-Skolem, possiamo supporre che $\mathcal{M}'$ e $\mathcal{M}''$ abbiano cardinalità α. A questo punto si arriva ad un assurdo come nella dimostrazione precedente usando il fatto che $\mathcal{T}$ è α-categorica. ∎

Come conseguenza di questa proposizione abbiamo che la teoria degli ordini densi senza massimo e minimo (che chiaramente non ha modelli finiti) è sintatticamente completa (vedi Paragrafo 3.2).

Il seguente risultato mette in relazione la completezza semantica con la completezza sintattica. Non dovrebbe sorprendere il fatto che il legame tra le due nozioni sia la categoricità.

Proposizione 3.18 *Ogni teoria $\mathcal{T}$ semanticamente completa e categorica è sintatticamente completa.*

Dim. Sia $\mathcal{M}$ l'unico modello di $\mathcal{T}$. Dalla completezza semantica di $\mathcal{T}$ segue che ogni formula vera in $\mathcal{M}$ è dimostrabile in $\mathcal{T}$. A questo punto possiamo osservare che, data una qualsiasi formula A, tale formula oppure la sua negazione sono vere in $\mathcal{M}$ e quindi dimostrabili in $\mathcal{T}$. ∎

Consideriamo per esempio la teoria $\mathcal{G}_p$, dove p è un numero primo, ottenuta aggiungendo agli assiomi G1-G3 per la teoria dei gruppi l'assioma

$$\exists x_1, \ldots, x_p \left(\bigwedge_{1 \leq i < j \leq p} x_i \neq x_j \wedge \forall x \left(\bigvee_{1 \leq i \leq p} x = x_i \right) \right)$$

Quest'ultima formula è verificata in una struttura con esattamente p elementi. Abbiamo già osservato che la teoria dei gruppi è p-categorica, e dunque la teoria $\mathcal{G}_p$ è categorica. In quanto teoria del primo ordine, $\mathcal{G}_p$ è anche semanticamente completa. Possiamo quindi usare la Proposizione 3.18 per concludere che $\mathcal{G}_p$ è sintatticamente completa. Ciò significa che ogni enunciato (del primo ordine) della teoria dei gruppi è dimostrabile o confutabile nella teoria $\mathcal{G}_p$.

3.6 Indipendenza.

Gli assiomi di una teoria assiomatica sono *indipendenti* se nessuno di essi può essere dedotto dagli altri. Anche in questo caso, come per la coerenza, stiamo considerando una proprietà che di fatto coinvolge tutte le possibili deduzioni in una data teoria: l'assioma A della teoria $\mathcal{T}$ è indipendente se, detta $\mathcal{T}'$ la teoria ottenuta togliendo l'assioma A da $\mathcal{T}$, *nessuna* deduzione in $\mathcal{T}'$ si conclude con A.

Analogamente a quanto si è visto per la coerenza, la proprietà (a) delle deduzioni logiche considerata nell'Osservazione 1.1 fornisce una tecnica più semplice per dimostrare che A è indipendente. Se infatti A fosse teorema di $\mathcal{T}'$ (cioè dipendente) allora A dovrebbe essere vero in ogni modello di $\mathcal{T}'$. Per dimostrare l'indipendenza di A basta quindi esibire una struttura in cui siano verificati tutti gli assiomi di $\mathcal{T}$ ad eccezione di A. L'indipendenza del quinto postulato di Euclide è stata dimostrata in questo modo. Per dimostrare che l'Assioma di Completezza (3.1) per i reali non è conseguenza degli altri, basta osservare che i razionali verificano gli assiomi dei campi ordinati, ma non l'Assioma di Completezza.

La costruzione di un opportuno modello non è comunque l'unica tecnica per risolvere positivamente questioni d'indipendenza. Per esempio, per dimostrare che l'Assioma di Completezza per i reali è indipendente possiamo anche osservare che, se non lo fosse, allora la teoria dei reali sarebbe equivalente ad una teoria del primo ordine e non potrebbe essere categorica. In alcuni casi, come per la coerenza, è poi possibile applicare tecniche dirette che di fatto prendono in considerazione tutte le possibili dimostrazioni in una data teoria assiomatica.

Supponiamo che gli assiomi di una teoria $\mathcal{T}$ siano $A_0, \ldots, A_n$ e che A_0 non sia indipendente. Ciò significa che A_0 è dimostrabile nella teoria $\mathcal{T}'$ avente $A_1, \ldots, A_n$ come assiomi. Non è difficile rendersi conto che, se trascuriamo

l'indipendenza, le teorie $\mathcal{T}$ e $\mathcal{T}'$ hanno le stesse proprietà, vale a dire, $\mathcal{T}$ è categorica se e solo se $\mathcal{T}'$ lo è, $\mathcal{T}$ è semanticamente completa se e solo se $\mathcal{T}'$ lo è, e così via. In effetti, le proprietà di una teoria dipendono da ciò che è dimostrabile, cioè dai teoremi, più che dalla scelta degli assiomi.

Da questo punto di vista sembrerebbe quindi che questioni legate all'indipendenza degli assiomi siano sostanzialmente questioni di eleganza formale. Come insegnano le geometrie non Euclidee, però, c'è qualcosa di più. Supponiamo che gli assiomi $A_0, \ldots, A_n$ della teoria $\mathcal{T}$ siano indipendenti. Dal Lemma 3.11 segue che la teoria $\mathcal{T}^*$ avente per assiomi $A_1, \ldots, A_n$ e la negazione di A_0 è coerente, per cui diventa interessante vedere quali siano i teoremi di $\mathcal{T}^*$ e soprattutto vedere come sono fatti, se ce ne sono, i suoi modelli. Lo studio delle geometrie non Euclidee è appunto lo studio delle strutture in cui è verificata qualche forma di negazione del quinto postulato.

4 I numeri naturali

La presentazione assiomatica dei numeri naturali è basata sugli *Assiomi di Peano* (o di *Peano-Dedekind*). In base a questa presentazione, i numeri naturali sono una struttura $\langle N, 0, \sigma\rangle$ dove N è un insieme, 0 è un elemento di N e σ è una funzione da N in N, tali che:

(N1) $\forall n\,(\sigma n \neq 0)$

(N2) $\forall n, m\,(\sigma n = \sigma m \rightarrow n = m)$

(N3) $\forall X\,[(0 \in X \wedge \forall k\,(k \in X \rightarrow \sigma k \in X)) \rightarrow \forall n,\, n \in X]$

Dove, in N3, $\forall X$ quantifica su $\mathbf{P}(N)$, l'insieme di tutti i sottoinsiemi di N. Questo assioma è il famoso *Principio di Induzione* ed è una proposizione del secondo ordine; vedremo più avanti che la teoria dei numeri naturali è categorica e che quindi il Principio di Induzione non può essere espresso al primo ordine. Si osservi che l'ultima parte di N3, cioè $\forall n,\, n \in X$ è equivalente a $X = N$. Una variante, più informale, ma molto usata, del Principio di Induzione è la seguente:

(N3$_\mathbf{P}$) Se il numero naturale 0 ha una certa proprietà P, e dal fatto che k ha la proprietà P segue che σk ha tale proprietà, allora ogni numero naturale n ha la proprietà P.

