# Elementi di Teoria degli Insiemi, 2012-13

Alessandro Berarducci

20 Maggio 2013 (ultime modifiche: 5 Luglio)

## Indice

# 1 Introduzione

La teoria degli insiemi nasce con Georg Cantor (i primi articoli risalgono al 1874) ed è stata successivamente assiomatizzata da Ernst Zermelo (1904, 1908), con successive integrazioni e sviluppi da parte di Fraenkel, Skolem, von Neumann ed altri matematici. Essa può essere vista come uno dei tanti settori della matematica, con i suoi risultati specifici sui numeri ordinali e cardinali, ma la sua importanza risiede soprattutto nel fatto che gli insiemi forniscono un fondamento per l'intera matematica. Tutti i concetti matematici possono infatti essere interpretati in termini insiemistici e, ciò fatto, qualunque dimostrazione matematica può essere formalizzata, almeno in linea di principio, entro la teoria assiomatica degli insiemi. Si può non essere d'accordo con questa impostazione, ma è bene sapere che essa è stata resa possibile da una serie di lavori che, a partire dalla rifondazione del calcolo infinitesimale ad opera di Weierstrass, Cantor e Dedekind, hanno gradualmente condotto ad una nuova concezione sui fondamenti della matematica che ancora non è stata superata.

Esistono tre principali assiomatizzazioni della teoria degli insiemi, che sono però strettamente imparentate: la teoria di Zermelo-Fraenkel (ZF), la teoria di Gödel-Bernays (GB) (anche detta teoria NBG di von Neumann, Bernays e Gödel), e la teoria di Morse-Kelley (MK). Delle tre, quella privilegiata in questo testo è GB, che trovo più efficace di ZF da un punto di vista didattico. Le differenze tra i diversi approcci riguardano sostanzialmente il modo in cui viene affrontano il problema della distinzione tra insiemi e classi e lo status che viene attribuito alle classi. Mentre in ZF possiamo parlare di classi solo ricorrendo a circonlocuzioni (in quanto il suo linguaggio non ha variabili su classi), in GB e in MK esse sono entità teoriche a pieno titolo. A titolo di esempio, il fatto che la classe dei numeri ordinali non sia un insieme, che è dimostrabile in questi termini in GB, può essere formulato in ZF solo ricorrendo alla perifrasi "non

esiste un insieme che contiene come elementi tutti gli ordinali". [1] Le differenze tra ZF e GB sono in ogni caso più formali che sostanziali: se ci si limita alle affermazioni che coinvolgono solo gli insiemi e non le classi, ZF e GB dimostrano esattamente le stesse cose. [2]

Il nostro scopo è quello di fornire un'esposizione motivata ed intuitiva, ma al tempo stesso precisa e succinta (obiettivi non facilmente conciliabili), della teoria assiomatica degli insiemi GB, presentandone i risultati fondamentali sui numeri ordinali e cardinali, e facendo vedere come gli oggetti basilari della matematica possano essere ricostruiti in termini insiemistici (relazioni, funzioni, numeri naturali, numeri reali, eccetera).

Un ruolo fondamentale lo giocherà l'induzione transfinita e il teorema di ricursione, che esporrò prima in forma semplice (definizioni ricorsive sui numeri naturali) e poi in forma sempre più generale, fino ad arrivare al teorema di ricursione per relazioni ben fondate. La ricursione transfinita su numeri ordinali ne sarà un caso particolare. In questo percorso metterò in evidenza il ruolo dei vari assiomi, tra cui l'assioma della scelta, di cui dimostreremo l'equivalenza con il lemma di Zorn.

I numeri cardinali verranno prima presentati nella versione di Frege, come classi di equivalenza rispetto alle bigezioni (cosa che può essere fatta in GB ma non in ZF), e solo successivamente, quando ne nascerà l'esigenza, come ordinali iniziali. Mentre per dimostrare i primi risultati (ad esempio il fatto che i numeri reali non sono numerabili) sarà sufficiente la versione di Frege, per alri risultati si renderanno necessari gli ordinali iniziali. Identificare i cardinali con gli ordinali iniziali permette in particolare di mostrare che non esiste alcuna successione decrescente infinita di cardinali. Da ciò segue che esiste un più piccolo cardinale tra quelli non numerabili, che però non sappiamo se coincida con la cardinalità dei reali: si tratta della cosiddetta "ipotesi del continuo", per la cui discussione rimandiamo a testi più avanzati come il "Set Theory" di Thomas Jech.

Una precisazione metodologica: ho cercato di presentare GB come teoria assiomatica nel senso euclideo o pre-hilbertiano del termine, ovvero ponendomi nell'ottica che i suoi assiomi corrispondano ad affermazioni contenutistiche su una supposta "realtà" degli insiemi. Tuttavia chi abbia un minimo di familiarità con la logica matematica non avrà difficoltà a rileggere GB come teoria formale del primo ordine. La scelta della doppia lettura mi è sembrata il miglior compromesso in considerazione dell'annosa questione se la logica preceda la teoria degli insiemi o viceversa: la semantica delle teorie del primo ordine si basa sugli insiemi, ma la teoria degli insiemi è essa stessa una teoria del primo ordine (e come tale è suscettibile di una pluralità di interpretazioni). Per realizzare il compromesso ho fatto precedere alla presentazione di GB dei brevi capitoli sulle notazioni logiche (connettivi e quantificatori), dandone una semantica intuitiva basata su esempi tratti dal linguaggio naturale. Ritengo che questa scelta, non presupponendo conoscenze antecedenti di logica, sia quella che permette la più ampia flessibilità nell'utilizzo del testo.

[1] Ciò è fattibile in quanto la proprietà "$x$ è un ordinale" è esprimibile in ZF, sebbene a tale proprietà non venga fatta corrispondere una classe.

[2] La teoria MK è invece strettamente più potente.

Se questa impostazione mi soddisfa a livello didattico, a livello teorico rimane il problema di come uscire dalla circolarità sopra evidenziata. Una possibilità, suggerita dalle riflessioni di Hilbert, è quella del "bootstrapping", ben familiare a chi si occupa del problema di come faccia un computer ad avviare i suoi programmi se per avviare un programma serve un altro programma. Fuori di metafora: serve solo una minima parte di GB per definire la sintassi a la semantica dei linguaggi del primo ordine. Questa minima parte può essere assunta in modo contenutistico, e poi se lo si desidera si è liberi di pensare al resto di GB in modo formale. Per limiti di tempo devo però lasciare lo sviluppo di queste considerazioni ad altra sede.

Ho scritto questo testo pensando in primo luogo ai miei studenti dei corsi di Logica e Teoria degli Insiemi presso il Dipartimento di Matematica dell'Università di Pisa, ma nello scriverlo ho cercato anche di intrattenere un dialogo ideale con alcuni colleghi e amici. Spero quindi che esso possa essere letto a vari livelli e apprezzato anche da chi si avvicini da autodidatta, o da semplice curioso, alla materia.

## 2 Paradosso dell'iperalbero

Una delle "scoperte" fondamentali della teoria degli insiemi è che non tutti gli insiemi sono sullo stesso livello, ma occorre distinguere almeno due livelli: insiemi e classi. Come vedremo gli insiemi sono quelle classi che possono appartenere ad altre classi. Se non si fanno distinzioni si incorre in vari paradossi, tra cui il cosiddetto "paradosso dell'iperalbero", che presento in questa sezione come piccolo antipasto alla teoria. A differenza di altri paradossi più noti (tra cui il paradosso di Russell che vedremo in seguito) esso ha un carattere "geometrico" o "visivo" che rende la sua paradossalità ancora più sorprendente. Se provvisti di sufficiente intuizione matematica, letteralmente non si crede ai propri occhi.

Immaginate un albero genealogico. C'è il capostipite, i suoi figli, i figli dei figli, e così via. Astraendo un po' si arriva alla seguente definizione.

**2.1 Definizione.** Un albero è un insieme di oggetti, chiamati nodi dell'albero, su cui è definita una relazione padre-figlio (o la corrispondente versione al femminile) che gode della seguente proprietà. Ogni nodo, tranne la radice, ha uno e un solo padre. La radice non ha padre. Ogni nodo ha zero o più figli. I nodi con zero figli si chiamano foglie dell'albero. È ammessa la possibilità che un nodo abbia infiniti figli. I discendenti di un nodo $x$ sono quelli che si ottengono a partire da lui tramite un cammino finito, ovvero una successione finita di nodi che parte da $x$ e in cui ogni nodo è figlio del precedente. Richiediamo, nella definizione di albero, che ogni nodo sia un discendente della radice (il capostipite).

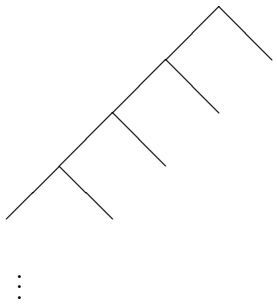
**2.2 Definizione.** Un albero è ben fondato se non ha cammini infiniti.

Dunque in un albero ben fondato un oggetto prezioso che passi di generazione in generazione dal padre ad uno dei figli, prima o poi rimarrebbe senza legittimo proprietario per mancanza di eredi. Osserviamo che le generazioni potrebbero

non esaurirsi mai, senza che con ciò esista un cammino infinito. Ad esempio la radice potrebbe avere infiniti figli, e ciascuno dei suoi figli potrebbe avere una discendenza finita, che però si estingue a scadenze sempre più lunghe a seconda del figlio, senza quindi che l'intera discendenza della radice si estingua mai.

**2.3 Proposizione.** *Se un albero contiene una copia di se stesso come sottoalbero, allora non è ben fondato.*

*Dimostrazione.* Partendo dalla radice dell'albero mi sposto sulla radice della sua copia, e da lì itero il procedimento, ovvero mi sposto sempre verso il sottoalbero che è copia di quello da cui sono partito, producendo in tal modo un cammino infinito. □



Un albero che ha una copia di se stesso come sottoalbero.

**2.4 Definizione.** L'iperalbero è definito nel modo seguente. Consideriamo la classe $C$ di tutti gli alberi ben fondati (o, per meglio dire, un rappresentante per ogni classe di isomorfimo di tali alberi). Consideriamo un nuovo nodo $r$ e stabiliamo che i figli di $r$ siano le radici degli alberi della classe $C$. Otteniamo in questo modo un nuovo albero, la cui radice è $r$, e che contiene come sottoalberi gli alberi di C. Ogni albero ben fondato ha dunque una copia tra i sottoalberi dell'iperalbero.

**2.5 Paradosso.** Ci chiediamo se l'iperalbero sia ben fondato. Poichè ogni cammino nell'iperalbero va a finire, dopo un passo, in uno dei suoi sottoalberi (che sono ben fondati), ne segue che l'iperalbero è ben fondato. Ma essendo tale, una copia dell'iperalbero deve comparire come uno dei sottoalberi di se stesso. Tuttavia un albero che contiene una copia di se stesso come sottoalbero non può essere ben fondato (Proposizione 2.3), il che è una paradosso.

Nella teoria assiomatica degli insiemi il paradosso si "risolve" per mezzo di una distinzione tra insiemi e classi che impedisce la possibilità di costruire l'iperalbero all'interno della teoria. Un problema molto simile lo troveremo quando considereremo la classe di tutti i numeri ordinali, che in qualche modo è un "iperordinale", ovvero sta agli ordinali come l'iperalbero sta agli alberi ben fondati. Parlando a livello informale il problema si pone in questi termini: i numeri ordinali servono per contare gli insiemi (sia finiti che infiniti), e la

domanda è se possano essi stessi essere contati. Come vedremo ciò equivale a chiedersi se la classe ON di tutti gli ordinali sia essa stessa un ordinale. Se non si distinguesse tra insiemi e classi si incorrerebbe nel paradosso di Burali-Forti, secondo il quale la classe ON degli ordinali è effettivamente un ordinale, e l'assurdo sta nel fatto che, se ON fosse un ordinale, sarebbe l'ordinale più grande di tutti, che però non può esistere in quanto posso sempre aggiungere uno. La soluzione proposta dalla teoria assiomatica degli insiemi è che, sebbene la classe ON abbia quasi tutte le proprietà richieste per essere un ordinale, gliene manca una: non è un insieme. Si tratta, se vogliamo, di una soluzione burocratica: si pongono degli assiomi che impediscono (almeno si spera) la costruzione di entità paradossali. Si tratta però anche di una soluzione pragmatica: si riesce fortunatamente a far ciò senza al contempo impedire la costruzione di tutte quelle entità che servono ai matematici.

