Appunti di Teoria degli Insiemi (08-09)

Lorenzo Carlucci (carlucci@di.uniroma1.it)
Scuola Normale Superiore

Appunti di un corso introduttivo alla Teoria degli Insiemi tenuto presso la Scuola Normale Superiore di Pisa durante l'anno accademico 2008-2009 (rivolto a studenti della Classe di Lettere e della Classe di Scienze).

Il corso e gli appunti del corso sono basati sui seguenti testi.

- Patrick Dehornoy, **Logique et théorie des ensembles**, *Notes de Cours* (`http://www.math.unicaen.fr/ dehornoy/surveys.html`).
- Thomas Jech, **Set Theory**, 2nd edition, Springer-Verlag 1997,
- Kenneth Kunen, **Set Theory - An Introduction to Independence Proofs**, *Studies in Logic and the Foundations of Mathematics*, vol. 102, North-Holland Publishing Company, 1980,
- Azriel Levy, **Basic Set Theory**, Springer-Verlag, Berlin, Heidelberg, New York, 1979,

CAPITOLO 1

Equipotenza e Antisimmetria

1. Premessa

La Teoria degli Insiemi si può avvicinare da due punti di vista: fondazionale (logico-filosofico) e matematico. Nel primo approccio la Teoria degli Insiemi è considerata come una teoria-quadro all'interno della quale è possibile sviluppare in un linguaggio unificato le usuali teorie matematiche (aritmetica, algebra, analisi, topologia etc.). Nel secondo approccio è considerata come una teoria sviluppata per rispondere a dei problemi matematici naturali che si incontrano quando si tenta di sviluppare una *teoria delle quantità infinite*.

Prediligeremo l'approccio matematico, per quanto possibile. La possibilità di trattare quantitativamente l'infinito ha imbarazzato filosofi e matematici per lungo tempo. Già Galilei aveva osservato alcune disarmanti stranezze di un insieme infinito molto naturale, quello dei numeri naturali $0, 1, 2, \dots$. Se associamo al numero n il numero $n+1$, otteniamo il risulato paradossale di un insieme di cose (l'insieme dei numeri $0, 1, 2, \dots$) che ha tanti elementi quanti ne ha una sua parte propria (l'insieme dei numeri $1, 2, 3, \dots$)! Se associamo ad un numero n il numero $2 \cdot n$ otteniamo un simile paradosso con l'aggravante che la parte propria che ha tanti elementi quanti ne ha il tutto ha anche infiniti elementi meno del tutto: ci sono tanti numeri naturali quanti sono i numeri pari, ma oltre ai numeri pari ci sono anche infiniti numeri dispari! Questi e altri paradossi avevano scoraggiato per secoli lo sviluppo di una teoria matematica delle quantità infinite. L'oggetto di queste note è la teoria che ha colmato questa lacuna: la Teoria degli Insiemi, iniziata da Georg Cantor alla fine del secolo XIX.

Cominceremo a sviluppare la teoria in un contesto non assiomatico, dando per scontato (indefinito) il concetto di *insieme* (una collezione di oggetti, completamente definita dai propri elementi). Scriviamo $a \in A$ per indicare che l'oggetto a appartiene a (è un elemento de) l'insieme A, e scriveremo $A \subseteq B$ per indicare che A è un sottinsieme di B, i.e., che ogni elemento di A è anche un elemento di B. Useremo le parentesi graffe per descrivere un insieme, così che $\{a, b, c\}$ denota l'insieme con elementi a, b, c, e $\{a \text{ t.c. } P(a)\}$ denota l'insieme di tutti e soli gli oggetti a che possiedono una certa proprietà P. Per un po' useremo in modo intuitivo anche i concetti di *finito* e *infinito*, chiamando finito un insieme del quale possiamo contare gli elementi con un numero naturale, e infinito ogni altro insieme. Infine useremo liberamente - negli esempi - i numeri naturali, interi, razionali, reali, etc., almeno finché non ne avremo indicate controparti puramente insiemistiche.

2. Equipotenza

Vogliamo gettare le basi di una teoria delle quantità infinite. In particolare vogliamo introdurre concetti che ci permettano di *distinguere* e *confrontare* insiemi

infiniti per grandezza. Partiamo - seguendo Cantor - dal concetto di *equipotenza*. Il concetto di equipotenza estende a insiemi qualunque una proprietà che è facile osservare nel caso di insiemi finiti: due insiemi finiti con lo stesso numero di elementi possono essere messi tra loro in corrispondenza biunivoca. [1]

DEFINIZIONE 2.1 (Equipotenza). Due insiemi A e B si dicono *equipotenti* (o *di stessa cardinalità*) se e solo se esiste tra di loro una corrispondenza biunivoca.

Intuitivamente, due insiemi sono equipotenti se hanno lo stesso 'numero' di elementi. Ci chiediamo ora: il concetto di equipotenza è banale oppure no? Vedremo che la risposta è no, almeno in due sensi, dimostrando che esistono diseguaglianze sorprendenti ed eguaglianze sorprendenti:

(1) Esistono insiemi infiniti non equipotenti, e
(2) Esistono insiemi infiniti che sono intuitivamente uno più grande dell'altro ma si dimostrano essere equipotenti.

Si noterà che i punti qui sopra riguardano solo insiemi infiniti. Per gli insiemi finiti è facile vedere che la nozione di equipotenza cattura il concetto di 'avere lo stesso numero di elementi': gli insiemi di numeri $\{1, \dots, p\}$ e $\{1, \dots, q\}$ sono equipotenti se e soltanto se $p = q$. La preoccupazione principale è dunque questa: la nozione di equipotenza può essere usata come il concetto base di una teoria delle quantità infinite?

Prima di procedere, alcune osservazioni sulle funzioni.

OSSERVAZIONE 2.2. Data una funzione F da A in B, possiamo invertire F ottenendo una funzione da B in A? Per un elemento $b \in B$, definiamo

$$F^{-1}(b) = \{a \in A \text{ t.c. } F(a) = b\}.$$

In generale, $F^{-1}(b)$ può contenere zero, uno o più elementi. Se contiene zero elementi, significa che l'elemento b non è immagine via F di nessun $a \in A$ (ossia b non è nell'immagine $F(A)$ di A via F). Se F è suriettiva, $F^{-1}(b)$ non è vuoto, per ogni $b \in B$ (perché $F(A) = B$ in questo caso). Se F è iniettiva, $F^{-1}(b)$ contiene al massimo un elemento, per ogni $b \in F(A)$.

OSSERVAZIONE 2.3. Se esiste una iniezione di A in B, esiste una suriezione di B su A? Sia F una iniezione di A in B. Ovviamente F è una suriezione di A su $F(A)$ (dove $F(A)$ denota l'insieme delle immagini di elementi di A via F). Pertanto, possiamo facilmente associare iniettivamente una immagine in A ad ogni elemento $b \in F(A)$, basta prendere l'unico elemento di A che viene mandato in b da F. Per ottenere una suriezione di B su A resta dunque da definire una immagine per ogni elemento $b \in B - F(A)$. A questo fine basta scegliere un qualunque elemento di A,

[1] Ricordiamo che una funzione è una legge che associa ad *ogni* elemento di un insieme A (il *dominio*) un *qualche* elemento in un insieme B (il *codominio*). Se F è una tale legge, scriveremo $F : A \to B$. Con $F(A)$ indicheremo l'immagine di A via F, ossia l'insieme di tutti gli elementi di B che si ottengono applicando F a un qualche elemento di A. Una corrispondenza biunivoca (o biiezione) tra A e B è una mappa (funzione) *iniettiva* e *suriettiva* tra A e B. Una mappa F tra A e B è iniettiva (e scriviamo $F : A \to_{in} B$) se non esistono due elementi di A che vengono associati allo stesso elemento di B; una mappa G tra A e B è suriettiva (e scriviamo $G : A \to_{su} B$) se ogni elemento di B è ottenuto come immagine di un elemento di A via G.

chiamiamolo a_0, e mandare tutti i $b \in B - F(A)$ in a_0. Riassumendo, la funzione definita come

$$G(b) := \begin{cases} F^{-1}(b) & \text{se } b \in F(A) \\ a_0 & \text{se } b \in B - F(A) \end{cases}$$

definisce una suriezione di B su A.

Osservazione 2.4. Se esiste una suriezione di A su B, esiste una iniezione di B su A? Sia F una suriezione di A su B. Sappiamo che ogni elemento b di B è immagine via F di *qualche* elemento di A. In generale, più di un elemento di A può avere come immagine lo stesso b (F è supposta suriettiva ma non necessariamente iniettiva). In altri termini, per ogni $b \in B$, l'insieme $F^{-1}(b) = \{a \in A \text{ t.c. } F(a) = b\}$ (detto controimmagine di b via F) contiene in generale più di un elemento. Inoltre, per due diversi $b, b' \in B$, $F^{-1}(b)$ e $F^{-1}(b')$ non hanno elementi in comune (si dice che sono *disgiunti*) perché F è una funzione (non si dà il caso che uno stesso $a \in A$ possa essere mandato da F sia in b che in b'). *Se potessimo scegliere un elemento in ciascun insieme* $F^{-1}(b)$ al variare di b in B, avremmo definito una iniezione di B in A. Vedremo più avanti che la condizione in corsivo è - in generale - tutt'altro che scontata!

3. Diseguaglianze sorprendenti

Diamo una prima dimostrazione della non banalità del concetto di equipotenza, dando due esempi di insiemi infiniti non equipotenti. Diamo due dimostrazioni, una più logica e l'altra più matematica. La prima è essenzialmente equivalente al noto Paradosso di Russell, mentre la seconda sfrutta una delle proprietà che caratterizzano i numeri reali, la Completezza.

Teorema 3.1 (Cantor, Russell). *L'insieme A e l'insieme dei sottinsiemi di A non sono equipotenti.*

Dimostrazione logica. Dato un insieme A, consideriamo l'insieme costituito da tutti i sottoinsiemi di A. Denotiamo un tale insieme con $\mathcal{P}(A)$ e chiamiamolo *insieme delle parti* o *insieme potenza* di A.[2] Per dimostrare il Teorema dimostriamo che *non esiste una mappa suriettiva* di A su $\mathcal{P}(A)$. Ragioniamo per assurdo e supponiamo che esista una tale mappa

$$F : A \to_{su} \mathcal{P}(A).$$

Ogni elemento a di A viene mappato in un sottinsieme di A, $F(a) \subseteq A$. Pertanto, per ogni elemento a di A possono darsi due casi:

i. L'elemento a è un membro dell'insieme $F(a)$, oppure
ii. L'elemento a non è un membro dell'insieme $F(a)$.

Possiamo dunque distinguere gli elementi di A in due tipi: quelli di tipo (i) appartengono alla loro immagine via F, quelli di tipo (ii) non appartengono alla loro

[2]Per esempio, se A è l'insieme $\{a, b, c\}$, i sottinsiemi di A sono $\{a\}$, $\{b\}$, $\{c\}$, $\{a, b\}$, $\{a, c\}$, $\{b, c\}$, $\{a, b, c\}$, a cui aggiungiamo il cosidetto *insieme vuoto*, denotato con $\emptyset$, e definito come l'insieme che non contiene alcun elemento. L'insieme $\mathcal{P}(A)$ è allora l'insieme che contiene come elementi tutti e soli i sottinsiemi di A, i.e., è il seguente insieme di otto elementi: $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

immagine via F. Diamo a questi ultimi il nome mnemonico di *self-avoiding*. Possiamo raccogliere tutti gli elementi di tipo (ii) di A in un insieme, l'insieme degli elementi *self-avoiding*:

$$S = \{a \in A \text{ t.c. } a \notin F(a)\}.$$

L'insieme S è un insieme di elementi di A e pertanto è un elemento di $\mathcal{P}(A)$.

Per ipotesi F è suriettiva (copre tutto $\mathcal{P}(A)$), e dunque sappiamo che *ogni* sottinsieme di A è l'immagine di un elemento di A via F. Per tanto, dato che l'insieme S è un tale sottinsieme, deve esistere un elemento di A, chiamiamolo s, tale che

$$F(s) = S.$$

s è un elemento di A e per tanto è o di tipo (i) o di tipo (ii) (self-avoiding) e non entrambi. Consideriamo queste due possibilità una alla volta.

Supponiamo che s è di tipo (i). Dunque s è un elemento della propria immagine via F, i.e., $s \in F(s)$. Ma $F(s)$ è l'insieme S (per scelta di s) e pertanto (per definizione di S), si ha che $s \notin F(s)$ e s è di tipo (ii).

Abbiamo dimostrato che l'ipotesi che s è di tipo (i) implica che s non è di tipo (i). Pertanto l'ipotesi che s è di tipo (i) deve essere falsa. Allora s è di tipo (ii).

Supponiamo dunque che s è di tipo (ii). Per definizione $s \notin F(s)$. Ma $F(s)$ è S (per scelta di s) e dunque (per definizione di S) si ha che $s \in F$ (altrimenti s sarebbe in S, che è $F(s)$, contro l'ipotesi).

Abbiamo così dimostrato una contraddizione: s non può essere né di tipo (i) né di tipo (ii), ma i tipi (i) e (ii) sono mutualmente esclusivi e coprono tutte le possibilità (ogni elemento di A è di tipo (i) o di tipo (ii)).

Concludiamo che la funzione F non può esistere. □

Diamo ora un'altra dimostrazione, più matematica, dell'esistenza di insiemi infiniti non equipotenti. Questa dimostrazione presuppone la conoscenza di una proprietà dei numeri reali, la cosidetta proprietà di Completezza (o esistenza dell'estremo superiore). Possiamo formularlo così:

> **Completezza:** Ogni insieme non vuoto A di $\mathbf{R}$ limitato superiormente ha un estremo superiore.

Un insieme A è detto *limitato superiormente* se esiste almeno un numero che è $\geq$ di tutti gli elementi di A. Ogni numero con questa proprietà è detto un *maggiorante* di A. L'*estremo superiore* di A è il minimo dei maggioranti di A, ossia un numero s che soddisfa:

- Per ogni a in A, $a \leq s$ (ossia s è un maggiorante di A), e
- Per ogni s', se s' è un maggiorante di A, allora non è più piccolo di s, i.e. $s \leq s'$ (ossia s è il minimo dei maggioranti di A).

Questa proprietà caratteristica dei numeri reali (non è soddisfatta per esempio, dai razionali) è quanto ci serve per dimostrare il seguente Teorema.

Teorema 3.2 (Cantor). *L'insieme dei numeri naturali* $\mathbf{N}$ *e l'insieme dei numeri reali* $\mathbf{R}$ *non sono equipotenti.*

Dimostrazione. Ragioniamo ancora per assurdo. Se si potessero mettere $\mathbf{N}$ e $\mathbf{R}$ in corrispondenza biunivoca, sarebbe allora possibile scrivere $\mathbf{R}$ come un insieme $\{c_0, c_1, c_2, \dots\}$, dove c_i è l'immagine del numero naturale i via l'ipotetica corrispondenza biunivoca (chiariamolo subito: non assumiamo che l'enumerazione sia crescente!). Dimostriamo ora che esiste un numero reale r diverso da ogni c_i.

A tal fine, cominciamo col definire due successioni, una crescente $a_0 < a_1 < \dots$ e una decrescente $b_0 > b_1 > \dots$ tali che ogni b è maggiore di ogni a.

Cominciamo col definire $a_0 := c_0$. Fatto ciò osserviamo che, se aspettiamo abbastanza, troveremo di certo un c_k che cade strettamente a destra di a_0. Perché? Perché per ipotesi i c_i esauriscono la retta reale $\mathbf{R}$ e ci sono infiniti punti da coprire a destra di a_0: è impossibile che tutti i c_i siano minori o uguali ad a_0! Appena troviamo un $c_k > a_0$ (immaginando di scorrere l'insieme $\{c_0, c_1, \dots\}$ da sinistra a destra), lo scegliamo come il nostro b_0. Più formalmente, poniamo

$$b_0 := c_k \text{ per il minimo } k \text{ tale che } a_0 < c_k.$$

Adesso che abbiamo definito un intervallo con estremi a_0 e b_0, se aspettiamo abbastanza, siamo sicuri di trovare, prima o poi, un c_k che cada strettamente tra a_0 e b_0. Siamo anche sicuri di trovare un tale c_k a destra del c_k scelto precedentemente come b_0. Perché? Perché i c_i per ipotesi esauriscono $\mathbf{R}$, e sappiamo che tra a_0 e b_0 esistono infiniti punti! Pertanto è impossibile che tutti gli infiniti c_i rimanenti dopo aver fissato b_0 caschino o a sinistra di a_0 o a destra di b_0. Non appena troviamo un c_k che cade strettamente tra a_0 e b_0, lo scegliamo come il nostro a_1. Più formalmente, poniamo

$$a_1 := c_k \text{ per il minimo } k \text{ tale che } a_0 < c_\ell < b_0.$$

Fatto ciò, procediamo analogamente: aspettiamo il primo c_k che cada tra a_1 e b_0 e lo prendiamo come il nostro b_1. Da notare che scegliamo i nuovi c_k sempre a destra dei c_k scelti precedentemente (gli indici dei c_k scelti crescono sempre, anche se non è vero che crescono i c_k).

Il procedimento si può descrivere succintamente come segue.

- $a_0 := c_0$,
- $b_0 := c_k$, k minimo tale che $a_0 < c_k$,
- $a_{n+1} := c_k$, k minimo tale che $a_n < c_k < b_n$,
- $b_{n+1} := c_k$, k minimo tale che $a_{n+1} < c_k < b_n$

Il procedimento descritto va avanti all'infinito, ossia, per ogni n sono definiti a_n e b_n. Le successioni $\{a_n\}_{n\in\mathbf{N}}$ e $\{b_n\}_{n\in\mathbf{N}}$ hanno le seguenti proprietà:

(1) $a_0 < a_1 < \dots$
(2) $b_0 > b_1 < \dots$
(3) Ogni b_i è (strettamente) maggiore di tutti gli a_j.

In altre parole, l'insieme degli a_n è un insieme di numeri reali limitato superiormente (dai b_n). Pertanto, per la proprietà di Completezza della retta reale, esiste un estremo superiore. Definiamo

$$r := \sup(\{a_0, a_1, \dots\}).$$

r è il minimo dei maggioranti dell'insieme $\{a_0, a_1, \dots\}$. Possiamo ora dimostrare che r è diverso da ogni c_i, ottenendo in tal modo una contraddizione. Diamo uno schizzo della dimostrazione.

Sia $r = c_i$ per un qualche i. Per ogni j $a_j \le c_i$ e $c_i \le b_j$ (perché tutti i b_j sono maggioranti e c_i è il minimo). Dato che gli a_j sono una sequenza strettamente crescente, esiste un j tale che $(a_j = c_k)$ o $(b_j = c_k)$ con $k > i$. Sia j minimo tale e supponiamo che sia $(a_j = c_k)$ (l'altro caso è simmetrico). Allora si hanno due casi per cui c_i - che compare nella enumerazione $\{c_0, c_1, \dots, c_i, \dots, c_k, \dots\}$ a sinistra di c_k - *non è stato scelto* come candidato per a_j: o $c_i \le a_{j-1}$ oppure $c_i \ge b_{j-1}$. Nel primo caso abbiamo che c_i non è un maggiorante di $\{a_j\}_{j\in\mathbf{N}}$, perché $c_i \le a_{j-1} < a_j$.

Nel secondo caso abbiamo che c_i non è il minimo dei maggioranti di $\{a_j\}_{j\in\mathbf{N}}$: infatti abbiamo che $b_{j-1} \leq c_i$ e dunque $b_j < b_{j-1} \leq c_i$, per come sono scelti i b_j. □

OSSERVAZIONE 3.3. Le due dimostrazioni di sopra dimostrano essenzialmente la stessa cosa. Si può infatti dimostrare (e lo faremo più avanti) che esiste una corrispondenza biunivoca tra l'insieme dei reali $\mathbf{R}$ e l'insieme delle parti dei naturali, $\mathcal{P}(\mathbf{N})$.

4. Eguaglianze sorprendenti

Abbiamo visto che non tutti gli insiemi infiniti sono equipotenti. Il concetto di equipotenza è dunque uno strumento non banale per distinguere tra insiemi infiniti. Ma quali intuizioni sulla grandezza degli insiemi sono soddisfatte dal concetto di equipotenza? Dimostreremo qui di seguito che in alcuni casi, il concetto di equipotenza dà luogo a sorprendenti eguaglianze, laddove ci aspetteremo una differenza di grandezza.

Denotiamo con $\mathbf{N}\times\mathbf{N}$ l'insieme costituito da tutte le coppie ordinate di numeri naturali. Per *coppie ordinate* di naturali intendiamo, informalmente, oggetti del tipo (a, b) dove a e b sono numeri naturali e dove l'ordine conta: la coppia $(4, 5)$ è diversa dalla coppia $(5, 4)$. Si può dire che, intuitivamente, esistono più coppie ordinate di naturali di quanti non siano i naturali stessi. Questa intuizione può giustificarsi così: se associamo al numero n la coppia $(n, 0)$ otteniamo una iniezione dei naturali nell'insieme $\mathbf{N}\times\mathbf{N}$. Ovviamente, in questa iniezione non abbiamo usato una infinità di coppie ordinate: solo una piccola parte di $\mathbf{N}\times\mathbf{N}$ è stata sufficiente ad accogliere un'immagine iniettiva di $\mathbf{N}$! Contro questa intuizione di dimostra il seguente Teorema.

TEOREMA 4.1. *L'insieme di tutte le coppie ordinate di numeri naturali è equipotente all'insieme dei numeri naturali.*

DIMOSTRAZIONE. Possiamo organizzare tutte le coppie di numeri naturali nella seguente tabella (infinita a destra e in alto):

⋮	⋮	⋮	⋮	⋮	
(0,4)	(1,4)	(2, 4)	(3,4)	(4,4)	...
(0,3)	(1,3)	(2, 3)	(3,3)	(4,3)	...
(0,2)	(1,2)	(2, 2)	(3,2)	(4,2)	...
(0,1)	(1,1)	(2, 1)	(3,1)	(4,1)	...
(0,0)	(1,0)	(2, 0)	(3,0)	(4,0)	...

Vogliamo dimostrare che è possibile mettere l'insieme di queste coppie in corrispondenza biunivoca con in numeri naturali. A questo fine è sufficiente tracciare un cammino attraverso la tabella in modo tale che (i) vi sia un punto di partenza ben definito, (ii) tutti i punti della tabella vengano toccati una volta e una sola, (iii) per ogni punto del cammino sia determinato un unico punto successivo, (iv) ogni punto del cammino abbia un numero finito di predecessori. Otterremo un tale cammino definendo un ordine tra le coppie.

Un possibile ordine tra le coppie è dato dall'ordine del dizionario, anche detto *ordine lessicografico*. Questo ordine è definito così:

$$(a, b) <_{lex} (c, d) \text{ sse } a < c \text{ oppure } a = c \text{ e } b < c$$

Se adottiamo quest'ordine *non* otteniamo il cammino desiderato. Se volessimo contare le coppie in ordine crescente lessicografico, non otterremmo direttamente una biiezione con i naturali. Per esempio la coppia (1,0) ha infiniti predecessori nell'ordina $<_{lex}$. Cominciando a contare da (0,0), esauriremmo tutti i numeri naturali prima d'essere usciti dalla prima colonna a sinistra della tabella!

Definiamo dunque un altro ordine che ci darà la corrispondenza biunivoca cercata.

$$(a,b) \prec (c,d) \text{ sse } \begin{cases} \max(a,b) < \max(c,d) \\ \max(a,b) = \max(c,d) \text{ e } a < c \\ \max(a,b) = \max(c,d) \text{ e } a = c \text{ e } b < d \end{cases}$$

L'ordine $\prec$ traccia un cammino con le proprietà desiderate lungo la tabella di tutte le coppie ordinate di naturali. Possiamo contare le coppie partendo dalla coppia minima secondo l'ordine $\prec$, che è $(0,0)$ e contando in ordine crescente seguendo $\prec$:

$$(0,0),(0,1),(1,0),(1,1),(0,2),(1,2),(2,0),(2,1),(2,2),(0,3),(1,3),(2,3),\ldots$$

□

Abbiamo dimostrato che due insiemi che a prima vista hanno grandezze diverse sono in realtà equipotenti. Come corollario del risultato precedente potremo ottenere una eguaglianza ancora più sorprendente: $\mathbf{N}$ è equipotente all'insieme dei numeri razionali, $\mathbf{Q}$. Cominciamo con alcune osservazioni.

Osservazione 4.2. Possiamo rappresentare o definire i numeri razionali come un insieme di coppie ordinate di naturali:

$$\mathbf{Q} = \{(a,b) \text{ t.c. } a,b \in \mathbf{N} \text{ e } b \neq 0 \text{ e } a,b \text{ sono relativamente primi}\}.$$

L'idea è ovvia: una coppia ordinata (a,b) rappresenta la frazione $\frac{a}{b}$, e considerando solo gli a,b relativamente primi evitiamo di contare due volte frazioni identiche come $\frac{a}{b}$, $\frac{2\cdot a}{2\cdot b}$, $\frac{3\cdot a}{3\cdot b}$, etc.

Osservazione 4.3. Con la definizione precedente otteniamo immediatamente una mappa iniettiva $\mathbf{Q} \to \mathbf{N}\times\mathbf{N}$ (questa iniezione è una inclusione se *identifichiamo* $\mathbf{Q}$ con l'insieme delle coppie di naturali descritto nella Osservazione precedente). Componendo questa mappa con una delle biiezioni esistenti tra $\mathbf{N}\times\mathbf{N}$ e $\mathbf{N}$, otteniamo una iniezione di $\mathbf{Q}$ in $\mathbf{N}$. Questo fatto è in un certo senso contro-intuitivo: una iniezione è una mappa rigida nel senso che non assegna la stessa immagine a due elementi. Intuitivamente dunque, l'esistenza di una iniezione di un insieme in un altro, sembra indicare che il primo insieme *non ha più elementi del secondo.* Nel nostro caso, che $\mathbf{Q}$ non ha più elementi di $\mathbf{N}$.

Osservazione 4.4. D'altro canto, è ovvio che esiste una iniezione di $\mathbf{N}$ in $\mathbf{Q}$ (ogni numero naturale è un razionale), per es. la mappa $n \mapsto (n,1)$.

Osservazione 4.5. Abbiamo dunque la seguente situazione:

$$\exists F : \mathbf{Q} \to_{in} \mathbf{N}\times\mathbf{N};\ \exists G : \mathbf{N}\times\mathbf{N} \to_{bi} \mathbf{N};\ \exists H : \mathbf{N} \to_{in} \mathbf{Q}$$

In altre parole:

- Esiste una iniezione di $\mathbf{Q}$ in $\mathbf{N}$ (componendo F e G), e
- Esiste una iniezione di $\mathbf{N}$ in $\mathbf{Q}$ (l'iniezione banale H).

Intuitivamente questo significa che

- **Q** non ha più elementi di **N**, e
- **N** non ha più elementi di **Q**.

Se davvero l'esistenza di un'iniezione corrispondesse al concetto intuitivo di *non avere più elementi di*, dovremmo poter concludere che **N** e **Q** hanno *lo stesso numero di elementi*!

In generale la domanda è questa:

> Se esiste una iniezione da A in B e una iniezione da B in A, esiste una biiezione tra A e B (A e B sono equipotenti)?

Vedremo che è proprio così!

5. Il Teorema di Cantor-Bernstein

TEOREMA 5.1 (Cantor-Bernstein). *Se A si inietta in B e B si inietta in A allora A e B sono equipotenti.*

DIMOSTRAZIONE. Le nostre ipotesi sono:

- $\exists F : A \to_{in} B$
- $\exists G : B \to_{in} A$

Consideriamo i seguenti insiemi

- $C = G(B)$ (l'immagine di B via G). C è un sottinsieme di A.
- $D = G(F(A))$ (l'immagine di $F(A)$ via G). D è un sottinsieme di C.

Abbiamo dunque le seguenti relazioni tra D, C e A:

$$D \subseteq C \subseteq A$$

Anche, osserviamo che D e A sono equipotenti: la funzione composta $F * G$ è una biiezione tra D e A (dimostrarlo per esercizio). Chiamiamo H tale funzione. Usiamo H per definire una biiezione di A su C. Questo è sufficiente a dimostrare il Teorema, dato che B e C sono equipotenti (C è il risultato ottenuto da B applicando l'iniezione G).

Cerchiamo di definire la suriezione $A \to C$ in modo tale da muovere il minor numero di elementi di A. Dato che l'immagine desiderata è C, non abbiamo bisogno di muovere gli elementi di C. Consideriamo allora gli elementi di $A - C$ (l'insieme degli elementi di A che non sono in C). Possiamo usare H per assegnare a questi elementi una immagine in C: mandiamo dunque $A - C$ in $H(A - C)$. Ciò fatto, abbiamo preso il posto degli elementi di $H(A-C)$, che sono pure elementi di A e che pertanto devono avere assegnata un'immagine dalla funzione che stiamo definendo. La funzione deve essere iniettiva e pertanto non possiamo lasciare fermi gli elementi in $H(A - C)$, dato che li abbiamo usati come immagini degli elementi di $A - C$! Che fare? Spostiamoli ancora usando H: mandiamo $H(A - C)$ in $H(H(A - C))$. Definiamo la nostra corrispondenza biunivoca tra A e C come segue:

$$J(a) := \text{ sse } \begin{cases} H(a) & \text{se } a \text{ appartiene a } H^n(A - C) \text{ per qualche } n \in \mathbf{N}, \\ a & \text{se } a \text{ non appartiene a } H^n(A - C) \text{ per nessun } n \in \mathbf{N} \end{cases}$$

Dimostriamo che J è iniettiva e suriettiva.

J è suriettiva: possiamo descrivere l'immagine di A via J come l'unione di ciò che otteniamo nei due casi della definizione di J. Gli elementi a che sono in $A - C$,

$H(A-C)$, $H(H(A-C))$, ... vengono mandati in $H(a)$, cosicché otteniamo che una parte dell'immagine di A via J è $H(\bigcup_{n=0} H(A-C)$ (dove $\bigcup_{n=0} H(A-C)$ denota $H(A-C) \cup H^2(A-C) \cup H^3(A-C) \cup \dots$). Tutti gli altri elementi di A, ossia gli a che non sono in nessuno degli insiemi $H(A-C)$, $H^2(A-C)$, $H^3(A-C)$,... (e che dunque non sono nell'unione $H(A-C) \cup H^2(A-C) \cup H^3(A-C) \cup \dots$), non vengono mossi, cosicché otteniamo che l'altra parte dell'immagine di A via J è $A - \bigcup_{n=0} H^n(A-C)$ (tutto ciò che non è in $\bigcup_{n=0} H^n(A-C)$). Per tanto, abbiamo quanto segue:

$$\begin{aligned} J(A) &= A - \textstyle\bigcup_{n=0} H^n(A-C) \cup H(\bigcup_{n=0} H(A-C)) \\ &= A - \textstyle\bigcup_{n=0} H^n(A-C) \cup \bigcup_{n=0} H(H(A-C) \\ &= A - \textstyle\bigcup_{n=0} H^n(A-C) \cup \bigcup_{n=1} H(A-C) \\ &= A - (H^0(A-C) \cup \textstyle\bigcup_{n=1} H(A-C)) \cup \bigcup_{n=1} H(A-C) \\ &= A - H^0(A-C) \\ &= A - (A-C) \\ &= C \end{aligned}$$

J è iniettiva: J è ottenuta incollando insieme due funzioni iniettive, i.e., l'identità e H. L'identità è usata sull'insieme $A - \bigcup_{n=0} H^n(A-C)$, mentre H è usata sull'insieme $\bigcup_{n=0} H(A-C)$, pertanto le due funzioni sono applicate a due insiemi disgiunti. Inoltre, le immagini delle due funzioni sono anch'esse disgiunte in questo caso: si tratta di $A - \bigcup_{n=0} H^n(A-C)$ e $\bigcup_{n=1} H(A-C)$. Pertanto, la funzione J è iniettiva (dimostrare per esercizio). □

6. Applicazioni del Teorema di Cantor-Bernstein

Possiamo ottenere come Corollari del Teorema di Cantor-Bernstein alcune identità sorprendenti, completando osservazioni abbozzate più sopra. Abbiamo osservato sopra che

(1) Esiste una iniezione di $\mathbf{Q}$ in $\mathbf{N}$, e
(2) Esiste una iniezione di $\mathbf{N}$ in $\mathbf{Q}$.

Dal Teorema di Cantor-Bernstein concludiamo immediatamente che $\mathbf{Q}$ e $\mathbf{N}$ sono equipotenti!

Allo stesso modo possiamo dimostrare che l'insieme delle coppie ordinate di numeri reali, che denotiamo con $\mathbf{R} \times \mathbf{R}$ è equipotente all'insieme dei numeri reali. Abbiamo infatti osservato sopra (senza dimostrazione) che

$$\exists F : \mathbf{R} \to_{bi} \mathcal{P}(\mathbf{N})$$

Pertanto abbiamo

$$\exists G : \mathbf{R} \times \mathbf{R} \to_{bi} \mathcal{P}(\mathbf{N}) \times \mathcal{P}(\mathbf{N})$$

dove $\mathcal{P}(\mathbf{N}) \times \mathcal{P}(\mathbf{N})$ denota l'insieme delle coppie ordinate di sottinsiemi di $\mathbf{N}$. Per ottenere G basta definire $G(r,s) = (F(r), F(s))$. D'altra parte si può dimostrare che l'insieme delle coppie ordinate di sottinsiemi di $\mathbf{N}$ si inietta nell'insieme dei

sottinsiemi delle coppie ordinate di $\mathbf{N}$ [3], ossia che

$$\exists H : \mathcal{P}(\mathbf{N}) \times \mathcal{P}(\mathbf{N}) \rightarrow_{in} \mathcal{P}(\mathbf{N} \times \mathbf{N})$$

Ma sappiamo che $\mathbf{N} \times \mathbf{N}$ è in biiezione con $\mathbf{N}$, e pertanto

$$\exists I : \mathcal{P}(\mathbf{N} \times \mathbf{N}) \rightarrow_{bi} \mathcal{P}(\mathbf{N}).$$

Mettendo insieme le osservazioni qui sopra, abbiamo che

$$\exists J : \mathbf{R} \times \mathbf{R} \rightarrow_{in} \mathcal{P}(\mathbf{N})$$

e dunque

$$\exists K : \mathbf{R} \times \mathbf{R} \rightarrow_{in} \mathbf{R}.$$

D'altro canto, è ovvio che $\mathbf{R}$ si inietta in $\mathbf{R} \times \mathbf{R}$ (per es. con la mappa $r \mapsto (r, 0)$ e dunque

$$\exists L : \mathbf{R} \rightarrow_{in} \mathbf{R} \times \mathbf{R}$$

Per il Teorema di Cantor-Bernstein, da $\mathbf{R} \times \mathbf{R} \rightarrow_{in} \mathbf{R} \rightarrow_{in} \mathbf{R} \times \mathbf{R}$ concludiamo:

$$\exists M : \mathbf{R} \rightarrow_{bi} \mathbf{R} \times \mathbf{R}.$$

7. Conclusione

Il Teorema di Cantor-Bernstein è un ingrediente importante per lo sviluppo di una teoria delle quantità infinite. Ci dice infatti che le nozioni di equipotenza e di iniezione si comportano in modo simile alle nozioni d'ordine tra i numeri: l'equipotenza corrisponde a $=$ (stesso numero di elementi), e l'iniezione a $\leq$ (non avere più elementi di). Con questa interpretazione, il Teorema di Cantor-Bernstein ci dice che vale la legge di antisimmetria:

$$A \leq B \leq A \Rightarrow A = B,$$

sostituendo $\rightarrow_{in}$ a $\leq$ e $\rightarrow_{bi}$ a $=$. Un'altra proprietà immediata è la transitività:

$$A \rightarrow_{in} B \rightarrow_{in} C \Rightarrow A \rightarrow_{in} C$$

Una proprietà essenziale delle usuali relazioni tra numeri (siano essi naturali, razionali o reali) è la totalità dell'ordinamento. In $\mathbf{N}$, $\mathbf{Q}$, $\mathbf{R}$ etc. si ha che

$$\text{Per ogni } a, b \ \ (a \leq b \text{ oppure } b \leq a).$$

Vale una stessa proprietà per la relazione d'ordine indotta da equipotenza ed iniezione? Ossia, vale che

$$\text{Per tutti gli insiemi } A, B \ \ (A \rightarrow_{in} B \text{ oppure } B \rightarrow_{in} A)?$$

[3]Esercizio: dimostrare che la mappa H definita come segue è una tale iniezione. Per $X \subseteq \mathbf{N}$ definisco $X^+ := \{x + 1 \text{ t.c. } x \in X\}$, se $X \neq \varnothing$ e $X^+ := \{0\}$ se $X = \varnothing$. Definisco H come la seguente mappa, per $S, T \subseteq \mathbf{N}$:

$$(S, T) \mapsto \{(s, t) \text{ t.c. } s \in S^+ \wedge t \in T^+\}$$

CAPITOLO 2

Buoni Ordini e Comparabilità

1. Sinossi

Abbiamo concluso la lezione precedente chiedendoci se, dati due insiemi A e B qualunque, fosse sempre possibile compararli, ossia ordinarli, rispetto alla relazione d'ordine indotta dall'esistenza di una iniezione tra un insieme e l'altro. In altre parole, dati A e B, è vero che

$$\exists F : A \rightarrow_{in} B \quad \text{oppure } \exists G : B \rightarrow_{in} A?$$

Per rispondere a questa domanda ci troviamo costretti a fare un *détour*: sposteremo la nostra attenzione dagli insiemi in generale agli insiemi ordinati, e infine a un tipo particolare di insieme ordinato: gli insiemi *bene ordinati*. Vedremo come stabilire un risultato di comparabilità per questa nozione più ristretta.

2. Ordini e buoni ordini

Se consideriamo gli insiemi finiti (ossia quelli insiemi che sono in corrispondenza biunivoca con un segmento iniziale di $\mathbf{N}$), è facile osservare che vale un risultato di comparabilità:

Per A, B insiemi finiti, A si inietta in B o B si inietta in A.

Infatti, se A è in biiezione con $\{0, \ldots, q\}$ e B in biiezione con $\{0, \ldots, p\}$, abbiamo che $A \rightarrow_{in} B$ se $q \leq p$ e $B \rightarrow_{in} A$ se $p \leq q$. Se consideriamo inoltre che è sempre possibile ordinare totalmente un insieme finito (per esempio usando l'ordine ereditato dalla biiezione dell'insieme con un segmento iniziale di $\mathbf{N}$), vediamo che vale qualcosa di più, ossia

- A è in biiezione con un segmento iniziale proprio di B, oppure
- B è in biiezione con un segmento iniziale proprio di A, oppure
- A e B sono equipotenti.

In altre parole l'insieme dei numeri naturali costituisce un insieme di *rappresentanti canonici* per le quantità finite: ogni insieme finito è in biiezione con un segmento iniziale di $\mathbf{N}$ e per tanto ogni coppia di quantità finite è comparabile usando l'ordine naturale dei numeri naturali. Due insiemi finiti hanno lo stesso rappresentante canonico se e solo se hanno lo stesso numero di elementi. Vedremo di seguito come la nozione di buon ordine ci permetta di estendere questa situazione a insiemi arbitrari, anche infiniti.

Introduciamo, per cominciare, un po' di terminologia sulle relazioni d'ordine.

DEFINIZIONE 2.1 (Ordini Parziali e Totali). Sia A un insieme e R una relazione binaria su A[1]. R è un *ordine parziale* su A se valgono le proprietà di

1 IRRIFLESSIVITÀ: Per ogni $a \in A$, non vale aRa.
2 TRANSITIVITÀ: Per ogni $a, b, c \in A$, se vale aRb e vale bRc, allora vale aRc.

R è detta *ordine totale* se è un ordine parziale e vale la proprietà di

3 COMPARABILITÀ: Per ogni $a, b \in A$, aRb o bRa o $a = b$.

Dato un insieme A, un elemento $a \in A$ e una relazione d'ordine R su A, indichiamo con A_a la *sezione* di A *determinata* da a, i.e., l'insieme definito come segue.

$$A_a := \{x \in A \text{ t.c. } xRa\}.$$

ESEMPIO 2.2. Gli ordini abituali sugli insiemi $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$ e $\mathbf{R}$ sono tutti ordini totali.

Concentriamoci ora su alcune proprietà caratteristiche dell'ordine $<$ sui naturali.

(1) **Principio del Minimo Numero**: Sia S un insieme non vuoto di numeri naturali. Allora esiste un minimo numero naturale contenuto in S. In altre parole esiste $s_0 \in S$ tale che per ogni $s \in \mathbf{N}$ non vale $(s < s_0 \& s \in S)$.
(2) **Principio di Induzione**: Sia P una proprietà dei numeri naturali $\mathbf{N}$. Supponiamo che, per un qualunque numero n, se P vale di tutti i numeri più piccoli di n (di tutti gli $m < n$) allora P vale anche di n. Allora P vale di tutti i numeri naturali.
(3) **Principio del Successore Immediato**: Sia S un sottinsieme di $\mathbf{N}$ strettamente limitato (ossia tale che esista un $n \in \mathbf{N}$ tale che, per ogni $s \in S$, $s < n$). Allora esiste un *successore immediato* di S. Più formalmente, diciamo che esiste l'*estremo superiore stretto* di S, definito come il *minimo dei maggioranti stretti* di S. I.e., esiste un $s^* \in \mathbf{N}$ tale che, per ogni $s \in S$, $s < s^*$, e, per ogni $s' \in \mathbf{N}$ maggiore di tutti gli S, non vale $s' < s^*$ (ossia vale $s^* \leq s$), perché $<$ è un ordine totale).

Otteniamo il concetto di buon ordinamento generalizzando le proprietà di $\mathbf{N}$ qui sopra osservate.

DEFINIZIONE 2.3 (Buon Ordinamento). Un insieme A si dice *bene ordinato* da una relazione binaria R (e la coppia (A, R) si dice un buon ordine) se R è un ordine totale su A che soddisfa il Principio del Minimo Numero, ossia tale che, per ogni sottinsieme S di A non vuoto, esiste un $s_0 \in S$ tale che per ogni $s \in S$ non vale sRs_0.

OSSERVAZIONE 2.4. Gli ordini abituali su $\mathbf{Z}$, $\mathbf{Q}$ e $\mathbf{R}$ non sono buoni ordinamenti. Si indicano facilmente sottinsiemi non vuoti senza elemento minimo. Ciò non significa che non sia possibile definire altri ordinamenti degli stessi insiemi numerici che siano buoni ordinamenti.

Mostriamo, per cominciare, che su un buon ordinamento vale il Principio di Induzione.

[1]Ossia R è una relazione che riguarda coppie di elementi di A. Scrviamo aRb per indicare che la relazione R vige tra gli elementi a e b di A, analogamente a quando scriviamo $m < n$ per indicare che m e n stanno nella relazione $<$.