Gli enunciati N3 e N3$_P$ risultano essere equivalenti in base alla seguente corrispondenza tra insiemi e proprietà. Ad ogni proprietà P possiamo associare l'insieme $\mathcal{K}_P$ dei naturali aventi tale proprietà e ad ogni insieme K di naturali possiamo associare la proprietà $\mathcal{P}_K$ di appartenere a K. Si verifica facilmente che $P = \mathcal{P}_{\mathcal{K}_P}$ e $K = \mathcal{K}_{\mathcal{P}_K}$ da cui segue che la corrispondenza tra proprietà dei naturali e sottoinsiemi di N è biunivoca.

Internamente alla teoria degli insiemi si dimostra che la teoria dei naturali è coerente. L'ordinale ω infatti è costituito dagli insiemi

$$\emptyset, \quad \{\emptyset\}, \quad \{\emptyset, \{\emptyset\}\}, \quad \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \quad \ldots$$

dove il successivo di ogni elemento α è $\alpha \cup \{\alpha\}$. Posto $\sigma n = n \cup \{n\}$, la terna $\langle \omega, \emptyset, \sigma \rangle$ risulta essere un modello di N1-N3.[13]

Dimostriamo ora che gli Assiomi di Peano sono indipendenti costruendo tre opportuni modelli della forma $\langle N, 0, \sigma \rangle$, dove tuttavia N, 0, e σ sono scelti in modo da rendere veri due degli assiomi e falsificare il terzo.

(1) Sia $N = \{0\}$, dove 0 è un arbitrario oggetto, e poniamo $\sigma 0 = 0$. Si verifica facilmente che gli assiomi N2 e N3 sono veri in questa struttura, mentre N1 è banalmente falso.

(2) Sia $N = \{0, a, b\}$, dove 0, a e b sono oggetti distinti, e poniamo $\sigma 0 = a$, $\sigma a = b$ e $\sigma b = a$. In questa struttura N1 e N3 sono verificati, ma σ non è iniettiva perché $\sigma 0 = \sigma b$, e quindi N2 non è verificato.

(3) Siano 0 e a due oggetti distinti e sia N l'insieme di tutte le sequenze finite 0, 00, 000, ... e a, aa, aaa, ... Data una sequenza $s \in N$, σs è la più piccola sequenza in N che contiene propriamente s. Questa struttura verifica N1 e N2. Sia X in sottoinsieme di N costituito da tutte le sequenze in cui compare solo 0. Abbiamo che l'antecedente del Principio di Induzione è verificato da X, ma ovviamente $X \neq N$.

D'ora in avanti, in questo paragrafo, parlando dei *numeri naturali* intenderemo sempre una arbitraria struttura insiemistica $\langle N, 0, \sigma \rangle$ in cui gli

[13] Abbiamo qui un esempio di situazione in cui diventa chiaro il senso di teoria assiomatica. La struttura $\langle \omega, \emptyset, \sigma \rangle$ è un modello di N1-N3, ma è anche dotato di una struttura insiemistica e in particolare la relazione $\in$ su ω è una relazione d'ordine stretto. Per potere parlare di relazione d'ordine sui naturali, tuttavia, abbiamo bisogno di una costruzione più complessa che vedremo in seguito, e che deve essere basata solo sugli assiomi N1-N3.

assiomi N1-N3 sono verificati. Come abbiamo visto sopra, esiste almeno una struttura con queste proprietà. In ognuna di queste strutture, diremo che σn è il *successore* del numero naturale n.

La dimostrazione dell'indipendenza del Principio di Induzione mette in luce il significato principale di questo principio, cioè che ogni numero naturale può essere raggiunto dallo 0 mediante successive applicazioni della funzione σ, cioè che l'insieme dei naturali può essere descritto come $\{0, \sigma 0, \sigma\sigma 0, \dots\}$. Più formalmente, se un insieme X contiene 0 ed è chiuso per l'operazione σ allora X esaurisce tutto N. Vale inoltre il seguente teorema, la cui dimostrazione è un primo esempio di *dimostrazione per induzione*.

Teorema 4.1 *Se $\langle N, 0, \sigma\rangle$ è un modello di* N1-N3*, allora, per ogni $n \neq 0$ in N, esiste un unico $m \in N$ tale che $n = \sigma m$.*

Dim. Sia X l'insieme $\{n \in N : n = 0$ *oppure* $\exists m : n = \sigma m\}$. L'insieme X contiene ovviamente 0. Se $k \in X$, allora σk appartiene a X perchè X contiene tutti gli elementi di N del tipo σn. Per l'assioma N3, possiamo concludere che $X = N$. Per quanto riguarda l'unicità, per N2 abbiamo che da $\sigma m = \sigma m'$ segue $m = m'$. ∎

Da questo teorema segue che l'immagine della funzione σ è $N \setminus \{0\}$ e quindi, per ogni $n \neq 0$, possiamo parlare del *predecessore* di n come dell'unico m tale che $\sigma m = n$; il predecessore di n verrà indicato con $\sigma^{-1} n$.

4.1 Definizione per induzione. Categoricità degli assiomi di Peano

Abbiamo visto nel paragrafo precedente che ogni naturale può essere raggiunto dallo 0 tramite successive applicazioni della funzione σ. Questa proprietà sta alla base della costruzione di molte funzioni definite sui naturali, incluse le usuali operazioni di somma e prodotto. Intuitivamente, possiamo definire una funzione f fornendo il valore $f(0)$ e fornendo una regola che permetta di calcolare $f(\sigma n)$ una volta calcolato $f(n)$. Per esempio, supponendo di aver già definito la moltiplicazione, il fattoriale può essere definito da $0! = 1$ e $(\sigma n)! = \sigma n \times n!$. Per accettare questo tipo di definizioni, dobbiamo però dimostrare che questa procedura definisce effettivamente una funzione.

Teorema 4.2 *Sia X un insieme, sia a un elemento di X, e sia φ una funzione da X in X. Allora, per ogni modello $\langle N, 0, \sigma\rangle$ di* N1-N3*, esiste un'unica*

funzione f da N in X con le seguenti proprietà: (1) $f(0) = a$, (2) *per ogni* $n \in N$, $f(\sigma n) = \varphi(f(n))$.

Dim.[14] Dimostriamo prima l'esistenza di f e poi l'unicità.

Insiemisticamente, una funzione da N in X è un insieme di coppie $\langle n, x\rangle \in N \times X$. Consideriamo l'insieme $\mathcal{F}$ costituito da tutti i sottoinsiemi W di $N \times X$ tali che

$$(1') \quad \langle 0, a\rangle \in W$$
$$(2') \quad \langle n, x\rangle \in W \;\Rightarrow\; \langle \sigma n, \varphi(x)\rangle \in W$$

L'insieme $\mathcal{F}$ non è vuoto perché l'intero insieme $N \times X$ ha le proprietà $(1')$ e $(2')$ e quindi appartiene a $\mathcal{F}$. Si osservi che queste proprietà corrispondono proprio alle proprietà (1) e (2) dell'enunciato del teorema; la scrittura $f(n) = x$ è equivalente infatti a $\langle n, x\rangle \in f$. Poniamo

$$f = \bigcap_{W \in \mathcal{F}} W \tag{4.2}$$

È immediato verificare che anche f definita in questo modo ha le proprietà $(1')$ e $(2')$. Per quanto riguarda $(2')$, se $\langle n, x\rangle \in f$, allora questa coppia appartiene a ogni W in $\mathcal{F}$ che quindi contiene anche $\langle \sigma n, \varphi(x)\rangle$, e quindi questa coppia appartiene all'intersezione f di tutti i W. La dimostrazione che f ha la proprietà $(1')$ è analoga e più semplice.