# 3 Connettivi logici

Assumiamo la concezione "classica" secondo cui una proposizione è o vera o falsa (principio del terzo escluso), ma non può essere sia vera che falsa (principio di non contraddizione). Diremo che una proposizione $P$ ha il *valore di verità* **1** se essa è vera, e il *valore di verità* **0** se essa è falsa. Un predicato è una proposizione che dipende da alcuni parametri, come ad esempio "$x > 3$, che è vero o falso a seconda di chi sia $x$. Useremo spesso dei nomi simbolici come $P, Q, \ldots$ per denotare generiche proposizioni e predicati. Per evidenziare la eventuale dipendenza da un parametro $x$ scriveremo anche $P(x), Q(x)$ eccetera. Ad esempio "$P(x)$" potrebbe essere il predicato "$x > 3$". Se ci sono più parametri useremo notazioni come $P(x, y)$ o simili. Ad esempio "$P(x, y)$" potrebbe essere "$x > y$".

I connettivi servono per costruire proposizioni e predicati complessi a partire da proposizioni e predicati più semplici. I connettivi di cui faremo maggiore uso sono indicati con i simboli $\neg, \wedge, \vee, \to, \leftrightarrow$ (oltre ai quantificatori che tratteremo più tardi). La loro traduzione approssimativa in italiano è la seguente:

"$\neg A$" significa "non $A$" (negazione),
"$A \wedge B$" significa "$A$ e $B$" (congiunzione),
"$A \vee B$" significa "$A$ o $B$" (disgiunzione),
"$A \to B$" significa "se $A$, allora $B$" (implicazione),
"$A \leftrightarrow B$" significa "$A$ se e solo se $B$" (doppia implicazione).

Le seguenti *tavole di verità* precisano il significato dei connettivi secondo la logica classica. Iniziamo con la tavola delle negazione:

| $A$ | $\neg A$ |
|---|---|
| **0** | **1** |
| **1** | **0** |

La tavola dice che la proposizione $\neg A$ è vera se $A$ è falsa, ed è invece falsa se $A$ è vera. La negazione inverte il valore di verità. Diamo ora le tavole degli altri connettivi.

| $A$ | $B$ | $A \wedge B$ | $A \vee B$ | $A \to B$ | $A \leftrightarrow B$ |
|---|---|---|---|---|---|
| **0** | **0** | **0** | **0** | **1** | **1** |
| **0** | **1** | **0** | **1** | **1** | **0** |
| **1** | **0** | **0** | **1** | **0** | **0** |
| **1** | **1** | **1** | **1** | **1** | **1** |

Le prime due colonne indicano i quattro possibili valori di verità di $A$ e $B$. Le altre colonne indicano i corrispondenti valori degli enunciati composti $A \wedge B$, $A \vee B$, $A \to B$, $A \leftrightarrow B$.

Le tavole della congiunzione e della disgiunzione non richiedono particolari commenti, salvo forse osservare che la disgiunzione è intesa in senso inclusivo, ovvero affinché $A \vee B$ sia vera basta che una tra $A$ e $B$ sia vera, incluso il caso in cui lo sono entrambe.

Più delicato è il caso dell'implicazione. Dalle tavole risulta che l'implicazione $A \to B$ è falsa solo nel caso in cui la premessa $A$ è vera e il conseguente $B$ è falso. In particolare se la premessa $A$ è falsa, l'implicazione $A \to B$ è vera. Ad esempio l'implicazione "$x$ è pari $\to$ il quadrato di $x$ è pari", è vera per ogni numero intero $x$ (anche per gli $x$ dispari!).

Per dimostrare una implicazione $A \to B$ si può assumere "in via ipotetica" che $A$ sia vera, e cercare di dimostrare $B$ (notando che se $A$ fosse invece falsa l'implicazione sarebbe comunque vera in base alle tavole). Se si riesce a dimostrare $B$ all'interno della dimostrazione subordinata in cui $A$ è assunta vera, si può a quel punto "scaricare l'ipotesi $A$" (ovvero uscire dalla dimostrazione subordinata) e concludere che $A \to B$ è vera. La validità di questo metodo argomentativo è giustificata dalle tavole.

Dai discorsi appena fatti si capisce che una dimostrazione matematica non ha sempre una struttura lineare, ma ha in generale una struttura annidata contenente al suo interno dimostrazioni subordinate (anche a più livelli), ciascuna delle quali inizia con l'introduzione di ulteriori ipotesi che poi vengono scaricate quando si torna alla dimostrazione principale (o a quella di livello immediatamente superiore). Occorre pertanto sempre fare attenzione a quali sono le ipotesi in vigore in ciascun momento della dimostrazione.

# 4 Quantificatori

I quantificatori sono speciali connettivi che hanno il ruolo di esprimere quanti oggetti verificano un dato predicato (da cui il nome "quantificatori"). Ad esempio, supponendo che il dominio del discorso siano i cittadini con diritto di voto, possiamo applicare il quantificatore "per la maggioranza degli $x$" al predicato "$x$ vota il partito del progresso " ottenendo la proposizione "(per la maggioranza degli $x$)($x$ vota il partito del progresso)", o più semplicemente "la maggioranza vota il partito del progresso".

Useremo il termine "proprietà" come sinonimo di "predicato", riferendolo però principalmente a predicati ad un solo argomento (in sequito incontreremo predicati a più argomenti).

I quantificatori di cui faremo maggior uso sono $\forall x$ (per ogni $x$) ed $\exists x$ (esiste almeno un $x$). Dato un predicato $P$, la proposizione

$$\exists x P(x)$$

esprime il fatto che esiste almeno un oggetto $a$ nel dominio del discorso che verifica il predicato, ovvero tale che valga $P(a)$. La proposizione

$$\forall x P(x)$$

dice che per tutti gli oggetti $a$ nel dominio del discorso vale $P(a)$.

Se abbiamo un predicato di due argomenti, ovvero della forma $Q(x, y)$, la proposizione

$$\exists x\, Q(x, y),$$

sarà vera o falsa a seconda di chi sia $y$. Ad esempio se $y =$ Maria, la proposizione $\exists x(x$ è figlio di $y)$, sarà vera o falsa a seconda che Maria abbia effettivamente un figlio.

Le variabili "legate", ovvero quelle che cadono sotto l'effetto di un quantificatore, possono essere ridenominate senza alterare il significato dell'enunciato. Ad esempio $\exists x P(x)$ significa la stessa cosa di $\exists y P(y)$, ovvero che esiste un oggetto del dominio del discorso verificano $P$. Se considero un predicato $Q$ di due argomenti, e scrivo $\exists x\, Q(x, y)$, posso ridenominare la $x$ (perché è legata) ma non la $y$, che è invece "libera", ovvero non legata. Se scrivo "$\exists x(x$ è figlia di $y)$", sto affermando che la persona $y$ ha una figlia (osserviamo che la "$x$" non compare affatto in questa parafrasi), che è la stessa cosa che dire "$\exists z(z$ è figlia di $y)$", mentre è diverso dal dire "$\exists x(x$ è figlia di $w)$", che esprime invece il fatto che è $w$ (anziché $y$) ad avere una figlia. Come si vede da questi esempi, le variabili libere si comportano come "nomi", mentre quelle legate sono espedienti linguistici che, pur non avendo un significato proprio, giocano il ruolo di segnaposto, ovvero fanno capire a quale parte del predicato si riferisce il quantificatore.

Per predicati a più argomenti possiamo avere diverse combinazioni di $\forall$ e $\exists$ ed è importante tenere conto dell'ordine in cui si alternano i quantificatori. Ad esempio

$$\forall x \exists y P(x, y)$$

significa che, dato un $x$, posso sempre trovare un $y$, che in genere dipenderà da $x$, tale che $P(x, y)$. Se invece scrivo

$$\exists y \forall x P(x, y)$$

sto dicendo che esiste un $y$ che va bene per tutti gli $x$, ovvero un $y$ tale che, per ogni $x$, vale $P(x, y)$. In particolare, se il dominio delle variabili è un insieme di persone, e $P(x, y)$ è il predicato "$y$ è uno dei genitori di $x$", allora $\forall x \exists y P(x, y)$ dice che ogni persona ha un genitore, mentre $\exists y \forall x P(x, y)$ dice che esiste una persona $y$ che è genitore di tutti (inclusa se stessa).

Sin dall'antichità sono state studiate le leggi che regolano il comportamento dei quantificatori in combinazione con i connettivi $\neg, \wedge, \vee, \rightarrow$. Aristotele ne

aveva enucleate alcune (i sillogismi). Per una lista completa (frutto dei lavori di Frege e dei suoi successori) rimandiamo a qualunque testo di logica che tratti del calcolo dei predicati. Vale tuttavia la pena ricordare almeno il comportamento dei quantificatori $\forall$ ed $\exists$ rispetto alla negazione. Secondo le regole della logica classica $\neg\forall x P(x)$ equivale a $\exists x \neg P(x)$ ("non è vero che tutti gli $x$ verificano $P$" equivale a "esiste almeno un $x$ che non verifica $P$"). Similmente $\neg\exists x P(x)$ equivale a $\forall x \neg P(x)$. Siccome le doppie negazioni si elidono, si ottiene anche che $\forall x P(x)$ equivale a $\neg\exists x \neg P(x)$ ("tutti gli $x$ verificano $P$" è la stessa cosa di "non esiste alcun $x$ che non verifichi $P$"). Dualmente, $\exists x P(x)$ equivale a $\neg\forall x \neg P(x)$.

Ricordiamo infine le regole più significative che riguardano i quantificatori $\exists$ e $\forall$ presi isolatamente. Mentre per dimostrare un enunciato della forma $\exists x P(x)$ basta trovare un oggetto $a$ che verifica il predicato $P$ (come quando dimostriamo che esiste un numero primo maggiore di 99 dando 101 come esempio), più problematico è il caso del $\forall x P(x)$, in quanto nella maggior parte dei casi non è possibile passare in rassegna tutti i possibili $x$ e provarli uno per uno. Si usa allora il seguente trucco, che richiede di comprendere bene la distinzione tra nomi e cose denotate. Se dico «Alessandro va al cinema» mi riferisco alla persona, ma se dico «"Alessandro" ha quattro sillabe», mi riferisco al nome della persona. Ovviamente non posso parlare di qualcosa se non nominandola, e se voglio parlare di un nome devo usare il nome del nome, ovvero mettere il nome tra virgolette. Ora per dimostrare $\forall x P(x)$ basta riuscire a dimostrare $P(a)$ senza fare ipotesi su $a$, ovvero senza sapere di quale oggetto "a" sia il nome. Supponiamo ad esempio che, dato un predicato $Q(x)$, io voglia dimostrare $\forall x(Q(x) \vee \neg Q(x))$. A tal fine mi basta dimostrare $Q(a) \vee \neg Q(a)$ senza sapere chi sia $a$. Questo è facile in quanto, pur non sapendo se $Q(a)$ sia vero o falso (in quanto non conosco $a$), in base alle tavole del $\neg$ posso sicuramente dire che se $Q(a)$ è falso $\neg Q(a)$ è vero e viceversa, e quindi in ogni caso $Q(a) \vee \neg Q(a)$ è vero in base alle tavole del $\vee$. In qualche caso dovrò basarmi su proposizioni precedentemente dimostrare o assunte come assioma. Se ad esempio voglio dimostrare che dato un numero reale $a$, il suo quadrato $a^2$ è maggiore o uguale a zero, non mi serve sapere quale numero sia $a$, ma mi basta distinguere tre casi a seconda che $a$ sia positivo negativo o zero, e ricordare che positivo per positivo è positivo, e negativo per negativo è ancora positivo.

# 5 Oggetti e classi nel linguaggio di tutti i giorni

Fissato un "universo del discorso" e una proprietà $P(x)$, possiamo considerare la classe degli oggetti $a$, nell'universo del discorso, per cui vale $P(a)$. Tale classe è indicata con la notazione "$\{x : P(x)\}$". Ad esempio, se sto parlando di persone (ovvero se le mie variabili variano su persone), la classe degli insegnanti è indicata con la notazione "$\{x : x$ è un insegnante$\}$". Nella notazione $\{x : P(x)\}$ la "$x$" si comporta come una variabile legata e pertanto può essere ridenominata: $\{x : P(x)\}$ è la stessa cosa di $\{y : P(y)\}$. In generale la $P$ potrebbe contenere dei parametri, ovvero $P(x)$ potrebbe essere della forma $Q(x, a)$. In tal caso la

classe $\{x : Q(x, a)\}$ dipenderà da $a$. Ad esempio $\{x : x$ è amico di $a\}$ è la classe degli amici di $a$, che dipende ovviamente da chi è $a$.

In generale sciviamo "$a \in X$" per esprimere il fatto che l'oggetto $a$ appartiene alla classe $X$. Quindi anzichè dire "$a$ è un insegnante", possiamo dire "$a \in \{x : x$ è un insegnante$\}$", ovvero "$a$ appartiene alla classe degli insegnanti".