PROPOSIZIONE 2.5. *Se (A, R) è un buon ordinamento allora vale il Principio di Induzione.*

DIMOSTRAZIONE. Si (A, R) un buon ordinamento e sia P una proprietà. Supponiamo che P soddisfi le ipotesi del Principio di Induzione, ossia che, per ogni $a \in A$, se P vale di tutti i b tali che bRa allora P vale di a. Supponiamo per assurdo che P non valga di tutti gli $a \in A$. Allora l'insieme

$$S := \{a \in A \text{ t.c. } \neg P(a)\}$$

è non vuoto. Per tanto possiede un minimo, chiamiamolo s. Allora s è tale che ogni s' minore di s soddisfa P. Per ipotesi su P, questo implica che s soddisfa P, il che è impossibile per definizione di S. □

Mostriamo adesso che il Principio del Minimo Numero è equivalente al Principio del Successore Immediato. La prima definizione di buon ordine, data da Cantor nel 1883, era basata su quest'ultimo principio. Cantor definiva (A, R) bene ordinato se il Principio del Successore Immediato è soddisfatto.

PROPOSIZIONE 2.6. *(A, R) è un buon ordinamento se e soltanto se vale il Principio del Successore Immediato, ossia se e soltanto se ogni sottinsieme di A strettamente limitato ha un estremo superiore stretto.*

DIMOSTRAZIONE. Supponiamo che (A, R) sia un buon ordinamento. Sia B un sottinsieme di A strettamente limitato. Dimostriamo che esiste in A un minimo estremo superiore stretto (un successore immediato) di B. Consideriamo l'insieme dei maggioranti stretti di B, ossia

$$C := \{a \in A \text{ t.c } \forall b \in B(bRc)\}.$$

C è non vuoto perché per ipotesi B è strettamente limitato. Dunque C ha un minimo. Sia c il minimo di C. Si vede facilmente che c è il minimo estremo superiore stretto di B, ossia il minimo elemento di A ad essere strettamente maggiore di tutti i $b \in B$.

Supponiamo ora che ogni sottinsieme strettamente limitato di (A, R) ha un estremo superiore stretto. Sia B un sottinsieme non vuoto di A. Dimostriamo che B ha un minimo in A. Consideriamo l'insieme C degli elementi di A minori di tutti gli elementi di B, i.e. poniamo

$$C := \{a \in A \text{ t.c } \forall b \in B(cRb)\}.$$

(N.B. C può essere vuoto). C è strettamente limitato (ogni $b \in B$ è un limite stretto). Per tanto, esiste un successore immediato di C in A. Sia s tale successore. Dimostriamo che s è il minimo di B.

Per prima cosa mostriamo che non esiste $b \in B$ tale che bRs. Se esistesse, s non sarebbe il minimo estremo superiore di C, perché b sarebbe più piccolo di s ma più grande di ogni $c \in C$ (per definizione di C). Mostriamo ora che $s \in B$. Altrimenti, per ogni $b \in B$, si avrebbe $s \neq b$. Ma abbiamo mostrato sopra che non esiste $b \in B$ tale che bRs. Dato che R è un ordine totale su A, si avrebbe dunque che per ogni $b \in B$, sRb. Dunque s apparterrebbe a C, il che è impossibile, dato che s è strettamente maggiore di ogni $c \in C$. Per tanto, $s \in B$, ed è il minimo di B. □

OSSERVAZIONE 2.7. Nella dimostrazione di sopra è essenziale che il principio del successore immediato sia formulato in modo da applicarsi ad ogni insieme strettamente limitato, compreso l'insieme vuoto. L'insieme vuoto, che denotiamo con il simbolo $\emptyset$, è strettamente limitato (a vuoto) da ogni elemento di a. Infatti vale a vuoto la seguente implicazione, che ha l'antecedente sempre falso.

$$(\forall a \in A)(\forall x)[x \in \emptyset \Rightarrow xRa].$$

Se si limitasse il principio del successore immediato a insiemi non vuoti, la dimostrazione di sopra si applicherebbe anche a $\mathbf{Z}$, che invece non è un buon ordinamento. Si vede facilmente, infatti, che ogni sottinsieme non vuoto e strettamente limitato in $\mathbf{Z}$ ha un successore immediato. Al contratio, l'insieme vuoto non ha un successore immediato in $\mathbf{Z}$, perché ogni $z \in \mathbf{Z}$ è maggiore (a vuoto) di ogni elemento dell'insieme vuoto, ma non esiste un minimo $z \in \mathbf{Z}$!

3. Isomorfismi e Comparabilità

Abbiamo spostato l'attenzione dagli insiemi agli insiemi ordinati. Per tanto è naturale sostituire l'equipotenza come criterio di comparazione tra insiemi con una nozione più fine, che tenga conto delle strutture d'ordine degli insiemi che intendiamo mettere a confronto. La nozione naturale per esprimere una somiglianza stretta tra due strutture ordinate (A, R) e (B, S) è l'isomorfismo, che definiamo come segue.

DEFINIZIONE 3.1 (Isomorfismo d'Ordine). Siano (A, R) e (B, S) due insiemi totalmente ordinati. Una funzione F da A in B è un *isomorfismo* tra (A, R) e (B, S) se

(1) F è una biiezione tra A e B, e
(2) Per ogni $a, a' \in A$, se aRa' allora $F(a)SF(a')$.

In breve, un isomorfismo tra due insiemi ordinati è una corrispondenza biunivoca che conserva l'ordine: se a è minore di a' in A, allora l'immagine di a è minore dell'immagine di a' in B. Scriviamo $(A, R) \cong (B, S)$ per indicare che esiste un isomorfismo tra (A, R) e (B, S).

ESEMPIO 3.2. Ogni traslazione $x \mapsto x + k$, $x \mapsto x - k$, è un isomorfismo dell'insieme $\mathbf{Z}$ dei numeri interi sull'insieme stesso. Analogamente, ogni traslazione $x \mapsto x - k$ è un isomorfismo dell'insieme $\mathbf{Z}^-$ degli interi negativi su una sua sezione. Notare che $(\mathbf{Z}, <)$ non è bene ordinato. Vedremo di seguito che gli insiemi ordinati non ammettono isomorfismi su una propria sezione.

OSSERVAZIONE 3.3. Se F è un isomorfismo tra (A, R) e (B, S), allora F^{-1} è un isomorfismo tra (B, S) e (A, R).

Dimostriamo ora due Lemmi utili a stabilire il risultato di comparabilità per buoni ordini.

LEMMA 3.4. *Nessun insieme bene ordinato (A, R) è isomorfo a una propria sezione.*

DIMOSTRAZIONE. Sia (A, R) un buon ordine e sia, per assurdo, F un isomorfismo di A su una sezione A_a di A, per un qualche $a \in A$. A priori possiamo dire che esistono due tipi di elementi di A:

(1) Gli elementi di a che vengono mossi da F, i.e., t.c. $F(a) \neq a$, e

(2) Gli elementi di a che non vengono mossi da F, i.e., t.c. $F(a) = a$.

Consideriamo l'insieme di tutti gli elementi di primo tipo, ossia

$$S := \{a \in A \text{ t.c. } F(a) \neq a\}.$$

S è un insieme non vuoto, perché altrimenti F è l'identità. R è un buon ordine, e per tanto S ha un minimo, sia s. Per definizione di S, si ha $F(s) \neq s$. Dato che R è un ordine totale, abbiamo due possibilità.

(i) $F(s)Rs$: Applicando di nuovo F otteniamo $F(F(s))RF(s)$, perché F è un isomorfismo. Per tanto, abbiamo trovato un elemento, $F(F(s))$, R-minore di $F(s)$, e ciò non ostante appartenente all'insieme S, contro la minimalità di s.

(ii) $sRF(s)$: Applicando l'inversa di F, otteniamo $F^{-1}(s)RF^{-1}(F(s))$, ossia $F^{-1}(s)Rs$. Allora $F^{-1}(s)$ è un elemento R-minore di s che appartiene ad S (perché $F(F^{-1}(s)) \neq F^{-1}(s)$), contro la minimalità di s.

□

LEMMA 3.5. *Se (A, R) e (B, S) sono insiemi bene ordinati isomorfi, esiste un unico isomorfismo tra loro.*

DIMOSTRAZIONE. Supponiamo per assurdo che (A, R) e (B, S) siano bene ordinati e che F e G siano due isomorfismi distinti tra (A, R) e (B, S). Possiamo distinguere a priori tra due tipi di elementi di A:

(1) Gli elementi di a sui quali F e G coincidono, e
(2) Gli elementi di a sui quali F e G non coincidono.

Consideriamo gli elementi del secondo tipo, definendo

$$S := \{a \in A \text{ t.c. } F(a) \neq G(a)\}.$$

L'insieme S è non vuoto (altrimenti F e G sono la stessa funzione). Per tanto, S ha un minimo. Sia s il minimo di S. Dato che $F(s) \neq G(s)$, e poiché S è un ordine totale su B, si hanno solo due casi.

(i) $F(s)SG(s)$: $F(s)$ è un elemento di B. Poiché G è un isomorfismo, $F(s)$ è anche l'immagine via G di un elemento di A. Sia $a \in A$ tale che $G(a) = F(s)$. Allora abbiamo $G(a)SG(s)$ e pertanto (G è un isomorfismo), si ha aRs. Dunque a è R-minore di s. Ma F è un isomorfismo, e dunque aRs implica $F(a)SF(s) = G(a)$, e dunque $F(a) \neq G(a)$. Per tanto abbiamo trovato un elemento R-minore di s e appartenente a S, contro la minimalità di s.

(ii) $G(s)SF(s)$: analogo (per esercizio).

□

COROLLARIO 3.6. *Se (A, R) è bene ordinato, l'unico isomorfismo di (A, R) su se stesso è l'identità.*

Concludiamo dimostrando che, dati due insieme bene ordinati, uno è sempre isomorfo a una sezione dell'altro.

TEOREMA 3.7 (Comparabilità dei Buoni Ordini). *Siano (A, R) e (B, S) due insiemi bene ordinati. Allora vale una e una sola delle seguenti:*

(1) *Esiste $b \in B$ tale che (A, R) è isomorfo a (B_b, S), o*
(2) *Esiste $a \in A$ tale che (A_a, R) è isomorfo a (B, S), o*

(3) (A, R) *e* (B, S) *sono isomorfi.*

Dimostrazione. Definiamo una relazione F tra elementi di A ed elementi di B ponendo che $a \in A$ e $b \in B$ sono nella relazione F se e solo se A_a e B_b sono isomorfi.

$$aFb \text{ se e solo se } A_a \cong B_b.$$

A priori, F non definisce neppure una funzione tra A e B[2], ma mostriamo subito che, di fatto, F è una funzione. Mostreremo poi che F è un isomorfismo tra il proprio dominio e la propria immagine. Infine, mostreremo che solo i casi (1), (2), (3) sono possibili.

F è una funzione: siano $b, b' \in B$, $a \in A$ tali che aFb e aFb'. Allora A_a è isomorfo a B_b e anche a $B_{b'}$. Per tanto, B_b e $B_{b'}$ sono isomorfi tra loro. Se bSb' allora $A_b = (A_{b'})_b$ è una sezione di $A_{b'}$. Se $b'Sb$ allora $A_{b'} = (A_b)_{b'}$ è una sezione di A_b. Allora avremmo un buon ordinamento ($A_{b'}$ o A_b) isomorfo a una propria sezione, contro il Lemma 3.4. Poiché F è una funzione, siamo autorizzati a scrivere $F(a) = b$ invece di aFb e a parlare del dominio di F (i.e. l'insieme degli $a \in A$ ai quali F associa un $b \in B$) e dell'immagine di F, $F(A)$ (ossia l'insieme dei $b \in B$ ottenuti come immagini di F applicata a qualche $a \in A$).

Il dominio di F è chiuso all'ingiù, ossia se a è nel dominio di F, e $a' \in A$ è tale che $a'Ra$, allora anche a' è nel dominio di F. Se a è nel dominio di F, esiste un $b \in B$ tale che $A_a \cong B_b$. Si osserva facilmente che la restrizione di F alla sezione $(A_a)_{a'}$ è un isomorfismo su $(B_b)_{F(a')}$, ossia $A_{a'} \cong B_{F(a')}$.

Analogamente si osserva che *l'immagine di F è chiusa all'ingiù*, ossia se $b \in B$ è nell'immagine di F, e $b' \in B$ è tale che $b'Sb$, allora anche b' è nell'immagine di F. Se b è nell'immagine di F, esiste un $a \in A$ tale che $A_a \cong B_b$, e si può argomentare analogamente a sopra.

F è iniettiva sul suo dominio. Supponiamo infatti che esistano $a, a' \in A$, a, a' nel dominio di F, e $b \in B$ tali che $F(a) = b = F(a')$. Allora $A_a \cong B_b \cong A_{a'}$ e si ottiene una contraddizione come sopra (poiché aRa' oppure $a'Ra$).

F è un isomorfismo tra il suo dominio e la sua immagine. Mostriamo che aRa' implica $F(a)SF(a')$, se $a' \in A$ è nel dominio di F. Poiché F è iniettiva abbiamo $F(a) \neq F(a')$. dunque si ha $F(a)SF(a')$ oppure $F(a')SF(a)$. Supponiamo $F(a')SF(a)$. Allora abbiamo $A_a \cong B_{F(a)}$ e $A_{a'} \cong B_{F(a')}$. Ma $A_a = (A_{a'})_a$ è una sezione di $A_{a'}$ e $B_{F(a')} = (B_{F(a)})_{F(a')}$ è una sezione di $B_{F(a)}$ e pertanto si ha $A_a \cong (A_{a'})_a$, un buon ordinamento isomorfo a una propria sezione, contro il Lemma 3.4.

Supponiamo che il dominio di F sia A e l'immagine sia B. Allora F è un isomorfismo tra (A, R) e (B, S), e si ha il caso (3) del Teorema.

Supponiamo che l'immagine di F non sia tutto B. Sia b il minimo in B che non è immagine di nessun $a \in A$, i.e., il minimo di $B - F(A)$. Allora si ha che l'immagine di F è la sezione B_b. Allora deve valere che il dominio di F è tutto A. Altrimenti, sia $a \in A$ il minimo non appartenente al dominio di F. Si avrebbe che F definisce un isomorfismo tra A_a e B_b, contro il fatto che a non è nel dominio di F e b non è nell'immagine di A via F! Per tanto F è definita su tutto A e siamo nel caso (1).

[2]Ossia non vale, a priori, che non esistono $b, b' \in B$, $a \in A$, tali che aFb e aFb'.

Supponiamo che il dominio di F non sia tutto A. Sia $a \in A$ il minimo su cui F non è definita. Allora il dominio di F è la sezione A_a. Deve allora valere che l'immagine di F è tutto B. Altrimenti, sia $b \in B$ il minimo non appartenente all'immagine di A via F. Allora si ha che F è un isomorfismo tra A_a e B_b, contro la scelta di a e di b. Per F è suriettiva su B e siamo nel caso (2). □

4. Conclusione

Il Teorema dimostrato qui sopra risolve il problema della comparabilità per insiemi bene ordinati. Vedremo di seguito come il problema della comparabilità di insiemi qualunque per iniezione verrà risolto assiomaticamente, con l'assunzione di un assioma, l'Assioma di Scelta, che equivale ad assumere che qualunque insieme può essere bene ordinato.

CAPITOLO 3

Aritmetica dei Buoni Ordini

1. Sinossi

Nella scorsa lezione abbiamo dimostrato che i buoni ordini sono tra loro comparabili per isomorfismo: dati due buoni ordini (A, R) e (B, S), o sono isomorfi, oppure uno è isomorfo a un pezzo iniziale dell'altro (in questo senso è *più piccolo* dell'altro). Oggi vedremo come è possibile sviluppare una vera e propria aritmetica sui buoni ordini, siano essi finiti o infiniti; aritmetica che *estende* l'aritmetica sui numeri naturali.

2. Aritmetica sui Buoni Ordini

Abbiamo visto come la nozione di isomorfismo determini una classificazione degli insiemi bene ordinati nel senso che due buoni ordinamenti qualunque sono comparabili: se non sono isomorfi, l'uno è isomorfo a una parte iniziale dell'altro. Abbiamo dunque una prima *classificazione* delle quantità infinite (bene ordinate). Con l'obiettivo di sviluppare una vera e propria matematica delle quantità infinite, è piuttosto naturale ora chiedersi: è possibile definire operazioni aritmetiche sui buoni ordinamenti, estendendo le operazioni note sui numeri naturali? Vedremo qui di séguito come definire somma, prodotto ed esponenziazione su buoni ordinamenti. In tal modo, ci avviciniamo all'idea di un vero e proprio *sistema numerico* valido per quantità finite e infinite.

Somma. Dati due buoni ordini (A, R) e (B, S) vogliamo definire un nuovo buon ordine, denotato con $(A, R) + (B, S)$, che estenda al caso generale l'idea della somma che ci è nota nel caso dei numeri naturali. Dati due insiemi finiti A e B, A con p elementi e B con q elementi, vogliamo naturalmente che l'insieme somma di A e B abbia $p + q$ elementi. Da notare subito che, se A e B hanno elementi in comune (per es. se A è $\{1, \dots, p\}$ e B è $\{1, \dots, q\}$), non basta prendere l'unione $A \cup B$ per ottenere un insieme con $p+q$ elementi. Il trucco è allora di fare una copia di A e una copia di B in modo tale che le copie siano disgiunte tra loro. Unendo le due copie disgiunte otteniamo un insieme che ha tanti elementi quanti quelli di A *più* gli elementi di B.

Definizione 2.1 (Unione Disgiunta). Dati due insiemi A e B, definiamo *unione disgiunta* di A e B l'insieme che contiene tutte le coppie ordinate di forma $(a, 1)$ con $a \in A$ e $(b, 2)$ con $b \in B$. Denotiamo l'unione disgiunta con $A \uplus B$.

Notiamo che 1 e 2 sono soltanto due etichette che ci servono per distinguere la copia di A dalla copia di B evitando che abbiano elementi in comune. Invece di 1 e 2 possiamo usare qualunque coppia di insiemi diversi, per esempio $\varnothing$ e $\{\varnothing\}$. Come dominio del nostro insieme somma di (A, R) e (B, S) prendiamo dunque $A \uplus B$. Resta ora da definire su $A \uplus B$ un buon ordinamento. L'idea è questa: nel nuovo

ordinamento tutti gli elementi di A (per la precisione: le loro copie etichettate $(a,1)$) vengono prima di tutti gli elementi di B (per la precisione: delle loro copie etichettate $(b,2)$). La copia di A è ordinata come A e la copia di B è ordinata come B. Formalmente, definiamo l'ordine T su $A \uplus B$ come segue.

$$(x,i) \prec_+ (y,j) \text{ sse } \begin{cases} i = j = 1 \ \& \ xRy \\ i = j = 2 \ \& \ xSy \\ i = 1 \ \& \ j = 2 \end{cases}$$

Resta da dimostrare che $(A \uplus B, \prec_+)$ è un buon ordine, e che l'operazione definita estende la somma sui naturali.

PROPOSIZIONE 2.2. *$\prec_+$ bene ordina $A \uplus B$.*

DIMOSTRAZIONE. (IRRIFLESSIVITÀ) Supponiamo che esista $(x,i) \in A \uplus B$ tale che $(x,i) \prec_+ (x,i)$. Allora xRx con $x \in A$ o xSx con $x \in B$, il che è impossibile.

(TRANSITIVITÀ) Siano $(x,i) \prec_+ (y,j) \prec_+ (z,k)$. Dimostriamo che $(x,i) \prec_+ (z,k)$. Dall'ipotesi e dalla definizione di $\prec_+$ si ha che $i \leq j \leq k$. Dunque $i \leq k$. Se $i = 1$ e $k = 2$, allora $(x,i) \prec_+ (z,k)$ per definizione di $\prec_+$. Se $i = k = 1$ allora anche $j = 1$ e si ha $xRyRz$ e dunque xRz, ergo $(x,i) \prec_+ (z,k)$. Se $i = k = 2$ allora anche $j = 2$ e si ha $xSySz$ e dunque xSz, ergo $(x,i) \prec_+ (z,k)$.

(COMPARABILITÀ) Siano (x,i) e (y,j) due elementi distinti in $A \uplus B$. Se $i = j$ allora o $x, y \in A$ e x, y sono comparabili rispetto a R, oppure $x, y \in B$ e x, y sono comparabili rispetto a B. Se $i = 1$ e $j = 2$, immediatamente $(x,i) \prec_+ (y,j)$ per definizione di $\prec_+$. Ergo (x,i) e (y,j) sono sempre comparabili secondop $\prec_+$.

(BUON ORDINE) Dato X un sottinsieme non vuoto di $A \uplus B$ dobbiamo dimostrare che X ha un minimo. Se X contiene elementi della forma $(a,1)$, $a \in A$, si ottiene il minimo di X prendendo il minimo $a \in A$ (rispetto a R) tale che $(a,1) \in X$ (un tale minimo esiste perché (A,R) è un buon ordinamento). Se X non contiene elementi di forma $(a,1)$ allora X è un sottinsieme del sottinsieme di $A \uplus B$ di forma $\{(b,2) \text{ t.c. } b \in B\}$. Prendendo l'$S$-minimo $b \in B$ t.c. $(b,2) \in S$ (esiste perché S bene ordina B) si ottiene il minimo di X. □

PROPOSIZIONE 2.3. *$(\{1,\dots,p\} + \{1,\dots,q\}, \prec_+)$ è isomorfo a $(\{1,\dots,p+q\}, <$).*

DIMOSTRAZIONE. Esercizio. □

PROPOSIZIONE 2.4. *La somma di buoni ordini è associativa, i.e.*

$$(A,R) + ((B,S) + (C,T)) \cong ((A,R) + (B,S)) + (C,T).$$

DIMOSTRAZIONE. Gli elementi di dell'insieme a sinistra sono le coppie $(a,1)$ con $a \in A$ e $(x,2)$ con $x \in B \uplus C$. Per definizione di $B \uplus C$, questi $(x,2)$ sono di forma $((b,1),2)$ con $b \in B$ o $((c,2),2)$ con $c \in C$.

Gli elementi dell'insieme a destra sono le coppie $(x,1)$ con $x \in A \uplus B$ e $(c,2)$. Per definizione di $A \uplus B$, le coppie $(x,1)$ sono di forma $((a,1),1)$, con $a \in A$, o $((b,2),1)$, con $b \in B$.

Otteniamo un isomorfismo tra i due insiemi associando gli elementi come segue:

$$(a,1) \mapsto ((a,1),1)$$
$$((b,1),2) \mapsto ((b,2),1)$$
$$((c,2),2) \mapsto (c,2)$$

(verificare per esecizio). Intuitivamente, non v'è mistero: nell'ordine della somma a sinistra si hanno gli elementi di A seguiti dagli elementi di $B + C$, ossia dagli elementi di B seguiti dagli elementi di C. Nell'ordine a destra si hanno gli elementi di $A + B$ (ossia gli elementi di A seguiti dagli elementi di B), seguiti dagli elementi di C, il che è dire la stessa cosa in due modi diversi. □

PROPOSIZIONE 2.5. *La somma di buoni ordini non è commutativa, i.e., in generale* $(A, R) + (B, S)$ *non è isomorfo a* $(B, S) + (A, R)$.

DIMOSTRAZIONE. Dimostriamo la Proposizione con un esempio. Sia $A = \{0\}$ (l'insieme che contiene solo il numero 0), sia $B = \mathbf{N}$. Consideriamo A e B ciascuno ordinato con l'ordine standard sui naturali. Consideriamo dapprima la somma $(A, <)+(B, <)$, ossia l'insieme bene ordinato $(\{0\}, <)+(\mathbf{N}, <)$, che è $(\{0\} \uplus \mathbf{N}, <_+)$. Per definizione l'insieme somma contiene gli elementi

$$(0, 1), (0, 2), (1, 2), (2, 2), (3, 2) \dots$$

e l'ordine $\prec_+$ è tale che

$$(0, 1) \prec_+ (0, 2) \prec_+ (1, 2) \prec_+ (2, 2) \prec_+ (3, 2) \prec_+ \dots$$

Si vede facilmente che un tale insieme ordinato è isomorfo a $(\mathbf{N}, <)$. Si ottiene un isomorfismo ponendo $(0, 1) \mapsto 0$ e $(n, 2) \mapsto n + 1$ per ogni $n \in \mathbf{N}$ (verificare per esercizio). Intuitivamente, l'ordine sull'insieme somma è ottenuto mettendo $(0, 1)$ come primo elemento, seguìto da tutti gli elementi $(n, 2)$, ossia da una copia dei numeri naturali. Un tale ordine è strutturalmente identico a quello sui naturali.

Consideriamo ora la somma $(B, <)+(A, <)$, ossia l'insieme bene ordinato $(\mathbf{N} \uplus \{0\}, <_+)$. La somma contiene gli stessi elementi di $(\{0\}, <) + (\mathbf{N}, <)$, ma ordinati in modo differente: prima viene una copia dei naturali, e, dopo tutti gli infiniti elementi di tale copia, viene la copia di $\{0\}$, ossia un elemento maggiore di tutti i precedenti. L'ordine ha questa forma:

$$(0, 2) \prec_+ (1, 2) \prec_+ (2, 2) \prec_+ (3, 2) \prec_+ \dots \prec_+ (0, 1).$$

Si vede facilmente che non è possibile definire un isomorfismo tra un tale ordine e $(\mathbf{N}, <)$: un isomorfismo preserva l'ordine e pertanto non si saprebbe scegliere in $\mathbf{N}$ una immagine appropriata per $(0, 1)$, che è maggiore di infiniti numeri. □

Prodotto. Per definire il prodotto partiamo ancora da un'intuizione valida nel dominio degli insiemi finiti e la generalizziamo. Il prodotto di $p \times q$ elementi si può visualizzare come q copie di un insieme di p elementi, una dopo l'altra. Il numero $p \times q$ è anche il numero delle possibili coppie (x, y), dove x è scelto tra p elementi e y tra q elementi. Per tanto, è naturale scegliere come l'insieme prodotto di due buoni ordini (A, R) e (B, S), l'insieme delle coppie (a, b) con $a \in A$ e $b \in B$. Un tale insieme è chiamato anche *prodotto cartesiano* di A e di B e si denota con $A \times B$. Notiamo che il prodotto cartesiano è definito per insiemi A e B qualunque, non necessariamente ordinati o bene ordinati, come l'insieme $\{(a, b) \text{ t.c. } a \in A,\ b \in B\}$. Resta invece da definire un buon ordinamento $\prec_\times$ su $A \times B$. Il prodotto dei buoni ordini (A, R) e (B, S) verrà allora definito come $(A \times B, \prec_\times)$ e denotato come $(A, R) \times (B, S)$ (l'operazione di prodotto cartesiano su insiemi qualunque e di prodotto su buoni ordini non sono la stessa operazione, ma la denotiamo con lo stesso simbolo, $\times$).

$$(a,b) \times (a',b') \text{ sse } \begin{cases} bSb', & \text{oppure} \\ b = b' & \text{e } aRa' \end{cases}$$

Resta da dimostrare che $(A \times B, \prec_\times)$ è un buon ordine, e che l'operazione definita estende la somma sui naturali.

PROPOSIZIONE 2.6. *$\prec_\times$ bene ordina $A \uplus B$.*

DIMOSTRAZIONE. (IRRIFLESSIVITÀ) Se $(a,b) \prec_\times (a,b)$ allora aRa per definizione di $\prec_\times$. Ma R è irriflessivo su A.

(TRANSITIVITÀ) Sia $(a,b) \prec_\times (a',b') \prec_\times (a'',b'')$. Consideriamo i quattri possibili casi.

- $(a,b) \prec_\times (a',b')$ perché bSb' e $(a',b') \prec_\times (a'',b'')$ perché $b'Sb''$: allora $bSb'Sb''$ implica bSb'', per transitività di S. Dunque $(a,b) \prec_\times (a'',b'')$.
- $(a,b) \prec_\times (a',b')$ perché bSb' e $(a',b') \prec_\times (a'',b'')$ perché $b' = b''$ e $a'Ra''$: $bSb' = b''$ implica bSb'' e dunque $(a,b) \prec_\times (a'',b'')$.
- $(a,b) \prec_\times (a',b')$ perché $b = b'$ e aRa' e $(a',b') \prec_\times (a'',b'')$ perché $b'Sb''$: $b = b'Sb''$ implica bSb'' e dunque $(a,b) \prec_\times (a'',b'')$.
- $(a,b) \prec_\times (a',b')$ perché $b = b'$ e aRa' e $(a',b') \prec_\times (a'',b'')$ perché $b' = b''$ e $a'Ra''$: $aRa'Ra''$ implica aRa'' per transitività di R. Dunque $(a,b) \prec_\times (a'',b'')$.

(COMPARABILITÀ) Siano (a,b) e (a',b') in $A \times B$. S è totale e dunque bSb' o $b'Sb$ o $b = b'$. Se bSb' allora $(a,b) \prec_\times (a',b')$. Se $b'Sb$ allora $(a',b') \prec_\times (a,b)$. Se $b = b'$, poiché R è totale su A, si ha aRa', oppure $a'Ra$ oppure $a = a'$. Se aRa' allora $(a,b) \prec_\times (a',b')$. Se $a'Ra$ allora $(a',b') \prec_\times (a,b)$. Se $a = a'$ allora $(a,b) = (a',b')$.

(BUON ORDINE) Sia S un sottinsieme non vuoto di $A \times B$. Dimostriamo che S ha un minimo. Scegliamo (a_0, b_0) tale che b_0 è il minimo (rispetto a S) b in B tale che esiste un $(a,b) \in S$, e a_0 è il minimo (rispetto a R) a in A tale che $(a,b_0) \in S$. L'esistenza di b_0 e a_0 è garantita dal fatto che B e A sono buoni ordinamenti. □

PROPOSIZIONE 2.7. *$(\{1,\dots,p\} \times \{1,\dots,q\}, \prec_\times)$ è isomorfo a $(\{1,\dots,p \cdot q\}, <)$.*

DIMOSTRAZIONE. Esercizio. □

PROPOSIZIONE 2.8. *Il prodotto di buoni ordini è associativo, i.e.*

$$(A,R) \times ((B,S) \times (C,T)) \cong ((A,R) \times (B,S)) \times (C,T).$$

DIMOSTRAZIONE. L'insieme a sinistra contiene gli elementi $(a,(b,c))$. L'insieme a destra contiene gli elementi $((a,b),c))$. Mandando $(a,(b,c)) \mapsto ((a,b),c)$ otteniamo un isomorfismo (verificare per esercizio). □

PROPOSIZIONE 2.9. *Il prodotto di buoni ordini è distributivo sulla somma, i.e.*

$$(A,R) \times ((B,S) + (C,T)) \cong ((A,R) \times (B,S)) + ((A,R) \times (C,T)).$$

DIMOSTRAZIONE. L'insieme a sinistra contiene gli elementi $(a,(b,1))$ e $(a,(c,2))$. L'insieme a destra contiene gli elementi $((a,b),1)$ e $((a,c),2)$. Associando come segue otteniamo un isomorfismo (verificare).

$$(a,(b,1)) \mapsto ((a,b),1),$$
$$(a,(c,2)) \mapsto ((a,c),2).$$

□

PROPOSIZIONE 2.10. *Il prodotto di buoni ordinamenti non è commutativo, i.e., in generale non vale che* $(A, R) \times (B, S)$ *è isomorfo a* $(B, S) \times (A, R)$.

DIMOSTRAZIONE. Dimostriamo l'asserto con un esempio. Sia $A = \{0, 1\}$, e $B = \mathbf{N}$, entrambi con l'ordine naturale.

Consideriamo dapprima $(A, <) \times (B, <)$ ossia $(\{0, 1\} \times \mathbf{N}, \prec_\times)$. Questo buon ordinamento consiste di infinite coppie dell'insieme $\{0, 1\}$, poste una di séguito all'altra. In altre parole abbiamo l'ordinamento seguente.

$$(0,0) \prec_\times (1,0) \prec_\times (0,1) \prec_\times (1,1) \prec_\times (0,2) \prec_\times (1,2) \prec_\times (0,3) \prec_\times (1,3) \prec_\times \dots$$

Si vede facilmente che un tale ordinamento è isomorfo a $(\mathbf{N}, <)$.

Consideriamo ora $(B, <) \times (A, <)$ ossia $(\mathbf{N} \times \{0, 1\}, \prec_\times)$. Questo buon ordinamento consiste di due coppie di $\mathbf{N}$, poste una di séguito all'altra. L'ordine è il seguente.

$$(0,0) \prec_\times (1,0) \prec_\times (2,0) \prec_\times \dots (0,1) \prec_\times (1,1) \prec_\times (2,1) \prec_\times \dots$$

Si vede facilmente che si tratta di un ordine non isomorfo a $(\mathbf{N}, <)$. Non sapremmo infatti che immagine assegnare in $\mathbf{N}$ a un elemento come $(0, 1)$ - che ha infiniti predecessori rispetto a $\prec_\times$ - senza alterare l'ordine. □

Esponenziazione. Analogamente a quanto fatto per la somma e il prodotto è possibile definire un'operazione

$$(A, R), (B, S) \to (A, R)^{(B,S)}$$

su buoni ordinamenti che estenda l'esponenziazione naturale. Come insieme di supporto si sceglie un sottinsieme di tutte le funzioni da B in A, e si procede a definire un buon ordinamento $\prec_{esp}$ di tale insieme. Omettiamo la definizione a questo punto (è solo leggermente più intricata di quelle di somma e prodotto), ripromettendoci di offrirne una definizione più avanti, quando disporremo di strumenti che ci permetteranno un approccio semplificato alla questione. Ci limitiamo qui ad osservare che l'operazione di esponeziazione gode delle seguenti proprietà generali.

$$(A, R)^{(B,S)+(C,T)} \cong (A, R)^{(B,S)} \times (A, R)^{(C,T)},$$

$$((A, R)^{(B,S)})^{(C,T)} \cong (A, R)^{(B,S)\times(C,T)}.$$

3. Ordinali

Grazie alla nozione di isomorfismo, possiamo dividere l'universo degli insiemi bene ordinati in classi disgiunte, raggruppando in una stessa classe insiemi isomorfi tra loro. Chiamiamo tali classi *classi di equivalenza per isomorfismo*.[1] In tal modo otteniamo che

(1) Ogni insieme bene ordinato appartiene ad una e ad una sola classe di equivalenza.
(2) Dati due insiemi appartenenti a due classi distinte, l'uno è isomorfo ad una sezione dell'altro (per il Teorema di Comparabilità dei buoni ordini).

[1] In generale, una relazione binaria E è detta *relazione d'equivalenza* se è riflessiva, simmetrica e transitiva. L'isomorfismo tra buoni ordini soddisfa ovviamente queste tre proprietà. Ogni relazione di equivalenza su un insieme determina univocamente una *partizione* dell'insieme, se si raggruppano in una medesima classe tutti gli insiemi che stanno tra loro nella relazione E.

(3) Le operazioni di somma, prodotto e esponenziazione sono stabili rispetto alle classi di equivalenza, i.e., per esempio, la somma di due buoni ordini (A, R) e (B, S) è isomorfa alla somma di (A', R'), (B', S') per qualunque (A', R') nella stessa classe di (i.e., isomorfo a) (A, R), e (B', S') nella stessa classe di (i.e. isomorfo a) (B, S).

In altre parole, abbiamo generalizzato con successo a buoni ordini qualunque la situazione valida nel caso degli insiemi finiti.

Un attimo di riflessione ci convincerà che ogni insieme finito può essere bene ordinato, e che il buon ordinamento è unico a meno di isomorfismo (gli elementi, in numero finito, vengono posti su una linea, in qualche ordine). Possiamo allora dividere in classi l'universo degli insiemi finiti raccogliendo nella stessa classe gli insiemi isomorfi tra loro (per l'osservazione sopra la partizione non cambia se ci limitiamo a raccogliere nella stessa classe gli insiemi equipotenti tra loro). Per ogni classe è possibile specificare un elemento della classe *rappresentante canonico* o *ambasciatore* o *elemento tipico* della classe, per es. l'insieme $\{1, \ldots, p\}$ come rappresentante della classe degli insiemi *con p elementi*. L'insieme $\{1, \ldots, p\}$ può essere essenzialmente identificato con il numero naturale p. Le relazioni di isomorfismo quali

$$\{1, \ldots, p\} + \{1, \ldots, q\} \cong \{1, \ldots, p + q\}$$

si traducono allora in relazioni di *identità*:

$$p + q = p + q,$$

che si può leggere come: *la classe ottenuta sommando un elemento della classe rappresentata p a un elemento della classe rappresentata da q è rappresentata da* $p + q$.

Estendiamo l'analogia a insiemi bene ordinati qualunque. Supponiamo cioè di poter specificare, per ciascuna classe di isomorfismo, un rappresentante canonico della classe. In altre parole assumiamo di disporre di una funzione, chiamiamola Ord, definita sull'insieme degli insiemi bene ordinati e tale da associare, a ciascun insieme, il rappresentante della classe d'isomorfismo cui l'insieme appartiene. Ord gode dunque della seguente proprietà:

$$(A, R) \cong (B, S) \text{ se e soltanto se } Ord(A, R) = Ord(B, S).$$

i.e. due buoni ordini hanno lo stesso rappresentante se e solo se sono isomorfi (i.e. sono nella stessa classe di isomorfismo).

Chiamiamo *ordinali* i rappresentanti delle classi di isomorfismo (ossia gli elementi dell'immagine di Ord). Usiamo da ora in poi minuscole greche α, β etc. per denotare ordinali. Da quanto visto sopra otteniamo immediatamente che sono definite operazioni di somma, prodotto ed esponenziazione tra ordinali, semplicemente ponendo

$$\alpha + \beta := Ord((\alpha, <_\alpha) + (\beta, <_\beta)),$$

$$\alpha \times \beta := Ord((\alpha, <_\alpha) \times (\beta, <_\beta)),$$

$$\alpha^\beta := Ord((\alpha, <_\alpha)^{(\beta, <_\beta)}),$$

considerando che α e β sono insiemi bene ordinati, e denotando con $<_\alpha$ e $<_\beta$ i rispettivi buoni ordini. Le proprietà di somma, prodotto, esponenziazione dei buoni ordini viste in precedenza si traducono allora così:

$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma,$$
$$\alpha \times (\beta \times \gamma) = (\alpha \times \beta) \times \gamma, \;\; \alpha \times (\beta + \gamma) = (\alpha \times \beta) + (\alpha \times \gamma),$$
$$\alpha^{(\beta+\gamma)} = (\alpha^\beta) \times (\alpha^\gamma), \;\; (\alpha^\beta)^\gamma = \alpha^{\beta \times \gamma}.$$

Abbiamo pertanto definito una vera e propria aritmetica per quantità finite o infinite, che coincide nel caso finito con l'aritmetica naturale.

CAPITOLO 4

Aritmetica Ordinale e Paradossi

1. Sinossi

Approfondiamo la nostra conoscenza degli ordinali, della loro aritmetica e delle loro proprietà d'ordine. Dimostriamo che gli ordinali sono bene ordinati e concludiamo con il paradosso di Burali-Forti.

2. Ordinali

Abbiamo dimostrato diverse proprietà sulla comparabilità per isomorfismo dei buoni ordini in generale. In particolare, il teorema di comparabilità dei buoni ordini per isomorfismo, ci dice che la relazione *'essere isomorfo a una sezione iniziale di'* ha le proprietà di ciò che abbiamo chiamato un ordine totale. Precisiamo questa osservazione come segue.

(1) Irriflessività: abbiamo visto che nessun buon ordine è isomorfo a una propria sezione.
(2) Transitività: si osserva facilmente che, se (A, R) è ismorfo a una sezione (B_b, S) e (B, S) è isomorfo a una sezione (C_c, T), allora (A, R) è isomorfo a una sezione (C'_c, T) con $c' < c$, perché la composizione di due isomorfismi è ancora un isomorfismo.
(3) Comparabilità: il teorema di comparabilità dei buoni ordini ci dà immediatamente questa proprietà.

Procediamo un po' più formalmente, e restringiamo l'attenzione ai rappresentanti delle classi di isomorfismo, ossia agli ordinali, e poniamo la seguente definizione.

Definizione 2.1. Siano α e β ordinali. Vale $\alpha < \beta$ se e solo se un insieme (B, S) di tipo β ha una sezione di tipo α. I.e., se $Ord(B, S) = \beta$, ed esiste $b \in B$ tale che $Ord(B_b, S) = \alpha$.

Osservazione 2.2. Se $Ord(B, S) = \beta$ e $\alpha < \beta$, allora esiste $b \in B$ tale che $Ord(B_b, S) = \alpha$. (Esercizio).

Dimostriamo che la relazione $<$, definita sull'insieme di tutti gli ordinali, che denotiamo con **ORD**, è un buon ordinamento.

Teorema 2.3. *La relazione* $<$ *bene ordina* **ORD**.

Dimostrazione. (Irriflessività) Supponiamo $\alpha < \alpha$. Per definizione esiste un buon ordine (A, R) tale che $Ord(A, R) = \alpha$, e un $a \in A$ tale che $\alpha = Ord(A_a, R)$. Ma allora $(A, R) \cong (A_a, R)$, il che è impossibile.

(Transitività) Siano $\alpha < \beta < \gamma$. Per definizione esistono buoni ordini (B, S), $b \in B$ e (C, T), $c \in C$ tali che

$$Ord(B, S) = \beta;\ Ord(B_b, S) = \alpha;\ Ord(C, T) = \gamma;\ Ord(C_c, S) = \beta$$

Dimostriamo che esiste $c' \in C$ tale che $\alpha = Ord(C_{c'}, T)$, così che per definizione $\alpha < \gamma$. Siano F, G, H tali che

$$\alpha \cong_F (B_b, S); \;\; (B, S) \cong_G \beta \cong_H (C_c, T).$$

Allora si verifica facilmente che $\alpha \cong (C_{G(F(b))}, T)$, e la composizione $G \cdot F$ testimonia che (B_b, S) è isomorfo a una sezione di (C, T), i.e. che $\alpha < \gamma$.

(Comparabilità) Siano $\alpha \neq \beta$ due ordinali qualunque. α e β sono buoni ordini, e per tanto si applica il Teorema di Comparabilità. α è isomorfo a una sezione di β e allora per definizione $\alpha < \beta$, oppure β è isomorfo a una sezione di α, e allora per definizione $\beta < \alpha$.

(Buon Ordine) Sia S un insieme non vuoto di ordinali. Dobbiamo dimostrare che S ha un minimo rispetto a $<$. Sia $\alpha \in S$. Se α è minimo, abbiamo finito. Supponiamo dunque che α non sia minimo in S. Sia $\alpha' < \alpha$, $\alpha' \in S$. Sia (A, R) un buon ordine tale che $Ord(A, R) = \alpha$. Allora esiste $a' \in A$ tale che $Ord(A_{a'}, R) = \alpha'$. Per tanto, l'insieme S' definito qui sotto è un sottinsieme non vuoto di A.

$$S' := \{a \in A \text{ t.c. } Ord(A_a, R) \in S\}.$$

Poiché (A, R) è un buon ordinamento, l'insieme S ha un minimo, rispetto alla relazione R. Sia a_0 tale minimo. Consideriamo allora l'ordinale associato a (A_{a_0}, R):

$$\alpha_0 := Ord(A_{a_0}, R)).$$

α_0 è l'ordinale della minima sezione di (A, R) il cui ordinale appartiene ad S. Dimostriamo ora che α_0 è il minimo di S (N.B. le due cose sono a priori distinte). Altrimenti, sia $\beta < \alpha_0$ tale che $\beta \in S$. Per l'osservazione di sopra, da $\beta < \alpha_0 = Ord(A_{a_0}, R)$ si deduce che esiste $b \in A_{a_0}$ tale che $Ord(A_b, R) = \beta$. $b \in A_{a_0}$ implica bRa_0. $\beta \in S$ e $Ord(A_b, R) = \beta$ implica $b \in S'$. Abbiamo dunque contraddetto la minimalità di a_0 in S'.