Dobbiamo ora dimostrare che f, definita da (4.2), è effettivamente una funzione da N in X, cioè che

$$(3) \quad \forall n \in N,\, \exists x \in X \,:\, \langle n, x\rangle \in f$$
$$(4) \quad \forall n \in N,\, \forall x_1, x_2 \in X,\, \langle n, x_1\rangle \in f \;\; e \;\; \langle n, x_2\rangle \in f \;\Rightarrow\; x_1 = x_2$$

È facile dimostrare (3) per induzione. Sia K l'insieme $\{n \in N : \exists x \in X : \langle n, x\rangle \in f\}$. Per $(1')$, abbiamo $0 \in K$ e, per $(2')$, se $k \in K$, allora $\sigma k \in K$. Abbiamo quindi $K = N$, cioè (3).

Anche (4) si dimostra per induzione. Poniamo

$$K = \{n \in N : \forall x_1, x_2 \in X,\, \langle n, x_1\rangle \in f \;\; e \;\; \langle n, x_2\rangle \in f \;\Rightarrow\; x_1 = x_2\}$$

[14] La dimostrazione di questo teorema e altre dimostrazioni in questo paragrafo sono tratte dal testo *The Number Systems - Foundations of Algebra and Analysis*, di Solomon Feferman (Addison-Wesley, 1964).

Dimostriamo che $0 \in K$. Supponiamo per assurdo $\langle 0, x_0\rangle \in f$ e $x_0 \neq a$, e consideriamo il sottoinsieme V di $N \times X$ definito da $V = f \setminus \{\langle 0, x_0\rangle\}$. L'insieme V verifica la proprietà $(1')$ perché f ha tale proprietà e $x_0 \neq a$. Se $\langle n, x\rangle \in V$, allora $\langle n, x\rangle \in f$ e, per $(2')$, $\langle \sigma n, \varphi(x)\rangle \in f$; ma ciò implica $\langle \sigma n, \varphi(x)\rangle \in V$ perché, per N1, $0 \neq \sigma n$ per ogni n. Abbiamo quindi che V ha le proprietà $(1')$ e $(2')$ e quindi $V \in \mathcal{F}$, ma ciò contraddice (4.2) perché V è contenuto propriamente in f.

Resta quindi da dimostrare che, $k \in K \Rightarrow \sigma k \in K$. L'antecedente di questa implicazione significa che, se $\langle k, x_1\rangle \in f$ e $\langle k, x_2\rangle \in f$, allora $x_1 = x_2$. Dobbiamo dimostrare che, sotto questa ipotesi, se $\langle \sigma k, y_1\rangle \in f$ e $\langle \sigma k, y_2\rangle \in f$, allora $y_1 = y_2$, ma ciò è equivalente a dimostrare che, se

$$\langle \sigma k, y\rangle \in f \;\Rightarrow\; \exists x : \langle k, x\rangle \in f \;\; e \;\; y = \varphi x \tag{4.3}$$

Infatti, dall'ipotesi induttiva sappiamo che esiste un unico x tale che $\langle k, x\rangle \in f$ e quindi, se $\langle \sigma k, y_1\rangle \in f$ e $\langle \sigma k, y_2\rangle \in f$, per (4.3), abbiamo $y_1 = \varphi(x) = y_2$. Supponiamo per assurdo che (4.3) non valga, cioè che esista una coppia $\langle \sigma k_0, y_0\rangle$ in f tale che, per ogni $\langle k_0, x\rangle \in f$, abbiamo $y \neq \varphi(x)$. Consideriamo l'insieme $V = f \setminus \{\langle \sigma k_0, y_0\rangle\}$; vogliamo dimostrare che $V \in \mathcal{F}$, cioè che verifica $(1')$ e $(2')$, in modo da contraddire (4.2) essendo V contenuto propriamente in f. La coppia $\langle 0, a\rangle$ appartiene a f e quindi anche a V. Supponiamo che $\langle n, z\rangle$ appartenga a V, cosicché $\langle n, z\rangle$ e $\langle \sigma n, \varphi(z)\rangle$ appartengono a f. Se $n \neq k_0$ allora $\langle \sigma n, \varphi(z)\rangle \neq \langle \sigma k_0, y_0\rangle$ e quindi $\langle \sigma n, \varphi(z)\rangle$ appartiene a V. Se invece $n = k_0$ e $\langle \sigma n, \varphi(z)\rangle = \langle \sigma k_0, y\rangle$, allora $\varphi(z) = y_0$. Abbiamo quindi determinato una coppia $\langle n, z\rangle$ in f, con $n = k_0$, e tale che $\varphi(z) = y_0$. Ciò contraddice l'ipotesi su k_0 e y_0. Questo conclude la dimostrazione che V appartiene a $\mathcal{F}$ e quindi anche la dimostrazione che l'insieme f definito in (4.2) è una funzione.

Supponiamo ora che due funzioni f_1 ed f_2 da N in X verifichino le condizioni (1) e (2) dell'enunciato di questo teorema. Vogliamo dimostrare che $f_1 = f_2$, cosicché la funzione f definita sopra risulterà unica.

Sia K l'insieme $\{n \in N : f_1(n) = f_2(n)\}$; dimostriamo per induzione che $K = N$. Dalla condizione (1) segue banalmente che $0 \in K$. Supponiamo $k \in K$, cioè $f_1(k) = f_2(k)$. Dalla condizione (2) abbiamo $f_1(\sigma k) = \varphi(f_1(k)) = \varphi(f_2(k)) = f_2(\sigma k)$, e quindi $\sigma k \in K$. ∎

Questo risultato ci permette di dimostrare il teorema dell'unicità del modello degli assiomi di Peano.

Teorema 4.3 *Siano* $\langle N, 0, \sigma\rangle$ *e* $\langle N', 0'\sigma'\rangle$ *strutture in cui sono verificati gli assiomi di Peano* N1-N3*. Allora le due strutture sono isomorfe.*

Dim. Per il Teorema 4.2, ponendo $X = N'$, $a = 0'$ e $\varphi = \sigma'$, esiste un'unica funzione f da N in N' tale che $f(0) = 0'$ e, per ogni $n \in N$, $f(\sigma n) = \sigma' f(n)$. Abbiamo quindi che f verifica le clausole (1)-(3) della Definizione 3.1 (si noti che in $\langle N, 0, \sigma\rangle$ e $\langle N', 0'\sigma'\rangle$ gli insiemi delle R_i e R'_i sono vuoti). Per concludere che f è un isomorfismo, dobbiamo dimostrare che f è suriettiva e iniettiva.