Assumeremo per le classi il seguente assioma:

**5.1 Assioma** (Assioma di estensionalità)**.** Due classi sono uguali se hanno gli stessi elementi.

In base all'assioma di estensionalità, se $P$ e $Q$ sono due proprietà sotto cui cadono gli stessi oggetti, le corrispondenti classi sono uguali. Se per puro caso nel nostro universo del discorso gli oggetti tondi fossero esattamente quelli blu, allora in base all'assioma di estensionalità la classe degli oggetti tondi coinciderebbe con la classe degli oggetti blu, sebbene la proprietà "$x$ è tondo" non coincida con la proprietà "$x$ è blu".

**5.2 Definizione.** Date due classi $X$ ed $Y$ diciamo che $X$ è inclusa in $Y$ (o che $X$ è una sottoclasse di $Y$) se ogni elemento di $X$ è un elemento di $Y$, ovvero

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

Scriviamo

$$X \subseteq Y$$

per esprimere il fatto che $X$ è inclusa in $Y$. Ciò equivale a dire che non vi sono elementi di $X$ che non appartengono ad $Y$.

**5.3 Osservazione.** In base all'assioma di estensionalità, $X = Y$ se e solo se $X \subseteq Y$ e $Y \subseteq X$.

Date due proprietà $P$ e $Q$, dire che vale l'inclusione $\{x : P(x)\} \subseteq \{x : Q(x)\}$ equivale a dire che, per ogni oggetto $x$, vale l'implicazione $P(x) \to Q(x)$. L'uguaglianza $\{x : P(x)\} = \{x : Q(x)\}$ corrisponde invece alla doppia implicazione $\forall x(P(x) \leftrightarrow Q(x))$.

**5.4 Definizione.** Scriveremo $X \subset Y$ (inclusione stretta) se vale l'inclusione $X \subseteq Y$ ma $X$ non è uguale ad $Y$.

# 6 L'algebra di Boole delle classi

Fissiamo una classe di oggetti $V$ come universo del discorso. Dire $a \in V$ equivale a dire che $a$ è un oggetto del nostro universo del discorso. Tutte le classi sono sottoclassi di $V$, ovvero sono incluse nella classe universale $V$.

Dato un oggetto $x \in V$ ed una classe $X \subseteq V$, scriviamo $x \notin X$ come abbreviazione per $\neg(x \in X)$. La classe complementare

$$X^{\complement} = \{x : x \notin X\}$$

è definita come la classe degli oggetti, nell'universo del discorso $V$, che non appartengono ad $X$. Più in generale date due classi $X$ ed $Y$ possiamo formare la loro differenza

$$Y \setminus X = \{x : x \in Y \wedge x \notin X\}$$

e osservare che

$$X^{\complement} = V \setminus X.$$

Possiamo inoltre considerare l'unione

$$X \cup Y = \{x : x \in X \vee x \in Y\}$$

delle due classi, definita come la classe i cui elementi sono gli oggetti che appartengono ad $X$ o ad $Y$ (senza escludere che appartengano ad entrambi), e la loro intersezione

$$X \cap Y = \{x : x \in X \wedge x \in Y\}$$

i cui elementi sono gli oggetti che appartengono sia ad $X$ che ad $Y$. Se $X$ ed $Y$ non hanno elementi in comune la loro intersezione $X \cap Y$ è la classe vuota. Essa può essere definita come la classe definita da un qualunque predicato contraddittorio. Ad esempio se $P(x)$ è il predicato $x \neq x$ allora la classe $\{x : P(x)\}$ è vuota, ovvero non ha elementi.

**6.1 Proposizione.** *Una classe vuota $X$ è inclusa in qualsiasi altra classe $Y$.*

*Dimostrazione.* In base alla definizione di inclusione tra classi, occorre dimostrare che, per ogni oggetto $a$, vale l'implicazione $a \in X \to a \in Y$. Tale implicazione è sempre vera (in base alle tavole di verità) in quanto la sua premessa "$a \in X$" è sempre falsa (essendo $X$ vuota).

Detto in altri termini, se $X$ non fosse inclusa in $Y$, ci dovrebbe essere un elemento che appartiene ad $X$ ma non ad $Y$, ma questo è assurdo in quanto nessun elemento appartiene ad $X$. □

Ne segue che due classi vuote sono incluse l'una nell'altra e pertanto sono uguali in base all'assioma di estensionalità. Esiste dunque un'unica classe vuota.

**6.2 Definizione.** La classe vuota $\emptyset$ è l'unica classe che non ha elementi. Essa può essere definita da un qualsiasi predicato contraddittorio. Abbiamo dunque $\emptyset = \{x : x \neq x\}$.

Data una classe qualsiasi $X$, valgono le inclusioni $\emptyset \subseteq X$ e $X \subseteq V$. In altre parole ogni classe include la classe vuota ed è inclusa nella classe universale $V$.

**6.3 Proposizione.** *Valgono le seguenti identità (esprimenti il fatto che le classi formano una "algebra di Boole"):*

1. *(leggi commutative)*
   (a) $X \cup Y = Y \cup X$,
   (b) $X \cap Y = Y \cap X$.
2. *(leggi associative)*

   (a) $(X \cap Y) \cap Z = X \cap (Y \cap Z)$,
   (b) $(X \cup Y) \cup Z = X \cup (Y \cup Z)$.
3. *(leggi distributive)*
   (a) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$,
   (b) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$.
4. *(identità)*
   (a) $X \cup \emptyset = X$,
   (b) $X \cap V = X$.
5. *(complemento)*
   (a) $X \cup X^{\complement} = V$,
   (b) $X \cap X^{\complement} = \emptyset$.

*Dimostrazione.* (Cenno) Visto che $\wedge, \vee, \complement$, sono definiti facendo ricorso ai connettivi logici $\wedge, \vee, \neg$, occorre far ricorso alle corrispondenti proprietà di questi ultimi. Consideriamo ad esempio la legge distributiva

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z).$$

Per dimostrarla si fissi un generico oggetto $x$ e si considerino le proposizioni $P, Q, R$ così definite: $P$ è la proposizione "$x \in X$", come $Q$ prendiamo "$x \in Y$", e come $R$ prendiamo "$x \in Z$". In base alle definizioni di $\cup$ e $\cap$, la proposizione

$$x \in X \cup (Y \cap Z)$$

equivale a

$$x \in X \vee (x \in Y \wedge x \in Z),$$

ovvero alla proposizione

$$P \vee (Q \wedge R).$$

Quest'ultima, in base alle tavole di verità dei connettivi logici, equivale a

$$(P \vee Q) \wedge (P \vee R),$$

come si può facilmente verificare assegnando a $P, Q, R$ i valori "vero" o "falso" negli otto modi possibili, e controllando che le due proposizioni composte risultano in ciascun caso entrambe vere o entrambe false in base alle tavole. Espandendo le definizioni di $P, Q, R$ otteniamo

$$(x \in X \vee x \in Y) \wedge (x \in X \vee x \in Z),$$

che a sua volta equivale a

$$x \in X \cup (Y \cap Z).$$

Abbiamo così dimostrato che $x \in X \cup (Y \cap Z)$ se e solo se $x \in (X \cup Y) \cap (X \cup Z)$, e visto che questo vale per ogni possibile oggetto $x$, ne segue per estensionalità che $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$. □

Nella sezione sui quantificatori abbiamo detto che le variabili libere sono "nomi" di oggetti, ma questa è in effetti una ipersemplificazione. In certi casi esse sono nomi di "oggetti ipotetici", come si vede nel seguente esercizio.

**6.4 Esercizio.** Data una classe $X$, si dimostri che $X \subseteq X^{\complement} \to X = \emptyset$.

*Dimostrazione.* Basta dimostrare $X = \emptyset$ assumendo $X \subseteq X^{\complement}$. Assumiamo dunque $X \subseteq X^{\complement}$. Se per assurdo $X \neq \emptyset$, allora $\exists x(x \in X)$, ovvero $X$ contiene almeno un oggetto[3]. Consideriamo un tale ipotetico oggetto e chiamiamolo "$a$" [4]. Dunque $a \in X$. Ma essendo $X \subseteq X^{\complement}$ abbiamo $\forall x(x \in X \to x \in X^{\complement})$. Questo deve valere per ogni $x$ e dunque anche per $a$. Dunque $a \in X \to a \in X^{\complement}$ [5]. Siccome stiamo assumendo che la premessa $a \in X$ sia vera, anche la conclusione $a \in X^{\complement}$ deve essere vera in base alla tavola di verità del $\to$. Dunque $a$ appartiene sia ad $X$ che al suo complemento $X^{\complement}$. Questo è assurdo per la definizione di $X^{\complement}$. Abbiamo dunque concluso la dimostrazione, ma riflettiamo: di quale oggetto "$a$" può essere il nome visto che in definitiva abbiamo dimostrato che $X$ è vuoto? □

# 7 Quantificatori limitati

Introduciamo i quantificatori limitati "$\exists a \in X$" e "$\forall a \in X$" (dove $X$ è una classe) nel modo seguente. Dato un predicato $P(x)$, conveniamo che "$(\exists a \in X)P(a)$" sia un'abbreviazione per "$\exists a(a \in X \wedge P(a))$", che possiamo leggere come "esiste $a$ appartenente ad $X$ tale che $P(a)$". Ciò equivale a dire che la classe $X$ interseca la classe $\{a : P(a)\}$, ovvero $X \cap \{a : P(a)\} \neq \emptyset$.

Dualmente definiamo "$(\forall a \in X)P(a)$" come abbreviazione per "$\forall a(a \in X \to P(a))$", che possiamo leggere come "per ogni $a$ appartenente ad $X$ vale $P(a)$". Ciò equivale a dire che vale l'inclusione $X \subseteq \{a : P(a)\}$.

# 8 Primi assiomi: estensionalità, astrazione, comprensione

Nei capitoli precedenti abbiamo visto come, fissato un "universo del discorso", possiamo considerare gli oggetti e le classi di tale universo. Ad esempio se consideriamo l'universo delle persone, gli oggetti saranno le singole persone, e le classi saranno classi di persone, ad esempio la classe degli insegnanti.

Vorremmo ora prendere come universo $V$ del discorso, l'universo di tutti gli oggetti matematici. Ciò non è semplice in quanto la nozione stessa di oggetto matematico è piuttosto problematica: ad esempio non è facile rispondere alla domanda se una classe di oggetti matematici sia essa stessa un oggetto

[3] Se non conoscete le dimostrazioni per assurdo potete ragionare nel modo seguente. I casi sono due: o $X = \emptyset$ e abbiamo finito. Oppure $X \neq \emptyset$. Consideriamo dunque questo secondo caso.

[4] Questa è una delle mosse permesse dalle leggi della logica: sapendo $\exists x P(x)$ possiamo scegliere un tale $x$ e dargli un nome. Ciò non va confuso con l'assioma della scelta studieremo nel seguito

[5] Abbiamo applicato un'altra legge logica: il passaggio da $\forall x P(x)$ a $P(a)$.

matematico. Sicuramente la classe di tutte le funzioni reali continue lo è (e viene studiata dai matematici in quanto tale). Ma la classe di tutti gli oggetti matematici? O la classe di tutti gli alberi ben fondati? (L'abbiamo incontrata nella sezione sull'iperalbero, ricordate?)

Seguiremo pertanto l'approccio assiomatico, ovvero, avendo in mente l'ambito matematico, non definiremo nè cosa sia un oggetto, nè cosa sia una classe, nè che cosa sia la relazione di appartenenza, lasciando che siano gli assiomi che via via daremo a suggerire implicitamente il significato di questi termini. Postuleremo dunque l'esistenza di una classe universale $V$ di tutti gli oggetti (matematici), e daremo degli assiomi che forniscono informazioni su $V$, i suoi elementi, e le sue sottoclassi. Della classe $V$ non faranno parte né le persone, né i pianeti, né alcun oggetto fisico, ma solo ed esclusivamente oggetti matematici come i numeri naturali, i numeri reali, le funzioni, eccetera. Alcune delle sottoclassi di $V$ saranno esse stesse elementi di $V$ e verranno chiamate "insiemi". Risulterà inoltre che sarà possibile economizzare: possiamo assumere (sebbene non sia strettamente indispensabile) che non vi siano "urelementi", ovvero oggetti che non siano essi stessi insiemi. Ciò può sembrare paradossale in quanto ogni insieme è un insieme di oggetti, e senza oggetti non vi sono nemmeno gli insiemi. Tuttavia almeno l'insieme vuoto c'è sempre ed è un oggetto, e vedremo che, a partire da esso, e considerando insiemi i cui elementi siano altri insiemi, possiamo modellare tutti gli oggetti matematici che ci interessano.