□

3. Dimostrazioni e Definizioni per Induzione sugli Ordinali

Dal fatto che $(\mathbf{ORD}, <)$ è un buon ordine, si deduce immediatamente il seguente Corollario.

Corollario 3.1 (Induzione su Ordinali). *Per il buon ordinamento* $(\mathbf{ORD}, <)$ *vale il Principio di Induzione, i.e. se P è una proprietà di insiemi, e se per ogni α è vero che: se P vale di tutti i $\beta < \alpha$ allora P vale per α, allora P vale per tutti gli ordinali; in formule:*

$$[(\forall \alpha)((\forall \beta < \alpha) P(\beta) \to P(\alpha))] \to (\forall \alpha)(P(\alpha)).$$

Analogamente, valgono il Principio del Minimo Numero e il Principio del Successore Immediato, che valgono su tutti i buoni ordini.

L'altra faccia delle *dimostrazioni* per induzione sono le *definizioni* per induzione o *ricorsione*. L'idea di definire una funzione per induzione su un insieme è questa: si definisce il comportamento della funzione per il minimo elemento dell'insieme (Base Induttiva), poi si definisce il comportamento della funzione per un generico elemento dell'insieme, supponendo che la funzione sia già definita per tutti gli elementi strettamente minori di esso (Passo Induttivo).

Nel campo del finito, e in particolare dei numeri naturali, le definizioni per induzione sono abituali. Per esempio, si può definire la funzione di somma, $+$, per induzione come segue:

- $n + 0 := n$
- $n + (m + 1) := (n + m) + 1$

Nel secondo punto stiamo definendo la somma di n e di $m+1$ supponendo di saper fare la somma di $n + m$ (perché $m < m + 1$). Oltre a ciò, il comportamento della somma sui numeri n e $m + 1$ è definito usando un'altra funzione, che supponiamo data, i.e., la funzione successore, il $+1$. Per rendere più chiaro lo schema generale, scriviamo $somma(x, y)$ invece di $x + y$ e $succ(x)$ invece di $x + 1$. Allora, nel passo induttivo, stiamo definendo il valore di $somma(n, succ(m + 1))$ supponendo di conoscere il valore di $somma(n, m)$ e il valore di $succ(x)$ per ogni x. Infatti $n + (m + 1) = (n + m) + 1$ equivale a

$$somma(n, (succ(m))) = succ(somma(n, m)).$$

Poiché gli ordinali sono bene ordinati da $<$, è possibile definire funzioni per induzione sugli ordinali, estendendo ciò che accade nel caso di $(\mathbf{N}, <)$. Il risultato seguente (del quale omettiamo la dimostrazione, che fa uso essenziale del teorema di buon ordinamento degli ordinali), mostra come, data una funzione G ben definita su insiemi (nel nostro esempio di sopra, la funzione successore) sia possibile definire per induzione in termini di essa una (unica) funzione F sugli ordinali: il valore di F su un ordinale α è determinato dal risultato di G applicata all'insieme dei valori di F sugli ordinali più piccoli di α (proprio come accadeva nel passo induttivo della definizione di somma).

Corollario 3.2 (Definizione per Induzione su Ordinali). *Per ogni funzione G esiste una unica funzione F definita sugli ordinali che soddisfa*

$$F(\alpha) = G(F(\{\beta \text{ t.c. } \beta < \alpha\})).$$

La definizione per Induzione su Ordinali è uno strumento essenziale della Teoria degli Insiemi. L'induzione su ordinali viene abitualmente chiamata *Induzione Transfinita*, per ricordare che gli ordinali costituiscono una estensione del sistema numerico ad un sistema che comprende il finito e l'infinito. Cantor introdusse il termine *transfinito* per i suoi numeri ordinali (e cardinali, cfr.*infra*) di insiemi infiniti, e riservò il termine *infinito* a Dio.

4. La Struttura degli Ordinali

Che particolarità ha il buon ordinamento $<$ sugli ordinali? Partiamo da una semplicissima analogia. Domanda: Quanti sono i numeri minori di 0? Risposta: 0... Domanda: Quanti sono i numeri minori di 1? Risposta: 1... Quanti sono i numeri minori di 2? Risposta: sono 2... etc. In generale vale

$$n = \text{ il numero dei numeri minori di } n.$$

Si osserva facilmente che esiste un unico buon ordine - a meno di isomorfismo - di un insieme finito. [1] Ovviamente l'insieme $\{m \text{ t.c. } m < n\}$ è bene ordinato dall'ordine naturale $<$. Per tanto, possiamo prendere la coppia $(\{m \text{ t.c. } m < n\}, <)$ come l'elemento tipico (il rappresentante) della classe di isomorfismo che raccoglie tutti gli insiemi di n elementi. Vedremo come questa situazione si generalizza ad ordinali qualunque. Cominciamo osservando che ogni ordinale è isomorfo all'insieme degli ordinali più piccoli di esso, bene ordinati da $<$.

[1] Dato un insieme con n elementi $a_1, \ldots, a_n$, tutti gli ordinamenti totali e bene ordinati sono isomorfi e hanno la forma generica di una successione di n elementi messi in fila!

TEOREMA 4.1. *Per ogni ordinale α vale $\alpha = Ord(\{\beta \text{ t.c. } \beta < \alpha\}, <)$.*

DIMOSTRAZIONE. Preso (A, R) un buon ordine tale che $\alpha = Ord(A, R)$, basterà definire un isomorfismo tra (A, R) e $\{\beta \text{ t.c. } \beta < \alpha\}$. Definiamo una mappa F ponendo:

$$F(a) := Ord(A_a, R).$$

Mostriamo che

$$(A, R) \cong_F \{\beta \text{ t.c. } \beta < \alpha\}.$$

(i) L'immagine di F è l'insieme $\{\beta \text{ t.c. } \beta < \alpha\}$. Dimostriamo l'inclusione da sinistra a destra. Sia x un elemento dell'immagine di F. Ovviamente x è un ordinale, e si ha $x = Ord(A_a, R)$ per qualche $a \in A$. Poiché $\alpha = Ord(A, R)$, si ha $x < \alpha$. Dimostriamo ora l'inclusione inversa. Sia $\beta < \alpha$. Poiché $\alpha = Ord(A, R)$, per definizione di $<$ e per l'Osservazione 2.2 si ha che esiste $a \in A$ tale che $\beta = Ord(A_a, R)$.
(ii) F conserva l'ordine: aRa' implica $F(a) < F(a')$. Supponiamo aRa'. Per definizione di F si ha $F(a) = Ord(A_a, R)$ e $F(a') = Ord(A'_a, R)$. Poiché A_a è una sezione di $A_{a'}$ si ha immediatamente il risultato: $Ord(A_a, R) < Ord(A'_a, R)$.

Per tanto si conclude

$$Ord(\{\beta \text{ t.c. } \beta < \alpha\}, <) = Ord(A, R) = \alpha.$$

□

Il risultato qui sopra ci permette di specificare con maggior precisione di quanto fatto finora, per ogni buon ordine, un rappresentante canonico ad esso isomorfo. Notiamo che finora abbiamo soltanto supposto di avere a disposizione la funzione Ord, senza descriverla minimamente. Per il risultato di sopra possiamo scrivere:

$$(A, R) \cong (\{\beta \text{ t.c. } \beta < Ord(A, R)\}, <).$$

Per tanto, possiamo scegliere come rappresentante canonico di (A, R) l'insieme degli ordinali più piccoli dell'ordinale di (A, R), ossia possiamo *definire* la funzione Ord ponendo:

$$Ord(A, R) := (\{\beta \text{ t.c. } \beta < Ord(A, R)\}, <).$$

La definizione di sopra non è in alcun modo una definizione esplicita, bensì implicita. Non garantisce l'esistenza della funzione Ord, ma ne descrive una proprietà essenziale, posto che una funzione di scelta dei rappresentanti canonici delle classi di isomorfismo esista (come abbiamo supposto finora). Inoltre, possiamo usare la definizione implicita per descrivere esplicitamente alcuni ordinali:

- L'insieme vuoto è un buon ordinamento, e ovviamente $\varnothing = \{\beta \text{ t.c. } \beta < Ord(\varnothing, <)\}$. Per tanto $\varnothing$ è ordinale, ed è il minimo!
- L'ordinale successivo, per la definizione di Ord, è $\{\varnothing\}$, che ha 1 elemento.
- I successivi sono $\{\varnothing, \{\varnothing\}\}$ (2 elementi), $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}$ (3 elementi) etc.

In questo modo, applicando la definizione implicita di Ord, otteniamo una successione di infiniti ordinali, uno per ogni $n \in \mathbf{N}$.

DEFINIZIONE 4.2. Chiamiamo *transitivo* un insieme X se ogni elemento di X è anche un sottinsieme di X, i.e. se vale

$$(\forall x \in X)(x \in X \to x \subseteq X).$$

PROPOSIZIONE 4.3. *Ogni ordinale è transitivo e bene ordinato dalla relazione di appartenenza $\in$.*

DIMOSTRAZIONE. Sia α un ordinale. Per tanto abbiamo $\alpha = \{\beta \text{ t.c. } \beta < \alpha\}$. Sia $\beta \in \alpha$. Allora $\beta = \{\gamma \text{ t.c. } \gamma < \beta\}$. Dimostriamo che $\beta \subseteq \alpha$. Per ogni $\gamma \in \beta$ vale $\gamma < \beta$ e poiché $\beta < \alpha$, si conclude che $\gamma < \alpha$ e per tanto che $\gamma \in \alpha$. Dunque α è transitivo.

Dal fatto che $\alpha = \{\beta \text{ t.c. } \beta < \alpha\}$ si deduce immediatamente che la relazione $<$ e la relazione di appartenenza $\in$ coincidono su α, ossia che $\beta < \alpha$ se e soltanto se $\beta \in \alpha$. Poiché sappiamo che $<$ bene ordina tutti gli ordinali, e dunque α come insieme di ordinali, lo stesso vale per $\in$ su α. □

OSSERVAZIONE 4.4 (Ordinali di Von Neumann). Come osservò Von Neumann, è possibile *definire* gli ordinali come insiemi che soddisfano le due proprietà della proposizione precedente. Si dice allora che un insieme è un ordinale se e solo se è transitivo e bene ordinato da $\in$. Questa è una *definizione esplicita* ed è quella che viene comunemente adottata per sviluppare la teoria degli ordinali. Si tratta semplicemente di scegliere i rappresentanti canonici delle classi di isomorfismo in un modo differente. In queste note ci atterremo invece alla definizione implicita per cui $\alpha = \{\beta \text{ t.c. } \beta < \alpha\}$, secondo cui un ordinale è l'insieme degli ordinali più piccoli, che consideriamo più intuitiva.

5. Ordinali limite e successori

Osserviamo qui di sotto come gli ordinali siano chiusi sotto alcune essenziali operazioni insiemistiche e come queste corrispondano naturalmente a nozioni relative al buon ordinamento degli ordinali, quali il successore, il minimo, e l'estremo superiore. Come vedremo, la dimostrazione che un insieme è un ordinale è piuttosto noiosa e controintuitiva, se usiamo la definizione implicita. Lo stesso è vero se usiamo la definizione di Von Neumann. Per tanto, ometteremo quanto possibile tali dimostrazioni, lasciandole alla cura del lettore.

OSSERVAZIONE 5.1 (Successore). Se α è un ordinale, allora $\alpha \cup \{\alpha\}$ è pure un ordinale ed è il successore immediato di α rispetto a $<$.

DIMOSTRAZIONE. Prima di tutto osserviamo che $\alpha \cup \{\alpha\}$ è un insieme bene ordinato da $<$ e che per tanto $Ord(\alpha \cup \{\alpha\})$ è ben definito ($\alpha \cup \{\alpha\}$ *ha* un ordinale).

Dimostriamo che $\alpha \cup \{\alpha\}$ *è* un ordinale, secondo la nostra definizione implicita, ossia dimostriamo che

$$\alpha \cup \{\alpha\} = \{\beta \text{ t.c. } \beta < Ord(\alpha \cup \{\alpha\})\}.$$

Mostriamo $\{\beta \text{ t.c. } \beta < Ord(\alpha \cup \{\alpha\})\} \subseteq \alpha \cup \{\alpha\}$. Sia $\beta < Ord(\alpha \cup \{\alpha\})$. Allora β è isomorfo a una sezione di $\alpha \cup \{\alpha\}$, i.e. esiste $x \in \alpha \cup \{\alpha\}$ tale che

$$\beta \cong (\alpha \cup \{\alpha\})_x.$$

$x \in \alpha \cup \{\alpha\}$ implica $x \in \alpha$ o $x = \alpha$. In entrambi i casi x è un ordinale. Se $x \in \alpha$, allora $x \subseteq \alpha$, perché α è transitivo. In questo caso la sezione $(\alpha \cup \{\alpha\})_x$ è necessariamente isomorfa a x stesso. Dunque $\beta \cong x$ e perciò $\beta = x$, perché entrambi sono ordinali. Se $x = \alpha$, si ha $(\alpha \cup \{\alpha\})_x = \alpha$ e dunque $\beta = \alpha \in \alpha \cup \{\alpha\}$.

Mostriamo ora l'inclusione $\alpha \cup \{\alpha\} \subseteq \{\beta \text{ t.c. } \beta < Ord(\alpha \cup \{\alpha\})\}$. Sia $x \in \alpha \cup \{\alpha\}$. Ovviamente x è un ordinale, perché $x \in \alpha$ oppure $x = \alpha$. Se $x \in \alpha$ allora $x < \alpha$, e dunque, in entrambi i casi, si ha $x < Ord(\alpha \cup \{\alpha\})$, perché $\alpha \cong (\alpha \cup \{\alpha\})_\alpha$.

Mostriamo ora che l'ordinale $\alpha \cup \{\alpha\}$ è il successore immediato di α. $\alpha \cup \{\alpha\}$ è ovvio perché α è uguale alla sezione $(\alpha \cup \{\alpha\})_\alpha$. Sia $\alpha \cup \{\alpha\} > \beta > \alpha$. Allora β è

una sezione iniziale di $\alpha \cup \{\alpha\}$, e α è una sezione iniziale di β. Esiste $x \in \alpha \cup \{\alpha\}$ tale che $\beta = x$, ed esiste $y \in \beta$ tale che $\alpha = y$. Dunque $y < x < \alpha \cup \{\alpha\}$, il che implica che $y < \alpha$, una contraddizione.

□

Osservazione 5.2 (Minimo). Se A è un insieme di ordinali non vuoto, allora $\bigcap A$ è pure un ordinale ed è il minimo di A rispetto a $<$.

Dimostrazione. Omettiamo la dimostrazione del fatto che $\bigcap A$ è un ordinale. Dimostriamo che $\bigcap A$ è il minimo di A. Per ogni $\alpha \in A$ si ha $\bigcap A \subseteq \alpha$. Dunque $bigcapA \leq \alpha$. Supponiamo che $\bigcap A > \alpha$ per ogni $\alpha \in A$. Allora $\bigcap A < \bigcap A$, il che è impossibile. □

Osservazione 5.3 (Estremo Superiore). Se A è un insieme di ordinali, allora $\bigcup A$ è pure un ordinale ed è l'estremo superiore di A rispetto a $<$. Lo denotiamo con $\sup(A)$.

Dimostrazione. Omettiamo la dimostrazione del fatto che $\bigcup A$ è un ordinale.

Dimostriamo che $\bigcup A$ è l'estremo superiore di A (il minimo dei maggioranti di A). Mostriamo prima che $\bigcup A$ è un maggiorante di A. Per $\alpha \in A$, si ha $\alpha = \{\beta \text{ t.c. } \beta < \alpha\} \subseteq \bigcup A$. Dunque $\alpha \leq \bigcup A$. Mostriamo che $\bigcup A$ è il minimo dei maggioranti. Sia $\beta < \bigcup A$. Allora esiste $\alpha \in A$ tale che $\beta \in \alpha$, il che implica $\beta < \alpha$. Dunque β è minore di un qualche elemento di A e per tanto non è un maggiorante di A.

□

Usando le precedenti nozioni possiamo osservare come il buon ordinamento degli ordinali cominci come una copia dei numeri naturali. Poniamo le seguenti definizioni.

Definizione 5.4 (Ordinali Finiti). Denotiamo con $S(\alpha)$ l'insieme $\alpha \cup \{\alpha\}$, il *successore* di α. Definiamo

$$\hat{0} := \varnothing; \hat{1} := S(\varnothing); \dots n \hat{+} 1 := S(\hat{n}); \dots$$

Per ogni n, $\hat{n}$ è un ordinale e ha n elementi. Chiamiamo gli $\hat{n}$ *ordinali finiti*.

Gli ordinali così definiti formano allora una copia isomorfa di $\mathbf{N}$:

$$\varnothing = \hat{0} < \hat{1} = \{\varnothing\} < \hat{2} = \{\hat{0}, \hat{1}\} = \{\varnothing, \{\varnothing\}\}, \dots$$

La nostra copia insiemistica di $\mathbf{N}$ è l'insieme

$$S = \{\hat{n} \text{ t.c. } n \in \mathbf{N}\}.$$

Usando l'esistenza dell'estremo superiore osservata qui sopra, sappiamo che esiste un sup di questo insieme. Definiamo

$$\omega := \sup(S) = \sup(\{\hat{0}, \hat{1}, \hat{2}, \dots\}).$$

Per definizione di sup sappiamo che $\omega \geq \hat{n}$ per ogni n. Da ciò si deduce anche che $\omega \notin S$, ossia che $\omega > \hat{n}$ per ogni n (perché S non ha massimo e dunque il sup non può essere uguale a nessun elemento dell'insieme).

Gli ordinali $\hat{n}$ definiti sopra sono tutti della forma $\alpha \cup \{\alpha\}$ per qualche α. Invece, ω non ha questa forma, e vale $\omega = \bigcup \omega$. Vedremo tra poco che tutti gli ordinali hanno una di queste due forme.

DEFINIZIONE 5.5 (Limiti e Successori). α è un *successore* se $\alpha = \beta \cup \{\beta\}$ per qualche β. α è un *limite* se è diverso da $\hat{0}$ e non è un successore.

OSSERVAZIONE 5.6. $\omega = \sup\{\hat{n} \text{ t.c. } n \in \mathbf{N}\})$ è un limite. Per ogni $n \in \mathbf{N}$ $\hat{n}$ è un successore.

Mostriamo ora che ogni ordinale è o un limite o un successore.

PROPOSIZIONE 5.7. *Per ogni ordinale α, vale*

(1) *Per ogni $\beta < \alpha$, anche $S(\beta) < \alpha$ (e in questo caso $\alpha = \bigcup \alpha$); oppure*
(2) *Esiste β tale che $\alpha = S(\beta)$ (e in questo caso vale $\beta = \bigcup \alpha$).*

DIMOSTRAZIONE. Se $\beta < \alpha$, si ha $S(\beta) \leq \alpha$, perché abbiamo visto che $S(\beta)$ è il minimo maggiore di α. Allora si danno due casi:

(i) per ogni $\beta < \alpha$ vale $\beta < S(\beta)$, oppure

(ii) Esiste $\beta < \alpha$ tale che $S(\beta) \geq \alpha$ e dunque $S(\beta) = \alpha$.

Mostriamo ora che nel caso (i) vale anche $\alpha \subseteq \bigcup \alpha$. Ciò è sufficiente a dimostrare $\alpha = \bigcup \alpha$, poiché l'inclusione $\bigcup \alpha \subseteq \alpha$ vale per ogni ordinale. [2] Nel caso (i) abbiamo $\beta < S(\beta) < \alpha$ per ogni $\beta < \alpha$ e per tanto $\beta \in S(\beta) \in \alpha$ e dunque $\beta \in \bigcup \alpha$, il che dimostra $\alpha \subseteq \bigcup \alpha$.

Dimostriamo che nel caso (ii) vale $\bigcup \alpha = \beta$. Mostriamo prima che $\beta \subseteq \bigcup \alpha$. Sia $\gamma < \beta$. Allora $\gamma < \beta < \alpha$ implica $\gamma \in \bigcup \alpha$, il che dimostra $\beta \subseteq \bigcup \alpha$. Mostriamo ora $\bigcup \alpha \subseteq \beta$. Per costruzione di ha

$$\bigcup \alpha = \bigcup S(\beta) = \bigcup (\beta \cup \{\beta\}) = (\bigcup \beta) \cup \beta \subseteq \beta.$$

Dunque $\bigcup \alpha \subseteq \beta$. □

6. Aritmetica Ordinale

Sappiamo già come definire operazioni di somma, prodotto ed esponenziazione su buoni ordini qualunque. Per tanto, sappiamo anche come definirle su ordinali (e come trasformare gli isomorfismi in identità). Poniamo

$$\alpha + \beta = Ord(\alpha + \beta, \prec_+),$$
$$\alpha \times \beta = Ord(\alpha \times \beta, \prec_\times),$$
$$\alpha^\beta = Ord(\alpha^{(\beta)}, \prec_{esp}).^3$$

In altre parole, definiamo la somma di ordinali come l'ordinale associato alla somma dei due ordinali (intesa come somma di buoni ordini), e analogamente per prodotto ed esponenziazione. Valgono allora tutte le proprietà che abbiamo dimostrato per le operazioni tra buoni ordini, ma gli isomorfismi diventano identità! (Perché?)

$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma.$$
$$\alpha \times (\beta \times \gamma) = (\alpha \times \beta) \times \gamma.$$
$$\alpha \times (\beta + \gamma) = (\alpha \times \beta) + (\alpha + \gamma).$$
$$\alpha^{(\beta+\gamma)} = (\alpha^\beta) \times (\alpha^\gamma); \quad (\alpha^\beta)^\gamma = \alpha^{\beta \times \gamma}.$$

[2] α è transitivo (ogni elemento di un suo elemento è a sua volta un elemento). Abbiamo visto sopra che $\bigcup \alpha$ è esso stesso un ordinale. Per tanto, da $\bigcup \alpha \subseteq \alpha$ possiamo concludere $\bigcup \alpha \leq \alpha$, i.e. che $\bigcup \alpha$ è al massimo grande quando α.

[3] $\alpha^{(\beta)}$ denota un particolare insieme di funzioni dall'insieme β all'insieme α, le funzioni a supporto finito. Questo insieme è usato per definire l'esponenziazione di buoni ordini, operazione della quale abbiamo omesso la definizione.

La Proposizione qui sotto mostra come è possibile esprimere somma, prodotto ed esponenziazione usando soltanto le operazioni di successore, S e di estremo superiore, (sup, i.e., $\bigcup$). Le proprietà qui sotto possono essere usate per *definire* - per induzione transfinita - le operazioni di somma, prodotto, esponenziazione. In particolare, per l'esponenziazione ordinale, questa è la sola definizione esplicita che diamo in queste note.

PROPOSIZIONE 6.1. *Per ogni α, β e λ limite, si ha*

(1) $\alpha + \hat{0} = \alpha$; $\alpha + S(\beta) = S(\alpha + \beta)$; $\alpha + \lambda = \sup_{\beta<\lambda}(\alpha + \beta)$.
(2) $\alpha \times \hat{0} = \hat{0}$; $\alpha \times S(\beta) = (\alpha \times \beta) + \alpha$; $\alpha \times \lambda = \sup_{\beta<\lambda}(\alpha \times \beta)$.
(3) $\alpha^{\hat{0}} = \hat{1}$; $\alpha^{S(\beta)} = \alpha^\beta \times \alpha$; $\alpha^\lambda = \sup_{\beta<\lambda}(\alpha^\beta)$.

Inoltre, è possibile dimostrare che valgono le seguenti proprietà d'ordine.

PROPOSIZIONE 6.2. *Somma, prodotto ed esponenziazione sono strettamente crescenti nel secondo argomento e continue.*

$$\beta < \beta' \Rightarrow \alpha + \beta < \alpha + \beta'; \;\; \alpha + \lambda = \sup_{\beta<\lambda}(\alpha + \beta).$$
$$\beta < \beta' \Rightarrow \alpha \times \beta < \alpha \times \beta'; \;\; \alpha \times \lambda = \sup_{\beta<\lambda}(\alpha \times \beta).$$
$$\beta < \beta' \Rightarrow \alpha^\beta < \alpha^{\beta'}; \;\; \alpha^\lambda = \sup_{\beta<\lambda}(\alpha^\beta).$$

$(\mathbf{ORD}, <)$ inizia dunque così:

$$\hat{0} < \hat{1} < \hat{2} < \cdots < \omega < \omega{+}1 < \omega{+}2 < \cdots < \omega{+}\omega = \sup(\omega{+}n) = \omega{\times}2 < \omega{\times}2{+}1 < \ldots$$
$$\omega \times 3 < \cdots < \omega \times 4 < \cdots < \omega \times \omega = \sup(\omega \times n) = \omega^2 < \ldots$$
$$\omega^2 \times \omega = \sup(\omega^2 \times n) = \omega^3 < \cdots < \omega^4 < \cdots < \omega^\omega = \sup(\omega^n) < \ldots$$
$$\omega^\omega + 1 < \ldots \omega^\omega \times 2 < \cdots < \omega^\omega \times \omega = \omega^{\omega+1} < \ldots$$
$$\omega^{\omega\times 2} < \cdots < \omega^{\omega^\omega} < \cdots < \omega^{\omega^{\omega^\omega}} < \ldots$$

OSSERVAZIONE 6.3. Il sup dell'insieme di ordinali $\{\omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}} \ldots\}$ viene denotato con ε_0, ed è strettamente maggiore di tutti gli ordinali dell'insieme (l'insieme non ha massimo). Ciò non ostante, è ancora un insieme *numerabile*, i.e. i suoi elementi possono essere posti in corrispondenza biunivoca con $\mathbf{N}$. Gli ordinali qui sopra formano dunque soltanto un piccolo pezzo iniziale di $\mathbf{ORD}$.

7. Il paradosso di Burali-Forti

TEOREMA 7.1. *L'esistenza dell'insieme degli ordinali è contraddittoria!*

DIMOSTRAZIONE. Abbiamo dimostrato che $(\mathbf{ORD}, <)$ è un buon ordinamento. Per tanto, la funzione Ord associa a questo buon ordine un ordinale. Sia

$$\Omega = Ord(\mathbf{ORD}, <).$$

Per quanto visto sopra, l'ordinale Ω è l'insieme degli ordinali minori di esso, i.e.,

$$\Omega = \{\alpha \text{ t.c. } \alpha < \Omega\}.$$

In altre parole

$$\Omega = \mathbf{ORD}_\Omega,$$

e per tanto

$$\mathbf{ORD} \cong \mathbf{ORD}_\Omega.$$

Ma nessun buon ordinamento può essere isomorfo a una propria sezione! □

Cosa abbiamo fatto di male?

CAPITOLO 5

Assiomi per la Teoria degli Insiemi

1. Sinossi

Introduciamo e motiviamo i primi assiomi della teoria di Zermelo-Fraenkel. Descriviamo le controparti insiemistiche delle comuni nozioni matematiche.

2. Paradossi e Assiomatizzazione

Il paradosso di Burali-Forti, che abbiamo incontrato proprio quando la nostra teoria delle quantità e dei numeri (ordinali) infiniti sembrava prendere una buona piega, ci costringe a ritornare sui nostri passi per capire quali passi falsi abbiamo fatto. I problemi possono derivare, per esempio, dalla libertà che abbiamo usato nell'applicare principii troppo potenti di *costruzione di insiemi*. La colpa potrebbe certo essere, a priori, anche di *principii di esistenza* troppo forti. Ma una breve rilettura dei nostri argomenti lo esclude. D'altra parte, un altro famoso paradosso, quello di Russell, che fa da controparte "filosofica" al paradosso puramente matematico di Burali-Forti, ci indica che la causa dei paradossi è da cercarsi nella liberalità dei principii che ci siamo concessi per la creazione di nuovi insiemi.

Il ricorso ad una assiomatizzazione fu la reazione naturale per i matematici del XIX secolo e probabilmente lo sarebbe anche oggi. Vogliamo dunque offrire una formulazione assiomatica della nostra Teoria degli Insiemi. Gli assiomi devono soddisfare almeno due *desiderata*.

- Devono essere abbastanza forti da permetterci di fare tutte quelle costruzioni che sono necessarie allo sviluppo della teoria.
- Non devono essere abbastanza forti da rendere possibile la costruzione di insiemi paradossali.

Qui sotto ci concentreremo sulla più nota e diffusa assiomatizzazione della teoria degli insiemi, la teoria di Zermelo-Fraenkel. La teoria può essere formalizzata nel linguaggio della logica del prim'ordine, con un unico simbolo extralogico $\in$ per l'appartenenza. Noi ci manterremo quasi sempre ad un livello semi-formale. Il principio fondamentale che informa la teoria di Zermelo-Fraenkel è il cosidetto *Limitation of Size Principle*, che riconosce la causa dei paradossi nell'esistenza di insiemi *molto grandi*.

3. Insiemi e Classi

Una volta decisi gli assiomi, la situazione sarà la seguente. La nozione intuitiva di *insieme* sarà sostituita con la nozione formale di *essere (la denotazione di) una* variabile x per cui si dimostra, nella teoria di Zermelo-Fraenkel, un asserto della forma

$$\exists x \varphi(x).$$

In altre parole, gli *insiemi* sono gli oggetti di cui si dimostra *l'esistenza* nella teoria assiomatizzata. Per esempio, nella nostra teoria assiomatica, la collezione di tutti gli ordinali, che abbiamo chiamato **ORD**, non sarà un insieme. Questo significa che dovremmo rinunciare alla nostra teoria degli ordinali infiniti? Assolutamente no. Potremmo senz'altro parlare di ordinali nella teoria, e anche quantificare sugli ordinali, fatto salvo che non potremmo dimostrare che la collezione di tutti e soli gli ordinali è un insieme. Si vede facilmente, infatti, che è possibile scrivere una formula $\theta(x)$ del primo ordine nel linguaggio con il solo simbolo extralogico $\in$, che esprima il concetto di *ordinale* così come definito da Von Neumann (un insieme bene ordinato da $\in$ e transitivo). (Esercizio: scrivere una tale formula), i.e. tale che

$$\theta(x) \text{ è vera } \Leftrightarrow x \text{ è un ordinale di Von Neumann.}$$

Possiamo dunque parlare di ordinali e dimostrare proprietà degli ordinali nella nostra teoria, anche se non possiamo dimostrare proposizioni del tipo

$$\exists y \forall x (x \in y \leftrightarrow \theta(x)).$$

Quando un concetto è definibile ma non si può dimostrare nella teoria che la sua estensione (la collezione di tutti gli oggetti che soddisfano il concetto) esiste, diciamo che il concetto definisce una *classe propria*. Gli ordinali nella teoria di Zermelo-Fraenkel, e con loro tutte le collezioni *troppo grandi* formano classi proprie e non insiemi. Ciò detto, tutto ciò che abbiamo dimostrato sugli ordinali rimane vero, a partire dalla definizione esplicita di ordinale di Von Neumann.

4. Alcune operazioni irrinunciabili

Quali sono i tipi di oggetto e le operazioni alle quali non possiamo rinunciare? Ricordiamo che ci sono due modi di vedere la teoria degli insiemi. Nella prima accezione, è la teoria delle quantità infinite in atto, o dei numeri infiniti. Nella seconda accezione, è una teoria fondazionale all'interno della quale vogliamo poter riformulare tutte le comuni nozioni matematiche e dimostrare tutti i comuni risultati delle varie branche della matematica. Nel primo caso, ci è sufficiente poter disporre di tutte le operazioni e di tutti gli insiemi necessari allo sviluppo della teoria dei numeri infiniti (ordinali prima e cardinali poi). Nel secondo caso, dobbiamo preoccuparci anche di avere assiomi sufficienti a condurre tutti gli argomenti di teoria dei numeri, di analisi, di topologia, etc., nonché di garantire l'esistenza di insiemi numerici fondamentali quali l'insieme dei naturali, degli interi, dei razionali, dei reali, dei complessi.

Vedremo come gli assiomi di ZF rispondono ad entrambe le esigenze. Cominciamo per tanto a concentrarci su alcune operazioni combinatorie irrinunciabili. In ciascun caso vogliamo anche sincerarci di rispettare il principio della *Limitation of Size*. Le operazioni non devono permetterci di costruire insiemi troppo grandi, relativamente agli insiemi di partenza.

4.1. Coppia. Un'operazione fondamentale è quella che ci permette di passare, da due oggetti dati separatemente, a e b, al considerarli insieme, ossia al considerare la coppia di a e di b. In termini di insiemi ciò si traduce nell'insieme $\{a, b\}$ che contiene a, b e nulla più. Sembra ragionevole supporre che, se a e b non sono troppo grandi, neanche $\{a, b\}$ è troppo grande. Il nostro primo assioma sarà

dunque l'Assioma della Coppia, che garantisce la buona definizione dell'operazione seguente:[1]

$$a, b \mapsto \{a, b\}.$$

4.2. Unione. Se, nella nostra teoria, possiamo considerare un insieme di insiemi A, molto probabilmente vorremo anche essere capaci di *guardare dentro gli elementi di* A e di considerare *insieme*, come un oggetto unitario, il risultato di questo *spacchettamento* di A. Per esempio, se abbiamo $A = \{A_1, A_2, A_3\}$, $A_1 = \{0, 1, 2\}$, $A_2 = \{1, 2, 3\}$, $A_3 = \{2, 3, 4\}$, vogliamo esser capaci di considerare l'insieme che riunisce in un unico tutto gli elementi di A_1, di A_2 e di A_3, ossia l'insieme $\{0, 1, 2, 3, 4\}$, che denotiamo con $\bigcup A$ (unione di A), o, equivalentemente, con $A_1 \cup A_2 \cup A_3$ (A_1 unione A_2 unione A_3). Il principio della *Limitation of Size* sembra ragionevolmente rispettato: se l'esistenza dell'insieme A è garantita dai nostri assiomi, e dunque A non è troppo grande, allora non contiene un numero troppo grande di elementi e ciascun elemento è a sua volta un insieme non troppo grande. Prendere l'unione degli elementi di un numero non troppo grande di insiemi non troppo grandi non dovrebbe risultare in un insieme troppo grande. Il nostro secondo assioma, l'Assioma dell'Unione, ci garantisce l'esistenza dell'insieme unione, per ogni insieme A dato, i.e. la buona definizione della seguente operazione.

$$a \mapsto \bigcup a.$$

Osserviamo che, denotando con $a \cup b$ l'insieme $\bigcup\{a, b\}$, l'operazione

$$a, b \mapsto a \cup b$$

resti definita dall'Assioma di Coppia e di Unione.

4.3. Potenza. Se un insieme A è un oggetto della nostra teoria, vogliamo essere capaci di considerare come un oggetto unitario, dunque come un insieme, anche l'insieme di tutti i sottinsiemi di A, ossia l'insieme delle parti o insieme potenza. L'intuizione sulla grandezza è qui decisamente più debole che nei casi precedenti. Cosa ci garantisce che l'insieme potenza di un insieme non troppo grande sia a sua volta non troppo grande? Nel caso di insiemi finiti, sappiamo esattamente quanti elementi contiene l'insieme delle parti (2^n se l'insieme di partenza ne contiene n) e possiamo giudicare questo salto come non problematico. Vedremo che lo stesso è vero nel caso degli insiemi infiniti. Ciò non ostante, non dovrà forse stupire che l'operazione che porta dal numero degli elementi di un insieme A al numero degli elementi dell'insieme delle parti di A è una delle più problematiche della teoria degli insiemi, ed è strettamente connessa al cosidetto Problema del Continuo, di cui discuteremo più avanti. Ciò non ostante, escludere l'assioma delle parti dalla nostra teoria significherebbe mutilarla troppo severamente, sia nella prospettiva di sviluppare una teoria fondazionale, sia dal punto di vista dello sviluppo di una teoria delle quantità infinite in atto. Per tanto, includiamo come nostro terzo assioma l'Assioma delle Parti, che garantisce l'esistenza dell' insieme $\mathcal{P}(a)$ per ogni insieme dato a, i.e. la buona definizione dell'operazione

$$a \mapsto \mathcal{P}(a).$$

[1]Osserviamo che l'Assioma della Coppia ci garantisce anche l'esistenza del *singoletto* di un qualunque insieme a dato. Infatti la coppia $\{a, a\}$ altro non è che l'insieme $\{a\}$, dato che gli insiemi sono oggetti estensionali (cfr. infra).

4.4. Separazione. Il paradosso di Russell ci ha resi diffidenti verso il Principio di Comprensione, i.e., l'idea che ogni concetto ben definito definisca un insieme come sua estensione. L'Assioma di Separazione è una restrizione del Princio di Comprensione: dato un insieme a, e un concetto ben definito C, è lecito *selezionare*, *separare* gli elementi di a che soddisfano C. In altre parole, esistono tutti gli insiemi che possiamo ritagliare da un insieme già dato, usando, come forbici, formule del prim'ordine. L'Assioma di Separazione garantisce dunque la buona definizione della seguente operazione, dove φ è una formula del prim'ordine[2]

$$a, \varphi \mapsto \{x \in a \text{ tali che } \varphi(x)\}.$$

Osservazione 4.1. Da notare che l'Assiome delle Parti garantisce, per ogni insieme dato A, l'esistenza di un insieme che contenga come elementi tutti e soli i sottinsiemi di A. Nulla nella formulazione dell'assioma ne restringe l'azione a sottinsiemi descritti o descrivibili da formule del primo'ordine. L'insieme $\mathcal{P}(A)$ contiene bensì *tutti (e soli)* i sottinsiemi di A, i.e. tutti quegli oggetti x di cui si può dimostrare che non contengono altro che elementi di A! Al contrario, l'Assioma di Separazione permette la selezione di sottinsiemi definibili al prim'ordine (con parametri) all'interno di un insieme dato.

Ora che abbiamo a disposizione un certo numero di principii di costruzione d'insiemi, consideriamo la domanda: quali tipi di oggetto sono necessari per la nostra teoria?

5. Rappresentazione dei concetti matematici

Nella nostra trattazione fino a questo punto, così come accade abitualmente nella matematica, abbiamo spesso usato *tipi* differenti di oggetti. Per esempio, abbiamo parlato di numeri naturali, razionali, etc., di coppie di oggetti, di coppie di numeri, di funzioni da un insieme a un altro, di dominio e codominio di funzioni, di isomorfismi, di relazioni, di successioni etc. Vedremo qui di seguito come non sia necessario moltiplicare i tipi fondamentali di oggetti considerati nella nostra teoria. Possiamo infatti limitarci ad una teoria degli insiemi 'pura', nella quale esistono solo insiemi e nella quale si possono indicare *controparti insiemistiche* di tutti gli altri tipi di oggetto matematico (coppie, funzioni, relazioni, insiemi numerici etc.). Questo risponde al duplice scopo di *semplicità* e di *onnicomprensività* della teoria.

Quando diciamo che tutti gli oggetti della nostra teoria sono *insiemi*, intendiamo dire che l'unica relazione primitiva prevista dalla teoria è la relazione d'appartenenza (denotata con $\in$) e che gli oggetti della teoria sono oggetti *estensionali*, i.e., caratterizzati completamente dai loro elementi. In altre parole, assumiamo l'Assioma di Estensionalità, che possiamo formulare come segue.

$$\forall x \forall y [\forall z (z \in x \leftrightarrow z \in y) \leftrightarrow x = y].$$

5.1. Coppie Ordinate. Abbiamo più volte parlato liberamente di coppie (ordinate) di oggetti, di numeri, di insiemi, etc. Per esempio, abbiamo definito un buon ordinamento come una coppia (A, R), dove A è un insieme e R è una relazione su A con certe proprietà. (A, R) indicava una coppia ordinata, una coppia cioè di due oggetti, uno dei quali possiamo univocamente indicare come il primo dei due (un oggetto (S, A) dove S è una relazione e A un insieme non è un buon ordine secondo

[2]Una formulazione completa include anche la dipendenza di φ da altri parametri: dati a insieme, φ formula, b insieme (parametro), esiste l'insieme degli x in a per cui vale $\varphi(x, b)$.

la nostra definizione). Un altro caso in cui abbiamo considerato le coppie è quando abbiamo definito un buon ordinamento dell'insieme di tutte le coppie di numeri naturali. Il concetto di coppia ordinata è fondamentale in matematica. Per tanto, vogliamo indicarne una controparte insiemistica. Nel fare ciò, teniamo presente quali sono le caratteristiche (per noi) essenziali del concetto di coppia ordinata. In altre parole, possiamo chiederci quale sia il *criterio di identità* per le coppie ordinate. Vediamo facilmente che due coppie ordinate (a, b) e (c, d) sono da considerarsi identiche se e soltanto se sono identici, termine a termine, i loro componenti, i.e.

$$(a, b) = (c, d) \Leftrightarrow a = b \& c = d.$$

Sarà allora sufficiente trovare un modo di associare, a qualunque paio di insiemi a, b dati, un insieme, chiamiamolo $C_{a,b}$, che soddisfi il criterio di identità delle coppie ordinate. Ossia deve valere che, per ogni a, b, c, d,

$$C_{a,b} = C_{c,d} \Leftrightarrow a = b \& c = d.$$

Vi sono tante scelte per un costrutto $C_{a,b}$ che soddisfi queste proprietà. La scelta canonica (introdotta da Kuratowski) è la seguente:

$$\{\{a, b\}, a\}.$$

Si verifica facilmente (Esercizio) che vale

$$\{\{a, b\}, a\} = \{\{c, d\}, c\} \Leftrightarrow a = b \& c = d.$$

Dunque possiamo prendere $\{\{a, b\}, a\}$ come controparte insiemistica della coppia ordinata di a e b, e denoteremo un tale insieme da ora in poi con (a, b).