Consideriamo l'insieme $K' = \{n' \in N' : \exists n \in N : f(n) = n'\}$. L'insieme K' contiene $0'$ perché $f(0) = 0'$. Se $k' \in K'$ e $f(k) = k'$, allora $f(\sigma k) = \sigma' f(k) = \sigma' k'$ e quindi anche $\sigma' k' \in K'$. Poiché $\langle N', 0', \sigma'\rangle$ verifica N3, abbiamo $K' = N'$ e quindi f è suriettiva.

Consideriamo ora l'insieme

$$K = \{n \in N : \forall m \in N,\ f(n) = f(m) \Rightarrow n = m\}$$

Anche in questo caso dimostriamo per induzione che $K = N$, da cui segue che f è iniettiva. Poiché $f(0) = 0'$, dobbiamo dimostrare che, per ogni m, $f(m) = 0' \Rightarrow m = 0$. Se, per assurdo, $f(m) = 0'$ e $m \neq 0$, allora, per il Teorema 4.1, esiste k tale che $m = \sigma k$ e quindi $0' = f(m) = \sigma' f(k)$, ma queste uguaglianze contraddicono N1 per σ'.

Sia ora $k \in K$ e supponiamo $f(\sigma k) = f(m)$. Poichè $f(\sigma k) = \sigma' f(k) \neq 0'$, abbiamo che m non può essere 0. Esiste quindi un n tale che $m = \sigma n$ e quindi $f(m) = \sigma' f(n)$, e, per l'assioma N2 applicato a σ' abbiamo che $\sigma' f(n) = \sigma' f(k)$ implica $f(n) = f(k)$. Poiché $k \in K$, abbiamo infine $n = k$ e $m = \sigma k$. Questo conclude la dimostrazione che f è iniettiva ∎

Quest'ultimo teorema dimostra che la teoria costituita dagli assiomi di Peano N1-N3 è categorica. Analogamente a quanto abbiamo visto nel caso degli assiomi per i reali, la categoricità di N1-N3 implica che l'assioma N3 non può essere sostituito da un insieme di proposizioni del primo ordine.

4.2 Operazioni sui naturali

Una volta dimostrato che gli assiomi N1-N3 determinano un'unica struttura matematica (Teorema 4.3) resta il problema di definire le usuali operazioni sui naturali. Ci aspettiamo ovviamente di dover usare una definizione per induzione e quindi il Teorema 4.2. In base a questo teorema, per esempio,

possiamo definire una funzione $+_m$ che applicata ad ogni naturale gli somma m: (1) $+_m(0) = m$, (2) $+_m(\sigma n) = \sigma(+_m(n))$. In questo caso, l'insieme X, l'elemento a, e la funzione φ del Teorema 4.2 sono rispettivamente N, m, e la funzione σ. Il problema è che la somma è una funzione binaria, e non un insieme $\{+_m : m \in N\}$ di funzioni unarie. Si potrebbe continuare su questa strada, definire una funzione binaria + tramite: $+(m, n) = +_m(n)$, e dimostrare che questa funzione ha le usuali proprietà della somma, per esempio, che $+_m(n) = +_n(m)$ (commutatività) e che $+_m(+_n(k)) = +_{+_m(n)}(k)$ (associatività). Un'altra possibilità è considerare una conseguenza del Teorema 4.2.

Teorema 4.4 *Date due funzioni $g : N \times N \to N$ e $h : N \to N$, esiste un'unica funzione f da $N \times N$ in N con le seguenti proprietà*

$$\begin{array}{ll} (1) & f(n, 0) = h(n) \\ (2) & f(n, \sigma(m)) = g(n, f(n, m)) \end{array}$$

La dimostrazione di questo teorema, che non verrà riportata, si basa sul Teorema 4.2 (con $X = N$), sostanzialmente sostituendo l'elemento a con un insieme di elementi $a_n = h(n)$ e la funzione φ con un insieme di funzioni φ_n tali che $\varphi_n(m) = g(n, m)$.

Siamo ora in grado di definire l'operazione di somma ponendo, nel Teorema 4.4, $g(n, m) = \sigma(m)$ e $h(n) = n$. In questo modo, la funzione f, che indicheremo con f_+, risulta definita da:

$$\begin{array}{ll} (1) & f_+(n, 0) = n \\ (2) & f_+(n, \sigma(m)) = \sigma f_+(n, m) \end{array} \tag{4.4}$$

La funzione f_+ è chiaramente la funzione somma; per poter arrivare in modo rigoroso a questa conclusione, dobbiamo però dimostrare che questa funzione gode effettivamente delle proprietà della funzione somma. Come esempio, dimostriamo che la funzione f_+ è associativa.

Teorema 4.5 *Sia f_+ la funzione da $N \times N$ in N definita in* (4.4)*. Allora, per ogni n, m, k,*

$$f_+(n, f_+(m, k)) = f_+(f_+(n, m), k)$$

Dim. Procediamo per induzione su k, facendo svolgere a n e m il ruolo di parametri. Poniamo

$$K = \{k \in N : f_+(n, f_+(m,k)) = f_+(f_+(n,m),k)$$

Il numero 0 appartiene a K; infatti, per (1) in (4.4), $f_+(n, f_+(m,0)) = f_+(n,m)$ e $f_+(f_+(n,m),0) = f_+(n,m)$. Supposto $k \in K$, usando (2) in (4.4) e l'ipotesi induttiva, abbiamo $f_+(n, f_+(m,\sigma k)) = f_+(n, \sigma f_+(m,k) = \sigma f_+(n, f_+(m,k) = \sigma f_+(f_+(n,m),k) = f_+(f_+(n,m),\sigma k)$; per cui anche $\sigma k \in K$. ∎

Funzioni definite sulla base del Teorema 4.2 del Teorema 4.4 possono a loro volta essere usate in questi teoremi per definire altre funzioni. Posto per esempio $h(n) = 0$ e $g(n,m) = f_+(n,m)$, otteniamo, in base al Teorema 4.4 la definizione della funzione prodotto che indichiamo con $f_\times$:

$$\begin{array}{ll} (1) & f_\times(n,0) = 0 \\ (2) & f_\times(n,\sigma(m)) = f_+(n, f_\times(n,m)) \end{array} \tag{4.5}$$

D'ora in avanti, torneremo alle usuali notazioni, scrivendo $n+m$ anziché $f_+(n,m)$ e $n \times m$ anziché $f_\times(n,m)$.