Senza ulteriori preamboli passiamo a dare i primi assiomi. Il primo assioma è per l'appunto che esiste una classe universale $V$ tale che ogni oggetto appartiene a $V$. Nelle versioni ufficiali di GB esso non compare in quanto si deduce dagli altri assiomi, ma per chiarezza ho deciso di includerlo. Possiamo quindi pensare alla parola "classe" come "sottoclasse di $V$", e alla parola "oggetto" come "elemento di $V$". Il primo assioma della lista ufficiale lo abbiamo già precedentemente incontrato:

**8.1 Assioma** (Assioma di estensionalità)**.** Due classi sono uguali se hanno gli stessi elementi.

Il secondo assioma (che è in effetti uno "schema di assiomi", uno per ogni $P$), è il seguente:

**8.2 Assioma** (Schema di assiomi di astrazione)**.** Data una proprietà ben definita $P$, esiste una classe i cui elementi sono gli oggetti $x$ che verificano $P$. Tale classe è unica per l'assioma di estensionalità e usiamo la notazione $\{x : P(x)\}$ per denotarla. Per definizione, $a \in \{x : P(x)\}$ se e solo se vale $P(a)$. In simboli:

$$a \in \{x : P(x)\} \iff P(a)$$

dove usiamo $\iff$ come sinonimo di $\leftrightarrow$, ovvero per dire che le due affermazioni che compaiono ai lati del simbolo sono entrambe vere o entrambe false (si vedano le tavole di verità).

Prima di procedere oltre, vanno fatte alcune precisazioni su cosa si intenda per proprietà ben definita. Nella teoria assiomatica di Gödel-Bernays, che è

quella trattata in queste note, per proprietà ben definita intendiamo qualsiasi proprietà che si possa esprimere (rispettando la sintassi) usando l'appartenenza $\in$, l'uguaglianza $=$, le variabili, e gli usuali connettivi logici $\wedge$ (congiunzione), $\vee$ (disgiunzione), $\to$ (implicazione), $\leftrightarrow$ (doppia implicazione), $\neg$ (negazione), $\exists x$ (quantificatore esistenziale), $\forall x$ (quantificatore universale), dove le variabili quantificate variano su oggetti (ovvero elementi di $V$) e non su classi. In MK ammettiamo invece che le proprietà che intervengono nello schema di astrazione contengano anche quantificatori su classi. Per il momento non è il caso di essere più precisi, salvo osservare che, tra le proprietà ammissibili nello schema di astrazione, non rientrano quelle proprietà che fanno riferimento alla realtà fisica come "$x$ è un insetto", o simili. Lo schema proposto sarà in ogni caso sufficiente per gli scopi della matematica.

Se non avessimo postulato a parte l'esistenza di $V$, essa potrebbe essere dedotta dall'assioma di astrazione definendo $V$ come la classe $\{x : x = x\}$. Tale classe contiene tutti gli oggetti in quanto, secondo la logica classica, ogni oggetto è uguale a se stesso.

Una precisazione importante è che nello schema di astrazione ammettiamo la possibilità che in $P(x)$ compaiano altre variabili non quantificate, oltre la $x$, che svolgono il ruolo di parametri, come nel seguente esempio.

**8.3 Esempio.** Date due classi $A, B$, l'esistenza della classe unione $A \cup B = \{x : x \in A \vee x \in B\}$, segue dallo schema di astrazione prendendo come $P(x)$ la proprietà (con parametri $A, B$) definita dalla disgiunzione $x \in A \vee x \in B$. Similmente otteniamo l'esistenza della classe intersezione $A \cap B$ e della classe complemento $A^{\complement}$.

Si potrebbe pensare che la definizione di proprietà ben definita sia troppo restrittiva e che ci possano essere classi $A \subseteq V$ che non possano essere definite da alcuna proprietà. Tuttavia questo è vero solo se ci limitiamo a proprietà definite senza parametri. Infatti, data una qualsiasi classe $A$, possiamo ovviamente "definire" $A$ usando come parametro $A$ stesso:

$$A = \{x : x \in A\}$$

come segue immediatamente dall'assioma di estensionalità.

Esiste in effetti una perfetta corrispondenza tra classi e proprietà: data una proprietà $P(x)$ posso formare la classe corrispondente $\{x : P(x)\}$, e viceversa, data una classe $A$, posso considerare la proprietà corrispondente $x \in A$. Il vero contenuto dell'assioma di astrazione in GB non è tanto quello di "costruire" classi a partire dalle proprietà, quanto quello di dire che ogni operazione che posso fare sulle proprietà ha un corrispettivo nelle classi. Ad esempio il fatto che posso prendere la disgiunzione $P(x) \vee Q(x)$ di due predicati corrisponde al fatto che posso prendere l'unione $A \cup B$ di due classi (ottenuta come la classe degli oggetti $x$ che verificano il predicato $x \in A \vee x \in B$). La filosofia della teoria degli insiemi è di ispirazione platonica, ovvero si assume che $V$ e le sue sottoclassi esistano già, non vengono costruite a partire dalle definizioni (il bello della matematica è che non ci si deve credere sul serio per poter utilizzare la teoria).

Cogliamo l'occasione per sottolineare che lo schema di astrazione non è un singolo assioma, ma una lista infinita di assiomi, uno per ogni proprietà ben definita $P$. Tuttavia si può dimostrare che basta una lista finita di istanze dello schema per poter dedurre tutte le altre, e ciò rende GB, a differenza di ZF e di MK, finitamente assiomatizzabile.

Gli assiomi che abbiamo fin qui dato presuppongono un universo del discorso $V$ consistente di "oggetti" dalla natura non ancora specificata. In particolare non abbiamo detto se le classi stesse siano oggetti. Nel seguito daremo altri assiomi che stabiliranno sotto quali condizioni una classe $X$ possa essere considerata un oggetto (ovvero per quali $X \subseteq V$ si abbia $X \in V$). L'intento sarà quello di avere un universo di oggetti il più vasto possibile (per gli scopi della matematica), ma come vedremo non potrà in ogni caso essere talmente vasto da poter contenere come oggetti anche tutte le classi, pena incorrere in paradossi. Parlando informalmente, qualsiasi cosa sia $V$, le sottoclassi di $V$ sono in un certo senso "di più" degli elementi di $V$, e quindi non è possibile che ogni classe sia un oggetto (può essere utile fare un confronto con il teorema di Cantor, sebbene esso si applichi a insiemi e non a $V$ stesso: le parti di un insieme sono più numerose degli elementi dell'insieme). In definitiva risuterà che alcune classi sono oggetti (e verranno chiamate "insiemi"), ma altre no (e verranno chiamate "classi proprie").

**8.4 Definizione.** Un insieme è una classe che è anche un oggetto, ovvero è uno degli elementi della classe universale $V$ di tutti gli oggetti. Equivalentemente, visto che tutte le classi sono incluse in $V$, un insieme è una classe che appartiene ad almeno un'altra classe. Una classe propria è una classe che non è un insieme.

Ci possiamo ora chiedere se la classe universale $V = \{x : x = x\}$ sia un oggetto, ovvero se $V \in V$. Visto che $V = V$ sembrerebbe di sì, essendo $x = x$ la proprietà definitoria della classe $V$. Tuttavia questo è un errore. Infatti secondo le nostre convenzioni la variabile $x$ in un'espressione della forma $\{x : P(x)\}$, e quindi in particolare nell'espressione $\{x : x = x\}$, varia su oggetti, e non possiamo quindi concludere che $V \in \{x : x = x\}$ senza prima aver stabilito se $V$ sia un oggetto. Vedremo che in effetti $V$ non è un oggetto. Abbiamo bisogno di un risultato preliminare.

**8.5 Definizione.** La classe di Russell è la classe $\{x : x \notin x\}$.

**8.6 Teorema.** *La classe di Russell non è un insieme.*

*Dimostrazione.* Sia $R = \{x : x \notin x\}$. Per ogni oggetto $a$ abbiamo per definizione $a \in R$ se e solo se $a \notin a$. Se $R$ fosse un oggetto potremmo prendere $a = R$ ottenendo $R \in R$ se e solo se $R \notin R$, il che è assurdo. □

**8.7 Assioma** (Assioma di comprensione)**.** Una sottoclasse di un insieme è un insieme.

Dato un insieme $A$ e una proprieà $P$ indichiamo con $\{x \in A : P(x)\}$ la classe $\{x : x \in A \wedge P(x)\}$, ovvero la classe consistente di quegli elementi di $A$

che verificano il predicato $P$. Siccome tale classe è inclusa in $A$, per l'assioma di comprensione $\{x \in A : P(x)\}$ è un insieme. Si noti che l'assioma di comprensione può solo servire a generare sottoinsiemi di altri insiemi, e quindi avremo bisogno di altri assiomi per ottenere degli insiemi di partenza a cui applicare il procedimento.

**8.8 Corollario.** *La classe $V$ di tutti gli oggetti non è un insieme (ovvero è una classe propria).*

*Dimostrazione.* Ogni classe è inclusa in $V$, quindi se $V$ fosse un insieme tutte le classi sarebbero insiemi, ma sappiamo che la classe $R$ di Russell non lo è. □

**8.9 Nota.** Alla fine del 1800 Gottlob Frege propose una assiomatizzazione della teoria degli insiemi che aveva come unici assiomi l'estensionalità e l'astrazione e in cui non esisteva distinzione tra insiemi e classi. In una famosa lettera del 1901 Bertrand Russell gli fece notare che la sua assiomatizzazione era contraddittoria. La dimostrazione si basava sulla classe di Russell $R = \{x : x \notin x\}$. Come abbiamo visto l'ipotesi che tale classe sia un insieme conduce ad un assurdo.

# 9 Insieme vuoto, coppia, unione

Il seguente assioma garantisce che esiste almeno un insieme.

**9.1 Assioma** (Insieme vuoto)**.** La classe vuota è un insieme.

Per dimostrare l'esistenza di altri oggetti abbiamo bisogno di ulteriori assiomi. Diamo intanto una definizione. Dati due oggetti $a, b$, sia $\{a, b\}$ la classe $\{x : x = a \vee x = b\}$. Tale classe ha solamente $a, b$ come elementi e viene chiamata la coppia degli elementi $a$ e $b$.

**9.2 Assioma** (Coppia)**.** Dati due oggetti $a, b$, la coppia $\{a, b\}$ è un insieme.

Non richiediamo che $a, b$ siano oggetti distinti: possiamo anche prendere $a = b$, ottenendo il singoletto di $a$, ovvero l'insieme $\{a, a\}$. Il singoletto di $a$ viene comunemente indicato con la notazione $\{a\}$ e contiene solamente $a$ come elemento.

In generale quando diciamo "dati due oggetti $a, b$", con la parola "due" intendiamo in realtà "degli", ovvero non escludiamo (a meno di dirlo esplicitamente) il caso che $a$ e $b$ siano in effetti lo stesso oggetto (che quindi è uno, e non due). Il fatto di usare lettere diverse per denotarli (o denotarlo) vuol solo dire che *potrebbero* essere diversi, non che lo siano. Scrivere $a = b$ significa che l'oggetto denotato dalla lettera "$a$" coincide con l'oggetto denotato dalla lettera "$b$", e non che la lettera "$a$" sia uguale alla lettera "$b$" (ovviamente non lo è). In ogni caso $a = a$ è sempre vero, in quanto lo stesso nome denota lo stesso oggetto. Facciamo però attenzione: la relazione di uguaglianza è una relazione tra gli oggetti, non tra i loro nomi, ma per parlare di oggetti li devo nominare.

**9.3 Assioma** (Unione binaria)**.** Dati due insiemi $X$ ed $Y$, la loro unione $X \cup Y$ è un insieme.

Avendo a disposizione le coppie e l'unione binaria possiamo formare le triple $\{a,b,c\} = \{a,b\} \cup \{c\}$, le quadruple $\{a,b,c,d\} = \{a,b,c\} \cup \{d\}$ e via dicendo. Dobbiamo però avere degli oggetti $a,b,c,d$ da cui partire. Dove li prendiamo? Per ora abbiamo definito un solo oggetto: l'insieme vuoto $\emptyset$. Abbiamo però anche il singoletto $\{\emptyset\}$, che non è vuoto in quanto contiene come elemento $\emptyset$. A livello intuitivo questo corrisponde al fatto che una scatola vuota non è la stessa cosa di una scatola che contiene al suo interno una scatola vuota. Abbiamo poi $\{\{\emptyset\}\}$ (il singoletto del singoletto del vuoto), oppure l'insieme di due elementi $\{\emptyset, \{\emptyset\}\}$, e procedendo in questo modo otteniamo una quantità potenzialmente illimitata di insiemi distinti. Li possiamo immaginare come scatole cinesi una entro l'altra e terminanti sempre con la scatola vuota. Tuttavia l'analogia tra insiemi e scatole ha dei limiti: uno stesso oggetto può appartenere a più insiemi, ma non può essere contenuto in due scatole diverse. Gli insiemi si possono intersecare, le scatole no.

Si noti che, avendo a disposizione l'unione binaria, la coppia $\{a,b\}$ si ottiene per unione dai singoletti di $a$ e $b$, ovvero $\{a,b\} = \{a\} \cup \{b\}$.