La domanda seguente è: gli assiomi introdotti finora ci assicurano l'esistenza della coppia ordinata (a, b), dati gli oggetti a e b? In altre parole, è ben definita l'operazione

$$a, b \mapsto (a, b)?$$

Vediamo che la risposta è sì, applicando due volte l'assioma della coppia (non ordinata):

$$a, b \mapsto \{a, b\}$$

$$\{a, b\}, a \mapsto \{\{a, b\}, a\}.$$

Osserviamo anche che la proprietà di essere una coppia ordinata con a al primo posto e b al secondo posto si può esprimere con una formula del primo ordine. Preliminarmente osserviamo che esiste una formula del primo ordine che esprime la proprietà di essere una coppia non ordinata:

$$\mathsf{coppia}(x) := \exists z \exists y (z \in x \wedge y \in x \wedge \forall w (w \in x \rightarrow w = z \vee w = y)).$$

Analogamente, per a e b qualunque, la formula seguente (con parametri a e b) esprime la proprietà d'essere una coppia non ordinata di a e b:

$$\mathsf{coppiaPar}(x, a, b) := (a \in x \wedge b \in x \wedge \forall w (w \in x \rightarrow w = a \vee w = b)).$$

Allora la proprietà d'essere la coppia ordinata (a, b) si può esprimere come segue.

$$\mathsf{coppiaOrdinata}(x, a, b) := \exists z \exists y (z \in x \wedge \mathsf{coppiaPar}(z, a, b) \wedge y = a \wedge \mathsf{coppia}(x)).$$

Osserviamo infine che la nozione di coppia ordinata ci permette di definire n-ple ordinate per qualunque n, semplicemente ponendo

$$(a, b, c) = ((a, b), c), (a, b, c, d) = ((a, b, c), d), etc.$$

5.2. Insieme Prodotto. Dati due insiemi a e b, è spesso utile e naturale considerare il prodotto (cartesiano) $a \times b$, costituito dalle coppie ordinate che hanno un elemento di a al primo posto ed un elemento di b al secondo posto. Abbiamo implicitamente utilizzato una simile costruzione - detta prodotto cartesiano - quando abbiamo menzionato insiemi come $\mathbf{N} \times \mathbf{N}$. Nella nostra teoria, il prodotto $a \times b$ sarà semplicemente identificato con l'insieme

$$\{(x, y) \text{ tali che } x \in a \wedge y \in b\}.$$

Resta dunque soltanto la domanda: è garantita l'esistenza di $a \times b$ dati a e b? L'operazione seguente è ben definita in base agli assiomi?

$$a, b \mapsto a \times b.$$

Vediamo che la risposta è sì. Chidiamoci prima: dove *vive* l'insieme $a \times b$, ossia, di quale insieme è elemento, oppure: di quale insieme è sottinsieme? Se individuiamo un insieme S tale che $a \times b$ è un sottinsieme di S, allora è immediato ottenere l'esistenza di $a \times b$ usando l'Assioma di Separazione (che tipo di elementi siano contenuti in $a \times b$ è facilmente descrivibile al primo ordine). $a \times b$ è un insieme di oggetti del tipo $\{\{x, y\}, x\}$, con $x \in a$ e $y \in b$. Gli oggetti del tipo $\{x, y\}$ sono sottinsiemi di $a \cup b$ (che esiste per Assioma dell'Unione). Dunque sono elementi di $\mathcal{P}(a \cup b)$, che esiste per Assioma delle Parti. Allora gli oggetti del tipo $\{\{x, y\}, x\}$ sono sottinsiemi di $\mathcal{P}(a \cup b) \cup a$, che esiste per Assioma dell'Unione. L'insieme $\mathcal{P}(a \cup b) \cup a$ contiene molti sottinsiemi oltre a $a \times b$, e dunque dobbiamo indicare una formula che ci permetta di *separare* l'insieme $a \times b$ dagli altri, nell'ambiente $\mathcal{P}(a \cup b) \cup a$. La formula è semplicemente quella che esprime che $a \times b$ è un insieme di coppie ordinate di elementi di a al primo posto e di b al secondo posto (Esercizio: scrivere esplicitamente una tale formula. Ci si può avvalere delle formule definite sopra per coppie, coppie ordinate etc.).

5.3. Relazioni. In teoria degli insiemi una relazione binaria non è altro che un insieme di coppie. Per tanto, ogni relazione tra oggetti di a e di b è un sottinsieme del prodotto cartesiano $a \times b$, i.e. è elemento di $\mathcal{P}(a \times b)$. Ciò ci garantisce, per Separazione, l'esistenza di tutte le relazioni tra elementi di a e di b che siano esprimibili da una formula del prim'ordine. L'insieme di tutte le relazioni tra elementi di a e di b coincide invece con l'insieme di tutti i possibili sottinsiemi di coppie ordinate con prima componente in a e seconda in b, i.e., con l'insieme $\mathcal{P}(a \times b)$. Analogamente, la controparte insiemistica di una relazione n-aria è un insieme di n-ple ordinate.

5.4. Funzioni. Abbiamo liberamente usato i concetti di funzione, dominio e codominio. In generale, in matematica una funzione può essere concepita come una operazione su elementi o come una regola di associazione di elementi. Come controparte insiemistica di una funzione se ne prende il grafico, ossia l'insieme delle coppie ordinate il cui primo elemento è l'argomento della funzione e il cui secondo elemento è il valore della funzione in corrispondenza di quell'argomento. Per esempio, la funzione $f(n) = n \times 2$ sui naturali è *identificata* con l'insieme delle coppie di (valore, argomento).

$$\{(0, 0), (1, 2), (2, 4), (3, 6), (4, 8), \dots\}.$$

Più rigorosamente, chiamiamo una *relazione funzionale* o *funzione* una relazione R che soddisfa la seguente proprietà: per nessun x, R contiene due coppie (x, y) e (x, z) con $y \neq z$. Il che significa che R non è uno-molti: ogni elemento viene

associato a non più di un elemento. Dunque una funzione è un tipo particolare di relazione. Il *dominio* di una funzione F è costituito dall'insieme degli elementi che appaiono con prime componenti di una coppia ordinata appartenente F. Il codominio di una funzione F è l'insieme degli elementi che appaiono come seconda componente di una coppia ordinata appartenente ad F.

5.5. Insiemi Numerici. Nella prospettiva che considera la teoria degli insiemi come una teoria fondazionale per l'intero edificio matematico, o comunque come una teoria-quadro onnicomprensiva, è necessario indicare le controparti insiemistiche degli insiemi numerici fondamentali. Lo facciamo qui, brevemente. Supponiamo per il momento di avere a disposizione $\mathbf{N}$ o una sua controparte insiemistica (beneducata) e indichiamo come definire controparti insiemistiche degli interi relativi, dei razionali, dei reali e dei complessi:

$$\mathbf{N} \longrightarrow \mathbf{Z} \longrightarrow \mathbf{Q} \longrightarrow \mathbf{R} \longrightarrow \mathbf{C}$$

Gli interi relativi, $\{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$ si possono ottenere come un particolare sottinsieme di coppie ordinate di naturali, ossia come un sottinsieme di $\mathbf{N} \times \mathbf{N}$. Si può prendere infatti la coppia $(0, n)$ come controparte del numero negativo $-n$. La controparte di $\mathbf{Z}$ è allora l'insieme $\mathbf{N} \cup \{(0, n)$ tali che $n \in \mathbf{N}\}$, su cui si definisce una appropriata relazione d'ordine (che soddisfi $(0, n) < (0, m)$ se $n < m$, e $(0, n) < m$ per ogni n, m, e coincida con l'usuale relazione d'ordine su $\mathbf{N}$). Analogamente possiamo rappresentare $\mathbf{Q}$ come un insieme di coppie ordinate con prima componente intera e seconda componente positiva, tale che le componenti siano relativamente prime tra loro: (k, ℓ) rappresenta allora la frazione $\frac{k}{\ell}$ (nella sua forma ridotta ai minimi termini). Un'opportuna relazione d'ordina completa la definizione. Una scelta per la controparte formale dei reali è la seguente. Possiamo vedere l'insieme dei reali come unione dell'insieme dei numeri razionali (già definiti) e dei numeri irrazionali. L'Analisi ci insegna come i numeri irrazionali si possano definire come sottinsiemi di $\mathbf{Q}$: un numero irrazionale è un segmento iniziale S di $\mathbf{Q}$, non vuoto, che non coincida con tutto $\mathbf{Q}$, privo di massimo, e tale che il complemento $\mathbf{Q} - S$ non ha minimo. Allora la controparte insiemistica di $\mathbf{R}$ si ottiene come unione di $\mathbf{Q}$ e dei numeri irrazionali come li abbiamo appena definiti. Infine, il campo dei numeri complessi si ottiene naturalmente come insieme di coppie ordinate di reali: la coppia (a, b) di reali rappresenta il complesso $a + ib$ (a è la parte reale, b la parte immaginaria, i è la radice di -1).

6. Infinito

Nella sezione precedente abbiamo definito controparti formali degli insiemi numerici fondamentali, supponendo di avere l'insieme $\mathbf{N}$. Vediamo ora come definire una controparte formale di questo insieme. Quando abbiamo sviluppato gli inizi della teoria degli ordinali abbiamo incontrato controparti insiemistiche dei numeri interi:

$$\varnothing < S(\varnothing) = \varnothing \cup \{\varnothing\} < S(S(\varnothing)) = S(\varnothing) \cup \{S(\varnothing)\} < \dots$$

Si vede facilmente che l'operazione di successore,

$$a \mapsto S(a)$$

è ben definita per qualunque a in base agli assiomi dati finora. Per definizione infatti $S(a) = a \cup \{a\}$ e pertanto bastano due applicazioni dell'Assioma dell'Unione per ottenere $S(a)$ da a. Ciò che gli assiomi non garantiscono è l'esistenza di un

insieme che contenga tutta la sequenza di successori dell'insieme vuoto. Trattando degli ordinali, avevamo ottenuto un tale insieme, ω, come sup, ossia unione, degli $S^n(\varnothing)$. Ma i nostri assiomi non ci permettono ancora di dimostrare l'esistenza di un tale sup. Anche se il sup è un'unione, l'Assioma dell'Unione è insufficiente, perché è l'esistenza dell'insieme di partenza su cui fare l'unione a non essere garantita! Ci manca un assioma che garantisca l'esistenza del seguente insieme.

$$\{\varnothing, S(\varnothing), S^2(\varnothing), \dots, S^n(\varnothing), \dots\}.$$

Il nostro nuovo assioma è l'Assioma dell'Infinito, che asserisce l'esistenza di un insieme *chiuso per successore*, ossia di un insieme tale che, se contiene un elemento x, contiene anche il successore $S(x)$ di x. In formule:

$$\exists x(x \neq \varnothing \wedge \forall y(y \in x \to S(y) \in x)).$$

L'insieme $\omega = \{\varnothing, S(\varnothing), S^2(\varnothing), \dots, S^n(\varnothing), \dots\}$ è allora ottenuto come il più piccolo insieme chiuso per successore.

7. Rimpiazzamento

Se a è un insieme non troppo grande, e F è una formula che definisce una funzione, allora è ragionevole aspettarsi che l'insieme degli elementi che F fa corrispondere agli elementi di a non è troppo grande. Da notare subito che qui con 'funzione' *non* intendiamo un insieme di coppie ordinate con una certa proprietà. Se intendessimo soltanto questo non staremmo aggiungendo nulla a ciò che possiamo già fare con i nostri assiomi: se F è una funzione, nel senso di insieme di coppie ordinate, allora è immediato concludere che l'immagine di F è un insieme. L'immagine di F è l'insieme $\{y \text{ t.c. } \exists x(x, y) \in F\}$. Quando diciamo che F è una formula che definisce una funzione su a, stiamo dicendo che esiste una formula $\varphi(x, y)$ tale che *si dimostra* nella teoria la seguente proprietà di *funzionalità*.

$$\forall x \forall y \forall z(\varphi(x, y) \wedge \varphi(x, z) \to y = z).$$

Si vede allora facilmente perché diciamo che una tale φ definisce una funzione: se si considerano le coppie ordinate (x, y) di oggetti per cui vale $\varphi(x, y)$, si ha una relazione funzionale. L'Assioma di Rimpiazzamento garantisce che la seguente operazione è sempre definita.

$$(\varphi \text{ formula che definisce una funzione }, x) \mapsto \{y \text{ t.c. } \exists x \varphi(x, y)\}.$$

Qual è l'utilità dell'Assioma di Rimpiazzamento? Se torniamo sui nostri passi, troviamo indicazioni della necessità di questo assioma in un punto chiave della teoria degli ordinali: il Teorema di Comparabilità dei buoni ordini. Nella dimostrazione di quel teorema, presi buoni ordini (A, R), e (B, S), si definiva una relazione $F(a, b)$ che metteva in relazione $a \in A$ e $b \in B$ che determinavano segmenti iniziali isomorfi, i.e. tali che $A_a \cong B_b$. Si procedeva poi dimostrando che F è una relazione funzionale, e che o il dominio di F era tutto A o il codominio di F era tutto B. Osserviamo ora che il medesimo argomento può condursi partendo dai buoni ordini (A, R) e $(\mathbf{ORD}, <)$. La relazione F è allora la seguente

$$F = \{(a, \alpha) \text{ tali che } a \in A, \alpha \in \mathbf{ORD} \wedge (A_a, R) \cong \alpha\}.$$

Si dimostra facilmente che F è funzionale e che ha dominio e codominio chiusi all'in giù. Ora possiamo argomentare come segue: il codominio di F non può essere **ORD**, perché sappiamo che ORD non può essere un insieme (Paradosso di Burali-Forti). Come nell'argomento precedente, ciò lascia la sola possibilità che il dominio

di F sia tutto A. Pertanto F definisce un isomorfismo tra A e un segmento iniziale di **ORD**, ossia un ordinale, e resta dimostrato, come Corollario del Teorema di Comparabilità (e con il medesimo argomento), che ogni buon ordine è isomorfo ad un (unico) ordinale.

L'argomento appena descritto contiene un'applicazione dell'Assioma di Rimpiazzamento: quando escludiamo che il codominio di F è **ORD**, perché **ORD** non è un insieme, stiamo presupponendo che il codominio di A è un insieme, se A è un insieme. Ma questo è esattamente quanto ci dice il Rimpiazzamento. Senza Assioma di Rimpiazzamento non potremmo trarre questa conclusione.

Un altro esempio. Se λ è un ordinale, non è difficile vedere che resta definito, per separazione, l'insieme delle terne (α, β, γ) tali che α, β, γ sono in λ (e per tanto minori di λ), e $\alpha + \beta = \gamma$. In altre parole, con l'Assioma di Separazione possiamo definire la somma ristretta ad ordinali minori di λ, per un qualunque ordinale λ dato. D'altra parte, *non possiamo* dimostrare che la somma è definita su **ORD**, ossia che vale:

$$\forall\alpha\beta\exists\gamma(\alpha + \beta = \gamma).$$

CAPITOLO 6

Cardinali

1. Sinossi

Riprendiamo lo sviluppo di una teoria quantitativa degli insiemi e definiamo il concetto di numero cardinale. Definiamo la serie dei cardinali transfiniti.

2. Classi di Equipotenza

Con il concetto di numero ordinale abbiamo ottenuto la comparabilità di insiemi infiniti che si differenziano *per quantità* e *per tipo d'ordine*. Un ordinale è infatti non altro che un rappresentante canonico della propria classe d'isomorfismo, e il teorema di comparabilità dei buoni ordini ci dice che l'ordine indotto dalla relazione di *'essere isomorfo ad un segmento iniziale di'* forma un ordine totale sulle classi di isomorfismo.

Ciò che ci manca per una teoria puramente quantitativa degli insiemi sono almeno due cose.

- La prima è la necessità di astrarre dal tipo d'ordine di un insieme e di badare soltanto alla quantità dei suoi elementi. In questo senso vogliamo tornare al concetto originale di equipotenza.
- La seconda è la necessità di paragonare per grandezza insiemi qualunque, mentre, con la nozione di isomorfismo, siamo costretti a considerare soltanto insiemi bene ordinati.

Se partizioniamo l'universo di tutti gli insiemi in classi di equipotenza otteniamo una partizione che è *meno fine* di quella ottenuta partizionando l'universo degli insiemi ordinati in classi di isomorfismo (ossia una classe di equipotenza raggruppa nella stessa cella insiemi che erano prima distinti in diverse classi di isomorfismo) ma *più completa*, nel senso che ogni insieme - sia esso bene ordinato, ordinato o non ordinato - cade in una e una sola classe di equipotenza (mentre gli insiemi non bene ordinati restano fuori da ogni classe di isomorfismo).

Come sappiamo, pur supponendo di saper scegliere un rappresentante canonico in ciascuna di queste classi, perdiamo immediatamente la proprietà di comparabilità. Dati due insiemi A e B, non vale che o A è equipotente ad un sottinsieme di B o viceversa.

Se, al contrario, consideriamo soltanto classi di equipotenza che contengono almeno un insieme bene ordinato, e dunque un ordinale (sappiamo che ogni insieme bene ordinato è isomorfo ad un unico ordinale), abbiamo non solo una scelta canonica di un rappresentante per quella classe di equipotenza (basta prendere il minimo ordinale della classe, nell'ordinamento degli ordinali) ma abbiamo anche la comparabilità di questi rappresentanti canonici.

La soluzione che adotteremo per risolvere la questione, e per avere botte piena e moglie ubriaca, è assiomatica. Assumeremo cioè un nuovo assioma, l'Assioma della Scelta, che garantisce proprio quel che ci serve.

(Assioma di Scelta) Ogni insieme è bene ordinabile.

L'Assioma di Scelta (che denoteremo AC da ora in poi, per *Axiom of Choice*) ci garantisce che ogni insieme *può* essere bene ordinato, ossia che per ogni insieme A *esiste* una relazione binaria R su di esso tale che R è un buon ordine. L'Assioma non ci permette di *esibire* una tale R, né di *definirlo*. L'Assioma si limita a garantircene l'esistenza. Perché l'Assioma di Scelta risolve la nostra *impasse* di sopra? Perché, se ogni insieme è bene ordinabile, allora

- Ogni insieme è equipotente ad un insieme bene ordinato,

o, in altre parole,

- Ogni classe di equipotenza contiene almeno un insieme bene ordinato,

e ciò implica a sua volta che

- Ogni classe di equipotenza contiene almeno un ordinale.

dunque, per concludere,

(1) In ogni classe di equipotenza possiamo scegliere il minimo ordinale come rappresentante canonico della classe; e
(2) I rappresentanti canonici di due classi di equipotenza sono sempre comparabili (perché sono ordinali!).

Abbiamo dunque fatto un bel passo avanti nello sviluppo di una teoria quantitativa degli insiemi. Ad ogni insieme A sappiamo come associare un ordinale α, i.e., il minimo ordinale in biiezione con A. Denotiamo l'ordinale associato ad A con $|A|$, e diamo la seguente definizione.

Definizione 2.1 (Cardinale). Un insieme è un *cardinale* se è un ordinale e se è il minimo ordinale nella propria classe di equipotenza. In altre parole un ordinale α è un cardinale se non esiste un ordinale β più piccolo di α che possa essere messo in biiezione con α.

Per esempio, tutti gli ordinali finiti sono anche cardinali. Infatti per ogni ordinale n vale che $n = \{0, 1, \dots, n-1\}$ non è in biiezione con nessun $m < n$.

Anche il primo ordinale infinito, l'ordinale ω, è un cardinale. Gli ordinali più piccoli di ω sono gli ordinali finiti e nessuno di essi è in biiezione con ω.

Al contrario, l'ordinale $\omega + 1$ (ossia l'insieme $\omega \cup \{\omega\}$) non è un cardinale. Si può infatti stabilire una biiezione tra questo ordinale e ω, che è un ordinale più piccolo. Ovviamente la biiezione non preserva l'ordine (non è un isomorfismo). Una biiezione è data dalle seguenti associazioni tra elementi di $\omega + 1$ e di ω.

$$\omega \mapsto 0; \quad \forall n \in \{0, 1, 2, \dots\})[n \mapsto n + 1].$$

In parole povere si manda l'elemento ω dell'insieme $\omega \cup \{\omega\}$ nello zero dell'insieme ω e l'elemento n di $\omega \cup \{\omega\}$ nell'elemento $n + 1$ di ω. Ovviamente è una biiezione, che testimonia che $|\omega + 1| = |\omega|$, e che dunque $\omega + 1$ non è un cardinale. Un ragionamento analogo si può fare per ogni ordinale infinito successore, ossia per ogni ordinale della forma $\alpha \cup \{\alpha\}$. Si ha dunque sempre, per ogni $\alpha \geq \omega$,

$$|\alpha + 1| = |\alpha|.$$

Dunque

Osservazione 2.2. Tutti i cardinali infiniti sono ordinali limite.

Osservazione 2.3. Se $|A| \leq |B|$ allora A si inietta in B.

Dimostrazione. Sia $\alpha = |A|$ e $\beta = |B|$. $\alpha \leq \beta$ implica che esiste un isomorfismo di α su un segmento iniziale di β (possibilmente su tutto β). In particolare un tale isomorfismo è una iniezione di α in β. Dato che α è in biiezione con A e β con B, si ottiene, componendo le biiezioni e l'isomorfismo, una iniezione di A in B. □

Osservazione 2.4. La serie dei cardinali è illimitata: dato un cardinale κ, esiste un cardinale μ maggiore di κ.

Dimostrazione. Dal Teorema di Cantor sappiamo che non esiste una iniezione di $\mathcal{P}(A)$ in A. Per tanto, non si può avere $|\mathcal{P}(A)| \leq |A|$. Dunque, per comparabilità degli ordinali, si ha $|A| < |\mathcal{P}(A)|$. Dato un qualunque insieme A, abbiamo determinata una sequenza illimiata di cardinali sempre più grandi:

$$|A| < |\mathcal{P}(A)| < |\mathcal{P}(\mathcal{P}(A))| < ...$$

□

Osservazione 2.5. Non esiste l'insieme di tutti i cardinali. I cardinali formano una classe propria.

Dimostrazione. Supponiamo per assurdo che esiste l'insieme A di tutti e soli i cardinali. Per ogni insieme x, si ha che $|x|$ è in A. Dato che i cardinali sono ordinali, A è un insieme di ordinali, e per tanto si può definire l'ordinale limite superiore di A. Poniamo

$$\alpha = \sup A.$$

Dunque, per ogni insieme x, $|x| \leq \alpha$. Poiché A è un insieme, per l'Assioma Potenza possiamo formare $\mathcal{P}(A)$ che è pure un insieme. Allora si ha che $|\mathcal{P}(A)|$ è un elemento di A, e per tanto che $|\mathcal{P}(A)| \leq \alpha$. Ma questo implica che esiste una iniezione dell'insieme potenza di A in A, il che sappiamo essere impossibile. □

Osservazione 2.6. Dato un cardinale κ, esiste il minimo cardinale strettamente maggiore di κ.

Dimostrazione. Abbiamo appena visto che esiste sempre un cardinale strettamente maggiore di un qualunque cardinale dato. Basta prendere il minimo. N.B. Se consideriamo *tutti* i cardinali strettamente maggiori di un cardinale dato, stiamo considerando una classe propria di ordinali. D'altra parte invece, dato un cardinale κ, sappiamo per Assioma di Potenza che esiste $\mathcal{P}(\kappa)$ e per quanto osservato sopra vale $\kappa < |\mathcal{P}(\kappa)|$. Per trovare il minimo cardinale strettamente maggiore di κ basta allora considerare l'insieme degli ordinali maggiori di κ e minori o uguali a $|\mathcal{P}(\kappa)|$. Questo è un insieme di ordinali (non una classe) e possiamo prendere il minimo (abbiamo già dimostrato che **Ord** è bene ordinato). □

Definizione 2.7. Dato un cardinale κ, denotiamo il minimo cardinale strettamente maggiore di κ con κ^+, e lo chiamiamo il *cardinale successore* di κ. Chiamiamo *cardinale limite* un cardinale che non è un successore.

PROPOSIZIONE 2.8. *Sia $(I, \prec)$ un ordine totale qualunque, e sia $(\kappa_i)_{i\in I}$ una successione strettamente crescente di cardinali indicizzata da elementi di I. Allora l'estremo superiore dell'insieme $\{\kappa_i \text{ t.c. } i \in I\}$ è un cardinale, che denotiamo anche con $\sup_{i\in I} \kappa_i$.*

DIMOSTRAZIONE. Che la successione $(\kappa_i)_{i\in I}$ è strettamente crescente significa che, per ogni $i, j \in I$, se $i \prec j$ allora $\kappa_i < \kappa_j$. Sappiamo per certo che $\sup_{i\in I} \kappa_i$ è un ordinale, perché gli ordinali sono chiusi per sup. Denotiamo allora $\sup_{i\in I} \kappa_i = \alpha$. Per mostrare che α è un cardinale basta mostrare che non è in biiezione con nessun ordinale più piccolo. Possiamo escludere subito il caso in cui l'ordine $(I, \prec)$ ha un massimo. Sia infatti i^* il massimo elemento di I (rispetto all'ordine $\prec$ di I). Allora, dato che $(\kappa_i)_{i\in I}$ è supposta strettamente crescente in i, ovviamente si ha che $\sup_{i\in I}$ è proprio κ_{i^*}, che è un cardinale...

Supponiamo dunque da ora in poi che I sia privo di massimo, ossia che per ogni $i \in I$ esiste $j \in I$ tale che $i \prec j$. Sia dunque $\beta < \alpha$. Per definizione di α si ha che esiste $i \in I$ tale che $\beta \leq \kappa_i$. Ma I non ha massimo, e per tanto esiste $j \in I$ tale che $i \prec j$. Poiché $(\kappa_i)_{i\in I}$ è strettamente crescente in i, si ha $\kappa_i < \kappa_j$. Dunque, si ha

$$\beta \leq \kappa_i < \kappa_j \leq \alpha.$$

Dalla relazione $\beta < \kappa_j$ concludiamo che κ_j non è in biiezione con l'ordinale β (perché κ_j è un cardinale e β un ordinale strettamente minore di esso). A fortiori α, che è almeno grande quanto κ_j non può essere in biiezione con β. Abbiamo dimostrato che α è un cardinale. □

I due ultimi risultati mostrano che la classe dei cardinali è chiusa sotto le seguenti operazioni.

- $\kappa \mapsto \kappa^+$,
- $(\kappa_i)_{i\in I} \mapsto \sup_{i\in I} \kappa_i$ (se $(\kappa_i)_{i\in I}$ è strettamente crescente).

Mostriamo qui di sotto come queste due operazioni siano sufficienti a descrivere *tutti* i cardinali.

Cominciamo con il descrivere una serie di cardinali, partendo dal più piccolo cardinale infinito, ω, e usando le operazioni di successore e estremo superiore. Poniamo allora

$$\omega, \omega^+, (\omega^+)^+, \dots \sup\{\omega, \omega^+, (\omega^+)^+, \dots\}, (\sup\{\omega, \omega^+, (\omega^+)^+, \dots\})^+, \dots$$

Possiamo riformulare la costruzione abbozzata qui sopra definendo una funzione F da **Ord** a **Card**

$$F : \mathbf{Ord} \longrightarrow \mathbf{Card},$$

usando gli ordinali per indicizzare (contare) i passi successivi della nostra costruzione. Ad ogni passo (valore di F) corrispondente ad un ordinale successore, si prende il cardinale successore del cardinale precedente, e ad ogni passo limite si prende il sup dei passi precedenti. Si pone dunque:

$$F(0) = \omega$$

$$F(\alpha + 1) = (F(\alpha))^+$$

$$F(\lambda) = \sup_{\gamma<\lambda} F(\gamma), \text{ per } \lambda \text{ limite.}$$

La serie qui sopra fu introdotta da Cantor, che invece di F usò il simbolo $\aleph$ per denotare i suoi cardinali transfiniti. La notazione di Cantor è tuttora in uso e la serie appena definita viene chiamata *serie degli aleph*, e inizia così:

$$\aleph_0, \aleph_1, \ldots, \aleph_\omega = \sup_{n\in\omega} \aleph_n, \aleph_{\omega+1}, \ldots,$$

Nota bene: questo è solo un altro modo di scrivere i valori

$$F(0), F(1), \ldots, F(\omega), F(\omega+1), \ldots.$$

In generale scriviamo $\aleph_\alpha$ invece di $F(\alpha)$. Forse Cantor aveva letto il seguente passo dello *Zohar*?

> Il Signore le disse: Aleph, Aleph, anche se inizierò la creazione del mondo con la lettera *beth*, tu resterai la prima delle lettere. Tu sola esprimerai la mia unità, su di te saranno basati tutti i calcoli e tutte le operazioni del mondo, e l'unità sarà espressa soltanto dalla lettera Aleph. (Zohar, I, 3a-3b)

Vediamo che proprietà ha la serie dei cardinali $(\aleph_\alpha)_{\alpha\in\mathbf{Ord}}$.

Osservazione 2.9. Per ogni α, $\aleph_\alpha$ è un cardinale, e la serie degli aleph è strettamente crescente, ossia

$$\beta < \alpha \Rightarrow \aleph_\beta < \aleph_\alpha.$$

Per il momento, sappiamo soltanto che la funzione $\aleph$ manda ordinali in cardinali, ossia ha tipo

$$\aleph : \mathbf{Ord} \longrightarrow \mathbf{Card}.$$

Vediamo ora che la funzione è suriettiva: ogni cardinale infinito è un aleph! In altre parole, con la serie degli aleph abbiamo fornito una descrizione esplicita di tutti e soli i numeri cardinali infiniti.

Proposizione 2.10. *Per ogni cardinale κ esiste un ordinale α tale che $\kappa = \aleph_\alpha$.*

Dimostrazione. Dimostriamo la proposizione per induzione sui cardinali, ossia dimostriamo la proprietà per un caso base ($\aleph_0$) e, supponendo che valga per tutti i cardinali minori di κ, la dimostriamo per κ. Distinguiamo a tal fine i casi successore e limite.

(Caso Base) $\kappa = \aleph_0$. In tal caso il risultato è ovvio.

(Caso Successore) Supponiamo κ cardinale successore, ossia $\kappa = \mu^+$ per qualche cardinale μ. Per ipotesi induttiva la tesi è vera per μ, i.e. esiste un ordinale β tale che

$$\mu = \aleph_\beta.$$

Ma allora

$$\kappa = \mu^+ = (\aleph_\beta)^+ = \aleph_{\beta+1},$$

dove l'ultima identità segue dalla definizione della funzione $\aleph$.

(Caso Limite) Supponiamo che κ sia un cardinale limite. Consideriamo l'insieme degli ordinali la cui immagine via $\aleph$ resta strettamente sotto κ, i.e.

$$A = \{\alpha | \aleph_\alpha < \kappa\}.$$

Dimostriamo che κ è l'immagine via $\aleph$ dell'estremo superiore di questo insieme A.

Poniamo $\beta = \sup A$. Osserviamo subito che β è un ordinale limite. Supponiamo infatti che β sia un ordinale successore, i.e. $\beta = \gamma + 1$. Allora β è un tipo d'ordine d'un ordine che ha un elemento massimo ($\beta+1$ è $\beta\cup\{\beta\}$). Dunque A ha un elemento

massimo, sia α. Allora α è il massimo ordinale tale che $\aleph_\alpha$ resta strettamente sotto il cardinale κ, il che significa che $\aleph_{\alpha+1}$ è $\geq \kappa$. Ma $\aleph_{\alpha+1}$ è $\aleph_\alpha^+$ e dunque si ha che

$$\aleph_\alpha < \kappa \leq \aleph_\alpha^+ = \aleph_{\alpha+1}.$$

Dato che κ è un cardinale, e non ci sono cardinali tra il cardinale $\aleph_\alpha$ e il suo successore cardinale $\aleph_{\alpha+1}$, si ha che $\kappa = \aleph_{\alpha+1}$. Ma allora κ è un cardinale successore, contro l'ipotesi!

Dunque abbiamo che $\beta = \sup A$ è un ordinale limite: l'insieme A non ha massimo, e per tanto il sup di A non è un elemento di A: $\beta \notin A$. Per definizione di A, si ha che

$$\alpha < \beta \Rightarrow \aleph_\alpha < \kappa.$$

Dunque κ è un maggiorante dell'insieme $\{\aleph_\alpha | \alpha < \beta\}$. Per definizione di $\aleph$ si ha

$$\aleph_\beta = \sup_{\alpha<\beta} \aleph_\alpha,$$

e per tanto segue che $\aleph_\beta$, minimo dei maggioranti di $\{\aleph_\alpha | \alpha < \beta\}$, non può essere più grande di κ, i.e. si ha

$$\aleph_\beta \leq \kappa.$$

D'altra parte, $\aleph_\beta$ non può neppure essere strettamente sotto κ, infatti:

$$\aleph_\beta < \kappa \Rightarrow \beta \in A$$

Ma sappiamo che $\beta \notin A$. Dunque resta, come unica possibilità, che

$$\aleph_\beta = \kappa.$$

□

CAPITOLO 7

Aritmetica Cardinale

1. Sinossi

Introduciamo le operazioni binarie di somma, prodotto ed esponenziazione su numeri cardinali, e ne dimostriamo le proprietà elementari.

2. Aritmetica sui Cardinali

Ora che abbiamo in mano una definizione adeguata di numero cardinale come rappresentante di una classe di equipotenza, e abbiamo assicurato la comparabilità dei cardinali assumendo l'Assioma di Scelta, possiamo sviluppare una aritmetica dei cardinali, analogamente a quanto abbiamo fatto con i numeri ordinali. Così come i cardinali sono ottenuti dai numeri ordinali astraendo dall'ordinamento i.e., sostituendo il concetto di equipotenza a quello di isomorfismo, le operazioni aritmetiche sui cardinali si ottengono dalle operazioni aritmetiche ordinali. Dati due insiemi A, B, denotiamo con ${}^{A}B$ l'insieme delle funzioni con dominio A e codominio B, ossia le funzioni $F : A \to B$.

DEFINIZIONE 2.1. Siano κ e λ cardinali. Definiamo

$$\kappa + \lambda = |\kappa \uplus \lambda|$$
$$\kappa \cdot \lambda = |\kappa \times \lambda|$$
$$\kappa^{\lambda} = |{}^{\lambda}\kappa|$$

OSSERVAZIONE 2.2. Non è difficile convincersi che per cardinali finiti p, q, le operazioni di sopra coincidono con quelle omonime dell'aritmetica finita.

La prima cosa da verificare è che le definizioni di sopra definiscono delle operazioni sulla cardinalità, nel senso che il risultato rimane invariato se sostituiamo un insieme con un altro insieme equipotente.

LEMMA 2.3. *Siano A e B insiemi tali che $|A| = \kappa$ e $|B| = \lambda$. Allora*

$$|A \uplus B| = \kappa + \lambda$$
$$|A \times B| = \kappa \cdot \lambda$$
$$|{}^{B}A| = \kappa^{\lambda}$$

DIMOSTRAZIONE. Dimostriamo la prima identità. Basta stabilire una biiezione tra $A \uplus B$ e $\kappa \uplus \lambda$. Sappiamo per ipotesi che esistono biiezioni $f : A \leftrightarrow \kappa$ e $g : B \leftrightarrow \lambda$. Utilizziamo f e g per definire una biiezione h tra $A \uplus B$ e $\kappa \uplus \lambda$. h resta definita dalle seguenti associazioni.

$$(a, 1) \in A \uplus B \mapsto (f(a), 1) \in \kappa \uplus \lambda,$$
$$(b, 2) \in A \uplus B \mapsto (g(b), 2) \in \kappa \uplus \lambda.$$

Per la seconda identità, definiamo una biiezione h da $A \times B$ su $\kappa \times \lambda$ utilizzando f e g come sopra. E' sufficiente porre

$$(a, b) \mapsto (f(a), g(b)).$$

Per esercizio, verificare la terza identità definendo una biiezione tra ${}^{B}A$ e ${}^{\lambda}\kappa$. In altre parole, per ogni funzione $F : B \to A$ occorre definire una funzione $F' : \lambda \to \kappa$. Presa F, occorre definire F' specificando, per ciascun $\ell \in \lambda$, qual è l'immagine di ℓ in κ secondo F'. A tale fine si useranno F, f, e g. □

Con le nuove operazioni cardinali abbiamo un'espressione aritmetica per la cardinalità dell'insieme potenza.

COROLLARIO 2.4. *Per ogni insieme A vale*

$$|\mathcal{P}(A)| = 2^{|A|}.$$

DIMOSTRAZIONE. Basta stabilire una biiezione tra $\mathcal{P}(A)$ e ${}^{A}2$. Una tale biiezione implica infatti $|\mathcal{P}(A)| = |{}^{A}2|$ e, per quanto visto sopra e per definizione di esponenziazione, vale $|{}^{A}2| = |{}^{|A|}2| = 2^{|A|}$.

Una biiezione standard tra $\mathcal{P}(A)$ e ${}^{A}2$ è definita usando la nozione di funzione caratteristica. Ad ogni sottinsieme di A occorre associare un elemento di ${}^{A}2$, ossia una mappa da $|A|$ nell'ordinale 2, i.e., nell'insieme $\{0, 1\}$. Dato un sottinsieme S di A, chiamiamo *funzione caratteristica* di S, denotata con c_S, la funzione definita come segue

$$c_S(a) = \begin{cases} 1 & \text{if } a \in S; \\ 0 & \text{if } a \notin S; \end{cases}$$

Una funzione caratteristica di un $S \subseteq A$ è una mappa da A in $\{0, 1\}$. Poiché ovviamente sottinsieme diversi hanno funzioni caratteristiche diverse, l'associazione

$$S \mapsto c_S$$

è una biiezione tra $\mathcal{P}(A)$ e l'insieme ${}^{A}2$. Dunque abbiamo

$$|\mathcal{P}(A)| = |{}^{A}2|.$$

Per quanto visto sopra vale $|{}^{A}2| = 2^{|A|}$. □

In particolare abbiamo un'espressione aritmetica per la cardinalità del continuo. Dato che $\mathcal{P}(\mathbf{N})$ è equipotente all'insieme dei numeri reali, abbiamo

$$|\mathbf{R}| = 2^{|\mathbf{N}|} = 2^{\aleph_0}.$$

Raccogliamo nella seguente proposizione le proprietà algebriche di base dell'addizione, moltiplicazione e esponenziazione cardinali. Omettiamo le dimostrazioni, che si ottengono in modo simile a quanto fatto per l'aritmetica ordinale, stabilendo opportune biiezioni e inizioni.

PROPOSIZIONE 2.5 (Proprietà Algebriche). *Per ogni κ, λ, μ*

$$\kappa + \lambda = \lambda + \kappa;\ \kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu;\ \kappa + 0 = 0 + \kappa = \kappa.$$
$$\kappa \cdot \lambda = \lambda \cdot \kappa;\ \kappa \cdot (\lambda \cdot \mu) = (\kappa \cdot \lambda) \cdot \mu;\ \kappa \cdot 0 = 0 \cdot \kappa = \kappa.$$
$$\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu, \kappa + \kappa = \kappa \cdot 2$$
$$\kappa^{\lambda+\mu} = \kappa^{\lambda} \cdot \kappa^{\mu}, (\kappa^{\lambda})^{\mu} = \kappa^{\lambda \cdot \mu},$$
$$(\kappa \cdot \lambda)^{\mu} = \kappa^{\mu} \cdot \kappa^{mu}, \kappa^1 = \kappa, \kappa^2 = \kappa \cdot \kappa,$$

$$\kappa \leq \kappa', \lambda \leq \lambda' \Rightarrow \kappa + \lambda \leq \kappa' + \lambda', \kappa \cdot \lambda \leq \kappa' \cdot \lambda', \kappa^\lambda \leq (\kappa')^{\lambda'}.$$

Per la Proposizione di sopra, addizione, prodotto e esponenziazione cardinali soddisfano le stesse proprietà algebriche di base delle corrispettive operazioni finite. Da notare però che, nella Proposizione precedente abbiamo da ultimo dimostrato che le operazioni cardinali sono non decrescenti in entrambi gli argomenti. Per contrasto, somma prodotto ed esponenziazione finite sono *strettamente* crescenti in entrambi gli argomenti, ossia vale

$$p < p', \ell < \ell' \Rightarrow p + \ell < p' + \ell', p \cdot \ell < p' \cdot \ell', p^\ell < (p')^{\ell'}.$$

Vedremo tra poco che non si può dire lo stesso nel caso di cardinali transfiniti. Dimostreremo, da una parte, che la somma e il prodotto di cardinali infiniti sono operazioni in un certo senso banali, perché vale, presi due cardinali qualunque λ e κ, di cui almeno uno infinito,

$$\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda).$$

Dunque in particolare, per ogni κ infinito e per ogni $n \in \mathbf{N}$, vale

$$\kappa + \kappa = \kappa \cdot \kappa = \kappa^n = \kappa.$$

D'altra parte, osserveremo che l'esponenziazione cardinale è un'operazione *estremamente complessa*, al punto tale che è *impossibile* deciderne il valore in base agli assiomi della teoria di Zermelo-Fraenkel con Assioma di Scelta. In altre parole, è impossibile determinare in generale il valore dell'esponenziazione di due numeri cardinali κ, λ:

$$\kappa^\lambda = ???$$

In altre parole, la situazione - leggermente paradossale - è la seguente.

- Somma e prodotto su cardinali infiniti sono *banali*,
- L'esponenziazione su cardinali infiniti è *indeterminata*!

Per dimostrare che la somma di due cardinali è banale dimostreremo che, per ogni insieme infinito A, l'insieme $A \times A$ (il cui cardinale è $|A| \cdot |A|$, per definizione), è equipotente ad A. In altre parole dimostreremo che per qualunque insieme infinito A è possibile definire una biiezione tra A e $A \times A$. (Abbiamo già visto il caso in cui A è l'insieme dei naturali $\mathbf{N}$).

A tale scopo supporremo dal cardinale $|A|$ - che è bene ordinato dato che è un ordinale - e definiremo un particolare buon ordinamento dell'insieme prodotto $|A| \times |A|$. Useremo poi questo buon ordinamento per dimostrare l'equipotenza di $|A|$ e di $|A| \times |A|$. Il buon ordinamento di $|A| \times |A|$ derivato da quello di $|A|$ è un'estensione del buon ordinamento sulle coppie di naturali che abbiamo introdotto per dimostrare che l'insieme $\mathbf{N} \times \mathbf{N}$ è in biiezione con $\mathbf{N}$. L'opportunità di partire dall'ordinale $|A|$ piuttosto che dall'insieme A è di natura tecnica e sarà chiara nel corso della dimostrazione. Definiamo il *buon ordinamento canonico* $\sqsubset$ di $(|A| \times |A|)$ come segue. [1] Per $\alpha, \beta, \gamma, \delta$ in $|A|$, poniamo

$$(\alpha, \beta) \sqsubset (\gamma, \delta) := \begin{cases} \max(\alpha, \beta) < \max(\gamma, \delta) \\ \max(\alpha, \beta) = \max(\gamma, \delta) \wedge \beta < \delta \\ \max(\alpha, \beta) = \max(\gamma, \delta) \wedge \beta = \delta \wedge \alpha < \gamma \end{cases}$$

[1] La costruzione è generale: dato un buon ordinamento $(X, <_X)$ si ottiene un buon ordinamento canonico su $X \times X$.

dove il max di due elementi in $|A|$ è da intendersi rispetto all'ordinamento ordinale standard[2].

Si dimostra facilmente che la relazione $\sqsubset$ appena definita è un buon ordinamento di $|A| \times |A|$. (Esercizio: analogo a quanto visto nel caso $A = \mathbf{N}$).

PROPOSIZIONE 2.6. *Per ogni insieme infinito A, esiste una biiezione di $A \times A$ su A.*

DIMOSTRAZIONE. Dimostriamo che esiste una biiezione tra $|A| \times |A|$ e $|A|$, avvalendoci del buon ordinamento canonico $\sqsubset$ di $|A| \times |A|$ definito a partire dal buon ordinamento dell'ordinale $|A|$ ($|A|$ è un cardinale ergo un ordinale ergo bene ordinato dall'ordinamento naturale $<$ degli ordinali).

$(|A| \times |A|, \sqsubset)$ è bene ordinato, e per tanto è isomorfo a un unico ordinale. Sia α questo ordinale. Vogliamo dimostrare che α è uguale al cardinale di A ossia

$$\alpha = |A|.$$

Osserviamo come prima cosa che α è necessariamente maggiore o uguale al cardinale di A. La mappa che assegna a un elemento $a \in |A|$ la coppia (a, a) è una iniezione di $|A|$ in $(|A| \times |A|, \sqsubset)$ e per di più conserva l'ordine. Ossia è un isomorfismo da $(|A|, <)$ su *un sottinsieme* di $(|A| \times |A|, \sqsubset)$. Da ciò segue immediatamente che il cardinale $|A|$ (che è ovviamente anche un ordinale) non può essere strettamente maggiore di α. Dunque $\alpha \geq |A|$ (l'ordine sugli ordinali è un ordine totale).