4.3 Ordinamento dei naturali

Una volta definita la somma di naturali e dimostrate le sue proprietà, la relazione d'ordine su N può essere semplicemente definita da

$$n \leq m \stackrel{\text{def}}{\equiv} \exists k : n + k = m \tag{4.6}$$

Anche in questo caso, bisogna dimostrare che la relazione $\leq$ gode delle usuali proprietà, cioè che è *riflessiva* ($\forall n \in N,\ n \leq n$), *transitiva* ($\forall m,n,k \in N$, $(m \leq n \ e\ n \leq k \Rightarrow m \leq k)$), *antisimmetrica* ($\forall n,m \in N$, $(n \leq m \ e\ m \leq n \Rightarrow n = m)$) e totale ($\forall n,m \in N$, $(n \leq m \ o\ m \leq n)$. Oltre a queste propritetà, bisognerà anche dimostrare le usuali relazioni tra relazione d'ordine e funzione successore, somma e prodotto. Tra queste, ricordiamo le seguenti proprietà che verranno usate in seguito. Come al solito, $n \leq m$ verrà anche scritto come $m \geq n$ e $n < m$ (o $n > m$) verrà usato come abbreviazione di $n \neq m$ e $n \leq m$ (o $n \geq m$).

$$\begin{array}{ll} \text{(i)} & \forall n\,(0 \leq n) \\ \text{(ii)} & \forall n,m\,(n < m \rightarrow \sigma n \leq m) \\ \text{(iii)} & \forall n\,(\sigma n \not\leq n) \end{array} \tag{4.7}$$

L'avere introdotto la relazione d'ordine $\leq$ sull'insieme dei naturali permette di ricavare due interessanti e utili conseguenze del Principio d'Induzione.

Teorema 4.6 *In ogni struttura* $\langle N, 0, \sigma\rangle$ *in cui sono verificati* N1-N3 *valgono anche le seguenti proposizioni.*

N3′ Ogni sottoinsieme non vuoto di N ha minimo.

N3″ $\forall X \subseteq N\,[\forall n\,(\forall m < n\,(m \in X) \to n \in X) \to X = N]$

Dim. Sia X un sottoinsieme non vuoto di N e supponiamo per assurdo che X non abbia minimo. Sia $K = \{n \in N : \forall m \in X,\, n \leq m\}$. Per (4.7.i), abbiamo che $0 \in K$. Supposto $k \in K$, cioè $\forall m \in X,\, k \leq m$, k non può appartenere a X, altrimenti ne sarebbe l'elemento minimo e quindi abbiamo che $\forall m \in X,\, k < m$, ma per (4.7.ii), ciò implica $\forall m \in X,\, \sigma k \leq m$, e quindi $\sigma k \in K$. Per il principio di induzione abbiamo quindi $K = N$, cioè

$$\forall n \in N, \forall m \in X\,(n \leq m) \tag{4.8}$$

Poiché X non è vuoto, possiamo considerarne un elemento k_0. Per (4.8), abbiamo $\forall n \in N,\, (n \leq k_0)$ e, in particolare $\sigma k_0 \leq k_0$, che contraddice (4.7.iii). Siamo quindi arrivati ad un assurdo e abbiamo dimostrato N3′.

Supponiamo che X sia tale che $n \in X$ ogniqualvolta $m \in X$ per ogni $m < n$. Se $X \neq N$, allora $N \setminus X$ è non vuoto e quindi, per N3′, possiamo considerare il minimo n_0 di questo insieme. A questo punto possiamo arrivare ad una contraddizione osservando che ogni $m < n_0$ appartiene ad X e che quindi per le ipotesi su X anche n_0 vi appartiene. ∎

In molte presentazioni assiomatiche, i numeri naturali vengono definiti come una struttura $\langle N, 0, \sigma, \leq\rangle$ in cui, oltre ad N1-N3, devono essere verificati altri assiomi che stabiliscono che $\leq$ è una relazione d'ordine totale, e che mettono in relazione $\leq$ con la funzione σ; tra questi assiomi avremo per esempio (4.7) o assunzioni equivalenti. Si legge spesso che in queste teorie assiomatiche, le proprietà N3′ e N3″ sono equivalenti al principio di induzione, cioè che possiamo sostituire N3 con N3′ o N3″, senza cambiare la teoria. Questa affermazione va però precisata.

In entrambi i casi, cioè sostituendo N3 con N3′ o con N3″, per ottenere effettivamente una teoria equivalente dobbiamo anche assumere che σ^{-1} *sia definita su ogni* $n \neq 0$, cioè che

$$\forall n \neq 0\,\exists m : \sigma(m) = n \tag{4.9}$$

Questa ulteriore assunzione non viene spesso esplicitata perché si suppone di considerare il più piccolo insieme in cui valgono gli assiomi. Il fatto poi che (4.9) sia effettivamente necessaria si dimostra facilmente osservando che N3′ o N3″ sono verificate in ogni ordinale, mentre N3 è verificata solo da ω. In teoria degli insiemi, N3″ prende il nome di *Principio di Induzione Transfinita*.

Tornando all'equivalenza di N3, N3′ e N3″, abbiamo visto nella dimostrazione del teorema precedente che N3 $\Rightarrow$ N3′ e N3′ $\Rightarrow$ N3″. Resta dunque da dimostrare che, assumendo (4.9), N3″ $\Rightarrow$ N3. Supponiamo che l'insieme X verifichi l'antecedente di N3, cioè $0 \in X \wedge \forall k(k \in X \rightarrow \sigma k \in X)$, e, usando N3″, dimostriamo che $X = N$. Per fare questo basta dimostrare che l'antecedente di N3 implica l'antecedente di N3″, cioè $\forall n\,(\forall m < n\,(m \in X) \rightarrow n \in X)$, perché $X = N$ è anche il conseguente di quest'ultimo principio. Consideriamo un arbitrario numero naturale n tale che $m \in X$ per ogni $m < n$; vogliamo concludere che $n \in X$. Se $n = 0$, allora $n \in X$ perché X verifica l'antecedente di N3. Se $n \neq 0$ allora, per (4.9), possiamo considerare $\sigma^{-1}n$. Dalla definizione (4.6) e dalle proprietà della somma abbiamo $\sigma^{-1}n \leq n$ e, per l'iniettività di σ, possiamo concludere $\sigma^{-1}n < n$. $\sigma^{-1}n$ appartiene dunque a X e, per l'antecedente di N3, abbiamo anche $n \in X$. ∎

5 Aritmetica al primo ordine. Modelli non-standard

L'assioma di induzione (N3) è una proposizione del secondo ordine perché in essa si quantifica su insiemi. Per i risultati enunciati nel paragrafo 3, questo assioma non può essere sostituito con una proposizione o da un insieme di proposizioni del primo ordine. La teoria assiomatica dei naturali, infatti, ha un modello infinito e quindi, per il teorema di Löwenheim-Skolem, se N3 fosse in qualche modo esprimibile al primo ordine, tale teoria non potrebbe essere categorica. Possiamo tuttavia chiederci cosa succede se sostituiamo N3 con un opportuno *schema d'assiomi* del primo ordine. Il motivo di un'indagine di questo tipo non è solo puramente speculativo. Poiché per i naturali siamo essenzialmente interessati ai modelli numerabili, una questione senza dubbio interessante è se una versione al primo ordine degli assiomi di Peano possa essere $\aleph_0$-categorica. Oltre a questo, ci possiamo chiedere quanta matematica possiamo effettivamente sviluppare abbandonando il secondo ordine. Come vedremo più avanti, a queste due questioni vendono date rispettivamente una

risposta negativa ed una positiva: la versione al primo ordine degli assiomi di Peano non è neanche $\aleph_0$-categorica, ma la parte di matematica che in questa possiamo sviluppare resta comunque considerevole.