Introdurremo ora il cosiddetto "assioma dell'unione", che in presenza dell'assioma della coppia implica l'assioma dell'unione binaria, rendendolo ridondante.

**9.4 Definizione.** Data una classe di insiemi $X$ (ovvero una classe i cui elementi sono insiemi) definiamo $\bigcup X$ (unione di $X$) come la classe di quegli oggetti che appartengono ad almeno un elemento di $X$. Quindi $x \in \bigcup X$ se e solo se $\exists a \in X$ tale che $x \in a$. Un'altra notazione per $\bigcup X$ è $\bigcup_{A \in X} A$.

Ad esempio se $A, B$ sono due insiemi e $X = \{A, B\}$, allora $\bigcup X = A \cup B$. Infatti per definizione $x \in \bigcup X$ se $x$ appartiene ad uno degli elementi di $X$, ovvero $x \in A$ o $x \in B$, il che equivale a dire che $x \in A \cup B$.

**9.5 Assioma** (Assioma dell'unione)**.** Se $X$ è un insieme di insiemi, $\bigcup X$ è un insieme.

Nel seguito useremo talvolta come sinonimi "famiglia di insiemi" ed "insieme di insiemi". Quindi l'assioma dell'unione dice che l'unione di una famiglia di insiemi è un insieme. Si noti che se $X$ fosse una classe propria potremmo ugualmente formare l'unione $\bigcup X$ in base allo schema di astrazione (ponendo $\bigcup X = \{x : (\exists y \in X)(x \in y)\}$), ma essa risulterebbe in generale una classe, mentre l'assioma dell'unione dice che se partiamo da un insieme otteniamo un insieme.

**9.6 Definizione.** Se $X$ è una classe di insiemi, definiamo $\bigcap X$ (intersezione di $X$) come la classe di quegli oggetti che appartengono a ciascuno degli elementi di $X$. Quindi $x \in \bigcap X$ se e solo se $\forall A \in X$ vale $x \in A$.

**9.7 Osservazione.** Se $X$ è la classe vuota, $\bigcap X$ è la classe universale $V$ (verificate!). Se $X$ è una classe non vuota di insiemi, allora la classe $\bigcap X$ è un insieme in base all'assioma di comprensione in quanto è inclusa in ciascuno degli insiemi di $X$ (non abbiamo bisogno di uno specifico assioma come nel caso dell'unione).

Gli assiomi fin qui dati non garantiscono l'esistenza di alcun oggetto che non sia un insieme (ad esempio non garantiscono l'esistenza di penne stilografiche). Poiché uno degli scopi della teoria degli insiemi è dimostrare l'esistenza degli usuali oggetti matematici (numeri naturali, numeri reali, funzioni), abbiamo due possibilità: o postuliamo l'esistenza di oggetti non-insiemistici (i cosiddetti "urelementi") e diamo per essi opportuni assiomi (ad esempio gli assiomi di Peano per i numeri naturali), oppure mostriamo come sia possibile modellare tutti gli oggetti della matematica in modo insiemistico. Sono possibili entrambe le strade, ma scegliamo la seconda. Diamo pertanto il seguente assioma:

**9.8 Assioma.** Non esistono urelementi, ovvero ogni oggetto è un insieme.

In presenza di questo assioma dire "classe di insiemi" è come dire "classe", e quindi l'assioma dell'unione assume la forma più semplice:

**9.9 Assioma** (Assioma dell'unione)**.** Se $X$ è un insieme, $\bigcup X$ è un insieme.

Se il lettore preferisce la versione con urelementi, non avrà difficoltà ad adattare gli assiomi tenendo conto della possibile presenza di urelementi. In questo caso la cosa principale a cui bisogna porre attenzione è che per gli urelementi non vale l'assioma di estensionalità (altrimenti gli urelementi sarebbero tutti uguali e coinciderebbero con l'insieme vuoto, visto che non hanno elementi).

# 10 I numeri naturali

**10.1 Definizione.** Gli assiomi di Peano per i numeri naturali (che non fanno parte degli assiomi della teoria degli insiemi) sono i seguenti.

1. 0 è un numero naturale.
2. Se $n$ è un numero naturale anche il suo successore $S(n)$ lo è (useremo anche la notazione $n+1$ per indicare il successore di $n$).
3. Se due numeri naturali hanno lo stesso successore sono uguali.
4. 0 è l'unico numero naturale che non è un successore.
5. Assioma di induzione: Sia $X$ un insieme di numeri naturali che contiene 0 ed è chiuso per successore (nel senso che, per ogni numero naturale $n$, $n \in X \to S(n) \in X$). Allora $X$ contiene ogni numero naturale $n$.

L'assioma di induzione è ciò che giustifica le "dimostrazioni per induzione" che spero conosciate già: per dimostrare che una certa proprietà $P(x)$ vale per tutti i numeri naturali, uno dei metodi (non l'unico!) è ragionare nel modo seguente. Si cerca di dimostrare la *base dell'induzione* $P(0)$, e il *passo induttivo* $\forall x \in \mathbb{N}\big(P(x) \to P(S(x))\big)$. Se ci si riesce, in base all'assioma di induzione si può concludere che l'insieme $X = \{x \in \mathbb{N} : P(x)\}$ contiene ogni numero naturale,

ovvero che $\forall x \in \mathbb{N}\, P(x)$. Avremo modo di familiarizzarci con questa tecnica nel seguito.

Il nostro scopo è quello di definire i numeri naturali in termini insiemistici in modo che risultino verificate le proprietà espresse dagli assiomi di Peano. Diamo la seguente definizione dovuta a von Neumann.

**10.2 Definizione.** $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$ e così via. In generale il successore $s(n)$ di $n$ è definito come $n \cup \{n\}$. Ad esempio $s(3) = 3 \cup \{3\} = \{0, 1, 2\} \cup \{3\} = \{0, 1, 2, 3\} = 4$.

Esistono altre definizioni dei numeri naturali in termini insiemistici, oltre a quella di von Neumann. Ad esempio si potrebbe definire il successore di $n$ come il singoletto $\{n\}$ anziché come $n \cup \{n\}$. La definizione di von Neumann ha il vantaggio che il numero $n$ ha esattamente $n$ elementi, nel senso comune del termine. Ad esempio il numero $4 = \{0, 1, 2, 3\}$ ha esattamente quattro elementi.

Osserviamo che sebbene gli assiomi sin qui dati ci forniscano infiniti insiemi (i numeri naturali), essi non ci forniscono ancora un insieme infinito. In particolare ancora non sappiamo se esista un insieme che contenga tutti i numeri naturali come elementi (in quanto la classe dei numeri naturali potrebbe non essere un insieme, ovvero potrebbe essere inclusa in $V$ senza appartenere a $V$). Questo ci è garantito dal seguente assioma.

**10.3 Assioma** (Assioma dell'infinito)**.** Esiste un insieme $X$ tale che

1. $\emptyset \in X$,
2. Se $a \in X$ allora $a \cup \{a\} \in X$.

In base all'assioma l'insieme $X$ contiene $\emptyset$ e, se contiene $n$, contiene anche il successore di $n$ (secondo la definizione di von Neumann). Possiamo quindi concludere che $X$ contiene tutti i numeri naturali di von Neumann $0, 1, 2, 3, \ldots$. Notiamo tuttavia che $X$ potrebbe contenere anche altri elementi oltre ai numeri naturali. Per trovare un insieme $X$ che contenga esclusivamente i numeri naturali dobbiamo innanzitutto definire in modo preciso cosa significhi "$n$ è un numero naturale" (la locuzione "e così via" nella Definizione 10.2 non può essere presa come sostituto di una definizione precisa). Potremmo essere tentati di definirli come quegli oggetti che si ottengono da $\emptyset$ applicando "un numero finito di volte" la funzione successore. Dovremmo però in questo caso dare una definizione di "numero finito di volte" che non faccia riferimento ai numeri naturali stessi. Fortunatamente possiamo uscire dalla circolarità nel modo seguente.

**10.4 Definizione.** Sia $\omega = \bigcap \mathcal{F}$, dove $\mathcal{F}$ è la classe di tutti gli insiemi $X$ tali che $\emptyset \in X$ ed $X$ è chiuso per successore (ovvero se $x \in X$ anche $x \cup \{x\} \in X$). Diciamo che $n$ è un numero naturale se $n \in \omega$. Si noti che $\mathcal{F}$ è non vuota per l'assioma dell'infinito, e che se $X$ è uno qualsiasi degli elementi di $\mathcal{F}$, abbiamo $\omega \subseteq X$. Ne segue che $\omega$ è un insieme per l'assioma di comprensione.

Notiamo che $\omega$ stesso appartiene alla classe $\mathcal{F}$, ovvero $\omega$ contiene $\emptyset$ ed è chiuso per successore (verificate!). La definizione appena data di $\omega$ è pertanto "impredicativa", ovvero per definire $\omega$ si fa riferimento ad una classe $\mathcal{F}$ di oggetti che contiene $\omega$ stesso come elemento. La possibilità di dare definizioni impredicative impedisce in generale di interpretare le definizioni come "costruzioni" degli oggetti definiti. Non possiamo dire che $\omega$ è "costruito" a partire da $\mathcal{F}$ in quanto $\omega$ doveva già esistere come uno degli elementi di $\mathcal{F}$. La giusta intepretazione è invece che sia $\omega$ che $\mathcal{F}$ esistevano già da sempre come elementi della classe universale $V$, e lo scopo della definizione è unicamente quello di "isolare" $\omega$ tra gli elementi di $V$, fornendone una descrizione che lo caratterizza.

Esistono scuole di pensiero che rifiutano le definizioni impredicative. Poincaré ad esempio era convinto che in esse risiedesse la fonte dei paradossi. Tuttavia in teoria degli insiemi esse sono accettate, e per il momento non si sono viste conseguenze nefaste. Sarebbe tuttavia possibile dare una definizione di $\omega$ un po' più predicativa. Prima si definiscono gli ordinali (li vedremo nel seguito), poi si definiscono gli ordinali finiti come quelli che non ammettono ordinali limite più piccoli di loro, e infine si definisce $\omega$ come l'insieme degli ordinali finiti. Il vantaggio di questa seconda definizione è che, anche senza l'assioma dell'infinito, $\omega$ risulta ben definito in GB in quanto classe (sebbene senza l'assioma dell'infinito non si possa dimostrare che tale classe sia un insieme).

Osserviamo che, in base alla definizione che ne abbiamo dato, $\omega$ è incluso in qualsiasi insieme $X$ che contiene $\emptyset$ ed è chiuso per successore. Infatti un tale $X$ appartiene alla famiglia $\mathcal{F}$ (quella che interviene nella definizione di $\omega$), ed essendone l'intersezione $\omega$ è incluso in ciascuno degli elementi di $\mathcal{F}$. Si può in effetti dimostrare un risultato più forte:

**10.5 Osservazione.** L'insieme $\omega$ è incluso in qualsiasi classe $X$ che contiene $\emptyset$ ed è chiusa per successore.

*Dimostrazione.* Sappiamo già che il risultato vale se $X$ è un insieme. Ci possiamo ricondurre a questo caso considerando $X' = X \cap \omega$. Anche $X'$ contiene $\emptyset$ ed è chiuso per successore, ed essendo incluso nell'insieme $\omega$ è un insieme per l'assioma di comprensione. Dunque per quanto visto $\omega \subseteq X'$, il che equivale a dire che $\omega \subseteq X$. □

**10.6 Teorema.** *I numeri naturali di von Neumann sono un "modello degli assiomi di Peano", ovvero verificano le proprietà espresse dagli assiomi di Peano.*

*Dimostrazione.* Iniziamo con l'induzione. Sia $X \subseteq \omega$ un insieme che contiene 0 ed è chiuso per successore. Essendo $\omega$ il più piccolo di tali insiemi, $X = \omega$. Avendo verificato l'induzione, nel verificare gli altri assiomi possiamo procedere per induzione.

Il punto più delicato il seguente. Supponiamo che $x, y$ abbiano lo stesso successore. Dobbiamo dimostrare che $x = y$. Innanzitutto dimostriamo, per induzione su $x \in \omega$, che $\bigcup(s(x)) = x$, dove $s(x) = x \cup \{x\}$. Il caso $x = \emptyset$ è immediato. Supponiamo dunque che $x = s(y)$ e che la tesi valga per $y$. Abbiamo $\bigcup(s(x)) = \bigcup(x \cup \{x\}) = \bigcup x \cup \bigcup(\{x\})$. Per ipotesi induttiva $\bigcup x = y$, mentre

ovviamente $\bigcup(\{x\}) = x$. Dunque $\bigcup(s(x)) = y \cup x = y \cup s(y) = y \cup y \cup \{y\} = y \cup \{y\} = x$. Abbiamo così dimostrato che $\bigcup$ si comporta da predecessore. Supponendo ora che $s(x) = s(y)$ otteniamo $\bigcup(s(x)) = \bigcup(s(y))$, e dunque $x = y$.