Ci resta dunque da dimostrare che vale l'inversa, i.e., che vale $\alpha \leq |A|$. Lo dimostriamo per **induzione transfinita** sul cardinale $|A|$. Consideriamo due casi.

(Caso 1) $|A| = \omega$. In tal caso si verifica facilmente che ogni segmento iniziale del buon ordinamento $\sqsubset$ definito su $|A| \times |A|$ è finito. In altre parole, scelti comunque $a, b \in |A|$, esistono solo un numero finito di coppie $(x, y) \in |A| \times |A|$ che sono minori della coppia (a, b) rispetto all'ordinamento $\sqsubset$. Ma se $(|A| \times |A|, \sqsubset)$ è un buon ordinamento tale che ogni segmento iniziale è finito, il suo tipo d'ordine è al massimo ω (altrimenti esisterebbe almeno un segmento iniziale di tipo ω). Per tanto, abbiamo $\alpha \leq \omega$, q.e.d.

(Caso 2) $|A| > \omega$. Ricordiamo che $|A|$ è un cardinale e per tanto è un ordinale limite. Scegliamo comunque $(a, b) \in |A| \times |A|$ e cerchiamo di capire come è fatto il segmento iniziale del buon ordinamento $\sqsubset$ su $|A| \times |A|$ determinato dalla coppia (a, b). In altre parole consideriamo l'insieme delle coppie minori della coppia (a, b) nel buon ordine $\sqsubset$:

$$(c, d) \text{ tali che } (c, d) \sqsubset (a, b).$$

Analogamente al caso finito, per come abbiamo definito $\sqsubset$, le coppie minori di (a, b) sono contenute nel 'quadrato' di lato $\max(a, b)$ (con questo intendiamo che sono tutte $\sqsubset$ di $(\max(a, b), \max(a, b))$). La differenza dal caso $\aleph_0$ è che in questo caso un tale quadrato può contenere infinite coppie e vogliamo informazioni sul tipo d'ordine di questo quadrato. Posto $\mu = \max(a, b)$, vale di certo

$$(a', b') \sqsubset (a, b) \Rightarrow \max(a', b') \leq \mu.$$

[2]Nel caso generale il max è da intendersi rispetto al buon ordinamento dell'insieme X di partenza. Cfr. nota precedente.

Inoltre, dato che $\max(a,b)$ è sicuramente un elemento di $|A|$, e poiché $|A|$ è un ordinale, abbiamo che μ è strettamente minore, come ordinale, di $|A|$.[3] Ossia vale

$$\max(a,b) = \mu < |A|.$$

Allora possiamo applicare su μ l'Ipotesi Induttiva, i.e., possiamo supporre che la proprietà che stiamo dimostrando sia valida per μ. Dunque abbiamo

$$|\mu \times \mu| = |\mu|.$$

Ovviamente vale $|\mu| \leq \mu$. Ora, per definizione di $\sqsubset$, ogni segmento iniziale del buon ordine $(|A| \times |A|, \sqsubset)$ determinato da una coppia (a,b) è contenuto (si immerge iniettivamente e preservando l'ordine) nel quadrato $\mu \times \mu$, e per tanto vale

$$|(|A| \times |A|)_{(a,b)}| \leq |\mu \times \mu| = |\mu| \leq \mu < |A|.$$

Dunque ogni segmento iniziale di $(|A| \times |A|, \sqsubset)$ ha cardinalità $< |A|$. Per tanto, il tipo d'ordine α di $(|A| \times |A|, \sqsubset)$ è al più $|A|$ (altrimenti almeno un segmento iniziale proprio sarebbe di cardinalità $|A|$): $\alpha \leq |A|$.

Abbiamo dunque dimostrato che $\alpha = |A|$. Per tanto $A \times A$ e A sono in biiezione, e dunque

$$|A \times A| = |A|.$$

□

Dato che ogni cardinale è un aleph, possiamo riformulare il risultato seguente come segue.

COROLLARIO 2.7. *Per ogni α,*

$$\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha.$$

Il seguente Corollario è presto dedotto.

COROLLARIO 2.8. *Per ogni α, β*

$$\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \max(\aleph_\alpha, \aleph_\beta) = \max(\aleph_\alpha, \aleph_\beta) = \aleph_{\max \alpha, \beta}.$$

DIMOSTRAZIONE. Supponiamo, senza perdita di generalità, che $\alpha \leq \beta$. Allora si ha:

$$\begin{aligned} \aleph_\alpha + \aleph_\alpha &\leq \aleph_\alpha + \aleph_\beta \\ &\leq \aleph_\beta \cdot \aleph_\beta \\ &= \aleph_\beta \cdot 2 \\ &\leq \aleph_\beta \cdot \aleph_\beta \\ &= \aleph_\beta. \end{aligned}$$

□

Per il caso particolare dell'addizione di un numero finito n e di un numero infinito $\aleph_\alpha$, abbiamo che

$$\aleph_\alpha + n = \aleph_\alpha = \aleph_\alpha \cdot n.$$

[3]Qui è chiara l'opportunità di lavorare fin dall'inizio con l'ordinale $|A|$ piuttosto che con l'insieme A. Ovviamente $\mu < |A|$ non implica $\mu \in A$, ma solo $\mu \in |A|$.

PROPOSIZIONE 2.9. *Sia λ un cardinale infinito, e sia $2 \leq \kappa \leq \lambda$. Allora*

$$^{\lambda}2 \rightarrow_{in} {}^{\lambda}\kappa \rightarrow_{in} {}^{\lambda}\lambda \rightarrow_{in} \mathcal{P}(\lambda \times \lambda) \rightarrow_{bi} \mathcal{P}(\lambda) \rightarrow_{bi} {}^{\lambda}2.$$

In altre parole, per $\alpha \leq \beta$ vale

$$2^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta}.$$

DIMOSTRAZIONE. La catena di iniezioni e di biiezioni nella prima formulazione della Proposizione è ovvia, a parte il passo $\mathcal{P}(\lambda \times \lambda) \rightarrow_{bi} \mathcal{P}(\lambda)$, che segue immediatamente dal fatto che abbiamo dimostrato prima, i.e. che $\lambda \times \lambda = \lambda$.

Quanto alla seconda formulazione, possiamo vedere le cose così, richiamandoci alle proprietà algebriche dell'esponenziazione e a quanto dimostrato precedentemente ($n \geq 2$ qui sotto).

$$2^{\aleph_\beta} \leq n^{\aleph_\beta} \leq \aleph_\alpha^{\aleph_\beta} \leq (2^{\aleph_\beta})^{\aleph_\beta} \leq 2^{\aleph_\beta \cdot \aleph_\beta} = 2^{\aleph_\beta}.$$

□

CAPITOLO 8

Somme e Prodotti Infiniti di Cardinali

1. Sinossi

Impariamo a fare somme e prodotti di un numero infinito di cardinali transfiniti.

2. Somme Infinite

Estendiamo l'operazione di somma ad un numero infinito di termini. A tale fine supponiamo di avere una successione di cardinali, *indicizzata* da elementi di un insieme I di indici, che scriviamo come $(\kappa_i)_{i\in I}$. Di fatto, si tratta di una funzione che associa ad ogni indice $i \in I$ un cardinale, che denotiamo con κ_i. L'indicizzazione è un modo per avere un'etichetta che individua l'i-esimo operando (notare che la successione $(\kappa_i)_{i\in I}$ può contenere ripetizioni). Definiamo ora la somma dei termini $(\kappa_i)_{i\in I}$. La definizione è un'estensione diretta del caso finito. Prendiamo una copia di ogni termine in modo tale da ottenere un insieme di insiemi due a due disgiunti (la copia del termine i-esimo è l'insieme prodotto $\kappa \times \{i\}$), e definiamo la somma come la cardinalità dell'insieme unione di tutti i termini. In simboli poniamo quanto segue.

$$\sum_{i\in I} \kappa_i := |\bigcup_{i\in I} (\kappa_i \times \{i\})|.$$

Dobbiamo per prima cosa assicurarci che l'operazione appena definita è davvero un'operazione *sulla cardinalità*: se sostituiamo ciascun termine con un termine di stessa cardinalità il risultato non deve cambiare.

Osservazione 2.1 (Buona Definizione (usa (AC))). Per ogni insieme di indici I e per ogni successione di insiemi disgiunti $(S_i)_{i\in I}$ indicizzata da I, vale

$$\left|\bigcup_{i\in I} S_i\right| = \sum_{i\in I} |S_i|.$$

Dimostrazione. Per definizione, abbiamo

$$\sum_{i\in I} |S_i| = \left|\bigcup_{i\in I} (|S_i| \times \{i\})\right|.$$

Per tanto basta stabilire una biiezione

$$f : \bigcup_{i\in I} S_i \leftrightarrow \bigcup_{i\in I} (|S_i| \times \{i\}).$$

Ovviamente $|S_i|$ e S_i sono equipotenti per ogni $i \in I$, ossia vale

$$(\forall i \in I)(\exists f)[f \text{ è una biiezione tra } S_i \text{ e } |S_i|].$$

In altre parole la famiglia $(B_i)_{i\in I}$ dove

$$B_i = \{ \text{ biiezioni tra } S_i \text{ e } |S_i|\},$$

è una famiglia di insiemi non vuoti. Per tanto l'Assioma di Scelta ci garantisce la possibilità di scegliere un elemento in ciascun membro della famiglia. In altre parole abbiamo un modo uniforme (una funzione di scelta) per selezionare in ogni S_i una biiezione. Abbiamo dunque una famiglia $(f_i)_{i\in I}$ di funzioni tale che

$$(\forall i \in I)[f_i \text{ è una biiezione tra } S_i \text{ e } |S_i|].$$

Notiamo che i B_i sono anche due a due disgiunti, perché per ipotesi gli S_i sono a due a due disgiunti. Dunque $f_i \neq f_j$ se $i \neq j$. Usiamo il sistema di biiezioni $(f_i)_{i\in I}$ per definire la biiezione f desiderata. Poniamo, per $s \in \bigcup_{i\in I} S_i$,

$$f(s) = (f_i(s), i) \in |S_i| \times \{i\},$$

dove i è l'indice dell'*unico* S_i tale che $s \in S_i$ (gli S_i sono disgiunti per ipotesi). Si verifica facilmente che f così definita è una biiezione del tipo desiderato. □

3. Prodotti Infiniti

Definiamo il prodotto di una successione di cardinali $(\kappa_i)_{i\in I}$ indicizzata in un insieme I. A tal fine definiamo una nozione di *prodotto cartesiano infinito*. Intuitivamente, l'insieme prodotto cartesiano di una serie infinita di insiemi $(S_i)_{i\in I}$ è l'insieme di tutte le successioni $(s_i)_{i\in I}$ indicizzate in I tali che $s_i \in I$. In altre parole, il prodotto cartesiano degli insiemi $(S_i)_{i\in I}$ è l'insieme di tutte le funzioni con dominio I e codominio in $\bigcup_{i\in I} S_i$ tali che l'immagine di i è in S_i. Denotiamo il prodotto cartesiano di $(S_i)_{i\in I}$ con $\mathsf{X}_{i\in I} S_i$. Definiamo il prodotto infinito di una successione di cardinali $(\kappa_i)_{i\in I}$ come la cardinalità del prodotto cartesiano dei termini della successione.

Definizione 3.1 (Prodotto Infinito).

$$\prod_{i\in I} \kappa_i := |\mathsf{X}_{i\in I} \kappa_i|.$$

Osservazione 3.2. Si vede facilmente che la nozione appena definita di prodotto è una generalizzazione diretta del prodotto di un numero finito di termini (e abbiamo già osservato che questo è a sua volta un'estensione del prodotto di un numero finito di termini finiti). Il prodotto di due cardinali κ e λ è stato definito come la cardinalità del prodotto cartesiano $\kappa \times \lambda$. Si vede facilmente come il prodotto cartesiano è essenzialmente identico (in particolare, equipotente), all'insieme delle funzioni con dominio $\{0, 1\}$ e codominio in $\kappa \cup \lambda$ tali che l'immagine di 0 è in κ e l'immagine di 1 è in λ. In altre parole l'insieme delle coppie ordinate (x, y) con $x \in \kappa$ e $y \in \lambda$ si identifica facilmente con l'insieme delle successioni di due elementi di cui il primo è in κ e il secondo in λ. Per la nostra definizione di sopra, ques'ultimo insieme è $\mathsf{X}_{i\in I} \kappa_i$, se $I = \{0, 1\}$ (o un qualunque insieme con due elementi), $\kappa_0 = \kappa$ e $\kappa_1 = \lambda$.

Come abbiamo fatto per la somma infinita, vogliamo ora assicurarci che l'operazione di prodotto dipenda soltanto dalla cardinalità dei suoi operandi.

Osservazione 3.3 (Buona Definizione). Per ogni insieme di indici I e per ogni successione di insiemi $(S_i)_{i\in I}$ indicizzata da I, vale

$$|\mathsf{X}_{i\in I} S_i| = \prod_{i\in I} |S_i|.$$

Dimostrazione. Per definizione, abbiamo

$$\prod_{i\in I} |S_i| = |\mathsf{X}_{i\in I} |S_i||\,.$$

Per tanto basta stabilire una biiezione

$$f : \mathsf{X}_{i\in I} S_i \leftrightarrow \mathsf{X}_{i\in I} |S_i|.$$

Esercizio (cfr. quanto fatto nel caso della somma). □

4. Relazioni basilari tra Somma e Prodotto Infiniti

Stabiliamo alcune relazioni basilari tra somma, prodotto ed esponenziazione.

Osservazione 4.1. $\forall \kappa, \lambda$

$$\sum_{i\in\lambda} \kappa = \kappa \cdot \lambda, \quad \prod_{i\in\lambda} \kappa = \kappa^{\lambda}.$$

Dimostrazione. Con la notazione $\sum_{i\in\lambda} \kappa$ stiamo ovviamente denotando $\sum_{i\in\lambda} \kappa_i$ con $\kappa_i = \kappa$ per ogni $i \in I$ (e analogamente per $\prod_{i\in\lambda} \kappa$). Il risultato è una conseguenza immediata della buona definizione di somma e prodotto infiniti. (Esercizio). □

Da osservare che la seconda identità esplicita l'intima relazione tra prodotto ed esponenziazione cardinale. Non ci stupirà dunque scoprire più sotto che non possiamo dire molto sul valore di un prodotto infinito di cardinali in generale.

5. Calcolo di Somme e Prodotti Infiniti

La Proposizione seguente ci dice che il calcolo di una somma infinita di cardinali è piuttosto banale. Il risultato è il numero più grande tra la cardinalità di I (ossia *quanti* termini stiamo sommando) e l'estremo superiore (il minimo dei maggioranti) dell'insieme dei termini. Useremo l'ovvia osservazione che, se $\kappa_i \leq \lambda_i$ per ogni $i \in I$ allora vale $\sum_{i\in I} \kappa_i \leq \sum_{i\in I} \lambda_i$.

Proposizione 5.1. *Sia data una successione di cardinali $(\kappa_i)_{i\in I}$ indicizzata in I con tutti i κ_i strettamente maggiori di zero. Allora vale*

$$\sum_{i\in I} \kappa_i = \max(|I|, \sup_{i\in I}(\kappa_i)).$$

Dimostrazione. Sia $\kappa = \sup_{i\in I}(\kappa_i)$. Ovviamente vale $\kappa_i \leq \kappa$. Dunque, per quanto osservato sopra, abbiamo

$$\sum_{i\in I} \kappa_i \leq \sum_{i\in I} \kappa = \kappa \cdot |I| = \max(|I|, \kappa).$$

D'altro canto abbiamo $1 \leq \kappa_i$, e perciò

$$|I| = \sum_{i\in I} 1 \leq \sum_{i\in I} \kappa_i. \tag{5.1}$$

Inoltre, poiché $\kappa_i \leq \sum_{i\in I} \kappa_i$ per ogni $i \in I$, vale anche

$$\kappa \leq \sum_{i\in I} \kappa_i. \tag{5.2}$$

Da (2.1) e (2.2) concludiamo che

$$\max(|I|, \kappa) \leq \sum_{i\in I} \kappa_i.$$

□

La Proposizione precedente permette di calcolare somme infinite qualunque. In sintesi, abbiamo, per ogni α, β,

$$\sum_{i\in \aleph_\beta} \aleph_\alpha = \max(\aleph_\alpha, \aleph_\beta) = \aleph_{\max(\alpha,\beta)} = \aleph_\alpha + \aleph_\beta.$$

Per contrasto, non sappiamo molto sul valore di un prodotto infinito. Poiché il prodotto infinito è (lo abbiamo osservato sopra) strettamente connesso all'operazione di esponenziazione, questo non deve stupire: l'operazione di esponenziazione cardinale resta quasi del tutto indeterminata dagli assiomi di Zermelo-Fraenkel. La Proposizione seguente riassume ciò che possiamo affermare circa il valore di un prodotto infinito in generale. La dimostrazione usa l'Assioma di Scelta.

PROPOSIZIONE 5.2 (Lemma di König (usa (AC))). *Siano $(\kappa_i)_{i\in I}$ e $(\lambda_i)_{i\in I}$ due successioni di cardinali indicizzate in I e tali che $\kappa_i < \lambda_i$ per ogni $i \in I$. Allora vale*

$$\sum_{i\in I} \kappa_I < \prod_{i\in I} \lambda_i.$$

DIMOSTRAZIONE. Il risultato segue se dimostriamo che esiste una iniezione dell'insieme

$$S := \bigcup_{i\in I} \kappa_i \times \{i\}, \text{ (somma disgiunta dei } \kappa_i)$$

nell'insieme

$$P := \mathsf{X}_{i\in I}\lambda_i, \text{(prodotto cartesiano dei } \lambda_i)$$

e che non esiste una iniezione di P in S.

Iniettare S in P è facile. Dobbiamo associare, iniettivamente, ad ogni coppia $(x, i) \in \kappa_i$ al variare di $i \in I$, una mappa $f_{(x,i)}$ da I in $\bigcup_{i\in I} \lambda_i$ tale che, per ogni $j \in I$, $f_{(x,i)}(j) \in \lambda_j$, i.e.

$$(x, i) \in \kappa_{\mathbf{i}} \times \{\mathbf{i}\} \mapsto f_{(x,i)} \in \mathsf{X}_{\mathbf{i}\in\mathbf{I}}\lambda_{\mathbf{i}}.$$

Per ogni $i \in I$, associamo a un elemento $(x, i) \in \kappa_i$, una funzione $f_{(x,i)}$ su I come segue.

$$(x, i) \in \kappa_i \mapsto f_{(x,i)} \text{ tale che, per } i \in I, f_{(x,i)}(j) := \begin{cases} x & \text{se } i = j; \\ \kappa_j & \text{se } i \neq j. \end{cases}$$

Dato che $x \in \kappa_i$ e che $\kappa_j < \lambda_j$ per ogni $j \in I$, la funzione è del tipo desiderato. In poche parole: a un elemento $(x, i) \in \kappa_i$ associamo la funzione che manda la i-esima coordinata in $x \in \lambda_i$ e ogni altra coordinata $j \neq i$ nel cardinale κ_j, che è comunque minore stretto di λ_j e per tanto elemento di λ_j. Otteniamo una associazione che è ovviamente iniettiva: presi due elementi (x, i) e (x', i') entrambi in

$\bigcup_{i\in I} \kappa_i \times \{i\}$, essi differiscono o per il primo o per il secondo elemento della coppia o per entrambi. In ogni caso le funzioni associate $f_{(x,i)}$ e $f_{(x',i')}$ differiranno su almeno una coordinata.

Dimostriamo ora che non esiste una iniezione di P in S. Se esiste una iniezione, sia f, di P in S, abbiamo una descrizione completa (una copertura) di P come unione di $|I|$ insiemi disgiunti $(P_i)_{i\in I}$ tale che P_i ha cardinalità $\leq \kappa_i$. Questa descrizione si ottiene semplicemente prendendo le controimmagini degli insiemi $(\kappa_i \times \{i\})$, la cui unione forma S, sotto la supposta iniezione di P in S. Ossia: se f è una iniezione di P in S, allora possiamo scrivere P come unione della famiglia $(P_i)_{i\in I}$ dove P_i è $P_i = \{p \in P \text{ t.c. } f(p) \in \kappa_i \times \{i\}\}$, anche denotato come $f^{-1}[\kappa_i \times \{i\}]$.

Dimostriamo che non può esistere nessuna scomposizione di P come unione di $|I|$ insiemi tale che l'i-esimo insieme ha cardinalità $\leq \kappa_i$. Supponiamo che esista una tale scomposizione. Sia $(S_i)_{i\in I}$ tale che

$$|S_i| \leq \kappa_i.$$

Dimostriamo che l'unione degli S_i non copre P, ossia dimostriamo

$$(\exists p)[p \in P - \bigcup_{i\in I} S_i].$$

Ricordando che P è $\mathsf{X}_{i\in I}\lambda_i$, dobbiamo definire p come una successione $(\ell_i)_{i\in I}$, con $\ell_i \in \lambda_i$. Definiamo una tale successione con un argomento diagonale. Gli elementi di un $S_i \subseteq P$ sono mappe da I in $\bigcup_{i\in I} \lambda_i$. Dato che

$$|S_i| \leq \kappa_i < \lambda_i,$$

S_i contiene meno di λ_i mappe. Costruiamo una tabella con $|I|$ colonne e $\leq \kappa_i < \lambda_i$ righe come segue. Nella colonna i-esima scriviamo tutti i valori che le mappe contenute in S_i assumono nella i-esima coordinata. Data una colonna i, denotiamo con V_i l'insieme dei valori che appaiono in quella colonna. Dato che la colonna i-esima ha $|S_i|$ righe, si ha che per ogni colonna (i.e. per ogni $i \in I$),

$$|V_i| \leq \kappa_i < \lambda_i.$$

Allora la differenza $\lambda_i - V_i$ è non vuota, e la famiglia

$$((\lambda_i - V_i))_{i\in I}$$

è una famiglia di insiemi non vuoti. Per ciascun i abbiamo un insieme non vuoto di candidati per l'i-esima coordinata che differiscono da *tutti* i valori usati da tutte le mappe in S_i nell'i-esima coordinata! Per l'Assioma di Scelta possiamo selezionare un tale valore per ogni i, ossia esiste un sistema

$$(\ell_i)_{i\in I}$$

tale che $\ell_i \in (\lambda_i - V_i)$. La sequenza $(\ell_i)_{i\in I}$ è un elemento di P che non appartiene all'unione $\bigcup_{i\in I} S_i$. Infatti, per come è stata scelta, la mappa definita da $i \mapsto \ell_i$ differisce nella i-esima coordinata da tutte le mappe contenute in S_i e per tanto non può essere un elemento di nessun S_i.

□

Il Lemma di König ci permette di ottenere una breve dimostrazione della diseguaglianza di Cantor sulla cardinalità dell'insieme potenza.

COROLLARIO 5.3. *Per ogni κ vale $\kappa < 2^\kappa$.*

DIMOSTRAZIONE. Basta esprimere κ come somma di una successione $(\kappa_i)_{i\in\kappa}$ e 2^κ come prodotto di una successione $(\lambda_i)_{i\in\kappa}$ tali che $\kappa_i < \lambda_i$ per ogni i. Ma questo è facile (anche in base a quanto osservato sopra).

$$\kappa = \sum_{i\in\kappa} 1 = \kappa \cdot 1, \quad \text{e} \quad \kappa = \prod_{i\in\kappa} 2 = 2^\kappa.$$

□

CAPITOLO 9

Assioma di Fondazione, Gerarchia Cumulativa

1. Sinossi

Introduciamo l'Assioma di Fondazione e la Gerarchia cumulativa di Von Neumann.

2. Assioma di Fondazione

Alla nostra lista di assiomi per la teoria degli insiemi di Zermelo-Fraenkel manca una voce: l'Assioma di Fondazione ((AF)). L'Assioma di Fondazione ha uno statuto un po' differente da quello degli altri assiomi. Gli assiomi introdotti finora possono essere giustificati almeno da due punti di vista (e così è stato fatto storicamente):

- Esprimono principii di costruzione irrinunciabili se vogliamo una teoria capace di rappresentare le matematiche generali (coppia, unione, potenza,...),
- Esprimono proprietà che sembrano consone alla 'nozione intuitiva' di insieme (ammesso che una tale nozione esista).

Per contrasto, l'Assioma di Fondazione pone una *restrizione esplicita* sul tipo di insiemi di cui si ammette l'esistenza nella teoria. Da un altro punto di vista, (AF) assicura che la relazione di appartenenza $\in$ (l'unica relazione primitiva della nostra teoria) soddisfa sempre alcune proprietà.

Cominciamo dunque con il considerare la relazione $\in$ in generale, come relazione binaria. Di quali proprietà gode? In base agli assiomi assunti finora, la relazione $\in$ è piuttosto selvaggia, e.g.,

- Non è transitiva (si prenda $a = \varnothing$, $b = \{\varnothing\}$, $c = \{\{\varnothing\}\}$).
- Non è totale (si prendano a e c come sopra).
- Non è simmetrica (si prendano a e b come sopra).
- Non è riflessiva (si prenda uno qualunque tra a, b, c qui sopra).
- Non sappiamo se è antisimmetrica (può darsi che $x \in y \in x$ ma $x \neq y$?).

Ricordiamo che una relazione binaria (non necessariamente totale) R è detta *ben fondata* su una classe $\mathbf{X}$ se per per ogni sottinsieme non vuoto $\subseteq \mathbf{X}$ esiste un elemento $s \in S$ che è minimale in S rispetto a R (ossia tale che non esiste un $t \in S$ tale che tRs). In simboli abbiamo

$$(\forall S \subseteq \mathbf{X})(S \neq \varnothing \rightarrow (\exists s \in S)(\forall t \in S)\neg(tRs)).$$

In altre parole, la buona fondatezza generalizza la nozione di buon ordine a relazioni non necessariamente totali (se R è un ordine totale e R è ben fondata, allora R è un buon ordine: l'elemento minimale è anche minimo). In base agli assiomi finora introdotti,

- Non sappiamo se la relaione $\in$ è ben fondata.

Per esempio, può esistere x tale che $x \in x$?

D'altro canto, conosciamo una classe di insiemi sui quali la relazione $\in$ è molto bene educata: gli ordinali, i nostri tipi d'ordine di insiemi bene ordinati. Come abbiamo visto, è possibile *definire* gli ordinali come gli insiemi sui quali la relazione $\in$ è transitiva ed è un buon ordine! Dunque, ristretta agli ordinali, la relazione $\in$

- È transitiva.
- È totale.
- È irriflessiva.
- È antisimmetrica.
- È ben fondata.

L'Assioma di Fondazione asserisce che *su tutti gli insiemi* la relazione $\in$ è ben fondata. Come vedremo più sotto, questo equivale ad assumere che tutti gli insiemi nell'universo della nostra teoria possono essere costruiti a partire dall'insieme vuoto iterando l'insieme potenza e l'unione. La formulazione standard dell'Assioma di Fondazione è la seguente.

$$((\text{AF})) \quad (\forall x)(x \neq \varnothing \Rightarrow (\exists y \in x)[y \cap x = \varnothing]).$$

In altre parole (AF) asserisce che ogni insieme x contiene almeno un elemento y che è minimale rispetto alla relazione $\in$ su x: per nessun altro elemento z di x vale $z \in y$.

3. Gerarchia di Von Neumann

La Gerarchia di Von Neumann è una descrizione dal basso di una famiglia di insiemi, i.e., gli insiemi ottenuti iterando l'operazione di potenza e di unione a partire dall'insieme vuoto. Si parte così

$$\varnothing, \mathcal{P}(\varnothing), \mathcal{P}(\mathcal{P}(\varnothing)), \ldots, \mathcal{P}^n(\varnothing), \ldots$$

dove $\mathcal{P}^n(\varnothing)$ denota il risultato ottenuto prendendo n volte l'insieme potenza a partire dall'insieme vuoto. Vogliamo proseguire la costruzione nel transfinito: come definire il passo successivo a tutti i passi $\mathcal{P}^n(\varnothing)$ appena definiti? Raccogliamo la collezione numerabile di insiemi $\mathcal{P}^n(\varnothing)$ appena definita semplicemente prendendone l'unione. Questo è il passo ω della costruzione:

$$\bigcup_{n \in \mathbf{N}} \mathcal{P}^n(\varnothing).$$

Osservazione 3.1. Quali assiomi servono per garantire l'esistenza dell'insieme $\bigcup_{n \in \mathbf{N}} \mathcal{P}^n(\varnothing)$? Per ogni n, $\mathcal{P}^n(\varnothing)$ esiste per l'Assioma delle Parti. Inoltre, la mappa che associa n a $\mathcal{P}^n(\varnothing)$ è dimostrabilmente funzionale, ossia se $n \neq m$ allora $\mathcal{P}^n(\varnothing) \neq \mathcal{P}^m(\varnothing)$. Dato che esiste $\omega = \{0, 1, \ldots, n, \ldots, \}$ (Assioma dell'Infinito), l'Assioma di Rimpiazzamento ci garantisce che esiste l'insieme $\{\mathcal{P}^n(\varnothing) \text{ t.c. } n \in \omega\}$, come immagine di ω sotto la relazione funzionale che associa ad n la potenza n-esima dell'insieme vuoto. Per l'Assioma dell'Unione esiste allora $\bigcup\{\mathcal{P}^n(\varnothing) \text{ t.c. } n \in \omega\}$ che altro non è che l'insieme che abbiamo sopra denotato con $\bigcup_{n \in \mathbf{N}} \mathcal{P}^n(\varnothing)$.

Procediamo analogamente lungo la scala degli ordinali: a un passo successore prendiamo la potenza dell'insieme ottenuto al passo precedente, mentre a ogni passo limite prendiamo l'unione di tutti gli insiemi ottenuti ai passi precedenti. In simboli diamo la seguente definizione per ricorsione transfinita sugli ordinali (sappiamo che queste definizioni sono giustificate nella nostra teoria).

DEFINIZIONE 3.2 (Gerarchia di Von Neumann).

$$V_0 := \varnothing,$$
$$V_{\alpha+1} := \mathcal{P}(V_\alpha),$$
$$V_\lambda := \bigcup_{\gamma<\lambda} V_\gamma \text{ per } \lambda \text{ limite.}$$

Poniamo $\mathbf{VN} := \bigcup\{V_\alpha \text{ t.c. } \alpha \in \mathbf{Ord}\}$. Vedremo a breve che $\mathbf{VN}$ è una classe propria. Vedremo anche che l'Assioma di Fondazione equivale a dire che $\mathbf{VN}$ esaurisce l'universo di tutti gli insiemi, i.e.

$$((\mathrm{AF})) \Leftrightarrow (\forall x)[x \in \mathbf{VN}].$$

Cominciamo con l'osservare due proprietà basilari degli insiemi in $\mathbf{VN}$.

LEMMA 3.3. *Per ogni α, V_α è transitivo.*

DIMOSTRAZIONE. Per induzione transfinita su α. Se $\alpha = 0$ è banalmente vero, dato che $V_0 = \varnothing$. Sia $\alpha = \beta + 1$. Per definizione $V_\alpha = V_{\beta+1} = \mathcal{P}(V_\beta)$. Sia $x \in V_\alpha$ e sia $y \in x$. Vogliamo mostrare che $y \in V_\alpha$. $x \in V_\alpha$ implica $x \subseteq V_\beta$ e dunque $y \in V_\beta$. Per ipotesi induttiva V_β è transitivo e dunque $y \subseteq V_\beta$. Dunque $y \in \mathcal{P}(V_\beta) = V_\alpha$ q.e.d. Sia α un limite. Per definizione $V_\alpha = \bigcup_{\beta<\alpha} V_\beta$. Sia $y \in x \in V_\alpha$. Mostriamo che $y \in V_\alpha$. $x \in V_\alpha$ implica che esiste un $\beta < \alpha$ tale che $x \in V_\beta$. Per ipotesi induttiva V_β è transitivo e dunque $y \in V_\beta$ e dunque $y \in \bigcup_{\beta<\alpha} V_\beta = V_\alpha$.

□

LEMMA 3.4. *Se $\alpha \leq \beta$, allora $V_\alpha \subseteq V_\beta$.*

DIMOSTRAZIONE. Ancora per induzione transfinita, questa volta su $\beta \leq \alpha$. Se $\beta = 0$, è banale. Sia $\beta = \gamma + 1$. Se $\beta = \alpha$ è banale e supponiamo dunque $\beta > \alpha$. Allora $\gamma \geq \alpha$ e per ipotesi induttiva $V_\alpha \subseteq V_\gamma$. Allora $V_\alpha \in \mathcal{P}(V_\gamma) = V_{\gamma+1}$. Concludiamo $V_\alpha \subseteq V_{\gamma+1}$ perché $V_{\gamma+1}$ è transitivo. Sia β un limite. Allora $V_\beta = \bigcup_{\alpha<\beta} V_\alpha$. La conclusione è allora ovvia. □

4. Rango

Dato un insieme che appartiene alla gerarchia $x \in \mathbf{VN}$ (per il quale cioè sappiamo esistere un $\alpha \in \mathbf{Ord}$ tale che $x \in V_\alpha$, chiediamoci: qual è il *primo* livello di $\mathbf{VN}$ in cui x appare come elemento? Che un tale primo livello esista è ovvio perché gli ordinali sono bene ordinati! Chiediamoci ora: di che tipo può essere un tale minimo ordinale? Sia λ un tale ordinale e supponiamo che sia un ordinale limite. Ossia abbiamo $x \in V_\lambda$ e per nessun $\gamma < \lambda$ vale $x \in V_\gamma$. Ma $x \in V_\lambda$ implica esiste un $\gamma < \lambda$ tale che $x \in V_\gamma$, perché per definizione V_λ è $\bigcup_{\gamma<\lambda} V_\gamma$. Per tanto, il primo livello in cui un insieme appare nella gerarchia $\mathbf{VN}$ è necessariamente un livello successore. Questo è d'altra parte intuitivo se guardiamo alla definizione di $\mathbf{VN}$: i livelli in cui introduciamo nuovi elementi sono i livelli successore (prendiamo la potenza del precedente), mentre ai livelli limite ci limitiamo a collezionare in un unico insieme tutti gli insiemi apparsi ai livelli precedenti. Risulta dunque naturale porre la seguente definizione, per cui si associa ad un $x \in \mathbf{VN}$ l'indicazione del livello in cui per primo x appare come elemento nella gerarchia.

DEFINIZIONE 4.1 (Rango). Per $\alpha \in \mathbf{VN}$ poniamo

$$\mathrm{rk}(\alpha) := \min\{\alpha \text{ tale che } x \in V_{\alpha+1}\}.$$

Vedremo presto che il rango si rivela estremamente utile: in particolare ci permette di condurre dimostrazioni per induzione transfinita sugli insiemi in **VN**. Preso un insieme qualunque di insiemi in **VN**, non necessariamente esiste il minino insieme rispetto alla relazione d'appartenenza $\in$, ma sicuramente esiste l'insieme con rango minimo! Mostriamo ora che il livello V_α altro non è che l'insieme degli elementi di rango minore di α.

PROPOSIZIONE 4.2. *Per ogni α,*

$$V_\alpha = \{x \in \mathbf{VN} \textit{ tali che } \mathrm{rk}(x) < \alpha\}.$$

DIMOSTRAZIONE. Dimostriamo prima l'inclusione $V_\alpha \subseteq \{x \in \mathbf{VN}$ tali che $\mathrm{rk}(x) < \alpha\}$. Se $x \in V_\alpha$ ovviamente $x \in \mathbf{VN}$. Se $\alpha = \beta + 1$, per definizione abbiamo $\mathrm{rk}(()x) \leq \beta < \alpha$. Se α è limite, per definizione esiste $\beta < \alpha$ tale che $x \in V_\beta$. Allora $\mathrm{rk}(()x) \leq \beta < \alpha$.

Dimostriamo l'altra inclusione. $\mathrm{rk}(()x) < \alpha$ implica che esiste $\beta < \alpha$ t.c. $x \in V_{\beta+1}$. Ma $\beta < \alpha$ implica $\beta + 1 \leq \alpha$ e sappiamo che questo implica $V_{\beta+1} \subseteq V_\alpha$. Dunque $x \in V_\alpha$. □

LEMMA 4.3. *Per ogni $x \in \mathbf{VN}$,*

$$(\forall y \in x)[y \in \mathbf{VN} \wedge \mathrm{rk}(y) < \mathrm{rk}(x)].$$

DIMOSTRAZIONE. $x \in \mathbf{VN}$ significa che esiste α tale che $x \in V_\alpha$. Ma V_α è transitivo e dunque $x \subseteq V_\alpha$, così che abbiamo $y \in V_\alpha$ per ogni $y \in x$. (In altre parole abbiamo dimostrato che $x \subseteq \mathbf{VN}$ se $x \in \mathbf{VN}$). Mostriamo ora che il rango di y è strettamente minore del rango di x se $y \in x$. In altre parole y deve apparire nella gerarchia **VN** prima di x. Sia $\mathrm{rk}(x) = \alpha$. Se $y \in x$ abbiamo $y \in V_\alpha$. Per definizione di rango questo implica $\mathrm{rk}(y) < \alpha$. □

LEMMA 4.4. *Per ogni $x \in \mathbf{VN}$*

$$\mathrm{rk}(x) = \sup\{\mathrm{rk}(y) + 1 \textit{ per } y \in x\}.$$

DIMOSTRAZIONE. Il lemma dice, in parole povere, che x non può apparire nella gerarchia prima del livello in cui tutti i suoi elementi appaiono, e che, d'altra parte, che x apparirà per la prima volta proprio al livello immediatamente successivo a quello in cui appaiono tutti i suoi elementi.

Per $y \in x$, il livello $V_{\mathrm{rk}(y)+1}$ è infatti il primo livello che contiene y come elemento. Il livello $V_{\sup\{\mathrm{rk}(y)+1 \text{ per } y\in x\}}$ è dunque il primo livello che contiene tutti gli elementi di x (è il primo perché abbiamo preso il sup, ossia il minimo dei maggioranti).

In termini tecnici, $\alpha = \sup\{\mathrm{rk}(y) + 1$ per $y \in x\}$. Allora per ogni $y \in x$ $y \in V_\alpha$. In altre parole $x \subseteq V_\alpha$. Ma allora $x \in V_{\alpha+1} = \mathcal{P}(V_\alpha)$. Questo dimostra che $\mathrm{rk}(x) \leq \alpha$, poiché x appare di certo al livello $\alpha + 1$. Resta da verificare che x non può apparire prima del livello $\alpha+1$. Supponiamo che x appaia al livello $\lambda+1$ per la prima volta, con $\lambda < \alpha$. Allo per ogni $y \in x$ abbiamo $\mathrm{rk}(y) \leq \lambda$. Ma allora λ è un maggiorante per l'insieme $\{\mathrm{rk}(y) + 1$ per $y \in x\}$. Dunque λ è sicuramente grande almeno quanto il *sup* di questo insieme, che è α, e perciò abbiamo $\alpha \leq \lambda$, contro l'ipotesi $\lambda < \alpha$.

□

Adesso ci chiediamo: la Gerarchia **VN** contiene ordinali? Se sì, quali? E quelli che appaiono, a che livello appaiono?

PROPOSIZIONE 4.5. *Per ogni* $\alpha \in \mathbf{Ord}$, $\alpha \in \mathbf{VN}$ *e* $\mathrm{rk}(\alpha) = \alpha$.

DIMOSTRAZIONE. Dimostriamo la prima parte (ossia che ogni ordinale appare nella gerarchia) per induzione transfinita. Se $\alpha = 0$ l'asserto è vero perché $0 = \varnothing \in V_1 = \mathcal{P}(V_0)$. Sia $\alpha = \beta + 1$. Per ipotesi induttiva esiste γ tale che $\beta \in V_\gamma$. Ma allora $\beta \cup \{\beta\}$ è un sottinsieme di V_γ (perché V_γ è transitivo). Per tanto $\beta \cup \{\beta\}$ è un elemento di $\mathcal{P}(V_\gamma)$, ossia $\beta + 1 \in V_{\gamma+1}$. Sia α un ordinale limite. Per ipotesi induttiva abbiamo che per ogni $\beta < \alpha$ esiste un γ_β tale che $\beta \in V_{\gamma_\beta}$. In altre parole

$$\alpha \subseteq \bigcup_{\beta<\alpha} V_{\gamma_\beta}.$$

Sia $\gamma = \sup\{\gamma_\beta \text{ t.c. } \beta < \alpha\}$. Ovviamente abbiamo

$$\bigcup_{\beta<\alpha} V_{\gamma_\beta} \subseteq \bigcup_{\lambda<\gamma} V_\lambda.$$

Dunque $\alpha \subseteq \bigcup_{\lambda<\gamma} V_\lambda$ e per tanto $\alpha \in V_{\lambda+1} = \mathcal{P}(\bigcup_{\lambda<\gamma} V_\lambda)$.

Abbiamo dimostrato che $\mathbf{Ord} \subseteq \mathbf{VN}$. L'altra parte della Proposizione, ossia che ogni ordinale α appare per la prima volta in $\mathbf{VN}$ a livello $\alpha+1$ è una conseguenza immediata di quanto abbiamo dimostrato nel Lemma precedente. Infatti abbiamo, per ogni $\alpha \in \mathbf{Ord}$,

$$\mathrm{rk}(\alpha) = \sup\{\mathrm{rk}(\beta) + 1 \text{ t.c. } \beta \in \alpha\} = \sup\{\mathrm{rk}(\beta) + 1 \text{ t.c. } \beta < \alpha\}.$$

Si verifica facilmente, per induzione, che $\sup\{\mathrm{rk}(\beta) + 1 \text{ t.c. } \beta < \alpha\}$ è proprio α. (Esercizio).

□

CAPITOLO 10

Gerarchia Cumulativa, Proprietà del Rango

1. Sinossi

Proprietà del rango. Proprietà di chiusura della Gerarchia di Von Neumann. Insiemi numerici nella Gerachia di Von Neumann.

2. Proprietà di Chiusura di VN

Abbiamo visto che **VN** contiene tutti gli ordinali (è dunque una classe propria), e che l'ordinale α appare per la prima volta come elemento dell'insieme $V_{\alpha+1}$ della gerarchia. Nell'intento di capire meglio la Gerarchia di Von Neumann, di avere una idea più chiara della sua struttura e dei suoi elementi, ci chiediamo: di quali *proprietà di chiusura* gode **VN**? In altre parole, dati $a_1 \ldots, a_n$ insiemi in **VN**, quali nuovi insiemi posso costruire *senza uscire da* **VN**? E a che livello appariranno questi nuovi insiemi? E come posso esprimere il rango dei nuovi insiemi in funzione del rango degli insiemi di partenza?

Consideriamo, per iniziare, le operazioni insiemistiche fondamentali.