Il discorso su cosa significhi sostituire una assioma del secondo ordine con uno schema di assiomi del primo ordine va ovviamente chiarito. Conviene partire innanzitutto da una definizione dei numeri naturali come una struttura $\mathbf{N} = \langle N, 0, \sigma, +, \times \rangle$ in cui includiamo anche la somma e il prodotto come nozioni primitive. Un primo insieme di assiomi dovrà quindi stabilire le relazioni tra queste funzioni:

(A1) $\forall n\,(\sigma n \neq 0)$

(A2) $\forall n, m\,(\sigma n = \sigma m \rightarrow n = m)$

(A3) $\forall n\,(n + 0 = n)$

(A4) $\forall n, m\,(n + \sigma m = \sigma(n + m))$

(A5) $\forall n\,(n \times 0 = 0)$

(A6) $\forall n, m\,(n \times \sigma m = n + (n \times m))$

Gli assiomi A1 e A2 sono chiaramente N1 e N2, e non è difficile riconoscere in A3-A6 le definizioni ricorsive di somma e prodotto considerate nel paragrafo precedente. Tutti questi assiomi sono proposizioni del primo ordine.

Diciamo che un'espressione A è una formula del linguaggio del primo ordine $\mathcal{L}_1$ per la struttura $\mathbf{N}$ se A contiene esclusivamente i simboli 0, σ, $+$, $\times$, il simbolo di uguaglianza ($=$), variabili (n, m, k, $n_1, n_2, \dots$)[15], connettivi logici ($\wedge$, $\vee$, $\neg$, $\rightarrow$, $\leftrightarrow$), e quantificatori ($\forall$, $\exists$) del primo ordine. Sono quindi formule del primo ordine gli assiomi A1-A6, le espressioni $\exists n\,(\sigma 0 + n = \sigma 0 \times n \vee n = 0)$, $\forall n, m\,\exists k, h\,(m + k = n \wedge m + h = n)$, mentre non lo è l'espressione $\forall n,\, \exists X\,(n \in X)$ se interpretiamo la variabile X come una variabile su sottoinsiemi di N.

[15]Per non appesantire il discorso introducendo nuovi simboli, useremo i simboli n, m, k, $n_1, n_2, \dots$ sia come variabili di $\mathcal{L}_1$, sia per indicare elementi di N nella struttura $\mathbf{N}$; il contesto permetterà sempre di non confondere i due diversi usi di questi simboli. Ogni formula di $\mathcal{L}_1$ contiene ovviamente un numero finito di variabili; è necessario tuttavia poter disporre di un insieme numerabile $n_1, n_2, \dots$ di variabili per poter scrivere formule arbitrariamente complesse.

Le occorrenze delle variabili n, m, k, h nelle formule precedenti sono tutte *vincolate* (o *quantificate*) perché queste variabili compaiono esclusivamente nel raggio d'azione dei corrispondenti quantificatori esistenziali o universali. Le occorrenze non vincolate di una variabile sono dette *libere*; per esempio, nella formula $\exists k(m + k = n \times \sigma 0)$ le variabili n ed m sono libere mentre k è vincolata. Non è difficile rendersi conto che, se tutte le variabili che compaiono nella formula A sono vincolate allora A è vera oppure falsa nella struttura $\mathbf{N}$; se invece A contiene qualche variabile libera, allora il valore di verità di A generalmente dipende dai valori attribuiti a quelle variabili. Per esempio, la formula $\forall n, m, \exists k\,(m + k = n)$ è ovviamente falsa, mentre $\exists k\,(m + k = n)$, in cui m e n sono variabili libere, è vera (falsa) se il valore attribuito alla variabile m è un numero naturale minore o uguale (maggiore) al valore attribuito a n. In particolare, se una formula contiene una sola variabile libera, allora quella formula definisce un sottoinsieme di $\mathbf{N}$: l'insieme dei numeri naturali che verificano quella formula. Per esempio, la formula $\exists m(m+m = n)$, in cui n è libera e m vincolata, definisce l'insieme dei numeri pari. Se n è l'unica variabile libera nella formula A, scriveremo spesso $A(n)$ anziché A.

Se $X_{A(n)}$ è l'insieme dei numeri naturali definiti dalla formula del primo ordine $A(n)$, in cui n è l'unica variabile libera, il principio di induzione relativo a tale insieme può essere espresso da

$$\mathbf{I}(A(n)) \qquad (A(0) \wedge \forall k(A(k) \to A(\sigma k))) \;\to\; \forall n\, A(n)$$

Questa formula può essere letta come: *se la formula $A(n)$ è vera per $n = 0$ e se, per ogni naturale k, dall'ipotesi che $A(n)$ sia vera per $n = k$ segue che $A(n)$ è vera per $n = \sigma k$, allora $A(n)$ è vera per ogni naturale n.*

Se teniamo presente che i naturali che rendono vera $A(n)$ sono proprio gli elementi di $X_{A(n)}$, vediamo che $\mathbf{I}(A(n))$ è equivalente a

$$(0 \in X_{A(n)} \wedge \forall k\,(k \in X_{A(n)} \to \sigma k \in X_{A(n)})) \to \forall n\,(n \in X_{A(n)})$$

che è l'istanza di N3 in cui $X = X_{A(n)}$.

Definiamo la teoria $\mathcal{T}_1$ del primo ordine per i numeri naturali come la teoria avente come assiomi A1-A6 e tutte le istanze dello *Schema d'Induzione*. Più coincisamente, possiamo dire che gli assiomi di $\mathcal{T}_1$ sono A1-A6 e

(SI): $\mathbf{I}(A(n))$, *per ogni formula $A(n)$ di $\mathcal{L}_1$.*

È importante tener presente che lo Schema d'Induzione SI rappresenta infinite formule e che quindi $\mathcal{T}_1$ è una teoria con infiniti assiomi. Questa teoria è inoltre del primo ordine perché A1-A6 sono formule del primo ordine, così come tutte le formule $\mathbf{I}(A(n))$ considerate nello schema d'assiomi SI.[16]

Se ogni sottoinsieme di N fosse uguale ad $X_{A(n)}$ per un'opportuna formula $A(n)$, lo schema d'assiomi SI risulterebbe equivalente ad N3, ma la seguente proposizione mostra che esistono insiemi X di naturali tali che $X \neq X_{A(n)}$ per ogni formula $A(n)$.