Resta da dimostrare che $0 = \emptyset$ è l'unico elemento di $\omega$ che non è un successore. Questo si dimostra per induzione applicata alla sequente proprietà $P(x)$: $x \neq 0 \to (\exists y \in \omega)(x = s(y))$. Per $x = 0$ la proprietà $P$ vale "a vuoto", essendo la premessa dell'implicazione falsa. Chiaramente se la proprietà $P$ vale per $z$, essa vale per $s(z)$ (difatti la proprietà vale per $s(z)$ anche senza sfruttare l'ipotesi che valga per $z$). Quindi per induzione $P$ vale per ogni numero naturale. □

Nel seguito scriveremo indifferentemente $\omega$ o $\mathbb{N}$ a meno che non ci siano specifiche ragioni di distinguere tra numeri naturali di von Neumann (per i quali useremo sempre $\omega$) e un generico modello degli assiomi di Peano.

# 11 La relazione d'ordine sui numeri naturali

Oltre ad uno zero e un successore, i numeri naturali hanno anche una struttura d'ordine, ovvero dati due numeri naturali possiamo dire se uno è maggiore o minore dell'altro. L'idea è che $x < y$ ($x$ è minore di $y$) se $y$ si può ottenere da $x$ applicando "un certo numero di volte" la funzione successore. Diamo ora la definizione precisa (essa si applica a qualunque modello degli assiomi di Peano, non solo dunque ai numeri naturali di von Neumann).

**11.1 Definizione.** Definiamo una relazione $\leq$ sui numeri naturali come segue: $x \leq y$ ($x$ è minore o uguale a $y$) se qualsiasi sottoinsieme di $\mathbb{N}$ chiuso per successore e contenente $x$ contiene necessariamente anche $y$. Se $x \leq y$ diciamo anche che $y$ è maggiore o uguale ad $x$, e scriviamo $y \geq x$. I numeri maggiori o uguali ad $x$ costituiscono dunque il più piccolo insieme chiuso per successore e contenente $x$. Scriviamo $x < y$ ($x$ è strettamente minore di $y$) se $x \leq y$ e $x \neq y$.

**11.2 Esercizio.** $\leq$ è una relazione d'ordine totale su $\mathbb{N}$, cioè valgono le seguenti quattro proprietà:

1. $x \leq x$ (riflessività);
2. se $x \leq y$ e $y \leq z$ allora $x \leq z$ (transitività);
3. se $x \leq y$ e $y \leq x$ allora $x = y$ (antisimmetria);
4. dati due numeri naturali qualsiasi $x, y$ abbiamo $x \leq y$ oppure $y \leq x$ (totalità).

Nello svolgere l'esercizio il lettore è pregato di affidarsi esclusivamente alle definizioni, agli assiomi, e alle leggi della logica, senza fare affidamento sull'intuizione geometrica, ovvero l'intuizione che gli consente di immaginare i numeri naturali disposti lungo una retta e in cui "maggiore di" vuol dire "sta a destra di" (non è questa la definizione che abbiamo dato di minore). Il tentativo di bandire l'intuizione geometrica dai fondamenti della matematica è una delle

costanti della filosofia della matematica del 1900; basti qui ricordare il nome di Bertrand Russell e gli intellettuali del "circolo di Vienna", tra cui Rudolf Carnap. Questa impostazione ha però anche portato a degli eccessi (i "Principia Mathematica" di Russell) e, in tempi più recenti, a delle rivalutazioni dell'approccio intuitivo, per lo meno a livello didattico.

Come al solito definiamo $x < y$ come $x \leq y \wedge x \neq y$.

**11.3 Esercizio.** Per ogni $x \in \mathbb{N}$ abbiamo:

1. $0 \leq x$.
2. $x < s(x)$.
3. Non vi è alcun alcun $z \in \mathbb{N}$ con $x < z < S(x)$.

**11.4 Lemma.** *Vale il* **principio del minimo***: ogni insieme non vuoto $X$ di numeri naturali ha un minimo elemento, ovvero esiste un $n \in X$ tale che per ogni $m \in X$ si ha $n \leq m$.*

*Dimostrazione.* Supponiamo per assurdo che esista un insieme non vuoto $X$ di numeri naturali senza un minimo elemento. Consideriamo un tale ipotetico insieme $X$, e sia $Y$ l'insieme di quei numeri naturali che sono strettamente minori di ogni elemento di $X$. Chiaramente $Y$ contiene lo 0. Inoltre se $Y$ contiene un numero $n$ deve contenere anche il suo successore $S(n)$, altrimenti per il Lemma 11.3 $S(n)$ sarebbe il minimo di $X$ (non essendovi altri elementi tra $n$ e $S(n)$). Dunque in base al principio di induzione $Y$ coincide con $\mathbb{N}$. Ma visto che $X$ è disgiunto da $Y$, ne segue che $X$ è vuoto, contro le nostre ipotesi. □

**11.5 Osservazione.** (Induzione forte) Il principio del minimo giustifica le dimostrazioni per "induzione forte": per dimostrare che una proposizione $P$ vale per ogni numero naturale, basta riuscire a dimostrare, dato un generico $n$, il seguente *passo induttivo*: se $P(m)$ vale per tutti gli $m < n$, allora vale anche $P(n)$.

Si noti che se $n = 0$ ciò equivale a dimostrare direttamente $P(0)$, quindi nell'induzione forte il caso base è incluso nel passo induttivo.

Per giustificare le dimostrazioni per induzione forte si ragiona per assurdo: supponendo di essere riusciti a dimostrare il passo induttivo, se $P$ non valesse per ogni $n$, ci sarebbe un minimo $n$ per cui non vale $P(n)$. Per ciascun $m < n$ deve dunque valere $P(m)$, ma allora per il passo induttivo vale anche $P(n)$, da cui l'assurdo.

L'induzione (forte o normale) e il principio del minimo sono in effetti equivalenti: ciò che si può dimostrare con uno di questi procedimenti si può dimostrare con gli altri.

I lemmi precedenti valgono per qualsiasi modello degli assiomi di Peano, ma i numeri di von Neumann abbiamo delle proprietà in più, come le seguenti:

**11.6 Esercizio.** Dati $n, m \in \omega$, abbiamo $n < m$ secondo la definizione sopra datane, se e solo se $n \in m$. Ad esempio $3 \in 5 = \{0, 1, 2, 3, 4\}$. Inoltre ogni

elemento di un numero naturale $n$ di von Neumann, è esso stesso un numero naturale di von Neumann. Dunque per ogni $n \in \omega$ sia ha

$$n = \{x : x \in n\} = \{x \in \omega : x < n\}.$$

# 12 Relazioni e Funzioni

**12.1 Definizione** (Coppia di Kuratowksi)**.** Dati due oggetti $a, b$ definiamo $(a, b) = \{\{a\}, \{a, b\}\}$ e chiamiamo $(a, b)$ la coppia ordinata di $a$ e $b$.

La proprietà fondamentale delle coppie ordinate è espressa dal seguente esercizio.

**12.2 Esercizio.** Se $(a, b) = (c, d)$ allora $a = b$ e $c = d$.

Si noti la differenza con la coppia non ordinata $\{a, b\}$. Ad esempio mentre $\{0, 1\} = \{1, 0\}$, abbiamo $(0, 1) \neq (1, 0)$. Nelle coppie ordinate ha senso parlare di primo e secondo elemento, ma nelle coppie non ordinate (quelle dell'assioma della coppia) tali nozioni non hanno senso. Esistono altri modi di definire la coppia ordinata $(a, b)$ in modo che valga la proprietà fondamentale. Per i nostri scopi una vale l'altra.

**12.3 Definizione.** Date due classi $X$ ed $Y$ definiamo il loro prodotto cartesiano $X \times Y$ come la classe i cui elementi sono le coppie ordinate $(a, b)$ con $a \in X$ e $b \in Y$.

**12.4 Osservazione.** Per esprimere in formule la definizione sopra data si usa scrivere

$$X \times Y = \{(a, b) : a \in X \wedge b \in Y\}.$$

Notiamo tuttavia che per dimostrare formalmente che $X \times Y$ è una classe dovremmo trovare una definizione della forma $X \times Y = \{x : P(x)\}$ dove $x$ è una variabile e $P$ è una opportuna proprietà. A tal fine basta scrivere

$$X \times Y = \{x : (\exists a \in X)(\exists b \in Y)\ x = (a, b)\},$$

dove la formula dopo i due punti esprime il fatto che $x$ è della forma $(a, b)$ con $a \in X$ e $b \in Y$.

**12.5 Definizione.** Una relazione $R$ tra due classi $X$ ed $Y$ è una sottoclasse di $X \times Y$. Diremo che $a, b$ sono in relazione (rispetto ad $R$) se $(a, b) \in R$. Scriveremo anche $aRb$ oppure $R(a, b)$ per esprimere il fatto che $a, b$ sono in relazione. Se $X = Y$, ovvero $R \subseteq X \times X$, diremo che $R$ è una relazione binaria su $X$.

**12.6 Definizione.** Una funzione $F$ da una classe $X$ ad una classe $Y$ è una relazione $F \subseteq X \times Y$ che gode delle seguenti proprietà: per ogni $x \in X$ esiste uno ed un solo $y \in Y$ tale che $(x, y) \in F$. Useremo la notazione $F : X \to Y$ per

esprimere il fatto che $F$ è una funzione da $X$ ad $Y$. Se $F : X \to Y$ ed $x \in X$, indichiamo con $F(x)$ l'unico oggetto $y \in Y$ tale che $(x, y) \in F$. Quindi $y = F(x)$ se e solo se $(x, y) \in F$. La classe $X$ viene chiamata dominio di $F$ e la classe $Y$ il suo codominio. L'immagine di $F$ è la classe consistente degli oggetti della forma $F(x)$ con $x \in X$, ovvero la classe $\{y : (\exists x \in X)(y = F(x))\}$. Per indicare l'immagine di $F$ si usa anche la notazione $\{F(x) : x \in X\}$, o più semplicemente $\mathrm{im}(F)$.

Diremo che $F$ è *iniettiva* se per per ogni $b$ nella sua immagine esiste uno ed un solo $x$ nel suo dominio tale che $F(x) = b$, ovvero da $F(x) = F(y)$ segue $x = y$. Diremo poi che $F$ è *surgettiva* se l'immagine coincide con il codominio, ed è *biunivoca* (o bigettiva) se è sia iniettiva che surgettiva, ovvero ad ogni elemento del codominio corrisponde uno ed un solo elemento del dominio.

Talvolta parleremo di funzioni senza specificare il dominio e il codominio. In questa accezione una funzione $F$ è semplicemente una classe di coppie ordinate tale che non vi sono due coppie in $F$ con la stessa prima componente e seconde componenti diverse. ll dominio di $F$ è la classe $\mathrm{dom}(F) = \{x : (\exists y)(x, y) \in F\}$ e la sua immagine è $\mathrm{im}(F) = \{y : (\exists x \in X)(y = F(x))\}$, mentre non ha molto senso parlare del codominio (può essere $V$, o $\mathrm{im}(F)$, o qualsiasi classe intermedia). Si noti che $F$ è sempre surgettiva se considerata come funzione da $\mathrm{dom}(F)$ a $\mathrm{im}(F)$, mentre può non esserla se cambiamo il codominio.

Analoghi discorsi valgono per le relazioni: se non specifichiamo il dominio e il codominio una relazione binaria $R$ non è altro che una classe di coppie ordinate e il dominio di $R$ è la classe degli $x \in V$ tali che esiste un $y \in V$ con $(x, y) \in R$.

**12.7 Definizione.** Data una funzione $F : X \to Y$ e una sottoclasse $Z \subseteq X$, la restrizione di $F$ a $Z$ è la funzione $F\restriction_Z : Z \to Y$ definita da $F\restriction_Z = F \cap (Z \times Y)$, ovvero l'insieme delle coppie di $F$ la cui prima componente è in $Z$.

**12.8 Osservazione.** Date due funzioni $F, G$, l'intersezione $F \cap G$ è una funzione se e solo se $F$ e $G$ coincidono su $\mathrm{dom}(F) \cap \mathrm{dom}(G)$, nel senso che le rispettive restrizioni a questa intersezione coincidono. Ciò equivale a dire che $F(x) = G(x)$ per ogni $x \in \mathrm{dom}(F) \cap \mathrm{dom}(G)$. In generale, data una famiglia $\mathcal{C}$ di funzioni, l'unione $\bigcup \mathcal{C}$ è una funzione se prese comunque due funzioni in $\mathcal{C}$ esse coincidono sull'intersezione dei loro domini. Infatti è ovvio che $\bigcup \mathcal{C}$ è un insieme di coppie, e resta dunque solo da dimostrare che se $(x, y)$ ed $(x, y')$ sono entrambi in $\bigcup C$, allora $y = y'$. Ciò segue dal fatto che per definizione di unione $(x, y)$ appartiene ad una delle $F \in \mathcal{C}$ e $(x, y')$ ad una delle $G \in \mathcal{C}$ (senza escludere il caso $F = G$), e poiché che $F$ e $G$ coincidono sull'intersezione dei loro domini, dobbiamo avere $y = y'$.