PROPOSIZIONE 2.1 (Chiusura sotto operazioni unarie). *Se a è un insieme in* **VN***, allora anche i seguenti insiemi sono in* **VN***.*

- $\mathcal{P}(a)$ (potenza)*, e* $\mathrm{rk}(\mathcal{P}(a)) = \mathrm{rk}(a) + 1$.
- $\{a\}$ (singoletto)*, e* $\mathrm{rk}(\{a\}) = \mathrm{rk}(a) + 1$.
- $\bigcup a$ (unione)*, e* $\mathrm{rk}(\bigcup a) \leq \mathrm{rk}(a)$.

DIMOSTRAZIONE. Sia $\alpha = \mathrm{rk}(a)$. Per definizione si ha $a \in V_{\alpha+1} = \mathcal{P}(a)$, e dunque $a \subseteq V_\alpha$. Perciò, ogni sottinsieme di a è un sottinsieme di V_α ($S \subseteq a \subseteq V_\alpha$). Allora ogni sottinsieme di a è un elemento di $V_{\alpha+1}$, perché $V_{\alpha+1}$ è per definizione $\mathcal{P}(V_\alpha)$. Dunque $\mathcal{P}(a) \in V_{\alpha+2} = \mathcal{P}(V_{\alpha+1})$. Inoltre, il rango di $\mathcal{P}(a)$ non può essere minore di $\alpha + 1$, perché $a \in \{a\} \in \mathcal{P}(a)$, e sappiamo che $x \in y \Rightarrow \mathrm{rk}(x) < \mathrm{rk}(y)$. Ma $\mathrm{rk}(a) = \alpha$.

Sia $\alpha = \mathrm{rk}(a)$. Allora $\{a\} \subseteq V_{\alpha+1}$ e per tanto $\{a\} \in \mathcal{P}(a)(V_{\alpha+1}) = V_{\alpha+2}$. Questo dimostra anche $\mathrm{rk}(\{a\}) \leq \alpha + 1$. D'altro canto, poiché $a \in \{a\}$, sappiamo già che $\mathrm{rk}(a) < \mathrm{rk}(\{a\})$.

Sia $\alpha = \mathrm{rk}(a)$. Allora $a \subseteq V_\alpha$. Per ogni $x \in \bigcup a$, esiste $y \in a$ tale che $x \in y$. Dunque esiste un $y \in V_\alpha$ tale che $x \in y$. Dunque $x \in V_\alpha$. Abbiamo così dimostrato che per ogni $x \in \bigcup a$, $x \in V_\alpha$. Per tanto, $\bigcup a$ è un sottinsieme di V_α, e dunque è un elemento di $V_{\alpha+1}$. □

PROPOSIZIONE 2.2 (Chiusura sotto operazioni binarie). *Se a e b sono insiemi in* **VN***, allora anche i seguenti insiemi sono in* **VN***.*

- $a \cup b$ (unione)*, e* $\mathrm{rk}(a \cup b) \leq \max(\mathrm{rk}(a), \mathrm{rk}(b))$.
- $a \cap b$ (intersezione)*, e* $\mathrm{rk}(a \cap b) \leq \min(\mathrm{rk}(a), \mathrm{rk}(b))$.

- $\{a, b\}$ (coppia), *e* $\mathrm{rk}(\{a, b\}) = \max(\mathrm{rk}(a), \mathrm{rk}(b)) + 1$.
- $\langle a, b\rangle$ (coppia ordinata), *e* $\mathrm{rk}(\langle a, b\rangle) = \max(\mathrm{rk}(a), \mathrm{rk}(b)) + 2$.
- $a \times b$ (prodotto cartesiano), *e* $\mathrm{rk}(a \times b) \leq \max(\mathrm{rk}(a), \mathrm{rk}(b)) + 2$.
- ${}^b a$ (funzioni da b in a), *e* $\mathrm{rk}({}^b a) \leq \max(\mathrm{rk}(a), \mathrm{rk}(b)) + 4$.

DIMOSTRAZIONE. Per tutti i casi che seguono, sia $\alpha = \mathrm{rk}(a)$, $\beta = \mathrm{rk}(b)$, e, senza perdita di generalità, supponiamo che $\alpha \leq \beta$.

(Unione). $a, b \subseteq V_\beta$, e, per transitività, anche $a, b \subseteq V_\beta$. Dunque anche $a \cup b \subseteq V_\beta$, da cui segue $a \cup b \in V_{\beta+1}$. Questo dimostra anche $\mathrm{rk}(a \cup b) \leq \mathrm{rk}(b)$.

(Intersezione). $a \cap b \subseteq a$ e per tanto $a \cap b \subseteq V_\alpha$. Dunque $a \cap b \in V_{\alpha+1}$.

(Coppia). $\{a, b\} \subseteq V_{\beta+1}$ e perciò $\{a, b\} \in \mathcal{P}(V_{\beta+1}) = V_{\beta+2}$. Questo dimostra anche $\mathrm{rk}(\{a, b\}) \leq \mathrm{rk}(b) + 1$. D'altra parte, poiché $b \in \{a, b\}$ sappiamo che $\mathrm{rk}(b) < \mathrm{rk}(\{a, b\})$ e perciò abbiamo che il rango della coppia è proprio $\mathrm{rk}(b) + 1$.

(Coppia Ordinata). $\langle a, b\rangle$ è, per definizione, $\{\{a, b\}, \{a\}\}$. Dato che $\{a, b\} \in V_{\beta+2}$, $\langle a, b\rangle$ è un sottinsieme di $V_{\beta+3}$ e, per tanto, un elemento di $V_{\beta+3}$. Questo dimostra anche $\mathrm{rk}(\langle a, b\rangle) \leq \mathrm{rk}(b) + 2$. D'altra parte, poiché $\{a, b\} \in \langle a, b\rangle$ e $\mathrm{rk}(\{a, b\}) = \mathrm{rk}(b) + 1$, sappiamo che $\mathrm{rk}(b) + 1 < \mathrm{rk}(\langle a, b\rangle)$ e perciò abbiamo che il rango della coppia ordinata è proprio $\mathrm{rk}(b) + 2$.

(Prodotto Cartesiano). $a \times b$ è, per definizione, l'insieme di tutte le coppie ordinate $\langle x, y\rangle$, con $x \in a$ e $y \in b$. Dato che, per $x \in a$ e $y \in b$ si ha $\mathrm{rk}(x) < \mathrm{rk}(a)$ e $\mathrm{rk}(y) < \mathrm{rk}(b)$, di certo $x, y \in V_\beta$. Per quanto dimostrato prima, la coppia ordinata $\langle x, y\rangle$ appare di certo in $V_{\beta+2}$. L'insieme di tutte le coppie ordinate di questo tipo apparirà allora come elemento in $V_{\beta+3}$. Questo dimostra anche la diseguaglianza sul rango.

(Funzioni). L'insieme delle funzioni con dominio uguale b e codominio incluso a è un insieme di insiemi di coppie ordinate $\langle y, x\rangle$ con $y \in b$ e $x \in a$. Ciascuna funzione $f : b \mapsto a$ (definita su tutto b) è un sottinsieme di $b \times a$. L'insieme di tutte le funzioni di questo tipo è per tanto un elemento di $\mathcal{P}(a \times b)$. Dato che $b \times a \subseteq V_{\beta+3}$, tutti i sottinsiemi di $b \times a$ sono elementi di $V_{\beta+4}$. Allora l'insieme ${}^b a$ appare come elemento in $V_{\beta+5}$. □

Possiamo riassumere le proprietà di chiusura di **VN** sotto le abituali operazioni insiemistiche come segue:

$$a \in \mathbf{VN} \Rightarrow \bigcup a, \mathcal{P}(a), \{a\} \in V_{\mathrm{rk}(a)+\omega} \tag{2.1}$$

$$a, b \in \mathbf{VN} \Rightarrow a \cup b, a \cap b, \{a, b\}, \langle a, b\rangle, a \times b, {}^b a \in V_{\max(\mathrm{rk}(a),\mathrm{rk}(b))+\omega} \tag{2.2}$$

3. Insiemi numerici in VN

Abbiamo visto sopra che **VN** è chiusa sotto le usuali operazioni insiemistiche. Inoltre, dal fatto che $\omega \in V_{\omega+1}$, sappiamo che $\omega \subseteq V_\omega$, e che per i V_α sono infiniti a partire dal livello ω e contengono come elementi insiemi infiniti a partire dal livello $\omega + 1$ (è facile verificare che V_n è finito per ogni $n \in \mathbf{N}$ (Esercizio)). D'altra parte, sappiamo come descrivere controparti insiemistiche degli insiemi numerici abituali, ossia di **N**, **Z**, **Q**, **R**, **C**. Ciò basta ad assicurarci che tali insiemi appaiono nella Gerarchia **VN**. Con un po' più di attenzione, analizzando le definizioni insiemistiche delle classi numeriche, si può verificare che il loro rango è strettamente minore di $\omega + \omega$. Per tanto, gli insiemi **N**, **Z**, **Q**, **R**, **C** sono tutti elementi di $V_{\omega+\omega}$.

(Naturali). **N** è identificato con ω, e sappiamo già che $\omega \in V_{\omega+1}$.

(Interi). **Z** si può identificare con un insieme di coppie ordinate di elementi di **N**. Per tanto, **Z** è un sottinsieme del prodotto cartesiano $\mathbf{N} \times \mathbf{N}$. Per quanto visto sopra, $\mathbf{N} \times \mathbf{N}$ ha rango minore di $\mathrm{rk}(\mathbf{N}) + \omega$, ossia di $\omega + \omega$. Dunque anche **Z** ha rango minore di $\omega + \omega$. Notare che un ordinale minore di $\omega + \omega$ è o un naturale o un numero della forma $\omega + k$ con k naturale. $\omega + \omega = sup(\{\omega, \omega + 1, \omega + 2, \dots\})$.

(Razionali). **Q** si può identificare con un insieme di coppie ordinate di elementi di **Z**. Dunque anche il rango di **Q** è minore di $\omega + \omega$.

(Reali). **R** può essere identificato con un insieme di coppie di sottinsiemi di **Q** (i *tagli di Dedekind*). In questo caso, ogni reale è identificato con una coppia di insiemi di razionali, dunque con un elemento di $\mathcal{P}(\mathbf{Q}) \times \mathcal{P}(\mathbf{Q})$. Dunque **R** è rappresentato da un sottinsieme di $\mathcal{P}(\mathbf{Q}) \times \mathcal{P}(\mathbf{Q})$. Per tanto, anche il rango di **R** è minore di $\omega + \omega$ (un'applicazione dell'insieme potenza e una del prodotto cartesiano a partire da **Q** che ha rango $< \omega + \omega$).

(Complessi). Infine, dato che ogni numero complesso può rappresentarsi come composto da una parte reale e da una parte immaginaria, ossia scriversi come $a + ib$, con $a, b \in \mathbf{R}$ e i radice quadrata di -1, si ha **C** si può identificare con un insieme di coppie di **R**.

Abbiamo con ciò dimostrato che la Gerarchia di Von Neumann contiene delle copie adeguate delle abituali classi numeriche. Inoltre, tutte queste classi appaiono piuttosto presto nella gerarchia, ovvero a livello $\omega + \omega$.[1] Per esercizio è possibile calcolare esattamente il rango delle classi numeriche.

4. Un'altra proprietà di VN

Dimostriamo che **VN** soddisfa una proprietà che da sola implica tutte le proprietà di chiusura dimostrate finora.

PROPOSIZIONE 4.1. *Per ogni a,*

$$a \in \mathbf{VN} \Leftrightarrow a \subseteq \mathbf{VN}.$$

DIMOSTRAZIONE. La direzione da sinistra a destra è già nota: se $a \in V_\alpha$, allora $a \subseteq V_\alpha$ perché V_α è transitiva.

Per l'altra direzione: osserviamo che $a \subseteq \mathbf{VN}$ ci dice solo che per ogni $x \in a$ esiste un livello della gerarchia in cui x appare come elemento, ma non sappiamo quale. Usiamo il rango per indicare un livello in cui siamo sicuri di trovare tutti gli elementi di a, ossia un livello in cui siamo sicuri di trovare a come sottinsieme. Ad ogni $x \in \alpha$ possiamo associare il suo rango $\mathrm{rk}(x) \in \mathbf{Ord}$. Allora siamo certi che $x \in \rho_x + 1$. Possiamo poi prendere l'estremo superiore dell'insieme dei $\mathrm{rk}(x) + 1$ per $x \in a$. Questo sarà ancora un ordinale, sia ρ, e siamo ora sicuri che tutti gli elementi di a sono elementi di V_ρ. Definiamo cioè

$$\rho = \sup\{\mathrm{rk}(x) + 1 \text{ tali che } x \in a\}.$$

Allora $a \subseteq V_\rho$. Per tanto, $a \in V_{\alpha+1}$, e abbiamo dimostrato $a \in \mathbf{VN}$. □

[1] Da notare che l'esistenza dell'ordinale $\omega + \omega$ non si dimostra senza l'Assioma di Rimpiazzamento, a partire da ω (dato dall'Assioma di Infinito). Possiamo infatti descrivere $\omega + \omega$ come l'unione dell'immagine della funzione $n \mapsto \omega + n$. Questa osservazione tornerà utile nel seguito.

La proprietà appena dimostrata implica facilmente tutte le proprietà di chiusura di **VN** dimostrate sopra. Bisogna però osservare che la proprietà appena dimostrata è *logicamente più forte* della validità delle proprietà di chiusura. Si ha infatti la seguente dicotomia:

- Se λ è un ordinale limite, allora l'insieme V_λ è chiusa sotto le operazioni insiemistiche abituali, ma
- Se $\mathcal{C}$ è una classe che soddisfa ($x \in \mathcal{C}$ sse $x \subseteq \mathcal{C}$), allora $\mathcal{C}$ contiene tutta la Gerarchia di Von Neumann, i.e. $\mathbf{VN} \subseteq \mathcal{C}$. In particolare $\mathcal{C}$ è una classe propria.

Il primo punto è implicito nelle implicazioni 2.1 e 2.2: l'applicazione di operazioni insiemistiche determina incrementi *finiti* nel rango, e pertanto non basta a saltare oltre un ordinale limite: se $\mu < \lambda$ e λ è limite, $\mu + 1 < \lambda$.

Dimostriamo il secondo punto. Lo facciamo per induzione transfinita dimostrando che, per ogni $\alpha \in \mathbf{Ord}$, $V_\alpha \subseteq \mathcal{C}$, dove $\mathcal{C}$ è la classe che, per ipotesi, soddisfa $x \in \mathcal{C}$ sse $x \subseteq \mathcal{C}$. $V_0 \in \mathcal{C}$ è evidente. Supponi $V_\alpha \subseteq \mathcal{C}$. Allora per ogni $S \in \mathcal{P}(V_\alpha)$ vale $S \subseteq \mathcal{C}$. Per la proprietà di $\mathcal{C}$ vale $S \in \mathcal{C}$. Abbiamo dimostrato allora che $V_{\alpha+1} = \mathcal{P}(V_\alpha) \subseteq \mathcal{C}$. Sia α limite e supponiamo, per Ipotesi Induttiva, di sapere che $V_\beta \subseteq \mathcal{C}$ per ogni $\beta < \alpha$. Facilmente si deduce che $V_\alpha \subseteq \mathcal{C}$, dato che $V_\alpha = \bigcup_{\beta<\alpha} V_\beta$.

CAPITOLO 11

Modelli per la Teoria degli Insiemi

1. Sinossi

Introduciamo le nozioni di modello della teoria degli insiemi, di relativizzazione di una formula ad una classe, e di soddisfazione in una classe.

2. Modelli della teoria degli Insiemi

Un modello di ZF è struttura $\mathfrak{A} = (A, E)$, dove X è un insieme (N.B. non una classe propria!) e E una relazione binaria su A (i.e. un insieme di coppie ordinate di elementi di A) che soddisfa - nel senso classico della semantica per la logica del primo ordine - tutti gli assiomi di ZF. Scriveremo $\mathfrak{A} \models \mathsf{ZF}$ per indicare che $\mathfrak{A}$ è un modello di ZF.

Dal Teorema di Gödel applicato a ZF segue immediatamente che non è possibile, lavorando in ZF (come metateoria), dimostrare l'esistenza di un modello di ZF. Per esempio, non è possibile definire una relazione E usando proprietà dimostrabili in ZF e operazioni valide in ZF tale che $(\mathbf{R}, E) \models \mathsf{ZF}$.

Per il Teorema di Completezza di Gödel, invece, studiare la *dimostrabilità* in ZF equivale a studiare la *soddisfacibilità in tutti i modelli* di ZF. In particolare, se per un dato enunciato φ troviamo che esiste un modello di ZF che soddisfa $\neg\varphi$, allora sappiamo anche che ZF non dimostra φ. D'altra parte, se $\mathsf{ZF} \nvdash \varphi$, allora siamo sicuri che esiste un modello (numerabile) che soddisfa ZF e $\neg\varphi$. In altre parole sappiamo che $\neg\varphi$ è *coerente con* ZF, ossia che la teoria $\mathsf{ZF} + \neg\varphi$ è coerente *se* ZF è coerente.

In quel che segue assumeremo la coerenza di ZF (in qualche caso di una teoria più debole) per dimostrare risultati di *coerenza relativa*. Assumere la coerenza di ZF equivale (ancora per il Teorema di Completezza), ad assumere l'esistenza di un modello di ZF.

Se $\mathfrak{A} = (A, E)$ è un modello di ZF, in A esistono controparti o realizzazioni di tutti gli insiemi che si dimostrano esistenti in base agli assiomi di ZF. Per esempio esisteranno in $\mathfrak{A}$ denotazioni per gli insiemi che finora abbiamo denotato con $\varnothing$, ω, $\aleph_0$, etc. Da notare che questi simboli finora sono stati usati soltanto come abbreviazioni di insiemi la cui esistenza è dimostrabile in ZF. Per esempio, $\varnothing$ è stato usato come un nome/abbreviazione per l'oggetto denotato da x nel teorema di ZF che asserisce l'esistenza dell'insieme vuoto $\exists x \forall y (y \notin x)$. In ciascun modello (A, E) di ZF deve esistere un oggetto $a \in A$ che soddisfa $\forall a' \in A \neg(a' E a)$. Indicheremo questo oggetto come $\varnothing^{\mathfrak{A}}$ (e analogamente useremo $\omega^{\mathfrak{A}}$, $\aleph_0^{\mathfrak{A}}$, etc.) Analogamente ogni modello $\mathfrak{A}$ di ZF contiene versioni (interpretazioni) di tutte le classi proprie definibili in ZF. In particolare $\mathfrak{A}$ contiene l'interpretazione della classe $\mathbf{V}$ (l'universo di tutti gli insiemi), e della relazione fondamentale $\in$. Queste sono da intendersi come le estensioni in $\mathfrak{A}$ del predicato $x = x$ e della relazione $x \in y$, rispettivamente.

Dal punto di vista di $\mathfrak{A}$ l'universo di tutti gli insiemi non è altro che il dominio A del modello, che denotiamo con $\mathbf{V}^{\mathfrak{A}}$, coerentemente a quanto fatto prima per i nomi di insiemi. Analogamente, dal punto di vista di $\mathfrak{A}$, la relazione E è (l'interpretazione de) la relazione di appartenenza $\in$, e possiamo scrivere $\in^{\mathfrak{A}} = E$ con la notazione di prima. Per tanto - una volta fissato un 'modello ambiente' $\mathfrak{A}$ - è naturale indicare semplicemente A con $\mathbf{V}$ e E con $\in$. Un'espressione come $(\mathbf{V}, \in) \models \varphi$ significa allora $(A, E) \models \varphi$.

Una volta fissato un 'modello ambiente' di riferimento (un $\mathfrak{A} = (A, E)$ anche denotato con $(\mathbf{V}, \in)$), possiamo studiarne i sottomodelli, ossia delle sottostrutture $(\mathbf{C}, E')$ dove $\mathbf{C}$ è una sottoclasse (propria o non propria) di $\mathbf{V}$ e E' è la restrizione di E alla classe $\mathbf{C}$. Se $\mathbf{C}$ è un insieme, sappiamo già cosa significa che $\mathbf{C}$ soddisfa una formula φ. La relazione $(\mathbf{C}, E') \models \varphi$ è quella della semantica classica. Per trattare l'argomento in piena generalità (considerando i casi di sottomodelli che sono insiemi e di sottomodelli che sono classi proprie) dobbiamo dire cosa significa che una classe propria soddisfa un enunciato. Per questo un'espressione del tipo $\mathbf{C} \models \varphi$ (omettiamo la menzione della relazione da usare come interpretazione del simbolo $\in$ nel 'modello' con dominio $\mathbf{C}$ perché questa sarà sempre scelta come la restrizione della relazione E del modello ambiente (A, E) alla classe $\mathbf{C}$) non ha senso se $\mathbf{C}$ indica una classe propria, perché la relazione $\models$ della semantica della logica classica è definita solo per insiemi.

Ma le classi proprie definibili in ZF sono soltanto *modi di dire*, non oggetti. In virtù di ciò, possiamo dare un senso al contempo esatto e naturale a una espressione come "la classe propria $\mathbf{C}$ soddisfa la formula φ". L'idea che vogliamo formalizzare è semplicemente questa: vogliamo vedere se un enunciato φ è valido *una volta che lo interpretiamo soltanto su elementi che stanno nella classe* $\mathbf{C}$. Ora, la classe $\mathbf{C}$ è definita da una formula del linguaggio. Denotiamo per semplicità questa formula con $\mathbf{C}(x)$. Per agevolare la lettura, scriviamo $x \in \mathbf{C}$ invece di $\mathbf{C}(x)$, ricordandoci che si tratta di una abbreviazione, e che $x \in \mathbf{C}$ non è direttamente una formula del linguaggio. Possiamo allora definire la *relativizzazione* di una qualunque formula del nostro linguaggio alla classe $\mathbf{C}$ come segue.

Definizione 2.1 (Relativizzazione). Sia φ una formula. Sia $\mathbf{C}$ una classe definibile e sia $\mathbf{C}(x)$ la formula che la definisce. Definiamo per induzione la *relativizzazione* di φ a $\mathbf{C}$ come segue.

- $(x = y)^{\mathbf{C}} := (x = y)$
- $(x \in y)^{\mathbf{C}} := (x \in y)$
- $(\psi \wedge \chi)^{\mathbf{C}} := \psi^{\mathbf{C}} \wedge \chi^{\mathbf{C}}$
- $(\psi \vee \chi)^{\mathbf{C}} := \psi^{\mathbf{C}} \vee \chi^{\mathbf{C}}$
- $(\psi \to \chi)^{\mathbf{C}} := \psi^{\mathbf{C}} \to \chi^{\mathbf{C}}$
- $(\neg\psi)^{\mathbf{C}} := \neg(\psi^{\mathbf{C}})$
- $(\exists x \psi(x))^{\mathbf{C}} := \exists x(\mathbf{C}(x) \wedge (\psi(x))^{\mathbf{C}})$
- $(\forall x \psi(x))^{\mathbf{C}} := \forall x(\mathbf{C}(x) \to (\psi(x))^{\mathbf{C}})$

In altre parole, la relativizzazione di una formula lascia immutate le formule atomiche, commuta con i connettivi proposizionali, e restringe il dominio delle variabili quantificate agli elementi della classe $\mathbf{C}$. Per ogni formula φ e per ogni classe definibile $\mathbf{C}$ (propria o non propria), $\varphi^{\mathbf{C}}$ è un'altra formula del linguaggio perfettamente definita. Diremo allora che un enunciato φ è *soddisfatto da una classe* $\mathbf{C}$ se, nel nostro modello di ZF di riferimento, vale (nel senso standard della

semantica classica) la relativizzazione $\varphi^{\mathbf{C}}$, ossia se $(\mathbf{V}, \in) \models \varphi^{\mathbf{C}}$. Se questo è il caso, scriveremo anche $\mathbf{C} \models \varphi$. Risulta chiaro che quest'ultima è solo una abbreviazione dell'enunciato $(\mathbf{V}, \in) \models \varphi^{\mathbf{C}}$, che è perfettamente definito nel quadro della semantica classica della teoria del primo ordine ZF.

Osservazione 2.2. Quando parliamo di classi, parliamo di classi proprie *e non proprie*. Solo quando parliamo di *classi proprie* escludiamo esplicitamente gli insiemi. Occorre osservare che la spiegazione di $\mathbf{C} \models \varphi$ data sopra funziona anche se $\mathbf{C}$ è un insieme, e in questo caso coincide con la nozione di soddisfacibilità classica. Sia $\mathbf{C}$ un insieme $\subseteq A$ definibile e sia E' la relazione E ristretta a $\mathbf{C}$. Allora

$$\mathbf{C} \models \varphi \Leftrightarrow (A, E) \models \varphi^{\mathbf{C}} \Leftrightarrow (\mathbf{C}^{\mathfrak{A}}, E') \models \varphi.$$

A sinistra abbiamo la relazione $\models$ definita sopra per qualunque classe definibile, al centro abbiamo la relazione di soddisfacibilità nel modello della formula relativizzata a $\mathbf{C}$, a destra abbiamo la relazione classica di soddisfacibilità nel modello $(\mathbf{C}^{\mathfrak{A}}, E')$ della formula φ. Qui occorre notare che $\mathbf{C}^{\mathfrak{A}}$ è sempre un insieme, dato che il dominio A di un modello è un insieme.

3. Condizioni di Soddisfazione degli Assiomi

Fissiamo un modello $(\mathbf{V}, \in)$ di ZF. Nelle Proposizioni seguenti diamo, per ogni assioma φ di ZF, condizioni sufficienti e necessarie affinché una classe definibile $\mathbf{M}$ soddisfi φ, ossia affinché valga

$$(\mathbf{V}, \in) \models \varphi^{\mathbf{M}}.$$

In ogni caso assumeremo che $\mathbf{M}$ è una classe transitiva.

Proposizione 3.1. *Se* $\mathbf{M}$ *è una classe transitiva allora* $\mathbf{M}$ *soddisfa l'Assioma di Estensionalità.*

Dimostrazione. Per definizione $\mathbf{M}$ soddisfa l'assioma di estensionalità se e solo se la relativizzazione dell'assioma è vera nel modello, i.e., se e solo se

$$\begin{aligned} & (\mathbf{V}, \in) \models (\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y))^{\mathbf{M}} \\ \Leftrightarrow \quad & (\mathbf{V}, \in) \models (\forall x \in \mathbf{M} \forall y \in \mathbf{M} (\forall z \in \mathbf{M} (z \in x \leftrightarrow z \in y) \rightarrow x = y)) \\ \Leftrightarrow \quad & (\mathbf{V}, \in) \models (\forall x \in \mathbf{M} \forall y \in \mathbf{M} (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)) \end{aligned}$$

L'ultima equivalenza è giustificata dal fatto che $\mathbf{M}$ è transitivo, e che $x, y \in \mathbf{M}$: allora la formula $\forall z \in \mathbf{M}(z \in x \leftrightarrow z \in y)$ equivale a $\forall z (z \in x \leftrightarrow z \in y)$. Ora è immediato vedere che l'enunciato nell'ultima riga è sicuramente soddisfatto in $(\mathbf{V}, \in)$. Sta infatti dicendo che, se due insiemi x, y di $\mathbf{M}$ (e dunque a fortiori di $\mathbf{V}$) hanno esattamente gli stessi elementi (non soltanto gli stessi elementi presi in $\mathbf{M}$) allora sono uguali. Questo è vero in $\mathbf{V}$ (che è un modello di ZF). □

Proposizione 3.2. *Se* $\mathbf{M}$ *è una classe transitiva allora* $\mathbf{M}$ *soddisfa l'Assioma di Fondazione.*

Dimostrazione. Per definizione $\mathbf{M}$ soddisfa l'assioma di fondazione se e solo se la relativizzazione dell'assioma è vera nel modello. Preso un $a \in \mathbf{M}$ non vuoto, esiste in $\mathbf{V}$ un $b \in a$ di rango minimo. Questo è vero perché il modello $\mathbf{V}$ soddisfa l'assioma di fondazione. Sappiamo che se b è di rango minimo tra gli elementi di a, allora non esiste (in $\mathbf{V}$ e dunque in $\mathbf{M}$) un elemento $c \in y$ tale che $c \in a$. Resta

solo da dimostrare che $b \in \mathbf{M}$. Ma questo è immediato perché $b \in a \in \mathbf{M}$ e $\mathbf{M}$ è transitivo. □

PROPOSIZIONE 3.3. *Se* $\mathbf{M}$ *è una classe allora* $\mathbf{M}$ *soddisfa l'assioma della Coppia se e solo se* $\forall a, b \in \mathbf{M} \exists c \in \mathbf{M}(\{a, b\} \subseteq c)$. *In altre parole se e solo se* $\mathbf{M}$ *è chiuso sotto l'operazione* $a, b \mapsto \{a, b\}$.

DIMOSTRAZIONE. Per definizione $\mathbf{M}$ soddisfa l'Assioma della Coppia se e solo se

$$\begin{aligned} & (\mathbf{V}, \in) \models (\forall x \forall y \exists z (x \in z \wedge y \in z))^{\mathbf{M}} \\ \Leftrightarrow \quad & (\mathbf{V}, \in) \models (\forall x \in \mathbf{M} \forall y \in \mathbf{M} \exists z \in \mathbf{M} (x \in z \wedge y \in z)) \\ \Leftrightarrow \quad & (\mathbf{V}, \in) \models (\forall x \in \mathbf{M} \forall y \in \mathbf{M} \exists z \in \mathbf{M} (x \in z \wedge y \in z)) \\ \Leftrightarrow \quad & (\mathbf{V}, \in) \models (\forall x \in \mathbf{M} \forall y \in \mathbf{M} \exists z \in \mathbf{M} (\{x, y\} \subseteq z) \end{aligned}$$

□

PROPOSIZIONE 3.4. *Se* $\mathbf{M}$ *è una classe transitiva allora* $\mathbf{M}$ *soddisfa l'Assioma dell'Unione se e solo se* $\forall a \in \mathbf{M} \exists b \in \mathbf{M}(\bigcup a \subseteq b)$. *In altre parole se e solo se* $\mathbf{M}$ *è chiuso sotto l'operazione* $a \mapsto \bigcup a$.

DIMOSTRAZIONE. Per definizione $\mathbf{M}$ soddisfa l'Assioma dell'Unione se e solo se

$$\begin{aligned} & (\mathbf{V}, \in) \models (\forall x \exists y \forall z (\exists w (w \in x \wedge z \in w) \rightarrow z \in y))^{\mathbf{M}} \\ \Leftrightarrow \quad & (\mathbf{V}, \in) \models (\forall x \in \mathbf{M} \exists y \in \mathbf{M} \forall z \in \mathbf{M} (\exists w \in \mathbf{M} (w \in x \wedge z \in w) \rightarrow z \in y)) \end{aligned}$$

Dato che $\mathbf{M}$ è transitivo, abbiamo $w \in x \in \mathbf{M}$ implica $w \in \mathbf{M}$ e $z \in w \in \mathbf{M}$ implica $z \in \mathbf{M}$. Dunque la condizione è equivalente a

$$(\mathbf{V}, \in) \models (\forall x \in \mathbf{M} \exists y \in \mathbf{M} \forall z (\exists w (w \in x \wedge z \in w) \rightarrow z \in y))$$

Ma questa condizione sta dicendo che per ogni $x \in \mathbf{M}$ esiste un $y \in \mathbf{M}$ che contiene (nel senso abituale di $\subseteq$) la *vera* unione di x, ossia tale che $\bigcup x \subseteq y$.

□

OSSERVAZIONE 3.5. Occorre riflettere con calma sul senso delle ultime proposizioni, che possono sembrare quasi tautologiche. Prendiamo il caso dell'unione. Letteralmente, una classe $\mathbf{M}$ soddisfa l'unione, se e solo se, preso un insieme nella classe, troviamo nella classe un altro insieme che contiene tutti gli elementi in $\mathbf{M}$ di elementi in $\mathbf{M}$ dell'insieme di partenza. Ciò lascerebbe in principio la possibilità seguente: una classe $\mathbf{M}$ potrebbe soddisfare l'assioma di Unione anche se contenesse un elemento a tale che $\bigcup a$ non è contenuta in nessun elemento di $\mathbf{M}$. Potrebbe cioè darsi il caso che siamo sempre capaci di raccogliere in un insieme tutti gli elementi in $\mathbf{M}$ degli elementi in $\mathbf{M}$ di a, ma così facendo lasciamo fuori alcuni elementi di elementi di a che non sono in $\mathbf{M}$. Ossia non ci curiamo degli elementi di eventuali $b \in a$ tali che $b \notin \mathbf{M}$. Se $\mathbf{M}$ è transitivo non esistono b siffatti.

PROPOSIZIONE 3.6. *Se* $\mathbf{M}$ *è una classe transitiva allora* $\mathbf{M}$ *soddisfa l'Assioma delle Parti se e solo se* $\forall a \in \mathbf{M} \exists b \in \mathbf{M}(\mathcal{P}(a) \cap \mathbf{M} \subseteq b)$. *In altre parole se e solo se per ogni* a *in* $\mathbf{M}$ *siamo capaci di raccogliere in un insieme tutti i sottinsiemi di* a *che si trovano in* $\mathbf{M}$.

DIMOSTRAZIONE. Per definizione $\mathbf{M}$ soddisfa l'Assioma delle Parti se e solo se

$$(\mathbf{V}, \in) \models (\forall x \exists y \forall z((z \subseteq x) \to z \in y))^{\mathbf{M}}$$
$$\Leftrightarrow \quad (\mathbf{V}, \in) \models (\forall x \in \mathbf{M} \exists y \in \mathbf{M} \forall z \in \mathbf{M}((z \subseteq x)^{\mathbf{M}} \to z \in y)$$

Soffermiamoci sulla formula $(z \subseteq x)^{\mathbf{M}}$. Che formula è? Dobbiamo ricordarci che la relazione $\subseteq$ non è un simbolo primitivo del nostro linguaggio, ma soltanto una comoda abbreviazione per una relazione definibile. L'espressione $(z \subseteq x)$ abbrevia la formula

$$(\forall w)(w \in z \to w \in x).$$

La relativizzazione della formula $(z \subseteq x)$ a $\mathbf{M}$ è allora la relativizzazione della formula definitoria, ossia:

$$\begin{aligned}(z \subseteq x)^{\mathbf{M}} \quad &\Leftrightarrow ((\forall w)(w \in z \to w \in x))^{\mathbf{M}} \\ &\Leftrightarrow (\forall w \in \mathbf{M})(w \in z \to w \in x)\end{aligned}$$

Ma se $\mathbf{M}$ è transitivo, e $z \in \mathbf{M}$, abbiamo

$$(\forall w \in \mathbf{M})(w \in z \to w \in x) \Leftrightarrow (\forall w)(w \in z \to w \in x),$$

ossia

$$(z \subseteq x)^{\mathbf{M}} \Leftrightarrow (z \subseteq x).$$

Abbiamo appena dimostrato che, se $\mathbf{M}$ è transitiva, allora la formula $(z \subseteq x)$ significa la stessa cosa della relativizzazione $(z \subseteq x)^{\mathbf{M}}$. (Diremo più avanti che una tale formula è *assoluta* per classi transitive). Tornando all'assioma della Potenza, abbiamo che $\mathbf{M}$ lo soddisfa se e solo se

$$\begin{aligned}&(\mathbf{V}, \in) \models \forall x \in \mathbf{M} \exists y \in \mathbf{M} \forall z \in \mathbf{M}((z \subseteq x)^{\mathbf{M}} \to z \in y) \\ \Leftrightarrow \quad &(\mathbf{V}, \in) \models \forall x \in \mathbf{M} \exists y \in \mathbf{M} \forall z \in \mathbf{M}((z \subseteq x) \to z \in y) \\ \Leftrightarrow \quad &(\mathbf{V}, \in) \models \forall x \in \mathbf{M} \exists y \in \mathbf{M} \forall z \in \mathbf{M}(z \in \mathcal{P}(x) \to z \in y) \\ \Leftrightarrow \quad &(\mathbf{V}, \in) \models \forall x \in \mathbf{M} \exists y \in \mathbf{M}(\mathcal{P}(x) \cap \mathbf{M} \to z \in y)\end{aligned}$$

□

OSSERVAZIONE 3.7. Va osservato che la situazione dell'Assioma Potenza è assai diversa da quella dei precedenti assiomi. Per esempio, abbiamo visto sopra che una condizione sufficiente e necessaria affinché una classe transitiva soddisfi l'Unione è che la classe sia chiusa sotto la *vera* unione (ossia l'unione nel modello $\mathbf{V}$ di riferimento). La stessa cosa non è vera per l'Assioma Potenza. Per soddisfare l'Assioma Potenza una classe transitivia $\mathbf{M}$ non deve necessariamente essere chiusa sotto la *vera* potenza, ossia non deve necessariamente contenere l'insieme di tutto i sottinsiemi che esistono in $\mathbf{V}$ di un qualunque insieme in $\mathbf{M}$. Basta che in $\mathbf{M}$ sia possibile, per ogni insieme a, raccogliere in un insieme tutti i sottinsiemi di a che si trovano in $\mathbf{M}$, senza curarci di quelli che eventualmente si trovano in $\mathbf{V} - \mathbf{M}$.

PROPOSIZIONE 3.8. *Se $\mathbf{M}$ è una classe transitiva allora $\mathbf{M}$ soddisfa l'assioma della Separazione se e solo se, per ogni formula $\varphi(w, \vec{z})$, per ogni $a, \vec{c} \in \mathbf{M}$, l'insieme*

$$\{w \in a \text{ tale che } \varphi^{\mathbf{M}}(w, \vec{c})\},$$

è in $\mathbf{M}$.

DIMOSTRAZIONE. Per definizione $\mathbf{M}$ soddisfa l'assioma della Separazione se e solo se, per ogni formula $\varphi(w, \vec{z})$, vale

$$(\mathbf{V}, \in) \models (\forall x \forall \vec{z} \exists y \forall w (w \in y \leftrightarrow (w \in x \wedge \varphi(w, \vec{z})))^{\mathbf{M}}$$
$$\Leftrightarrow \quad (\mathbf{V}, \in) \models \forall x \in \mathbf{M} \forall \vec{z} \in \mathbf{M} \exists y \in \mathbf{M} \forall w \in \mathbf{M} (w \in y \leftrightarrow (w \in x \wedge (\varphi(w, \vec{z}))^{\mathbf{M}})$$

Dato che $\mathbf{M}$ è transitivo abbiamo $w \in x \in \mathbf{M}$ implica $x \in \mathbf{M}$ e per tanto la condizione si semplifica in

$$\Leftrightarrow \quad (\mathbf{V}, \in) \models \forall x \in \mathbf{M} \forall \vec{z} \in \mathbf{M} \exists y \in \mathbf{M} \forall w (w \in y \leftrightarrow (w \in x \wedge (\varphi(w, \vec{z}))^{\mathbf{M}})$$

Dunque y è proprio $\{w \in x$ tali che $(\varphi(w, \vec{z}))^{\mathbf{M}})\}$. □

Una condizione sufficiente e più semplice da verificare segue immediatamente.

COROLLARIO 3.9. *Se* $\mathbf{M}$ *è una classe transitiva allora* $\mathbf{M}$ *soddisfa l'assioma della Separazione se per ogni* $a \in \mathbf{M}$ *vale* $\mathcal{P}(a) \subseteq \mathbf{M}$.

PROPOSIZIONE 3.10. *Se* $\mathbf{M}$ *è una classe transitiva allora* $\mathbf{M}$ *soddisfa l'assioma del Rimpiazzamento se e solo se, per ogni formula* $\varphi(x, y, \vec{z})$*, per ogni* $a, \vec{c} \in \mathbf{M}$ *tali che vale* $\forall x \in a \exists! y \varphi^{\mathbf{M}}(x, y, \vec{z})$*, esiste un* $b \in \mathbf{M}$ *che contiene l'insieme immagine*

$$\{y \text{ tale che } \exists x \in a \varphi^{\mathbf{M}}(x, y, \vec{c})\}.$$

DIMOSTRAZIONE. Esercizio (analogo a quanto fatto per la Separazione). □

OSSERVAZIONE 3.11. Osserviamo che le condizioni necessarie e sufficienti per la soddisfazione degli Assiomi di Separazione e Rimpiazzamento in una classe transitiva costituiscono semplificazioni delle condizioni che avremmo per definizione. In teoria, la validità della Separazione in una classe $\mathbf{M}$ richiederebbe soltanto la capacità, per ogni proprietà definibile P di raccogliere in un nuovo insieme - dato un insieme $a \in \mathbf{M}$ - tutti e soli gli elementi che si trovano in $\mathbf{M}$, che sono in a, e che soddisfano P. In teoria dunque potremmo non curarci degli eventuali elementi in a che soddisfano P ma che non sono in $\mathbf{M}$. Se $\mathbf{M}$ è transitiva non esistono elementi siffatti.

Come Corollario delle dimostrazioni fatte finora, otteniamo che l'insieme V_ω è un modello di tutti gli assiomi di ZF meno l'Assioma dell'Infinito.

Nella dimostrazione che segue, consideriamo V_ω come una classe definibile in qualunque modello di ZF. Da osservare che in un tale modello sono dimostrabili tutte le proprietà di V_ω che abbiamo dimostrato precedentemente. Le dimostrazioni di tali proprietà si svolgevano ovviamente in ZF (spesso in una teoria più debole). Useremo quanto dimostrato finora sulle condizioni necessarie e sufficienti affinché una classe transitiva soddisfi gli assiomi di ZF.

COROLLARIO 3.12. V_ω *soddisfa tutti gli assiomi di* ZF *meno l'Assioma dell'Infinito.*

DIMOSTRAZIONE. Sappiamo che V_ω è transitivo. Abbiamo dimostrato, studiando la Gerarchia di Von Neumann, che V_ω è chiuso per coppia, unione, potenza, ossia: se $a, b \in V_\omega$ allora $\bigcup a$, $\{a, b\}$ e $\mathcal{P}(a)$ sono in V_ω. Per quanto dimostrato nelle Proposizioni precedenti, ciò è sufficiente per concludere che V_ω soddisfa

gli assiomi di Coppia, Unione e Potenza. Verifichiamo che soddisfa l'Assioma di Rimpiazzamento. Siano $a, \vec{c} \in V_\omega$ e φ tale che valga $\forall x \in a \exists! y(\varphi^{V_\omega}(x, y, \vec{c})$. Sia

$$b = \{y \text{ tale che } \exists x \in a(\varphi^{V_\omega}(x, y, \vec{c})\}.$$

b è un sottinsieme di V_ω. Ricordiamo che $V_\omega = \bigcup_{n\in\omega} V_n$ e che V_ω non contiene insiemi infiniti. Dunque a è finito. Dato che vale $\forall x \in a \exists! y(\varphi^{V_\omega}(x, y, \vec{c})$, esiste una suriezione di a su b e pertanto b è finito. Dunque b è un sottinsieme di V_n per qualche $n \in \omega$ (basta prendere $n >$ il massimo di b). Dunque $b \in V_\omega$ e le condizioni per la soddisfazione dell'Assioma di Rimpiazzamento sono soddisfatte. □

CAPITOLO 12

Assolutezza e Riflessione

1. Sinossi

Introduciamo la nozione di assolutezza di una formula rispetto a una classe. Rimandiamo la trattazione dettagliata di questa nozione e dimostriamo il Principio di Riflessione. Deduciamo l'impossibilità di ottenere una assiomatizzazione finita di ZF.