Proposizione 5.1 *Per ogni modello* $\mathbf{N} = \langle N, 0, \sigma, +, \times \rangle$ *di* A1-A6 *e* SI*, l'insieme* $\{X : X \subseteq N\}$ *è più che numerabile, mentre l'insieme* $\{X : X = X_{A(n)}$ *per qualche formula* $A(n)$ *di* $\mathcal{L}_1\}$ *è numerabile.*

Dim. Per dimostrare la prima parte dell'enunciato, mostriamo che N ha un sottoinsieme infinito e che quindi N stesso è infinito[17]. Sia N_0 l'insieme $\{0, \sigma 0, \sigma\sigma 0 \dots\}$, cioè l'intersezione di tutti i sottoinsiemi di N che contengono 0 e sono chiusi per la funzione σ. L'immagine $\sigma(N_0)$ di N_0 tramite σ è ovviamente contenuta in N_0 e, per A2, σ è una biiezione tra N_0 e $\sigma(N_0)$. Per A1, $\sigma(N_0)$ è un sottoinsieme proprio di N_0 perché $0 \notin \sigma(N_0)$. Abbiamo quindi che N_0 è equipotente ad un suo sottoinsieme proprio e quindi è infinito.[18]

La seconda parte dell'enunciato segue dal fatto che l'insieme delle formule di $\mathcal{L}_1$ è numerabile. Ogni formula infatti è una successione finita di oggetti (i simboli del linguaggio) scelti in un insieme numerabile e l'insieme di queste successioni è numerabile. ∎

D'ora in avanti, $\mathbf{N} = \langle N, 0, \sigma, +, \times \rangle$ indicherà un arbitrario modello di A1-A6 e SI, mentre useremo il simbolo $\mathbf{N}_0 = \langle N_0, 0, \sigma \rangle$ per indicare un (o meglio *il*) modello di N1-N3. Poiché la somma ed il prodotto possono essere definiti in $\mathbf{N}_0$ e si dimostra che queste operazioni hanno le solite proprietà, abbiamo che $\mathbf{N}_0$ può essere visto anche come modello $\langle N_0, 0, \sigma, +, \times \rangle$ di A1-A6 e SI.

[16] Si osservi che $\mathcal{T}_1$ soddisfa anche il requisito di decidibilità degli assiomi: per verificare che una formula è un assioma di $\mathcal{T}_1$, basta (che compaia nell'elenco A1-A6, oppure) che abbia la struttura di $\mathbf{I}(A)$ per qualche formula A.

[17] La definizione di insieme infinito usata in questo contesto è quella di Dedekind: un insieme è infinito se e solo se è in corrispondenza biunivoca con un suo sottoinsieme proprio.

[18] È importante osservare che abbiamo dimostrato solo che N_0 è contenuto in N. Come vedremo più avanti la dimostrazione dell'uguaglianza $N_0 = N$ richiede il principio di induzione nella forma forte N3; esistono infatti modelli di A1-A6 e SI in cui N_0 è contenuto propriamente in N.

La Proposizione 5.1 mostra che N3 è più espressivo dello schema d'assiomi SI. La teoria assiomatica $\mathcal{T}_1$ permette tuttavia di sviluppare un frammento molto considerevole dell'aritmetica. Per precisare (informalmente) questo discorso, ci limitiamo a ricordare che, se un programma in un dato linguaggio di programmazione (per esempio, il *Pascal*) determina una funzione f da N_0^k in N_0, allora esiste una formula $A_f(n_1, \ldots, n_k, n)$ di $\mathcal{L}_1$ con $k+1$ variabili libere tale che, dati comunque k numeri naturali $m_1, \ldots, m_k$, se $f(m_1, \ldots, m_k) = m$ e $f(m_1, \ldots, m_k) \neq m'$, allora risulta dimostrabile in $\mathcal{T}_1$ la formula

$$A_f(\overline{m_1}, \ldots, \overline{m_k}, \overline{m}) \ \wedge \ \neg A_f(\overline{m_1}, \ldots, \overline{m_k}, \overline{m'})$$

dove $\overline{m_i}$ indica il termine di $\mathcal{L}_1$ che rappresenta m_i, cioè $\sigma \ldots \sigma 0$ con σ ripetuto m_i volte. Abbiamo cioè che in $\mathcal{T}_1$ possiamo descrivere completamente la funzione f.[19]

La teoria $\mathcal{T}_1$ è una teoria del primo ordine che ha un modello infinito e quindi, per il Teorema di Löwenheim-Skolem, non può essere categorica. Come abbiamo osservato al paragrafo 3, tuttavia, questo teorema non esclude la possibilità che tutti i modelli di una data cardinalità siano isomorfi. In particolare, ci si può chiedere se tutti i modelli di numerabili di $\mathcal{T}_1$ siano isomorfi, cioè se $\mathcal{T}_1$ sia $\aleph_0$-categorica. Se ciò fosse vero, questa teoria, pur avendo modelli di cardinalità arbitraria, avrebbe un unico (a meno di isomorfismi) modello numerabile che quindi dovrebbe essere isomorfo a $\mathbf{N}_0$. Purtroppo, $\mathcal{T}_1$ non è neanche $\aleph_0$-categorica; dimostriamo questo risultato usando il Teorema di Compattezza Semantica (T. 3.13) ed il Teorema di Löwenheim-Skolem.

Consideriamo il linguaggio $\mathcal{L}_1'$ ottenuto aggiungendo un nuovo termine costante, c, ad $\mathcal{L}_1$; nelle formule di $\mathcal{L}_1'$ abbiamo quindi che, oltre a 0 ed alle varibili, può comparire anche c come termine elementare. Sia $\mathcal{N}_0$ l'insieme di tutte le formule di $\mathcal{L}_1$ vere nella struttura $\mathbf{N}_0$ e sia $\mathcal{N}'$ l'insieme di formule di $\mathcal{L}_1'$ definito da

$$\mathcal{N}' \ = \ \mathcal{N}_0 \cup \{\, \overline{m} < c : m \in N_0\}$$

dove $\overline{m} < c$ indica ovviamente la proposizione $\overline{m} \neq c \wedge \exists n(\overline{m} + n = c)$.

[19] Questo risultato è basato sul teorema, dimostrato in molti testi di logica matematica, che asserisce che "ogni funzione ricorsiva è rappresentabile" e su teoremi che stabiliscono l'uguaglianza tra l'insieme delle funzioni ricorsive e l'insieme delle funzioni definibili in qualche linguaggio di programmazione.

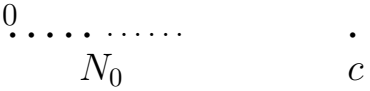
Una struttura $\mathbf{N} = \langle N, 0, \sigma, +, \times \rangle$ diventa una interpretazione del linguaggio $\mathcal{L}_1'$ se indichiamo l'interpretazione del termine c; tale interpretazione sarà un elemento di N che, come abbiamo fatto con la costante 0 e le funzioni σ, $+$, $\times$, indicheremo pure con c (anche se, a rigore, bisognerebbe distinguere tra simbolo del linguaggio e sua interpretazione in una struttura insiemistica). Un'interpretazione di $\mathcal{L}_1'$ diventa un modello di $\mathcal{N}'$ se in essa, per il fissato valore di c, sono vere tutte le formule di $\mathcal{N}'$. In particolare, gli assiomi di $\mathcal{T}_1$ sono formule del primo ordine vere in $\mathbf{N}_0$ e quindi questi assiomi appartengono ad $\mathcal{N}_0$. Da ciò segue che ogni modello di $\mathcal{N}'$ è un modello di $\mathcal{T}_1$.