Le funzioni si prestano a modellare il concetto di successione. In genere le successioni vengono indicate usando i puntini di sospensione $a_0, a_1, \ldots, a_n$, ma è più corretto dire che, dato $n \in \omega$, una successione $(a_i : i < n)$ di oggetti $a_i$, non è altro che la funzione con dominio $n = \{i : i < n\}$ che manda $i$ in $a_i$. Non dobbiamo confondere $(a_i : i < n)$, che è una funzione, con $\{a_i : i < n\}$, che è la sua immagine. Più in generale, dato un insieme di indici $I$, indichiamo con

$(a_i : i \in I)$ la funzione da $I$ a $V$ che manda $i \in I$ in $a_i$, e con $\{a_i : i \in I\}$ l'immagine di tale funzione. In altre parole i sottoindici indicano l'applicazione di una funzione al suo argomento: $a_i$ è la funzione $a$ applicata ad $i$. Ogni insieme si può scrivere in molti modi come immagine di una funzione (basta ad esempio considerare la funzione identità dall'insieme in se stesso), e pertanto, ove convenga, ogni insieme si può scrivere nella forma $\{a_i : i \in I\}$ per un certo insieme di indici $I$. Analoghi discorsi valgono per le classi.

# 13 Assioma potenza e di rimpiazzamento

**13.1 Assioma** (Assioma potenza)**.** Dato un insieme $X$, la classe $\mathcal{P}(X) = \{Y : Y \subseteq X\}$ dei sottoinsiemi di $X$ è un insieme.

**13.2 Assioma** (Assioma di rimpiazzamento)**.** Se $F : X \to Y$ è una funzione tra classi e il suo dominio $X$ è un insieme, allora la sua immagine $\mathrm{im}(F)$ è un insieme.

Come prima applicazione dell'assioma di rimpiazzamento dimostriamo la seguente proposizione.

**13.3 Proposizione.** *Se $A$ ed $B$ sono insiemi, $A \times B$ è un insieme.*

*Dimostrazione.* Fissato $b \in B$, per l'assioma di rimpiazzamento esiste l'insieme $\{(a, b) \mid a \in A\}$, che non è altro che $A \times \{b\}$. Ancora per l'assioma di rimpiazzamento esiste l'insieme $F = \{A \times \{b\} \mid b \in B\}$. Infine per l'assioma dell'unione esiste l'insieme $\bigcup F = \bigcup_{b \in B} A \times \{b\} = A \times B$. □

La dimostrazione appena data funziona per qualunque definizione di $(a, b)$ che verifichi la proprietà fondamentale delle coppie ordinate. Se utilizziamo le coppie di Kuratowski esiste una seconda dimostrazione che usa l'assioma potenza anziché l'assioma di rimpiazzamento. Basta infatti osservare che se $a \in A$ e $b \in B$, allora $\{a\}$ ed $\{a, b\}$ appartengono a $\mathcal{P}(A \cup B)$ e quindi $(a, b) = \{\{a\}, \{a, b\}\} \subseteq \mathcal{P}(A \cup B)$, ovvero $(a, b) \in \mathcal{P}\,\mathcal{P}(A \cup B)$. Riassumendo abbiamo:

**13.4 Osservazione.** $A \times B \subseteq \mathcal{P}\,\mathcal{P}(A \cup B)$.

**13.5 Corollario.** *Se $F : X \to Y$ è una funzione tra classi e $X$ è un insieme, allora $F$ è un insieme.*

*Dimostrazione.* Per l'assioma di rimpiazzamento $\mathrm{im}(F)$ è un insieme, ed essendo $F$ inclusa nell'insieme $X \times \mathrm{im}(F)$, anche $F$ è un insieme. □

Il seguente risultato ha bisogno dell'assioma delle parti.

**13.6 Proposizione.** *Se $X$ ed $Y$ sono insiemi, la classe $C$ di tutte le funzioni da $X$ ad $Y$ è un insieme.*

*Dimostrazione.* Se $f$ è una funzione da $X$ ad $Y$, allora $f$ è inclusa in $X \times Y$, e quindi $f \in \mathcal{P}(X \times Y)$. Abbiamo quindi $C \subseteq \mathcal{P}(X \times Y)$, da cui $C \in \mathcal{P}\,\mathcal{P}(X \times Y)$. □

# 14 Definizioni ricorsive sui numeri naturali

Consideriamo la funzione fattoriale. Essa viene normalmente definita per induzione, o meglio per "ricursione", come segue: $0! = 1$, $(n+1)! = (n+1) \cdot n!$. All'interno della teoria assiomatica degli insiemi questo genere di definizioni, in cui il valore di una funzione $f$ su un dato argomento $n$ viene definito utilizzando i valori della funzione stessa su alcuni argomenti "precedenti" è giustificato dal "Teorema di Ricursione". Nella sua forma più semplice detto teorema afferma che è possibile definire una funzione $f$ sui numeri naturali fornendo il valore di $f(0)$ e dando una regola $H$ che permette di determinare $f(n+1)$ conoscendo $n$ ed $f(n)$. Più formalmente abbiamo:

**14.1 Teorema.** *Sia $A$ una classe. Data una funzione $H\colon \omega \times A \to A$ ed un elemento $a \in A$, esiste una ed una sola funzione $f\colon \omega \to A$ tale che $f(0) = a$ ed $f(n+1) = H(n, f(n))$.*

*Dimostrazione.* L'unicità della $f$ è facile da dimostrare. Se infatti $g : \omega \to A$ verifica le stesse equazioni ricorsive della $f$, ovvero $g(0) = a$ e $g(n+1) = H(n, g(n))$, allora per induzione su $n$ si ottiene facilmente $f(n) = g(n)$ per ogni $n \in \omega$.

Prima di dimostrare l'esistenza ci occorre un risultato preliminare. Mostriamo, per induzione su $m \in \omega$, che esiste una ed una sola funzione $f$, con dominio $\{x \in \omega : x \leq m\}$, che verifica le equazioni $f(0) = a$ ed $f(n+1) = H(n, f(n))$ per ogni $n$ nel suo dominio. Il caso $m = 0$ è ovvio. Basta considerare la funzione $\{(0, a)\}$ (ovvero la funzione che manda 0 in $a$). Supponendo per ipotesi induttiva che $f : \{x \in \omega : x \leq m\} \to A$ verifichi le equazioni (e sia l'unica che le verifichi), cerchiamo una funzione $g : \{x \in \omega : x \leq m+1\} \to A$ che verifichi le equazioni. Posto che $g$ esista, sugli elementi $x$ minori o uguali ad $m$ si deve necessariamente avere $g(x) = f(x)$ (per l'unicità fino ad $m$). Resta da definire $g(m+1)$. Siccome vogliamo che $g(m+1) = H(m, g(m))$, e visto che dobbiamo avere $g(m) = f(m)$, occorre necessariamente porre $g(m+1) = H(m, f(m))$. Questo dimostra che se $g$ esiste è unica. Per mostrare che esiste, basta considerare la funzione $g = f \cup \{(m+1, H(m, f(m)))\}$, ovvero la funzione $g$ che coincide con $f$ sugli elementi $\leq m$ e manda $m+1$ in $H(m, f(m))$.

Avendo dimostrato che, per ogni $m$, esiste una ed una sola funzione $f : \{x \in \omega : x \leq m\} \to A$ che verifica le equazioni ricorsive, possiamo trovarne una definita su tutto $\omega$ come segue. Definiamo $F : \omega \to A$ ponendo $F(n) = f(n)$ dove $f$ è l'unica funzione che verifica le equazioni ricorsive fino ad $n$. Il "dove" che appare nella definizione di $F$ può essere esplicitato come segue: $F$ è la classe di tutte le coppie $(n, a)$ tali che esiste una $f : \{x : x \leq n\} \to A$ tale che $f(n) = a$ ed $f$ verifica le equazioni ricorsive fino ad $n$. La $F : \omega \to A$ così defnita è a priori una funzione classe, tuttavia visto che il suo dominio $\omega$ è un insieme, essa è un insieme per l'assioma di rimpiazzamento.[6] □

[6] Se $A$ è un insieme non serve l'assioma di rimpiazzamento. In questo caso per dimostrare che $F$ è un insieme basta osservare che $F \subseteq \omega \times A$ e che se $A$ è un insieme $\omega \times A$ è un insieme.

**14.2 Esempio.** Possiamo definire per induzione sul secondo argomento la somma di numeri naturali nel modo seguente

$$x + 0 = x, \quad x + S(y) = S(x + y).$$

Per applicare il teorema di ricursione si fissa $x$ e si definisce per ricursione la funzione $f$ (che dipenderà dal parametro $x$) che manda $y$ in $x + y$. Basta porre $f(0) = x$ ed $f(S(n)) = S(f(n))$ (in questo caso la $H$ del Teorema 14.1 applicata ad $n, f(n)$ fornisce in output $S(f(n))$, senza utilizzare $n$ stesso).

Avendo definito la somma possiamo definire il prodotto per induzione sul secondo argomento nel modo seguente

$$x \cdot 0 = 0, \quad x \cdot S(y) = x \cdot y + x.$$

Analogamente avendo il prodotto possiamo definire per induzione l'esponenziale:

$$x^0 = 1, \quad x^{n+1} = x^n \cdot x.$$

Infine la funzione fattoriale: $0! = 1, \quad (n + 1)! = n! \cdot (n + 1)$.

**14.3 Esercizio.** Dati due numeri naturali $x, y$ con $x \leq y$, esiste uno ed un solo $z$ tale che $x + z = y$ e definiamo la sottrazione ponendo per definizione $y - x = z$.

# 15 Ricursione forte

Consideriamo ora un esempio differente:

**15.1 Esempio.** La successione di Fibonacci $F : \omega \to \omega$ è definita da $F(0) = 1$, $F(1) = 1$, $F(n + 2) = F(n + 1) + F(n)$.

Per dimostrare l'esistenza e l'unicità della funzione di Fibonacci il Teorema 14.1 non basta e abbiamo bisogno di un risultato più generale che ci consente di definire funzioni $f$ tali che $f(n)$ dipenda da più valori precedenti (nel caso di Fibonacci da due valori precedenti). In generale possiamo ammettere che $f(n)$ dipenda dall"intera successione $(f(i) : i < n)$ dei valori precedenti. Visto che tale successione non è altro che la restrizione di $f$ all'insieme $\{i : i < n\}$, la definizione di $f$ prende la forma $f(n) = H(n, f \restriction_{\{i:i<n\}})$. In particolare per $n = 0$ abbiamo $f(0) = H(0, \emptyset)$, quindi non abbiamo bisogno di specificare separatamente il valore di $f(0)$.

**15.2 Teorema.** *Sia $A$ una classe. Data una funzione $H \colon \omega \times V \to A$, esiste una ed una sola funzione $f \colon \omega \to A$ tale che*

$$f(n) = H(n, f \restriction_{\{i:i<n\}})$$

*per ogni $n \in \omega$.*

Notiamo che il secondo argomento di $H$ è una funzione $f \restriction_{\{i:i<n\}}$ da $n$ ad $A$, dove $n$ può variare. Quindi in generale $H$ riceve come secondo argomento una funzione da qualche $n \in \omega$ ad $A$. Per non stare a specificare con esattezza, per semplicità abbiamo assunto che $H$ sia una funzione con dominio $\omega \times V$.

*Dimostrazione.* In seguito dimostreremo un risultato ancora più generale. Diamo comunque un cenno di dimostrazione. Diciamo che una funzione $g$ è buona se esiste $m \in \omega$ tale che $\mathrm{dom}(g) = m$ e $g$ verifica l'equazione ricorsiva

$$g(n) = H(n, g\restriction_{\{i:i<n\}})$$

per ogni $n \in \mathrm{dom}(g)$. Per induzione si dimostra che per ogni $m$ esiste una ed una sola funzione buona con dominio $m$. In effetti se abbiamo una funzione buona con dominio $m$ l'equazione ricorsiva permette di estenderla ad $m+1$ in quanto ci fornisce una regola per calcolare il suo valore su $m+1$ a partire dai valori precedenti. Definiamo ora $f$ come l'unione di tutte le funzioni buone. Lasciamo al lettore la verifica che $f$ è una funzione da $\omega$ ad $A$ e verifica l'equazione ricorsiva. Si ricordi che per dimostrare che un'unione di funzioni è una funzione occorre dimostrare che a due a due esse coincidono nel loro dominio comune (l'intersezione dei due domini), ma questo è facile per la parte sull'unicità. □

# 16 Unicità a meno di isomorfismo dei numeri naturali

Abbiamo visto che i numeri naturali di von Neumann sono un modello degli assiomi di Peano ma potrebbero essercene altri, ad esempio quello ottenuto definendo lo zero come $\emptyset$ e il successore di $x$ come $\{x\}$.