2. Assolutezza e Criterio di Vaught

Abbiamo dimostrato che, se $\mathbf{M}$ è una classe transitiva, e $a, b \in \mathbf{M}$, allora a è un sottinsieme di b dal punto di vista di $\mathbf{M}$ se e solo se a è 'veramente' un sottinsieme di b (ossia dal punto di vista del modello ambiente $\mathbf{V}$). In termini più esatti, abbiamo osservato che

$$(a \subseteq b)^{\mathbf{M}} \Leftrightarrow (a \subseteq b).$$

In altre parole

$$(\mathbf{V}, \in) \models (a \subseteq b) \Leftrightarrow (\mathbf{V}, \in) \models (a \subseteq b)^{\mathbf{M}}.$$

Ricordiamo che $a \subseteq b$ è un'abbreviazione di $\forall z(z \in x \rightarrow z \in y)$ e che dunque $(a \subseteq b)^{\mathbf{M}}$ è la formula $\forall z \in \mathbf{M}(z \in x \rightarrow z \in y)$. Un altro modo di descrivere questa situazione è dire che la relazione di sottinsieme significa *la stessa cosa* in $\mathbf{M}$ e in $\mathbf{V}$, per qualunque $\mathbf{M}$ transitiva.

Quando una formula insiemistica è soddisfatta relativamente a una classe se e solo se è soddisfatta nell'universo (i.e., nel modello ambiente), diciamo che la formula è *assoluta* rispetto alla classe. Se la formula definisce una relazione (come accadeva per la formula che definisce $\subseteq$), diciamo che la relazione è assoluta. Una formula può anche definire una operazione, come accade per es. per l'operazione che abbiamo indicato con $\bigcup$. Anche il simbolo $\bigcup$ è una abbreviazione e non appartine al linguaggio formale. $x \in \bigcup y$ è una abbreviazione per dire che esiste un elemento di y che contiene x. Per parlare di operazioni assolute dobbiamo fare un po' più di attenzione. Diremo che una operazione è assoluta rispetto a una classe se è assoluta la formula che definisce l'operazione, e se sappiamo che quella formula definisce un'operazione in $\mathbf{M}$, ossia se è vero che per ogni scelta di argomenti in $\mathbf{M}$ esiste *un unico* elemento ad essi associato come risultato dell'operazione.

Definizione 2.1 (Assolutezza). Una formula $\varphi(\vec{x})$ è *assoluta* per una classe $\mathbf{M}$ se, per ogni $\vec{a} \in \mathbf{M}$,

$$(\mathbf{V}, \in) \models \varphi(\vec{a}) \Leftrightarrow \mathbf{M} \models \varphi(\vec{a}).$$

Una relazione definita è *assoluta* per $\mathbf{M}$ se e solo se è assoluta per $\mathbf{M}$ la formula che definisce la relazione.

Una operazione definita da una formula $\varphi(\vec{x}, y)$ è *assoluta* per $\mathbf{M}$ se e solo se è assoluta la formula $\varphi(\vec{x}, y)$ e se vale $\mathbf{M} \models \forall \vec{x} \exists! y \varphi(\vec{x}, y)$.

Vedremo più in là che molte relazioni e operazioni sono assolute per classi transitive. Sapere che una relazione o una operazione è assoluta per una classe ci permette di studiare la classe più agevolmente: possiamo assumere che all'interno della classe le relazioni in questione hanno il significato usuale.

Rimandiamo la trattazione dettagliata della nozione di assolutezza e dimostriamo un risultato rilevante che ne fa uso in modo cruciale.

3. Principio di Riflessione

Dimostriamo (in ZF) il seguente risultato: preso comunque un numero *finito* di formule insiemistiche, esiste un ordinale β tanto grande che le formule scelte sono assolute tra V_β e l'universo. In altre parole, V_β è sufficiente per *riflettere* il significato dell'insieme finito di formule scelto (chiamiamo V_β un *punto di riflessione* per le formule in questione). Verificare che quelle formule valgono relativizzate in V_β equivale a verificare che valgono in tutto il modello. Dimostriamo anche che β può essere scelto arbitrariamente grande, più grande di un qualunque α prefissato.

Dimostriamo un utile strumento per verificare l'assolutezza di un insieme finito di formule rispetto ad una classe (è una variante del Criterio di Vaught per l'equivalenza elementare): per verificare l'assolutezza di un insieme S di formule basta verificare che $\mathbf{M}$ contiene un testimone per ogni formula esistenziale in S vera nell'universo, se gli altri parametri sono scelti in $\mathbf{M}$.

PROPOSIZIONE 3.1 (Criterio di Vaught). *Sia $\{\varphi_1, \dots, \varphi_n\}$ un insieme di formuile chiuso per sotto-formula e sia $\mathbf{M}$ una classe definibile. Allora sono equivalenti:*

(1) *Le formule $\varphi_1, \dots, \varphi_n$ sono assolute per $\mathbf{M}$,*
(2) *Per ogni formula esistenziale $\varphi_i \equiv \exists x \varphi_j(x, \vec{y})$*

$$\forall \vec{y} \in \mathbf{M}[\exists x \varphi_j(x, \vec{y}) \to \exists x \in \mathbf{M} \varphi_j(x, \vec{y})].$$

DIMOSTRAZIONE. (1) implica (2): Sia $\vec{y} \in \mathbf{M}$ tali che $\exists x \varphi_j(x, \vec{y})$. Allora $\varphi_i(x, \vec{y})$. Allora, $\varphi_i^{\mathbf{M}}(x, \vec{y})$, per l'ipotesi di assolutezza. Ma $\varphi_i^{\mathbf{M}}(x, \vec{y})$ è proprio $\exists x \in \mathbf{M} \varphi_j^{\mathbf{M}}(x, \vec{y})$. Dato che φ_j è assoluta per $\mathbf{M}$, ciò implica $\exists x \in \mathbf{M} \varphi_j(x, \vec{y})$.

(2) implica (1): Per induzione sulla lunghezza di φ_i. Se φ_i è atomica, non c'è niente da dimostrare (tutte le formule atomiche sono assolute per tutte le classi, per come è definita la relativizzazione). Lo stesso vale per le combinazioni proposizionali. L'unico caso rilevante è φ_i di forma $\exists x \varphi_j(x, \vec{y})$. Fissiamo $\vec{y} \in \mathbf{M}$. Allora

$$\varphi_i^{\mathbf{M}}(\vec{y}) \Leftrightarrow \exists x \in \mathbf{M} \varphi_j^{\mathbf{M}}(x, \vec{y}) \Leftrightarrow_{(*)} \exists x \in \mathbf{M} \varphi_j(x, \vec{y}) \Leftrightarrow_{(2)} \exists x \varphi_j(x, \vec{y}) \Leftrightarrow \varphi_i(\vec{y}).$$

(*) è vero per Ipotesi Induttiva (φ_j è più corta di φ_i). □

TEOREMA 3.2 (Riflessione). *Date formule $\varphi_1, \dots, \varphi_n$,*

$$\mathsf{ZF} \vdash \forall \alpha \exists \beta > \alpha (\varphi_1, \dots, \varphi_n \text{ sono assolute per } V_\beta).$$

DIMOSTRAZIONE. Supponiamo, senza pregiudizio della generalità, che l'insieme di formule sia chiuso per sottoformula (se non lo è già, lo chiudiamo!). Consideriamo le formule esistenziali nell'insieme. Sia φ_i di forma $\exists x \varphi_j(x, \vec{y})$. Per ogni scelta di parametri $\vec{a}$ in $\mathbf{M}$ da sostituire alle variabili $\vec{y}$, possiamo chiederci se la formula

$$\exists x \varphi_j(x, \vec{a})$$

è vera o no (nel modello $\mathbf{V}$). Se è vera, dato che $\mathbf{V} = \bigcup_{\alpha \in \mathbf{Ord}} V_\alpha$ perché vale l'Assioma di Fondazione, possiamo prendere nota del minimo livello della Gerarchia di Von Neumann in cui compare un testimone del quantificatore esistenziale, ossia il minimo ordinale η tale che $\exists x \in V_\eta$ che soddisfa $\varphi_j(x, \vec{a})$. Resta così associata, ad ogni formula esistenziale φ_i, una funzione G_i definita come segue, al variare di $\vec{a} \in \mathbf{M}$.

$$G_i(\vec{a}) = \begin{cases} 0 & \text{se } \neg(\exists x \varphi_j(x, \vec{a})) \\ \min\{\eta \text{ tale che } \exists x \in V_\eta \varphi_j(x, \vec{a})\} & \text{altrimenti.} \end{cases}$$

Vogliamo ora chiederci: data una formula esistenziale φ_i, fino a quale livello della Gerarchia di Von Neumann devo salire per trovare testimoni del quantificatore esistenziale *se gli altri parametri sono scelti a livello* V_ξ? Ossia: quanto in alto possono andare i valori di $G_i(\vec{a})$ se $\vec{a}$ varia solo su V_ξ? Fissato V_ξ, ad ogni scelta di parametri $\vec{a} \in V_\xi$ corrisponde un valore ordinale $G_i(\vec{a})$. Inoltre, V_ξ è un insieme e per tanto $\{G_i(\vec{a}) \text{ tale che } \vec{a} \in V_\xi\}$ è un insieme, e possiamo prenderne l'estremo superiore. Definiamo così una funzione F_i da ordinali a ordinali

$$F_i(\xi) = \sup\{G_i(\vec{a}) \text{ tale che } \vec{a} \in V_\xi\}.$$

Possiamo pensare all'operazione

$$V_\xi \mapsto V_{F_i(\xi)},$$

come alla chiusura del livello V_ξ sotto la formula esistenziale φ_i. In $V_{F_i(\xi)}$ troviamo testimoni universali della formula per ogni scelta di parametri in V_ξ. Se φ_i non è esistenziale, poniamo senza danno $F_i(\xi) = 0$ per ogni ξ. Se ora facciamo variare i parametri nel nuovo insieme $V_{F_i(\xi)}$, in generale non possiamo essere sicuri di trovare in $V_{F_i(\xi)}$ testimoni esistenziali per φ_i. Ma possiamo ripetere l'operazione di chiusura a partire da $V_{F_i(\xi)}$ e ottenere un nuovo livello $V_{F_i(F_i(\xi))}$.

Vogliamo ora partire dall'ordinale α prefissato e arbitrario e iterare l'operazione di chiusura. In tal modo vogliamo trovare il primo livello β della gerarchia che contiene testimoni universali per la formula i se i parametri sono scelti a livello β.

Definiamo una successione partendo da α e applicando, ad ogni passo, l'operazione di chiusura F_i, per ogni formula esistenziale φ_i. (Ad ogni passo prendiamo il massimo tra l'ordinale chiusura del passo precedente e il successore del passo precedente per assicurarci di ottenere una successione strettamente crescente).

$$\beta_0 = \alpha, \beta_{p+1} = \max\{\beta_p + 1, F_1(\beta_p), \ldots, F_n(\beta_p)\}.$$

Definiamo infine $\beta = \sup\{\beta_p \text{ tale che } p \in \omega\}$. Si osserva facilmente che

$$\xi < \xi' \Rightarrow F_i(\xi) \leq F_i(\xi').$$

Se ξ è minore di β, allora per definizione di β esiste un p tale che $\xi < \beta_p$. Dunque

$$F_i(\xi) \leq F_i(\beta_p) \leq \beta_{p+1} < \beta.$$

Quanto appena detto $(\xi < \beta \Rightarrow (\forall i \leq n)[F_i(\xi) < \beta])$ significa che a livello V_β troviamo testimoni per la verità di φ_i per qualunque scelta di parametri nello stesso V_β. □

4. Assiomatizzare ZF

Un interessante Corollario del Principio di Riflessione è l'impossibilità di assiomatizzare ZF con un numero finito di assiomi. Il risultato fa uso di alcuni risultati di assolutezza che dimostreremo in seguito.

COROLLARIO 4.1. *Sia $\varphi_1, \ldots, \varphi_n$ un insieme di enunciati tali che $\varphi_1, \ldots, \varphi_n \vdash$ ZF. Allora* ZF *è incoerente.*

DIMOSTRAZIONE. Ragioniamo in ZF. Per il Teorema di Riflessione, esiste un livello della Gerarchia di Von Neumann che riflette le formule $\varphi_1, \ldots, \varphi_n$. Dato che le φ_i sono enunciati (formule chiuse), e dato che bastano a dimostrare tutto ZF, il Teorema di Riflessione in questo caso dice che

$$\varphi_1, \ldots, \varphi_n \vdash \forall\alpha\exists\beta > \alpha((\varphi_1^{V_\beta} \leftrightarrow \varphi_1) \wedge \ldots (\varphi_n^{V_\beta} \leftrightarrow \varphi_n)).$$

Dunque

$$\varphi_1, \ldots, \varphi_n \vdash \exists\beta(\varphi_1^{V_\beta} \wedge \cdots \wedge \varphi_n^{V_\beta}).$$

Sia β il minimo ordinale tale che valgono

$$\varphi_1^{V_\beta}, \ldots, \varphi_n^{V_\beta}.$$

Allora, per ipotesi, $V_\beta \vdash$ ZF. Dunque in V_β valgono tutti i risultati di assolutezza dimostrabili in ZF (che dimostreremo più avanti). In particolare vale la seguente implicazione (che dimostreremo più avanti in ZF per ogni modello transitivo di ZF e non solo per V_β):

$$\alpha \in V_\beta \Rightarrow V_\alpha^{V_\beta} = V_\alpha \cap V_\beta.$$

Dunque $V_\alpha^{V_\beta} = V_\alpha$. In altre parole, l'operazione

$$\alpha \mapsto V_\alpha$$

è assoluta per V_β. Per il Principio di Riflessione,

$$\mathsf{ZF} \vdash \exists\alpha(\varphi_1^{V_\alpha}, \ldots, \varphi_n^{V_\alpha}).$$

Dunque, dato che V_β è un modello di ZF,

$$(\exists\alpha(\varphi_1^{V_\alpha}, \ldots, \varphi_n^{V_\alpha}))^{V_\beta}.$$

ossia

$$(\exists\alpha \in V_\beta)((\varphi_1^{V_\alpha})^{V_\beta}, \ldots, (\varphi_n^{V_\alpha})^{V_\beta}).$$

Per l'assolutezza dell'associazione $\alpha \mapsto V_\alpha$ rispetto a V_β (e dato che $(\mathbf{Ord})^{V_\beta} = \mathbf{Ord} \cap V_\beta$ come dimostreremo più avanti) ciò vale se e solo se

$$(\exists\alpha < \beta)(\varphi_1^{V_\alpha}, \ldots, \varphi_n^{V_\alpha}).$$

Ma questo contraddice la supposta minimalità di β.

□

CAPITOLO 13

Nozioni Assolute

1. Sinossi

Dimostriamo alcuni risultati basilari di assolutezza e caratterizziamo le relativizzazioni di alcune operazioni fondamentali rispetto a modelli transitivi di ZF. In altre parole rispondiamo alla domanda: quali oggetti e quali operazioni sono le stesse se viste in $\mathbf{V}$ o in qualunque modello transitivo di ZF? Che forma hanno l'insieme potenza, gli ordinali, le classi V_α, in arbitrarie classi transitive modelli di ZF?

2. Formule Limitate

Cominciamo con un risultato semplice ma generale. Diciamo che una formula insiemistica è *limitata* se contiene soltanto quantificatori limitati. Un quantificatore è limitato se è della forma $\forall x \in y$ o $\exists x \in y$ [1] La variabile vincolata da un quantificatore limitato varia all'interno di un insieme, e non su tutto l'universo.

Dimostriamo che tutte le formule transitive sono assolute per classi transitive. Il motivo è semplice: se consideriamo la relativizzazione di una formula limitata, e.g., $\forall x \in y\varphi$, a una classe $\mathbf{M}$, stiamo scegliendo $y \in \mathbf{M}$. Ma se $\mathbf{M}$ è transitiva e $x \in y$ anche x è in $\mathbf{M}$ e non dobbiamo guardare fuori da $\mathbf{M}$ per verificare la validità della formula che stiamo considerando.

PROPOSIZIONE 2.1. *Tutte le formule limitate sono assolute per classi transitive.*

DIMOSTRAZIONE. Se la formula è atomica non c'è niente da dimostrare. Se sono assolute φ e ψ, è facile vedere che sono assolute anche le combinazioni proposizionali $\neg\varphi$, $\varphi \wedge \psi$, etc. (per come è definita la relativizzazione). L'unico caso interessante è quello di una formula esistenziale. Sia φ di forma $(\exists y \in x)\psi(x, y)$ e sia $\psi(x, y)$ assoluta. Sia $a \in \mathbf{M}$.

$$\begin{aligned}
\mathbf{M} \models \varphi(a) &\Rightarrow \mathbf{M} \models (\exists y)(y \in a \wedge \psi) \text{ (per definizione di } \varphi) \\
&\Rightarrow \mathbf{V} \models (\exists y \in \mathbf{M})(y \in a \wedge \psi^{\mathbf{M}}) \text{ (per definizione di } \mathbf{M} \models) \\
&\Rightarrow \mathbf{V} \models (\exists y \in \mathbf{M})(y \in a \wedge \psi) \text{ (per ipotesi induttiva)} \\
&\Rightarrow \mathbf{V} \models \varphi(a)
\end{aligned}$$

D'altra parte:

[1] Notare che i quantificatori limitati non fanno parte del linguaggio: sono abbreviazioni. Una formula $\forall x \in y\varphi$ abbrevia $\forall x(x \in y \to \varphi)$, e una formula $\exists x \in y\varphi$ abbrevia $\exists x(x \in y \wedge \varphi)$.

$$\begin{aligned}\mathbf{V} \models \varphi(a) &\Rightarrow \mathbf{V} \models (\exists y \in \mathbf{M})(y \in a \wedge \psi) \text{ (per definizione di } \varphi) \\ &\Rightarrow \mathbf{V} \models (\exists y \in \mathbf{M})(y \in a \wedge \psi^{\mathbf{M}}) \text{ (per ipotesi induttiva)} \\ &\Rightarrow \mathbf{M} \models \varphi(a) \text{ (per definizione di } \mathbf{M} \models)\end{aligned}$$

Dunque, per $a \in \mathbf{M}$,

$$\mathbf{V} \models \varphi(a) \Leftrightarrow \mathbf{M} \models \varphi(a).$$

□

3. Alcune nozioni assolute

Dal risultato precedente otteniamo facilmente l'assolutezza di un buon numero di nozioni insiemistiche. Da ora in poi consideriamo soltanto classi transitive $\mathbf{M}$ e, per i fini della nostra trattazione, possiamo anche limitarci a considerare classi transitive che soddisfano gli assiomi di ZF. Formuleremo una serie di risultati di assolutezza di formule, relazioni e operazioni, che sono validi rispetto a qualunque classe transitiva $\mathbf{M}$ tale che $\mathbf{M}\varphi\varphi$ per ogni assioma φ di ZF. In verità, come sarà osservato di volta in volta, molte delle nozioni che dimostreremo essere assolute sono assolute rispetto a qualunque classe transitiva $\mathbf{M}$ che soddisfa una sottoteoria di ZF, per esempio ZF meno l'Assioma delle Parti.

Corollario 3.1 (Nozioni Assolute, I). *Le seguenti relazioni e operazioni sono assolute per classi transitive che soddisfano* ZF *meno l'Assioma delle Parti, di Fondazione e di Infinito.*

- $x \in y$
- $\langle x, y\rangle$
- $S(x)$
- $x = y$
- $\varnothing$
- x *è transitivo*
- $x \subseteq y$
- $x \cup y$
- $\{x, y\}$
- $x \cap y$
- $\{x\}$
- $x - y$
- $\cap x$.

Dimostrazione. La dimostrazione consiste nell'indicare, caso per caso, una formula limitata che definisce il concetto, la relazione o l'operazione. Da notare che nel caso delle operazioni occorre sempre verificare che la formula in questione definisce una operazione (funzione) all'interno di $\mathbf{M}$. Per questo è necessario sapere che $\mathbf{M}$ soddisfa un certo numero di assiomi di ZF! Dimostriamo solo alcuni casi. Il resto è per Esercizio. Per ogni nozione troviamo una formula definitoria limitata.

$$z = \{x, y\} \Leftrightarrow [x \in z \wedge y \in z \wedge \forall w \in z(w = x \vee w = y)]$$
$$z = \varnothing \Leftrightarrow \forall w \in z(w \neq w)$$
$$z = S(x) \Leftrightarrow [x \in z \wedge x \subseteq z \wedge \forall w \in z(w = x \vee w \in x)]$$
$$z = \bigcup x \Leftrightarrow [\forall w \in x(w \subseteq z) \wedge \forall v \in z \exists w \in x(v \in w)]$$

□

COROLLARIO 3.2 (Nozioni Assolute, II). *Le seguenti relazioni e operazioni sono assolute per classi transitive che soddisfano* ZF *meno l'Assioma delle Parti, di Fondazione e di Infinito.*

- *z è una coppia ordinata*
- *$x \times y$ (prodotto cartesiano)*
- *R è una relazione (insieme di coppie ordinate)*
- *$dom(R)$ (dominio di una relazione)*
- *$cod(R)$ (codominio di una relazione)*
- *R è una funzione (relazione funzionale)*
- *$R(x)$*
- *R è iniettiva.*

DIMOSTRAZIONE. Diamo definizioni con formule limitate, usando liberamente nozioni che abbiamo già dimostrato essere assolute.

$$z \text{ è coppia ordinata } \Leftrightarrow \exists x \in \bigcup z \exists y \in \bigcup z(z = \langle x, y\rangle).$$

$$z = x \times y \Leftrightarrow \forall w \in x \forall v \in y(\langle w, v\rangle \in z \wedge \forall u \in z \exists w \in x \exists v \in y(u = (x, y))).$$

$$R \text{ è iniettiva } \Leftrightarrow R \text{ è una funzione } \wedge \forall x \in dom(R) \forall y \in dom(R)(R(x) = R(y) \rightarrow x = y)).$$

□

TEOREMA 3.3.

(1) *Sia* $\mathbf{M}$ *una classe transitiva che soddisfa* ZF *meno gli assiomi di Fondazione, Potenza e Infinit. Se* $\omega \in \mathbf{M}$*, allora* $\mathbf{M}$ *soddisfa l'Assioma di Infinito.*
(2) *V_ω non soddisfa l'Assioma di Infinito.*

DIMOSTRAZIONE. (1) La relativizzazione dell'Assioma dell'Infinito ad $\mathbf{M}$ è la formula seguente.

$$\exists x \in \mathbf{M}(\varnothing^{\mathbf{M}} \in x \wedge \forall y \in x(S^{\mathbf{M}}(y) \in x)).$$

Dato che $\varnothing$ e S sono assolute per $\mathbf{M}$, questo equivale a quanto segue.

$$\exists x \in \mathbf{M}(\varnothing \in x \wedge \forall y \in x(S(y) \in x)).$$

Ovviamente ω soddisfa l'enunciato precedente.

(2) Se un insieme soddisfa le condizioni dell'Assioma di Infinito, ossia contiene $\varnothing$ ed è chiuso sotto successore, allora ha rango infinito (cfr. proprietà del rango). Ma ogni insieme in V_ω ha rango finito. □

COROLLARIO 3.4 (Nozioni Assolute, III). *Le seguenti relazioni e operazioni sono assolute per classi transitive che soddisfano* ZF *meno l'Assioma delle Parti.*

- *x è un ordinale*
- *x è un ordinale limite*
- *x è un ordinale successore*
- *x è un ordinale finito*
- *ω*
- *tutti gli ordinali finiti.*

DIMOSTRAZIONE. Osserviamo che in presenza dell'Assioma di Fondazione (ma non in sua assenza), la nozione di ordinale si semplifica da *insieme transitivo e bene ordinato da* $\in$ in *insieme transitivo e totalmente ordinato da* $\in$ (dato che $\in$ è ben fondata su ogni insieme se vale la Fondazione). Abbiamo già visto che "x è transitivo" è una nozione assoluta. La totalità dell'ordine indotto da $\in$ su x si può esprimere con la seguente formula limitata

$$(\forall y \in x)(\forall z \in x)(y \in z \vee z \in y \vee y = z)$$

x è un ordinale limite se x è un ordinale e se non ha massimo rispetto a $\in$, ossia se $\forall y \in x \exists z \in x(y \in z)$.

Per l'assolutezza di ω, osserviamo che

$$x \in \omega \Leftrightarrow x \text{ è ordinale limite e ogni } y \in x \text{ è successore.}$$

□

Consideriamo ora i buoni ordinamenti. Se R è un buon ordinamento di A all'interno di una classe transitiva, lo è anche nell'universo?

LEMMA 3.5 (Assolutezza dei Buoni Ordini). *La nozione "essere un buon ordinamento di un insieme" è assoluta per classi transitive che soddisfano* ZF *meno l'Assioma delle Parti.*

DIMOSTRAZIONE. Supponiamo che la formula che esprime il fatto che R bene ordina A sia vera in $\mathbf{M}$. Sappiamo che ZF dimostra il Teorema seguente (perché lo abbiamo dimostrato noi stessi in ZF!):

> Un insieme è bene ordinato se e solo se è isomorfo a un ordinale.

Dunque, dato che $\mathbf{M}$ soddisfa ZF, l'enunciato che esprime il suddetto teorema applicato al buon ordinamento (A, R) è vero anche relativamente a $\mathbf{M}$. Possiamo scriverlo così, con ovvie abbreviazioni:

$$(\exists f, \alpha \in \mathbf{M})[\alpha \text{ è ordinale } \wedge f \text{ è isomorfismo tra } (A, R) \text{ e } \alpha)^{\mathbf{M}}.$$

Le nozioni "α è un ordinale" e "f è un isomorfismo" sono assolute rispetto a $\mathbf{M}$ e per tanto α è *veramente* un ordinale e f è *veramente* un isomorfismo tra α e (A, R). Allora R è veramente un buon ordinamento di A!

Nell'altra direzione, supponiamo che R sia un buon ordinamento di A, dal punto di vista del modello ambiente. Il fatto che R è un ordine totale su A vale anche relativizzato a $\mathbf{M}$, come si verifica facilmente guardando la definizione di ordine totale. Resta da controllare la relativizzazione a $\mathbf{M}$ della proprietà:

> Per ogni sottinsieme X non vuoto di A esiste un $y \in X$ tale che non esiste uno $z \in X$ più piccolo di y rispetto a R.

Ma si vede bene che questa proprietà - chiamiamola $\varphi(A, X, R)$ - è assoluta per $\mathbf{M}$ (si esprime con una formula limitata). Dato che R è un buon ordinamento di A, $\varphi(A, X, R)$ vale per ogni $X \in \mathbf{M}$, e per assolutezza vale $\varphi(A, X, R)^{\mathbf{M}}$. Dunque R bene ordina A anche dal punto di vista di $\mathbf{M}$. □

OSSERVAZIONE 3.6. Nel Lemma precedente la seconda implicazione: "Se R bene ordina A in $\mathbf{V}$, allora R bene ordina A in $\mathbf{M}$" vale anche se $\mathbf{M}$ non soddisfa l'Assioma delle Parti, di Fondazione e di Infinito. Invece per la prima implicazione serve che $\mathbf{M}$ soddisfi almeno l'Assioma delle Parti, perché questo serve a dimostrare l'equivalenza tra "essere un buon ordinamento di un insieme" e "essere isomorfo a un ordinale".

Vediamo ora che buona parte dell'aritmetica ordinale è assoluta.

COROLLARIO 3.7 (Nozioni Assolute, IV)). *Le seguenti operazioni sono assolute per classi transitive che soddisfano* ZF *meno Assioma delle Parti.*

- $\alpha \mapsto \alpha + 1$
- $\alpha, \beta \mapsto \alpha + \beta$
- $\alpha, \beta \mapsto \alpha \cdot \beta$
- $\alpha, \beta \mapsto \alpha^\beta$
- $x \mapsto rank(x)$.

DIMOSTRAZIONE. Omettiamo la dimostrazione, che si basa sul fatto seguente: le operazioni definite per ricorsione transfinita partendo da nozioni assolute sono anch'esse assolute. Sappiamo già che le operazioni qui sopra si definiscono agevolmente per ricorsione transfinita. □

4. Alcune nozioni non assolute

Passiamo ora a osservazioni riguardo operazioni e insiemi definiti che non sono assoluti.Tra queste un posto di riguardo ha la potenza, ossia l'operazione

$$x \mapsto \mathcal{P}(x).$$

Se $\mathbf{M}$ non soddisfa l'Assioma delle Parti, allora $\mathcal{P}^{\mathbf{M}}$ non è definito e non ha senso interrogarsi sull'assolutezza dell'operazione di potenza. Se $\mathbf{M}$ soddisfa l'Assioma delle Parti, allora l'operazione è definita ma in generale non è assoluta. Come dimostrato nel seguente Lemma, in classi transitive $\mathbf{M}$ che sono modelli di ZF, l'insieme potenza di un insieme coincide con l'intersezione tra il vero insieme potenza e la classe $\mathbf{M}$. Ossia l'insieme delle parti di un insieme $x \in \mathbf{M}$ dal punto di vista di $\mathbf{M}$ è l'insieme di tutti i sottinsiemi di x *che sono in* $\mathbf{M}$.

LEMMA 4.1. *Sia* $\mathbf{M}$ *una classe transitiva modello di* ZF. *Allora, per* $x \in \mathbf{M}$,

$$\mathcal{P}(x)^{\mathbf{M}} = \mathcal{P}(x) \cap \mathbf{M}.$$

DIMOSTRAZIONE. Ricordiamo $\mathcal{P}(x)^{\mathbf{M}}$ denota l'insieme definito in $\mathbf{M}$ dalla relativizzazione a $\mathbf{M}$ della formula che definisce l'insieme potenza. Ossia

$$y \in \mathcal{P}(x)^{\mathbf{M}} \Leftrightarrow (y \subseteq x)^{\mathbf{M}}.$$

Per assolutezza di $\subseteq$ abbiamo

$$\begin{aligned} a \in \mathbf{M} \wedge a \subseteq x &\Rightarrow (a \subseteq x)^{\mathbf{M}} \\ &\Rightarrow a \in \mathcal{P}(x)^{\mathbf{M}} \\ &\Rightarrow \mathcal{P}(x)^{\mathbf{M}} \supseteq \mathcal{P}(x) \cap \mathbf{M}. \end{aligned}$$

Per l'inclusione inversa supponiamo che $a \in \mathcal{P}(x)^{\mathbf{M}}$. Allora

$$\begin{aligned} \mathbf{M} \models a \in \mathcal{P}(x) &\Rightarrow (a \subseteq x) \\ &\Rightarrow a \in \mathcal{P}(x) \\ &\Rightarrow \mathcal{P}(x)^{\mathbf{M}} \subseteq \mathcal{P}(x) \cap \mathbf{M}. \end{aligned}$$

□

Consideriamo ora un'altra operazione fondamentale, ossia quella che associa a un ordinale α l'α-simo livello della Gerarchia di Von Neumann.

$$\alpha \mapsto V_\alpha.$$

Gli insiemi V_α, come sappiamo, sono definiti per induzione transfinita a partire dall'insieme vuoto, ma le operazioni usate in questa definizione non sono assolute. In particolare, per i livelli indicizzati da un ordinale successore, si usa la potenza per definire il nuovo livello della gerarchia. Se $\mathbf{M}$ non soddisfa l'Assioma della Parti, allora $V_\alpha^{\mathbf{M}}$ non è definito. Diamo qui sotto una caratterizzazione dell'insieme V_α visto in qualunque classe transitiva $\mathbf{M}$ che soddisfa ZF. Come sopra per l'insieme potenza, abbiamo che l'insieme V_α visto in $\mathbf{M}$ è l'intersezione del vero V_α con $\mathbf{M}$.

LEMMA 4.2. *Sia $\mathbf{M}$ una classe transitiva modello di ZF. Allora, per $\alpha \in \mathbf{M}$,*

$$V_\alpha^{\mathbf{M}} = V_\alpha \cap \mathbf{M}.$$

DIMOSTRAZIONE. Ragioniamo per induzione transfinita su α. Per il caso $\alpha = 0$, abbiamo

$$V_\alpha^{\mathbf{M}} = \varnothing^{\mathbf{M}} = \varnothing = V_0 = V_0 \cap \mathbf{M}.$$

Per il caso $\alpha = \beta + 1$ usiamo quanto visto sopra per l'insieme delle parti.

$$V_\alpha^M = \mathcal{P}^{\mathbf{M}}(V_\beta^{\mathbf{M}}) = \mathcal{P}(V_\beta^{\mathbf{M}}) \cap \mathbf{M} = \mathcal{P}(V_\beta) \cap \mathbf{M} = V_\alpha \cap \mathbf{M}.$$

L'identità $\mathcal{P}(V_\beta^{\mathbf{M}}) \cap \mathbf{M} = \mathcal{P}(V_\beta) \cap \mathbf{M}$ vale perché $x \in \mathbf{M} \to x \subseteq \mathbf{M}$ ($\mathbf{M}$ è transitiva).

Per il caso α limite abbiamo

$$\begin{aligned}
V_\alpha^{\mathbf{M}} &= \bigcup{}^{\mathbf{M}}(V_\beta \,:\, \beta < \alpha\}^{\mathbf{M}} \text{ (per definizione)} \\
&= \bigcup{}^{\mathbf{M}}\{V_\beta^{\mathbf{M}} \,:\, \beta < \alpha\} \\
&= \bigcup{}^{\mathbf{M}}\{V_\beta \cap \mathbf{M} \,:\, \beta < \alpha\} \text{ (ipotesi induttiva)} \\
&= \bigcup\{V_\beta \,:\, \beta < \alpha\} \cap \mathbf{M} \text{ ($\cup$ è distributiva su $\cap$)} \\
&= V_\alpha \cap \mathbf{M} \text{ (per definizione di } V_\alpha).
\end{aligned}$$

La seconda riga vale perché il concetto di "funzione con dominio α" è assoluto per $\mathbf{M}$. Dunque la relativizzazione a $\mathbf{M}$ dell'insieme che contiene le immagini V_β della funzione $\beta \mapsto V_\beta$ per $\beta < \alpha$ è uguale all'insieme che contiene le immagini della funzione $\beta \mapsto V_\beta^{\mathbf{M}}$ per $\beta < \alpha$. □

COROLLARIO 4.3. *Sia $\mathbf{M}$ una classe transitiva che soddisfa ZF. Allora*

1. *$\mathbf{M}$ contiene tutti gli ordinali ed è una classe propria, oppure*
2. *esiste un minimo ordinale μ non in $\mathbf{M}$ e $\mathbf{M}$ è un insieme incluso in V_μ, e gli ordinali in $\mathbf{M}$ sono tutti e soli gli ordinali minori di μ.*

DIMOSTRAZIONE. Supponiamo che $\mathbf{M}$ non contiene tutti gli ordinali. Dato che $\mathbf{M}$ è definibile, e che **Ord** è bene ordinata, ZF dimostra che esiste un minimo ordinale μ non in $\mathbf{M}$. Dato che $\mathbf{M}$ è transitiva, non esiste $\beta > \alpha$ tale che $\beta \in \mathbf{M}$ (altrimenti anche $\mu \in \mathbf{M}$). Dunque gli insiemi che sono ordinali dal punto di vista di $\mathbf{M}$ (che coincidono con i veri ordinali che si trovano in $\mathbf{M}$, dato che il concetto di ordinale è assoluto per $\mathbf{M}$) sono gli elementi dell'insieme $\{\alpha \,:\, \alpha < \mu\}$, ossia μ stesso. Per ogni insieme $a \in \mathbf{M}$, il rango di a relativizzato a $\mathbf{M}$ è definito ed è un ordinale in $\mathbf{M}$. Per tanto $a \subseteq V_\mu$, dato che il rango è assoluto per $\mathbf{M}$. Dunque $\mathbf{M} \subseteq V_\mu$, e $\mathbf{M}$ è un insieme. □

CAPITOLO 14

Insiemi Costruibili e Assioma di Scelta

1. Sinossi

Definiamo la classe **L** degli insiemi costruibili e dimostriamo che è un modello di **ZF** e dell'Assioma di Scelta.

2. Sottinsiemi definibili

L'idea chiave degli insiemi costruibili di Gödel è questa: sostituire nella costruzione della Gerarchia di Von Neumann l'operazione di insieme potenza con l'operazione che associa ad un insieme a l'insieme di tutti e soli i sottinsiemi di a *definibili* da una formula insiemistica.

Intuitivamente è naturale dire che, dato un insieme a, un sottinsieme b di a è definito da una formula $\varphi(x, \vec{c})$ se

$$b = \{x \in a \ : \ \mathbf{V} \models \varphi(x, \vec{c})\}.$$

Verrebbe allora naturale definire l'insieme dei sottinsiemi definibili di un insieme a come l'insieme di tutti i sottinsiemi di a che sono definiti - nel senso appena descritto - da una qualche formula insiemistica. In altre parole, come l'insieme di tutti i sottinsiemi di a ottenuti per separazione. Potremmo allora definire la *potenza definibile* di un insieme a come

$$\{b \in \mathcal{P}(a) \ : \ \text{esiste una formula } \varphi(x, \vec{y}), \ \text{esistono } \vec{c}\, (b = \{x \in a \ : \ \mathbf{V} \models \varphi(x, \vec{c})\})\}.$$

Una simile definizione ha due problemi.

(1) Le formule insiemistiche *non sono insiemi* e pertanto non sono oggetti della teoria e non possono rientrare direttamente in una definizione insiemistica!
(2) La relazione $\mathbf{V} \models$ di soddisfazione nell'universo $\mathbf{V}$ *non è definibile* da una formula insiemistica (Teorema di Tarski applicato al modello dato di **ZF**).

Il primo problema è facilmente aggirabile: analogamente a quanto accade per il caso dell'aritmetica (aritmetizzazione della sintassi), è possibile definire rigorosamente insiemi che rappresentino adeguatamente la sintassi di **ZF**. In particolare si avrà un insieme dei rappresentanti insiemistici delle formule. Il secondo problema non si può aggirare! Siamo pertanto condotti a indebolire la definizione e a considerare una relazione di soddisfazione ristretta abbastanza da essere definibile nella teoria. Invece di considerare la relazione di soddisfacibilità nell'universo $\mathbf{V}$ (ossia nell'intero modello), consideriamo la soddisfacibilità nel modello costituito dall'*insieme* a, ossia nella struttura $(a, \in)$. Definiamo dunque la *potenza definibile* di a come segue.

$$D(a) = \{b \in \mathcal{P}(a) \ : \ \text{esiste una formula } \varphi(x, \vec{y}) \exists \vec{c} \in a (b = \{x \in a \ : \ (a, \in) \models \varphi(x, \vec{c})\})\}.$$

Abbiamo ora una definizione insiemistica rigorosa dell'idea di *sottinsieme definibile di un insieme*: i sottinsiemi definibili di un insieme a sono tutti e soli quelli che possiamo ottenere come estensione di una formula con parametri in a e valutata in $(a, \in)$.

3. La gerarchia dei costruibili

Definiamo la gerarchia $\mathbf{L} = \bigcup_{\alpha \in \mathbf{Ord}} L_\alpha$ degli insiemi costruibili in maniera analoga a come abbiamo definito $\mathbf{V} = \bigcup_{\alpha \in \mathbf{Ord}} V_\alpha$, solo sostituendo l'operazione potenza con la potenza definibile. Poniamo

$$L_0 = \varnothing, \quad L_{\alpha+1} = D(L_\alpha), \quad L_\alpha = \bigcup_{\beta<\alpha} L_\beta \text{ (se } \alpha \text{ è limite).}$$

Dimostriamo alcune proprietà fondamentali degli L_α.

LEMMA 3.1. *Per ogni α, L_α è transitivo e se $\beta < \alpha$ allora $L_\beta \subseteq L_\alpha$.*

DIMOSTRAZIONE. La dimostrazione è per induzione transfinita su α. Il caso non banale è il caso successore. Sia $\alpha = \beta + 1$. Per ipotesi induttiva L_β è transitivo e per definizione $L_\beta = D(L_\beta)$. Dunque $L_\beta \subseteq L_\alpha$. Inoltre sappiamo che se un insieme x è transitivo allora anche l'insieme potenza $\mathcal{P}(x)$ è transitivo. Dunque L_α è transitivo perché $L_\alpha = D(L_\beta) \subseteq \mathcal{P}(L_\beta)$. □

LEMMA 3.2. *Per ogni α, $L_\alpha \cap \mathbf{Ord} = \alpha$.*

DIMOSTRAZIONE. La dimostrazione è per induzione transfinita su α. Dimostriamo il caso successore. Sia $\alpha = \beta + 1$. Per ipotesi induttiva $L_\beta \cap \mathbf{Ord} = \beta$. Dimostriamo prima l'inclusione $L_\alpha \cap \mathbf{Ord} \subseteq \alpha$. Se $\gamma \in L_\alpha$ allora per definizione di L_α come $D(L_\beta)$ vale γ è un sottinsieme di L_β e dunque vale $\gamma \subseteq L_\beta$. Dato che per ipotesi induttiva $L_\beta \cap \mathbf{Ord} = \beta$, abbiamo che $\gamma \subseteq \beta$ e perciò $\gamma < \beta + 1 = \alpha$ e per tanto $\gamma \in \alpha$.

Dimostriamo ora l'altra inclusione ossia $\alpha \subseteq L_\alpha \cap \mathbf{Ord}$. Per il Lemma precedente sappiamo che $L_\beta \subseteq L_\alpha$, e sappiamo che per definizione $L_\alpha \subseteq \mathcal{P}(L_\beta)$. Ma per ipotesi induttiva vale $L_\beta \cap \mathbf{Ord} = \beta$. Dunque $\beta \subseteq L_\alpha \cap \mathbf{Ord}$. Resta da dimostrare che $\beta \in L_\alpha$, così avremmo dimostrato che $\beta \cup \{\beta\} \subseteq L_\alpha$. Sappiamo che la formula "x è un ordinale" si può esprimere con una formula limitata e per tanto è assoluta per classi transitive. Abbiamo

$$\beta = L_\beta \cap \mathbf{Ord} = \{x \in L_\beta \ : \ \varphi^{L_\beta}(x)\} = \{x \in L_\beta \ : \ L_\beta \models \varphi(x)\},$$

che testimonia che β è un sottinsieme definibile di L_β, ossia che $\beta \in L_\alpha$. □

Dal Lemma precedente segue che tutti gli ordinali sono in $\mathbf{L}$ e che ciascun ordinale appare in $\mathbf{L}$ allo stesso livello in cui appare in $\mathbf{V}$, ossia, il primo livello in cui appare l'ordinale α in $\mathbf{L}$ è $L_{\alpha+1}$. In altre parole è possibile definire una nozione di *rango* in $\mathbf{L}$, assegnando ad ogni $x \in \mathbf{L}$ il minimo α tale che $x \in \text{Ł}_{\alpha+1}$. Per gli ordinali, il rango in $\mathbf{L}$ coincide con il rango in $\mathbf{V}$, ossia ogni ordinale α appare per la prima volta a livello $\alpha + 1$ (ha rango α) (nota bene: in generale L_α e V_α sono diversi!).

4. L è un modello di ZF

Dimostriamo che la classe **L** degli insiemi costruibili soddisfa tutti gli assiomi di ZF. In base alla definizione che abbiamo dato di soddisfazione in una classe ciò significa che, fissato un modello di ZF, la relativizzazione di tutti gli assiomi di ZF alla classe definibile **L** è soddisfatta nel modello. Per ogni φ assioma di ZF,

$$\mathbf{V} \models \varphi^{\mathbf{L}}.$$

TEOREMA 4.1. *La classe* **L** *soddisfa tutti gli assiomi di* ZF.