Le formule di $\mathcal{N}_0$ sono vere nella struttura $\mathbf{N}_0$, ma tale struttura non può essere un modello di $\mathcal{N}'$; l'interpretazione di c, infatti, dovrebbe essere un elemento n di N_0 e quindi la formula $\overline{n} < c$ non può essere vera in $\mathbf{N}_0$ con c interpretato in quel modo.

Dato un qualsiasi sottoinsieme finito $\mathcal{F}$ di $\mathcal{N}'$, tuttavia, la struttura $\mathbf{N}_0$ può essere vista come modello di $\mathcal{F}$. Questo insieme infatti è costituito da un insieme finito $\mathcal{F}_0 \subseteq \mathcal{N}_0$ e da un insieme finito di formule $\{\overline{m_1} < c, \ldots, \overline{m_k} < c\}$. Poiché le formule di $\mathcal{F}_0$ sono vere in $\mathbf{N}_0$, basta interpretare c in un numero naturale maggiore di ogni m_i per avere che tutte le formule di $\mathcal{F}$ sono vere in $\mathbf{N}_0$. Abbiamo quindi che ogni sottoinsieme finito di $\mathcal{N}'$ ha modello e dunque, per il Teorema di Compattezza Semantica, anche $\mathcal{N}'$ avrà un modello $\mathbf{N}'$. Tale modello sarà ovviamente infinito e quindi, per il Teorema di Löwenheim-Skolem, possiamo supporre che sia numerabile. Abbiamo visto sopra che $\mathbf{N}_0$ non può essere un modello di $\mathcal{N}'$; ciò implica in particolare che $\mathbf{N}_0$ e $\mathbf{N}'$ non possono essere isomorfi. Tenendo poi presente che queste due strutture sono modelli di $\mathcal{T}_1$, abbiamo che questa teoria non è $\aleph_0$-categorica. ∎

I modelli di $\mathcal{T}_1$ non isomorfi a $\mathbf{N}_0$ sono chiamati *modelli non-standard* dei naturali. Concludiamo questo paragrafo mostrando alcune interessanti caratteristiche dei modelli di $\mathcal{N}'$. Sia $\mathbf{N}' = \langle N', 0, \sigma, +, \times \rangle$ uno di questi modelli. Osserviamo innanzitutto che $\mathbf{N}'$ contiene una copia di $\mathbf{N}_0$ perché contiene 0 ed è chiuso per l'operazione σ. Come abbiamo visto sopra, l'interpretazione del termine c non può essere un elemento di N_0 ed in particolare abbiamo che $n < c$ per ogni $n \in N_0$. Una prima bozza (incompleta) della struttura $\mathbf{N}'$ è quindi quella della Figura 1.

Figura 1

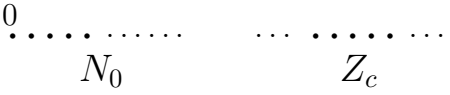


Consideriamo ora le formule

$$\forall n\, \exists n'\, (n' = \sigma n)$$
$$\forall n\, (n \neq 0 \rightarrow \exists n'\, (n = \sigma n'))$$

che asseriscono che ogni elemento ha successore e che ogni elemento diverso da 0 ha predecessore. Queste formule (che appartengono ad $\mathcal{L}_1$) sono vere nella struttura $\mathbf{N}_0$; appartengono quindi ad $\mathcal{N}'$ e devono essere vere in $\mathbf{N}'$. Ciò significa in particolare che in N' possiamo considerare gli elementi $\sigma^{-1}c$ e σc. Questi due elementi non possono appartenere ad N_0 (altrimenti c stesso vi apparterrebbe) e quindi devono essere aggiunti alla Figura 1. Il discorso può ovviamente essere iterato infinite volte ottenendo infiniti nuovi elementi della forma $\sigma^{-1} \ldots \sigma^{-1}c$ e $\sigma \ldots \sigma c$. In definitiva, nella Figura 1, il singolo elemento c deve essere sostituito da un insieme di elementi isomorfo (come insieme ordinato) all'insieme $\mathbf{Z}$ dei numeri interi; indichiamo con Z_c questo insieme.

Figura 2



Consideriamo ora altre due formule del primo ordine vere in $\mathbf{N}_0$ e quindi in $\mathbf{N}'$:

$$\forall n\, \exists n'\, (n' = n + n)$$
$$\forall n\, \exists n'\, (n' + n' = n \ \vee \ n' + n' = \sigma n)$$

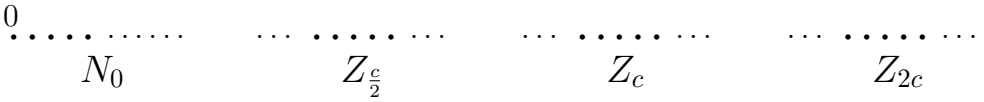
La prima di queste due formule asserisce che il doppio di ogni elemento di N' è in N', mentre la seconda asserisce che ogni elemento o il suo successore può essere diviso per due. In particolare $\mathbf{N}'$ contiene $2c = c + c$ ed un elemento n' tale che $n' + n' = c$, oppure $n' + n' = \sigma c$; indicheremo n' con $\frac{c}{2}$.

Si può dimostrare che il numero $2c$ non può appartenere a Z_c. L'idea intuitiva è ovviamente che, altrimenti, avremmo $c + c = \sigma \ldots \sigma c$ per una opportuna sequenza finita di σ, cioè $c + c = c + m$ con $m \in N_0$, ma da questa uguaglianza seguirebbe $c \in N_0$. Da ciò segue facilmente anche che $2c$

è maggiore di ogni elemento di Z_c. Dobbiamo quindi aggiungere un nuovo elemento, $2c$, alla Figura 2. Anche per questo elemento possiamo considerare l'insieme dei successori e dei predecessori come abbiamo fatto per c e quindi dobbiamo di fatto aggiungere una nuova copia dell'insieme degli interi che indichiamo con Z_{2c}.

Per quanto riguarda $\frac{c}{2}$, si può invece dimostrare che questo elemento non può appartenere né a Z_c né ad N_0, e che ogni elemento di $n < \frac{c}{2} < n'$ per ogni $n \in N_0$ e $n' \in Z_c$ Abbiamo quindi bisogno di un altro insieme isomorfo agli interi che indichiamo con $Z_{\frac{c}{2}}$ e che si trova tra N_0 e Z_c.

Figura 3



A questo punto dovrebbe essere chiaro come si può procedere per dimostrare l'esistenza di ulteriori copie di **Z**. Dato per esempio un qualsiasi elemento x di $Z_{\frac{c}{2}}$ e un elemento y di Z_c abbiamo che dovrà esistere un elemento z di N' tale che $z + z = x + y$ oppure $z + z = \sigma(x + y)$ e questo elemento determinerà una copia di **Z**, diciamo $Z_{\frac{3}{4}c}$ che si troverà tra $Z_{\frac{c}{2}}$ e Z_c.

Alla fine abbiamo che l'insieme N' contiene infinite copie di **Z**, che l'insieme di queste copie è ordinato, e che tale ordine è denso e privo di massimo e minimo. Tenendo poi presente che N' è numerabile, l'ordine delle copie di **Z** sarà pure numerabile e sarà quindi isomorfo all'ordine dell'insieme **Q** dei razionali.