DIMOSTRAZIONE. Gli assiomi di Estensionalità e di Fondazione valgono - come abbiamo visto - perché **L** è transitiva.

Dato che **L** è transitiva, la condizione per la validità dell'Assioma di Separazione in **L** è come segue. Per ogni formula $\psi(x, z, \vec{v})$ si deve verificare che, per ogni scelta di $z, \vec{v}$ in **L** l'insieme

$$\{x \in z \ : \ \psi^{\mathbf{L}}(x, z, \vec{v})\} \in \mathbf{L}.$$

Sarà qui essenziale il Teorema di Riflessione applicato alla classe (stratificata) **L** (cfr. l'Osservazione qui sotto): da $\psi^{\mathbf{L}}$ voglio passare a ψ^{L_β} per un β grande abbastanza.

Iniziamo con lo scegliere un α grande abbastanza da soddisfare

$$z, \vec{v} \in L_\alpha.$$

(Esiste perché $z, \vec{v} \in \mathbf{L}$.) Per il Teorema di Riflessione esiste un $\beta > \alpha$ tanto grande che $\psi(x, z, \vec{v})$ è assoluta tra L_β e **L**, ossia tale che, per ogni $x \in L_\beta$, vale $\psi(x, z, \vec{v})^{\mathbf{L}}$ se e solo se vale $\psi(x, z, \vec{v})^{L_\beta}$. Allora si ha

$$\{x \in z \ : \ \psi^{\mathbf{L}}(x, z, \vec{v})\} = \{x \in L_\beta \ : \ x \in z \wedge \psi^{L_\beta}(x, z, \vec{v})\}.$$

La scrittura dell'insieme a destra garantisce che l'insieme in questione è nella potenza definibile di L_β, e dunque in **L**!

La validità degli assiomi di Coppia, Unione, e Potenza si verifica agevolmente (usando le condizioni di validità dei suddetti assiomi in classi transitive).

Per verificare la validità del Rimpiazzamento, occorre verificare che, per ogni formula $\varphi(x, y, z, \vec{w})$ e per qualunque scelta di $z, \vec{w} \in \mathbf{L}$, se

$$(\forall x \in z)(\exists! y \in \mathbf{L})[\varphi^{\mathbf{L}}(x, y, z, \vec{w})],$$

allora vale

$$(\exists t \in \mathbf{L})[\{y \ : \ (\exists x \in z)\varphi^{\mathbf{L}}(x, y, z, \vec{w}))$$

Sia $\alpha = \sup\{rk(y)+1 \ : \ \exists x \in z \varphi^{\mathbf{L}}(x, y, z, \vec{w})\}$. Allora $t = L_\alpha$ verifica la conclusione.

L'Assioma di Infinito vale perché $\omega \in \mathbf{L}$ (sappiamo che $\mathbf{Ord} \subseteq \mathbf{L}$.

□

OSSERVAZIONE 4.2. Benché abbiamo dimostrato il Teorema di Riflessione solo per il caso di **V**, il risultato vale, con la stessa dimostrazione, per qualunque classe stratificata. Una classe **C** è detta stratificata se per ogni α è definito un insieme C_α, $C_\alpha = \bigcup_{\beta<\alpha} C_\beta$ se α è limite, $\mathbf{C} = \bigcup C_\alpha$. Il Teorema di Riflessione assicura allora, dato un numero finito di formule e un ordinale α, l'esistenza di un β tanto grande che le formule sono assolute tra C_β e **C**. Ovviamente **L** è una classe stratificata.

5. Operazioni di Gödel

Si può dare una definizione alternativa e più algebrica dei costruibili. Introduciamo le cosidette *operazioni di Gödel*. Sono semplici operazioni insiemistiche. Otterremo una definizione alternativa di potenza definibile di un insieme come chiusura sotto le operazioni di Gödel. Questa definizione alternativa, oltre ad essere la definizione originale di Gödel, facilita la prova di coerenza relativa dell'Assioma di Scelta e aggira il problema della formalizzazione del concetto di formula nella teoria.

- $F_1 : a, b \mapsto \{a, b\}$
- $F_2 : a, b \mapsto a \times b$
- $F_3 : a, b \mapsto a - b$
- $F_4 : a \mapsto \{(x, x) \ : \ x \in a\}$
- $F_5 : a \mapsto \{(x, y) \ : \ x \in y \wedge x, y \in a\}$
- $F_6 : a \mapsto \{a \ : \ \exists y (x, y) \in a\}$
- $F_7 : a \mapsto \{(x, (z, y)) \ : \ (x, (y, z)) \in a\}$
- $F_8 : a \mapsto \{(y, (x, z)) \ : \ (x, (y, z) \in a\}$
- $F_9 : a \mapsto \{(y, x) \ : \ (x, y) \in a\}$
- $F_{10} : a, b \mapsto a \cap b$

Dato un insieme a, la *chiusura* di a sotto le operazioni di Gödel è il minimo soprainsieme di a che è chiuso rispetto all'applicazione delle operazioni $F_1, \ldots, F_{10}$. Si denota la chiusura di a con $Ch_G(a)$ e la si definisce come $\bigcup W_n(a)$, dove $W_0(a) = a$, e

$$W_{n+1}(a) = W_n(a) \cup \{F_i(u, v) \ : \ u, v \in W_n(a), i\{1, \ldots, 10\}\}.$$

Vale la seguente relazione tra potenza definibile e chiusura sotto operazioni di Gödel.

LEMMA 5.1. *Per ogni a transitivo, vale*

$$D(a) = \mathcal{P}(a) \cap Ch_G(a \cup \{a\}).$$

In particolare vale

$$L_{\alpha+1} = \mathcal{P}(L_\alpha) \cap Ch_G(L_\alpha \cup \{L_\alpha\}),$$

e potremmo dunque definire $\mathbf{L}$ senza parlare di formule, in maniera puramente algebrica.

6. L'Assioma di Scelta in L

Dimostriamo che esiste un buon ordinamento della classe $\mathbf{L}$. Con ciò resta dimostrata la validità dell'Assioma di Scelta nel modello dei costruibili. Ciò equivale a una dimostrazione di coerenza relativa: se esiste un modello di ZF, allora esiste un modello di ZF più l'Assioma di Scelta.

Per induzione definiamo per ogni α un buon ordinameto $<_\alpha$ di L_α. Se $\alpha < \beta$ avremmo che $<_\beta$ è una estensione finale di $<_\alpha$, i.e. $x <_\alpha y \Rightarrow x <_\beta y$ e tutti gli elementi in L_β ma non in L_α sono maggiori rispetto all'ordine $<_\beta$ di tutti gli elementi di L_α (i.e. se $x \in L_\alpha$ e $y \in L_\beta - L_\alpha$ allora $x <_\beta y$).

(Caso Limite) Il caso in cui α è un ordinale limite è facile: per definire $<_\alpha$ prendiamo l'unione degli ordinamenti $<_\beta$ per $\beta < \alpha$. Per ipotesi induttiva tutti i $<_\beta$ sono buoni ordinamenti e non vanno in conflitto gli uni con gli altri perché se $\beta < \beta'$ allora $<'_\beta$ è una estensione finale di $<_\beta$.

(Caso Successore) Questo è il caso delicato. Per definire un buon ordinamento su $L_{\alpha+1}$ ci avvaliamo della descrizione di $L_{\alpha+1}$ come chiusura sotto le operazioni di Gödel, i.e.

$$L_{\alpha+1} = \mathcal{P}(L_\alpha) \cap Ch_G(L_\alpha \cup \{L_\alpha\}) = \mathcal{P}(L_\alpha) = \bigcup_{n=0}^{\infty} W_n(\alpha).$$

Ricordiamo che $W_0(\alpha) = L_\alpha \cup \{\alpha\}$ e che

$$W_{n+1}(\alpha) = \{F_i(x,y) \ : \ x,y \in L_\alpha \cup \{L_\alpha\}, i \in \{1,\dots,10\}\}.$$

Costruiamo il buon ordinamento $<_{\alpha+1}$ come segue (descrizione informale): prima vengono tutti gli elementi di L_α nell'ordine $<_\alpha$ (che supponiamo già definito); come primo elemento più grande di tutti gli elementi di L_α poniamo l'insieme L_α stesso; poi i restanti elementi di $W_1(\alpha)$, poi i restanti elementi di $W_2(\alpha)$, etc. Dobbiamo quindi dire come ordinare gli elementi di $W_{n+1}(\alpha)$. A tal fine usiamo i buoni ordinamenti sui W_n, e il fatto che ogni elemento $x \in W_{n+1}$ che non è già in W_n è ottenuto applicando una delle operazioni di Gödel a elementi di W_n, ossia è di forma $F_i(u,v)$ per $i \in \{1,\dots,10\}$ e $u,v \in W_n$. Definiamo ora, per ogni n, un ordinamento $<^n_{\alpha+1}$ di W_n. Per alleggerire la notazione omettiamo il pedice $\alpha+1$ e scriviamo $<^n$ per $<^n_{\alpha+1}$.

(i) $<^0$ è il buon ordinamento di $L_\alpha \cup \{L_\alpha\}$ che estende $<_\alpha$ ponendo L_α come ultimo elemento.

(ii) $<^{n+1}$ è il buon ordinamento di $W_{n+1}(\alpha)$ definito come segue. Diciamo che $x <^{n+1} y$ se e solo se

(a) x e y sono entrambi in W_n e x è già minore di y come elemento di W_n, ossia vale $x <^n y$, oppure
(b) x è un elemento di W_n mentre y no (y è un elemento di W_{n+1} che non era già in W_n), oppure
(c) x e y non sono in W_n, e allora distinguiamo i tre casi qui sotto. In questo caso x e y sono nuovi elementi di W_{n+1} e per tanto sono il risultato dell'applicazione di una operazione di Gödel a elementi di W_n. Fissiamo $i,j \in \{1,\dots,10\}$ minimi tali che $x = F_i(u,v)$ per qualche $u,v \in W_n$ e $y = F_j(s,t)$ per qualche e $s,t \in W_n$. Poniamo $x <^{n+1} y$ o $y <^{n+1} x$ in base ai *tre casi seguenti.*

  (c1) $i < j$.
  (c2) $i = j$. Sia u il $<^n$-minimo elemento di W_n tale che per qualche $w \in W_n$ vale $x = F_i(u,v)$ e sia s il $<^n$-minimo elemento di W_n tale che per qualche $t \in W_n$ vale $y = F_i(s,t)$. $u <^n s$.
  (c3) $i = j$ e $u = s$ (dove u e s sono scelti come nel caso (c2)). Sia v il $<^n$-minimo in W_n tale che $x = F_i(u,v)$ e sia t il $<^n$-minimo in W_n tale che $y = F_i(u,t)$. $v <_n t$.

Definiamo la relazione binaria $<_{\alpha+1}$ come l'unione delle relazioni $<^n_{\alpha+1}$ ristrette a sottinsiemi di L_α, ossia poniamo

$$<^n_{\alpha+1} = \bigcup_{n=0}^{\infty} \cap(\mathcal{P}(L_\alpha) \times \mathcal{P}(L_\alpha)).$$

Si verifica agevolmente che $<_{\alpha+1}$ è una estensione finale di α e un buon ordinamento di $L_{\alpha+1}$. Per definire il buon ordinamento su tutta la classe $\mathbf{L}$ poniamo infine

$$x < y \Leftrightarrow (\exists \alpha)\ x <_\alpha y.$$

CAPITOLO 15

Insiemi Costruibili e Ipotesi del Continuo

1. Sinossi

Dimostriamo che l'ipotesi generalizzata del continuo è vera in $\mathbf{L}$ e che è dunque coerente relativamente a ZF.

2. GCH

L'Ipotesi Generalizzata del Continuo è l'asserzione che, per ogni cardinale infinito κ, il numero dei sottinsiemi di κ è κ^+. D'altro canto sappiamo che il numero dei sottinsiemi di κ è 2^κ. La GCH si esprime dunque succintamente così

$$(\forall\kappa)(2^\kappa = \kappa^+).$$

Con la notazione degli aleph, si scrive così

$$(\forall\alpha)(2^{\aleph_\alpha} = \aleph_{\alpha+1}).$$

Sia che pensiamo a 2^κ come al numero dei sottinsiemi di κ o come al numero delle funzioni con dominio κ e codominio $\{0,1\}$, abbiamo lo stesso problema: in entrambi i casi non ci sono restrizioni sulla natura della definizione degli oggetti che vogliamo contare (sottinsiemi o funzioni).

3. Schema della Dimostrazione

Nel modello dei costruibili abbiamo un controllo proprio sui sottinsiemi: ad ogni livello ammettiamo soltanto i sottinsiemi definibili da una formula insiemistica (ve ne sono una infinità numerabile) con parametri nel livello precedente. Come vedremo, questo ci darà un controllo sul punto della gerarchia costruibile oltre il quale non appariranno più nuovi sottinsiemi di un dato insieme.

Dato un L_α, consideriamone i sottinsiemi. Dato che $\mathbf{L}$ soddisfa ZF, in particolare $\mathbf{L}$ soddisfa l'Assioma delle Parti, e quindi in $\mathbf{L}$ esiste un insieme X che contiene, dal punto di vista di $\mathbf{L}$, tutti e soli i sottinsiemi di $\mathbf{L}$. Questo X è l'insieme che possiamo denotare anche con $\mathcal{P}(L_\alpha)^{\mathbf{L}}$, e dato che $\mathbf{L}$ è transitivo, sappiamo già che $\mathcal{P}(L_\alpha)^{\mathbf{L}} = \mathcal{P}(L_\alpha)\cap\mathbf{L}$. Questo insieme *non* coincide con la potenza definibile di L_α, che abbiamo denotato $\mathcal{D}(L_\alpha)$: $\mathcal{D}(L_\alpha)$, che coincide per definizione con $L_{\alpha+1}$, contiene i sottinsiemi di L_α *definibili* con parametri in L_α da una formula relativizzata ad L_α; $\mathcal{P}(L_\alpha)^{\mathbf{L}}$ invece contiene tutti e soli i sottinsiemi di L_α *costruibili*, i.e. tutti gli $S \subseteq A$ tali che $\exists\beta$ tale che $S \in L_\beta$. Questi ultimi possono essere molti di più degli insiemi in $\mathcal{D}(L_\alpha)$: in altre parole, nuovi sottinsiemi costruibili di L_α possono apparire ben oltre il livello $L_{\alpha+1}$ di $\mathbf{L}$. Vedremo però che è possibile determinare il punto $\alpha' > \alpha$ tale che tutti i sottinsiemi costruibili di L_α appaiono entro il livello α'. In altre parole calcoleremo α' tale che $\mathcal{P}(L_\alpha) \subseteq L_{\alpha'}$. Da questa relazione segue immediatamente che $|\mathcal{P}(L_\alpha)| \leq |L_{\alpha'}|$.

A questo punto dovremmo preoccuparci di due cose: i) di conoscere la relazione tra la grandezza (cardinalità) dell'indice α' e la grandezza (cardinalità) dell'insieme $L_{\alpha'}$, e ii) di trovare un α' ragionevolmente piccolo.

Per la precisione faremo vedere che nel modello dei costruibili per ogni α,

- la cardinalità di L_α è uguale alla cardinalità di α.
- tutti i sottinsiemi di L_α compaiono in L_{α^+}, e

Da questo, dato che per ogni ordinale vale $\alpha \subseteq L_\alpha$, segue immediatamente l'Ipotesi Generalizzata del Continuo segue immediatamente:

$$\mathcal{P}(\kappa) \subseteq \mathcal{P}(L_\kappa) \subseteq L_{\kappa^+}.$$

4. Cardinalità degli L_α

Dimostriamo in dettaglio quanto ci serve sapere sulla cardinalità degli L_α, ossia che è uguale a quella di α. Che la cardinalità degli L_α non sia tanto grande dipende dal fatto che gli L_α sono stati definiti come chiusure sotto un numero finito di operazioni (e la chiusura implica una iterazione numerabile di iterazioni). Da notare che i risultati sulla cardinalità qui sotto usano l'Assioma Di Scelta. Ma questo non è un problema perché già sappiamo che vale in $\mathbf{L}$.

La Proposizione seguente è un Corollario di un risultato di aritmetica cardinale già dimostrato. Ci dice che una unione di κ insiemi ciascuno di cardinalità al massimo κ ha cardinalità al massimo κ. È un risultato semplice ma lo useremo tante volte in modo essenziale in quel che segue.

PROPOSIZIONE 4.1. *Sia κ un cardinale infinito. Sia $(X_\alpha)_{\alpha<\kappa}$ una famiglia di insiemi ciascuno di cardinalità $\leq \kappa$. Allora $|\bigcup_{\alpha<\kappa} X_\alpha| \leq \kappa$. In altre parole, se una unione di κ insiemi ha cardinalità maggiore di κ, almeno un insieme ha cardinalità maggiore di κ.*

In quel che segue, in diversi casi, ci servirà avere un controllo sulla cardinalità della chiusura di un insieme sotto funzioni di arietà finita. Dato un insieme A diciamo che una funzione f è una *funzione finita* su A se f è di tipo $A^n \to A$ per qualche numero n. f è una funzione di arietà finita definita su A e con immagine in A. Ammettiamo anche il caso in cui $n = 0$, e in questo caso f è semplicemente una costante (un elemento di A). Se f è una funzione finita su A e $D \subseteq A$, scriviamo fD per denotare l'immagine di f a D, ossia $f(D^n)$, dove n è l'arietà di f, se $n \geq 1$, e $\{f\}$ se $n = 0$ (in questo caso $f \in A$).

Se $\mathcal{F}$ è un insieme di funzioni finite su A, la *chiusura* di A sotto $\mathcal{F}$ si ottiene con una semplice costruzione ricorsiva.

- $C_0 = A$,
- $C_{n+1} = C_n \cup \bigcup_{f\in\mathcal{F}}\{fC_n\}$,
- $C = \bigcup_{n\in\omega} C_n$.

Una semplice applicazione del risultato precedente ci permette di misurare la cardinalità della chiusura C in funzione di quella dell'insieme di partenza A e della cardinalità dell'insieme di funzioni $\mathcal{F}$.

TEOREMA 4.2. *Sia κ un cardinale infinito. Sia $A \subseteq X$, con $|A| \leq \kappa$. Sia $\mathcal{F}$ un insieme di $\leq \kappa$ funzioni finite su X. Allora la chiusura di A sotto $\mathcal{F}$ ha cardinalità $\leq \kappa$.*

DIMOSTRAZIONE. Per ogni $D \subseteq X$, se $|D| \leq \kappa$ allora $|fD| \leq \kappa$. Infatti sappiamo che $|D^n| = |D|$ e ovviamente $|fD| \leq |D|$ perché f è una funzione. Per induzione su n, si ha che ogni insieme C_n nella definizione della chiusura C di B sotto $\mathcal{F}$ ha cardinalità $\leq \kappa$. Allora la chiusura $C = \bigcup_{n\in\omega} C_n$ di B sotto $\mathcal{F}$ è una unione di $\omega \leq \kappa$ insiemi ciascuno di cardinalità $\leq \kappa$. Dunque ha anch'essa cardinalità $\leq \kappa$, per la Proposizione precedente. □

Come prima applicazione dei risultati qui sopra calcoliamo la cardinalità degli L_α. Cominciamo mostrando che la cardinalità della potenza definibile di un insieme infinito è uguale alla cardinalità dell'insieme stesso!

PROPOSIZIONE 4.3 (usa (AC)). *Se $|A| \geq \omega$, allora $|\mathcal{D}(A)| = |A|$.*

DIMOSTRAZIONE. Abbiamo visto che - usando la caratterizzazione della potenza definibile con operazioni di Gödel - $\mathcal{D}(A)$ è uguale a $\mathcal{P}(A) \cap Ch_G(A \cup \{A\})$. La chiusura $Ch_G(A \cup \{A\})$ è definita nel modo naturale come $\bigcup_{n\in\omega} W_n$, dove $W_0 = A \cup \{A\}$, e

$$W_{n+1} = W_n \cup \{F_i(u, v) | u, v \in W_n, i \in \{1, \ldots, 10\}\}.$$

Allora $\mathcal{D}(A)$ è la chiusura di A sotto un insieme finito di funzioni finite su A. Per i risultati precedenti, abbiamo che $|\mathcal{D}(A)| \leq |A|$. Dato che, per ogni $a \in A$, $\{a\}$ è un sottinsieme definibile di A, $\mathcal{D}(A)$ ha almeno $|A|$ elementi, e dunque $|\mathcal{D}(A)| = |A|$. □

Osserviamo che la cardinalità di L_n è finita per ogni n (sappiamo che $L_n \subseteq V_n$). Mostriamo che per α infinito, L_α ha $|\alpha|$ elementi.

PROPOSIZIONE 4.4. *Per ogni $\alpha \geq \omega$, $|L_\alpha| = |\alpha|$.*

DIMOSTRAZIONE. Dato che α è incluso in L_α, si ha $|\alpha| \leq |L_\alpha|$. Dimostriamo l'altro verso per induzione transfinita su α. Supponiamo che per ogni β infinito minore di α valga il risultato. Allora per ogni $\beta < \alpha$ si ha $|L_\beta| \leq |\alpha|$, dato che tutti i L_n sono finiti e α è infinito. Se α è limite, allora $L_\alpha = \bigcup_{\beta<\alpha} L_\beta$ è l'unione di $|\alpha|$ insiemi di cardinalità $\leq |\alpha|$. Dunque ha cardinalità $\leq |\alpha|$ per i risultati precedenti. Dato che $\alpha \subseteq L_\alpha$ (abbiamo dimostrato che in generale $L_\alpha \cap \mathbf{Ord} = \alpha$), vale anche $|\alpha| \leq |L_\alpha|$. Dunque $|L_\alpha| = |\alpha|$. Se $\alpha = \beta + 1$, allora $L_\alpha = \mathcal{D}(L_\beta)$. Dunque $|L_\alpha| = |L_\beta|$ per la Proposizione precedente. Per ipotesi induttiva $|L_\beta| = |\beta|$. Ma dato che $\alpha = \beta + 1$ vale $|\alpha| = |\beta|$ e perciò concludiamo $|L_\alpha| = |\alpha|$. □

5. Assioma di Costruibilità

Nell'argomento per la coerenza relativa dell'Ipotesi del Continuo, vogliamo mostrare che l'Ipotesi del Continuo vale nell'universo degli insiemi costruibili, $\mathbf{L}$. Questo significa che, fissato un qualunque modello di ZF, vale in esso $\mathsf{GCH}^{\mathbf{L}}$. Questo equivale a dimostrare in ZF l'implicazione: "Se tutti gli insiemi sono costruibili, allora l'Ipotesi Generalizzata del Continuo è vera". Si osserva che l'enunciato "Tutti gli insiemi sono costruibili" si può esprimere con una formula insiemistica, dato che gli L_α e la loro unione $\mathbf{L}$ sono definibili in ZF. L'enunciato $\forall x \exists \alpha (x \in L_\alpha)$ viene chiamato Assioma di Costruibilità, e abbreviato con $\mathbf{V} = \mathbf{L}$. Asserisce che l'universo degli insiemi coincide con la Gerarchia dei Costruibili. Dimostrare in un generico modello ambiente di ZF che $\mathbf{L}$ soddisfa GCH *equivale* a dimostrare, in ZF, l'implicazione $(\mathbf{V} = \mathbf{L}) \to \mathsf{GCH}$.

Qual è lo statuto dell'Assioma di Costruibilità rispetto agli assiomi di ZF? Esiste un modello di ZF che soddisfa anche l'Assioma di Costruibilità? Il candidato ideale è il modello interno $\mathbf{L}$. Sappiamo già che è modello di ZF, ed è plausibile che soddisfi l'Assioma di Costruibilità. Osserviamo che quest'ultimo fatto non è tautologico, dato che chiedersi se $\mathbf{L} \models (\mathbf{V} = \mathbf{L})$ equivale a chiedersi se vale (nel modello ambiente) la relativizzazione dell'Assioma di Costruibilità ad $\mathbf{L}$, ossia se vale $(\mathbf{V} = \mathbf{L})^{\mathbf{L}}$, che, per esteso è

$$(\forall x \in \mathbf{L})(\exists \alpha \in \mathbf{Ord}^{\mathbf{L}} \cap \mathbf{L})(x \in L_\alpha^{\mathbf{L}}).$$

$L_\alpha^{\mathbf{L}}$ è l'insieme L_α visto dall'interno della classe $\mathbf{L}$. Se $L_\alpha^{\mathbf{L}}$ fosse il vero L_α, allora di certo avremmo che tutti gli $x \in \mathbf{L}$ sono in qualche $L_\alpha^{\mathbf{L}}$. Vediamo subito che è proprio così: la costruzione di L_α è assoluta per modelli transitivi di ZF.

PROPOSIZIONE 5.1. *La funzione $\alpha \mapsto L_\alpha$ è assoluta per modelli transitivi di* ZF *(anche senza l'Assioma delle Parti).*

DIMOSTRAZIONE. (SCHIZZO). L'assolutezza di $\alpha \mapsto L_\alpha$ segue dall'assolutezza di $a \mapsto \mathcal{D}$ e dall'assolutezza delle definizioni per induzione transfinita sugli ordinali. Per convincersi dell'assolutezza della potenza definibile $\mathcal{D}(a)$ conviene pensare alla sua definizione come chiusura di $a \cup \{a\}$ sotto le operazioni di Gödel $F_1, \ldots, F_{10}$. □

Segue allora che $\mathbf{L}$ è un modello di $(\mathbf{V} = \mathbf{L})$. Questo dimostra la coerenza relativa dell'Assioma di Costruibilità: se ZF è coerente, allora esiste un modello di ZF, sia $(M, \in)$. All'interno di tale modello esiste $\mathbf{L}$, e abbiamo dimostrato che $\mathbf{L}$ soddisfa ZF, l'Assioma di Scelta e l'Assioma di Costruibilità. Dunque esiste un modello di $\mathsf{ZFC} + (\mathbf{V} = \mathbf{L})$ e dunque questa teoria è coerente. Da notare che "$\mathbf{L}$ soddisfa $\mathsf{ZFC} + (\mathbf{V} = \mathbf{L})$" significa che *per ogni assioma* φ di $\mathsf{ZFC} + (\mathbf{V} = \mathbf{L})$, $\mathsf{ZF} \vdash \varphi^{\mathbf{L}}$. (Da tenere sempre presente: l'ipotesi iniziale "se ZF è coerente" è essenziale e indimostrabile in ZF, per il Teorema di Gödel).

Facciamo ora una osservazione generale sulle dimostrazioni di assolutezza. Ogni volta che abbiamo dimostrato che una data formula è assoluta per modelli transitivi di una teoria $T \subseteq \mathsf{ZF}$, abbiamo svolto una dimostrazione in ZF (o in una sottoteoria, tipicamente ZF senza Assioma delle Parti). Una tale dimostrazione usa, come tutte le dimostrazioni, solo *un numero finito di assiomi* di ZF. Per tanto, per ogni nozione che abbiamo dimostrato assoluta, esiste un numero finito di assiomi di ZF che sono sufficienti a dimostrare l'assolutezza di tale nozione. Questo signfica che possiamo dimostrare che se un insieme soddisfa quegli assiomi allora la nozione in questione è assoluta per quell'insieme. Abbiamo uanto segue.

PROPOSIZIONE 5.2. *Per ogni formula φ dimostrata assoluta per modelli transitivi di* ZF *esiste un numero finito di assiomi di* ZF $\varphi_1, \ldots, \varphi_n$ *tale che*

$$\mathsf{ZF} \vdash \forall M(M \text{ transitivo } \wedge \bigwedge_i \varphi_i^M \to (\varphi^M \leftrightarrow \varphi)).$$

È quindi possibile, per esempio, scegliere un numero finito di assiomi sufficiente a dimostrare l'assolutezza della nozione di ordinale per ogni insieme transitivo che li soddisfa, e analogamente per ogni altra nozione assoluta.

Vogliamo ora dire qualcosa sulla struttura di un insieme transitivo che soddisfa la teoria $\mathsf{ZF} + (\mathbf{V} = \mathbf{L})$. Dimostriamo che, se M è un modello transitivo di $\mathsf{ZF} + (\mathbf{V} =$

$\mathbf{L}$) è un insieme, allora è uguale a L_μ, dove μ è il minimo ordinale non in M (μ è anche uguale a $M \cap \mathbf{Ord}$). (Analogamente si può dimostrare che, se è una classe propria, allora è uguale a $\mathbf{L}$). Per la precisione dimostriamo che ogni insieme transitivo che soddisfa un certo insieme finito di assiomi di ZF più l'Assioma di Costruibilità ha la struttura desiderata.

TEOREMA 5.3. *Esiste una congiunzione finita* $\varphi = \bigwedge_{i=1}^{i=n} \varphi_i$ *di assiomi* $\varphi_1, \ldots, \varphi_n$ *di* $\mathsf{ZF} + (\mathbf{V} = \mathbf{L})$ *tale che*

$$\forall M((M \text{ insieme transitivo } \wedge \varphi^M) \rightarrow M = L_\mu),$$

dove μ *è il minimo ordinale* $\notin M$.

DIMOSTRAZIONE. Sia φ una congiunzione di abbastanza assiomi di ZF t.c.

- φ è sufficiente per dimostrare l'assolutezza delle nozioni di ordinale, rango, e dell'operazione $\alpha \rightarrow L_\alpha$ per modelli transitivi,
- φ contiene l'assioma $\mathbf{V} = \mathbf{L}$,
- φ è sufficiente per dimostrare il teorema che dice che non esiste un ordinale massimo: $\forall\alpha\exists\beta(\alpha < \beta)$.

(Si osserva che si può fare a meno dell'Assioma delle Parti in φ). Vediamo com'è la struttura di un insieme transitivo che soddisfa una φ siffatta.

Se M è transitivo e soddisfa φ, allora $(\forall x(x \in \mathbf{L}))^M$ (perché φ contiene l'Assioma di Costruibilità) e dunque $M = \mathbf{L}^M$.

Se M è transitivo e soddisfa φ^M, allora μ è un ordinale limite (perché φ dimostra che non esiste un massimo ordinale). Dunque, per la definizione della Gerarchia dei Costruibili,

$$L_\mu = \bigcup_{\alpha \in M} L_\alpha.$$

Ma per assolutezza di L_α si ha

$$\mathbf{L}^M = \{x \in M \text{ t.c. } (\exists\alpha(x \in L_\alpha))^M\} = \bigcup_{\alpha \in M} L_\alpha.$$

Dunque

$$L_\mu = \mathbf{L}^M.$$

□

6. Riflessione raffinata

Si può raffinare la dimostrazione del Teorema di Riflessione in modo tale da mantenere un controllo sulla cardinalità sull'insieme di riflessione (l'insieme rispetto al quale le formule scelte sono assolute). In particolare si possono ottenere insiemi di riflessioni numerabili. Se però si desidera che l'insieme di riflessione contenga un certo insieme X fissato in anticipo come base, ciò che si può garantire è che la cardinalità dell'insieme di riflessione resta sotto al massimo tra la cardinalità di X e ω.

Occorre fare una premessa. Per la prima dimostrazione del Teorema di Riflessione abbiamo usato il Criterio di Vaught-Tarski, che mette in relazione l'assolutezza di formule tra una classe $\mathbf{M}$ e l'universo con la possibilità di trovare in $\mathbf{M}$ testimoni esistenziali per formule con parametri in $\mathbf{M}$, qualora un testimone esista in $\mathbf{V}$. Si può definire una nozione più generale di assolutezza.

DEFINIZIONE 6.1 (Assolutezza, estesa). Date due classi $\mathbf{M}$ e $\mathbf{N}$, tali che $\mathbf{M} \subseteq \mathbf{N}$, diciamo che una formula $\varphi(x_1, \ldots, x_s)$ è *assoluta tra* $\mathbf{M}$ e $\mathbf{N}$ se, per ogni $m_1, \ldots, m_s \in \mathbf{M}$ vale

$$\varphi^{\mathbf{M}}(m_1, \ldots, m_s) \leftrightarrow \varphi^{\mathbf{N}}(m_1, \ldots, m_s).$$

In altre parole: per parametri in $\mathbf{M}$ la verità di φ relativamente ad $\mathbf{M}$ e a $\mathbf{N}$ non varia. Si osserva facilmente che la nozione di assolutezza usata finora è il caso particolare in cui $\mathbf{N}$ è la classe propria universale $\mathbf{V}$. Con un argomento identico a quello usato per $\mathbf{N} = \mathbf{V}$, si dimostra il seguente criterio di Tarski-Vaught.

PROPOSIZIONE 6.2 (Criterio di Tarski-Vaught, esteso). *Siano $\mathbf{M}$ e $\mathbf{N}$ classi definibili con $\mathbf{M} \subseteq \mathbf{N}$. Sia $\varphi_1, \ldots, \varphi_n$ un insieme di formule (chiuso per sottoformula). Sono allora equivalenti i seguenti punti.*

1. *$\varphi_1, \ldots, \varphi_n$ sono assolute tra $\mathbf{M}$ e $\mathbf{N}$,*
2. *Per ogni φ_i di forma $\exists x_j \varphi_j(x, y_1, \ldots, y_\ell)$, per ogni $m_1, \ldots, m_\ell \in \mathbf{M}$, se $\exists n \in \mathbf{N}$ tale che $\varphi_j^{\mathbf{N}}(n, m_1, \ldots, m_\ell)$ allora $\exists m \in \mathbf{M}$ tale che $\varphi_j^{\mathbf{M}}(m, m_1, \ldots, m_\ell)$.*

Faremo uso di questo criterio nella dimostrazione della versione raffinata del Teorema di Riflessione. Nel nostro caso $\mathbf{M}$ e $\mathbf{N}$ saranno insiemi.

TEOREMA 6.3 (Riflessione raffinata, 1). *Siano $\varphi_1, \ldots, \varphi_n$ formule. Allora per ogni X esiste un soprainsieme $A \supseteq X$ tale che $\varphi_1, \ldots, \varphi_n$ sono assolute per A e*

$$|A| \leq \max(\omega, |X|).$$

DIMOSTRAZIONE. Sia α grande abbastanza tale che $X \subseteq V_\alpha$. Per il Teorema di Riflessione semplice esiste $\beta > \alpha$ tale che $\varphi_1, \ldots, \varphi_n$ sono assolute per V_β. Troveremo un insieme A che soddisfa il nostro Teorema come sottinsieme di V_β.

Per l'Assioma di Scelta, V_β è bene ordinabile. Sia $\prec$ un buon ordinamento di V_β.

Ad ogni formula esistenziale φ_i associamo una funzione S_i che trova il testimone esistenziale della formula in V_β, se gli altri parametri sono scelti in V_β. S_i è detta una funzione di Skolem per φ_i. Per uniformità, definiamo S_i anche se φ_i non è una formula esistenziale. Sia ℓ_i il numero delle variabili libere in φ_i. Definiamo una funzione di tipo

$$S_i : V_\beta^{\ell_i} \to V_\beta$$

associata a φ_i.

Se φ_i è una formula esistenziale $\exists x \varphi_j(x, y_1, \ldots, y_{\ell_i})$ e, per una scelta di $a_1, \ldots, a_{\ell_i}$ parametri in V_β esiste un testimone $a \in V_\beta$ che soddisfa

$$\varphi_j^{V_\beta}(a, a_1, \ldots, a_{\ell_i}),$$

sia $S(a_1, \ldots, a_{\ell_i})$ il minimo tale a (rispetto al buon ordinamento $\prec$).

Altrimenti, se φ_i non è esistenziale, o se è esistenziale ma non c'è testimone in V_β per la verità di $\exists x \varphi_j(x, a_1, \ldots, a_{\ell_i})$, sia $S_i(a_1, \ldots, a_{\ell_i})$ il minimo di V_β (rispetto al buon ordinamento $\prec$). Se φ_i non ha variabili libere (ossia $\ell_i = 0$), identifichiamo S_i con un qualunque elemento di V_β.

Per il Teorema di Tarski-Vaught esteso, se un insieme A è chiuso sotto tutte le funzioni S_i, allora tutte le φ_i sono assolute tra A e V_β. Dato che V_β è tale che tutte le φ_i sono assolute per V_β (ossia tra V_β e l'universo $\mathbf{V}$), segue che se un insieme A è chiuso sotto tutte le funzioni S_i, allora le φ_i sono assolute per A! Se esiste in $\mathbf{V}$ un testimone esistenziale di una φ_i con parametri in $A \subseteq V_\beta$ allora esiste già in V_β

e se esiste in V_β allora esiste già in A. Definiamo allora A come la chiusura di X sotto $S_1, \ldots, S_n$.

La cardinalità di questa chiusura è al più $\max(\omega, |X|)$, per i risultati della sezione precedente. □

Si osserva che l'insieme A costruito nel Teorema precedente non può essere uno dei V_β e non può essere transitivo, in generale. Il motivo è che l'operazione di insieme potenza non può essere assoluta per un modello transitivo e numerabile. In quanto segue abbiamo però bisogno di ottenere un punto di riflessione transitivo e con cardinalità non troppo grande. Vedremo come è possibile ottenere un tale insieme, se ci limitiamo all'assolutezza di enunciati (formule chiuse) e non di formule in generale (ciò esclude il problema della potenza, che come operazione è definita da una formula con una variabile libera).

7. Collasso di Mostowski

Diamo una formulazione debole contiene solo quello che ci serve. Diciamo che la relazione di appartenenza è *estensionale* su un insieme A se vale l'Assioma di Estensionalità ristretto ad A, ossia se vale

$$(\forall a, b \in A)(\forall c \in A(c \in a \leftrightarrow c \in b) \rightarrow a = b).$$

Due insiemi A e M si dicono $\in$-isomorfi se esiste una mappa iniettiva $G : A \rightarrow M$ tale che

$$(\forall a, b \in A)(a \in b \leftrightarrow G(a) \in G(b)).$$

Una tale G è detta un $\in$-isomorfismo, ossia una isomorfismo rispetto alla relazione d'appartenenza.

Teorema 7.1. *Se A è estensionale, allora è $\in$-isomorfo ad un insieme transitivo.*

Dimostrazione. Definiamo G su A come segue.

$$G(a) = \{G(b) \text{ t.c. } b \in A \wedge b \in a\}.$$

L'immagine di A sotto G viene detto il *collasso di Mostowski* di A. Dimostriamo che G è un $\in$-isomorfismo.

Dimostriamo prima che G è iniettiva. Se supponiamo che non lo sia, possiamo scegliere il controesempio a minimale rispetto a $\in$ (qui usiamo l'Assioma di Fondazione). a è l'elemento minimale che soddisfa

$$a \in A \wedge \exists b \in A(a \neq b \wedge G(a) = G(b)).$$

Sia $b \in A$ tale che $(a \neq b \wedge G(a) = G(b))$. Dato che vale l'Estensionalità, o esiste un $c \in A$ che sta in a ma non in b, o viceversa. Sia $c \in A$ tale che $c \in a$ ma $c \notin b$. Allora $G(c) \in G(a)$. Ma $G(a) = G(b)$ e dunque esiste $d \in A$ tale che $d \in b$ e $G(d) = G(c)$. Ma allora deve valere $c \neq d$, perché $c \notin b$. Ma allora abbiamo contradetto la minimalità di a perché abbiamo trovato un elemento più piccolo $(c \in a)$ con la stessa proprietà! Il caso in cui esiste un $c \in A$ tale che $c \notin a$ ma $c \in b$ è simmetrico.

Segue che G è un $\in$-isomorfismo.

□

8. Un'altra Riflessione

Torniamo al Teorema di Riflessione con controllo della cardinalità. Vogliamo applicare il collasso di Mostowski per ottenere un punto di riflessione transitivo. Da osservare che ci limitiamo qui alla riflessione di enunciati (formule chiuse) e non formule in generale.

PROPOSIZIONE 8.1 (Riflessione raffinata, 2). *Siano $\varphi_1, \ldots, \varphi_n$ enunciati. Allora per ogni X transitivo esiste un soprainsieme $M \supseteq X$ transitivo tale che $\varphi_1, \ldots, \varphi_n$ sono assolute per M e*

$$|M| \leq \max(\omega, |X|).$$

DIMOSTRAZIONE. Assumiamo senza pregiudizio della generalità che φ_n sia l'Assioma di Estensionalità (altrimenti lo aggiungiamo alla lista). Sia A l'insieme costruito con l'argomento per il Teorema di Riflessione raffinata. Possiamo applicare il Teorema di Mostowski ad A e ottenere un insieme transitivo M $\in$-isomorfo ad A. M è l'immagine di A sotto il collasso di Mostowski G. Occorre verificare che $X \subseteq M$. Per $x \in X$ abbiamo

$$G(x) = \{G(y) \text{ t.c. } y \in A \wedge y \in x\} = \{G(y) \text{ t.c. } y \in x\},$$

perché X è transitivo e $X \subseteq A$: se $y \in x \in X$ allora anche $y \in X$ e dunque $y \in A$. Allora l'isomorfismo G non muove X, ossia

$$(\forall x \in X)(G(x) = x).$$

□

9. Conclusione

Mettiamo insieme tutti gli ingredienti.

TEOREMA 9.1. *Se $\mathbf{V} = \mathbf{L}$, allora per ogni α infinito vale*

$$\mathcal{P}(L_\alpha) \subseteq L_{\alpha^+}.$$

DIMOSTRAZIONE. Sia φ come nella Proposizione 5.3. φ è tale da garantirci che ogni M transitivo che soddisfa φ è uguale a L_μ, dove μ è il minimo ordinale non in M.

Sia $A \in \mathcal{P}(L_\alpha)$. Sia $X = \{A\} \cup L_\alpha$. Nota che $|X| = |L_\alpha| = |\alpha|$. Per il Teorema di Riflessione raffinato, esiste un insieme transitivo M tale che

$$X \subseteq M, |M| = |\alpha|, \varphi^M \leftrightarrow \varphi^{\mathbf{V}}.$$

Dato che stiamo lavorando sotto l'ipotesi ($\mathbf{V} = \mathbf{L}$), e φ contiene ($\mathbf{V} = \mathbf{L}$) più qualche assioma di ZF, φ è vero nel nostro modello. Dunque vale φ^M. Dunque, per la scelta di φ, abbiamo $M = L_\mu$. Dato che $|M| = |\alpha|$, abbiamo che il minimo ordinale non in M non può essere maggiore del primo cardinale dopo α, ossia di α^+. Dunque $|\mu| < \alpha^+$ Per tanto,

$$A \in X \subseteq M = L_\mu \to A \in L_{\alpha^+}.$$

□

COROLLARIO 9.2. $\mathsf{GCH}^{\mathbf{L}}$, *e* $\mathsf{ZF} \vdash (\mathbf{V} = \mathbf{L}) \to \mathsf{GCH}$.

DIMOSTRAZIONE. Se $\mathbf{V} = \mathbf{L}$, abbiamo dimostrato che, per ogni cardinale κ infinito,

$$\mathcal{P}(\kappa) \subseteq \mathcal{P}(L_\kappa) \subseteq L_{\kappa^+}.$$

Questo implica

$$2^\kappa \leq |L_{\kappa^+}| = \kappa^+.$$

□