**16.1 Teorema.** *Sia $(N', S', 0')$ un modello degli assiomi di Peano, non necessariamente uguale al modello $(\omega, S, 0)$ dei numeri naturali di von Neumann. Allora esiste una funzione biunivoca $h : \omega \to N'$.*

*Dimostrazione.* Definiamo per ricursione $h : \omega \to N'$ ponendo $h(0) = 0'$ e $h(S(n)) = S'(h(n))$. È facile dimostrare, ragionando per induzione, che $h$ è crescente, e quindi iniettiva. Per dimostrare che è surgettiva si consideri la sua immagine $\mathrm{im}(h) \subseteq N'$. Essa contiene $0'$ ed è ovviamente chiusa per $S'$, in quanto se $y = h(n)$, allora $S'(y) = h(S(n))$. Ne segue, per induzione in $(N', S', 0')$ (che ci è data dagli assiomi di Peano), che $\mathrm{im}(h) = N'$. □

Si noti che la $h$ definita nella dimostrazione non solo è biunivoca, ma è un "isomorfismo" tra $(\omega, S, 0)$ ed $(N', S', 0')$, ovvero manda 0 in $0'$ e preserva il successore, nel senso che se $m = S(n)$, allora $h(m) = S'(h(n))$.

In generale tutte le strutture matematiche sono sempre studiate "a meno di isomorfismo". Data una teoria assiomatica, essa non potrà mai avere un solo modello, in quanto insieme ad esso vi saranno tutti i modelli a lui isomorfi. Gli assiomi possono solo determinare i rapporti reciproci tra gli elementi del modello, ma non la natura degli elementi isolatamente presi, che quindi possono essere rimpiazzati con altri elementi mantenendo i rapporti reciproci (e in ciò consistono gli isomorfismi).

# 17 Assioma della scelta

L'assioma della scelta ha segnato la nascita della teoria assiomatica degli insiemi in due lavori di Zermelo del 1904 e del 1908. Inizialmente esso è stato accolto con grande scetticismo, ma oggi è accettato senza riserve dalla quasi totalità dei matematici.

**17.1 Assioma** (Assioma della scelta)**.** Dato un insieme $X$ i cui elementi sono insiemi non vuoti a due a due disgiunti, esiste un insieme $S$ che interseca ciascuno degli elementi di $X$ in un singolo elemento.

La motivazione per l'assioma è chiara: se gli insiemi della famiglia $X$ sono non vuoti, possiamo immaginare di scegliere idealmente un elemento in ciascun di loro per formare l'insieme $S$. L'assioma della scelta ha varie versioni equivalenti:

**17.2 Assioma** (Assioma della scelta, forma equivalente)**.** Data una famiglia $(X_i : i \in I)$ di insiemi non vuoti $X_i$, esiste una funzione $f$ che associa a ciascun $i \in I$ un elemento $f(i)$ di $X_i$.

Per dedurre questa seconda forma a partire dalla prima basta considerare gli insiemi disgiunti $X_i \times \{i\}$. Per la prima versione dell'assioma esiste un insieme $S$ che interseca ciascun $X_i \times \{i\}$ in un singolo punto $(a, i) \in X_i \times \{i\}$, ed è quindi sufficiente considerare la funzione $f$ che manda $i$ nell'unico $a$ tale che $(a, i) \in S$.

Nella formulazione appena data si ammette la possiblità che $f(i) \neq f(j)$ anche nei casi in cui $X_i = X_j$. Se insistiamo che la scelta dipenda solo dall'insieme $X_i$ e non dall'indice $i$, otteniamo la seguente versione che si dimostra equivalente alle precedenti:

**17.3 Assioma** (Assioma della scelta, forma equivalente)**.** Data una famiglia $\mathcal{F}$ di insiemi non vuoti, esiste una funzione $g$ che associa a ciascun $X \in \mathcal{F}$ un elemento $g(X) \in X$. In particolare, fissato un insieme non vuoto $A$, possiamo considerare la famiglia $\mathcal{F} = \mathcal{P}(A) \setminus \{\emptyset\}$ di tutti i sottoinsiemi non vuoti di $X$ ottenendo una funzione $g : \mathcal{P}(A) \setminus \{\emptyset\} \to A$ che associa a ciascun sottoinsieme non vuoto $X \subseteq A$ un elemento $g(A) \in A$.

In molti casi l'esistenza della funzione di scelta $g$ può essere dimostrata senza far ricorso all'assioma della scelta. Supponiamo ad esempio di prendere $A = \mathbb{N}$. In questo caso non serve l'assioma della scelta per mostrare l'esistenza di una funzione $g : \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\} \to \mathbb{N}$ tale che $g(X) \in X$ per ogni sottoinsieme non vuoto $X$ di $\mathbb{N}$. Basta infatti definire $g(X)$ come il minimo elemento di $X$ rispetto all'ordine $\leq$ di $\mathbb{N}$. Se però tentiamo di dimostrare l'esistenza di una funzione di scelta per i sottoinsiemi dell'insieme $\mathbb{R}$ dei numeri reali (che in seguito definiremo all'interno della teoria degli insiemi), ci rendiamo subito conto che la cosa non è così semplice. Vorremmo una funzione $g$ che dato un insieme non vuoto $X \subseteq \mathbb{R}$ restituisca un elemento $g(X) \in X$. Se $X$ è di una forma particolare, ad esempio un intervallo aperto con estremi $a, b \in \mathbb{R}$, basta prendere il punto di mezzo $\frac{a+b}{2}$, ma non essendo possibile dare una regola che funzioni per tutti gli $X$, l'unico modo per dimostrare l'esistenza della $g$ è usare l'assioma della scelta.

L'assioma della scelta è spesso usato per passare da una situazione in cui i quantificatori sono disposti nell'ordine $\forall\exists$, ad una in cui sono disposti nell'ordine $\exists\forall$, come nella formulazione seguente.

**17.4 Assioma** (Assioma della scelta, altra forma equivalente)**.** Siano $X, Y$ due insiemi e sia $R \subseteq X \times Y$ una relazione tra $X$ ed $Y$. Supponiamo che

$$(\forall x \in X)(\exists y \in Y)R(x, y).$$

Allora esiste $f : X \to Y$ tale che $(\forall x \in X)R(x, f(x))$.

Detto in altre parole l'assioma asserisce che ogni relazione $R$ include una funzione $f$ con lo stesso dominio. Si noti che dato $x \in X$ ci possono in genere essere molti $y \in Y$ con $xRy$. La funzione $f$ sceglie uno dei tanti $y$ in funzione di $x$. In generale non esiste un'unica funzione di scelta (a meno che la relazione $R$ sia essa stessa una funzione). L'assioma di scelta asserisce che ne esiste almeno una, e sapendo che esiste sta poi a noi "sceglierne" una, dove questo secondo passaggio può essere fatto in base alle leggi della logica.

Per dedurre la 17.4 dalla 17.2 basta considerare, per ciascun $x \in X$, l'insieme $Y_x = \{y : R(x, y)\}$. Otteniamo in tal modo una famiglia $(Y_x : x \in X)$ di insiemi non vuoti e possiamo considerare una funzione $f$ che associa a ciascun $x \in X$ un elemento di $Y_x$.

**17.5 Definizione.** Data una famiglia di insiemi $(X_i : i \in I)$ (vista come funzione che manda $i \in I$ in $X_i$) definiamo il prodotto cartesiano $\Pi_{i\in I}X_i$ come l'insieme di tutte le funzioni $a : I \to \bigcup_{i\in I} X_i$ tali che per ogni $i \in I$, $a(i) \in X_i$. Ogni elemento $a \in \Pi_{i\in I}X_i$ è pertanto una "$I$-upla" $(a(i) : i \in I)$ la cui $i$-esima coordinata è $a(i)$.

Il fatto che di tali $I$-uple ne esista almeno una è dato dalla 17.2. Otteniamo pertanto il seguente:

**17.6 Osservazione.** L'assioma della scelta equivale al seguente enunciato: per ogni famiglia $(X_i : i \in I)$ di insiemi non-vuoti, il prodotto cartesiano $\Pi_{i\in I}X_i$ è non vuoto.

Anche il seguente enunciato equivale all'assioma della scelta.

**17.7 Lemma.** *Data una funzione surgettiva $f : X \to Y$ tra due insiemi, esiste una funzione iniettiva $g : Y \to X$ tale che $f(g(y)) = y$ per ogni $y \in Y$ (diciamo che $g$ è una inversa destra di $f$).*

*Dimostrazione.* Dato $y \in Y$ consideriamo l'insieme non vuoto $X_y = \{x \in X : f(x) = y\}$. Per l'assioma della scelta esiste una funzione $g$ che associa a ciascun $y \in Y$ un elemento di $X_y$. □

Lasciamo al lettore la verifica dell'altro verso dell'equivalenza.

# 18 Numeri cardinali (nel senso di Frege)

**18.1 Definizione.** Dati due insiemi $X$ e $Y$, scriviamo $|X| = |Y|$ se esiste un funzione biunivoca da $X$ ad $Y$, e diciamo in tal caso che $X$ è *equipotente* ad $Y$, o che ha la stessa cardinalità di $Y$. Scriviamo $|X| \leq |Y|$ se esiste una funzione iniettiva da $X$ ad $Y$, o equivalentemente se $X$ è equipotente ad un sottoinsieme di $Y$. Infine scriviamo $|X| < |Y|$ se vale $|X| \leq |Y|$ ma $|X| \neq |Y|$, ovvero esiste una funzione iniettiva da $X$ ad $Y$ ma non ne esiste una, possibilmente diversa, che sia biunivoca.

L'uso delle notazioni $\leq$ e $<$ non è ancora pienamente giustificato in quanto dovremo dimostrare, per le relazioni appena definite, le proprietà degli ordini. La proprietà riflessiva $|X| \leq |X|$ e quella transitiva $|X| \leq |Y| \wedge |Y| \leq |Z| \to |X| \leq |Z|$, sono di facile verifica. Nel seguito dimostreremo la proprietà antisimmetrica $|X| \leq |Y| \wedge |Y| \leq |X| \to |X| = |Y|$ (Teorema di Cantor-Bernstein), e la totalità, ovvero il fatto che vale sempre una delle due alternative $|X| \leq |Y|$ o $|Y| \leq |X|$ (Corollario 35.3). Fino a che non le avremo dimostrate non potremo dunque usare queste ultime proprietà.

**18.2 Osservazione.** Un insieme $X$ può essere equipotente ad un suo sottoinsieme proprio. Ad esempio l'insieme dei numeri naturali è equipotente all'insieme dei numeri pari.

Osserviamo che nella Definizione 18.1 non abbiamo definito $|X|$, ma solo uguaglianze e disuguaglianze che coinvolgono tale notazione, quindi il segno di $=$ che compare nella definizione di $|X| = |Y|$ è per il momento solo un abuso di notazione.

**18.3 Definizione.** (Cardinali di Frege) Seguendo Frege possiamo definire $|X|$ come la classe i cui elementi sono gli insiemi equipotenti ad $X$. Chiamiamo $|X|$ la cardinalità di $X$ (nel senso di Frege). In questo modo $|X| = |Y|$ nel senso della Definizione 18.1, se effettivamente $|X|$ ed $|Y|$ sono uguali come classi, ovvero hanno gli stessi elementi. Questo giustifica l'uso del simbolo di uguaglianza. Per quanto riguarda il $\leq$, possiamo mantenere la Definizione 18.1, ma per mostrare che la definizione è ben posta occorre mostrare che se $|X| = |X'|$ e $|X| \leq |Y|$ allora $|X'| \leq |Y|$ (altrimenti $|X| \leq |Y|$ esprimerebbe solo un rapporto tra $X$ ed $Y$, e non tra $|X|$ e $|Y|$). Lasciamo al lettore le facili verifiche.

Osserviamo che, nella definizione di Frege, $|X|$ risulta una classe propria e non un insieme. Questo comporta certi svantaggi: ad esempio la collezione dei cardinali minori di un dato cardinale $|X|$ risulterebbe una "iperclasse" i cui elementi sono classi (anche se $X$ avesse un numero finito di elementi!). Nel seguito daremo una definizione alternativa della cardinalità di un insieme dovuta a von Neumann, in modo che $|X|$ risulti sempre un insieme, ma continuino a valere le proprietà espresse dalla 18.1. Per il momento useremo solo le proprietà espresse dalla 18.1 e quindi sarà indifferente quale definizione usare.

**18.4 Teorema.** *$|Y| \leq |X|$ se e solo se $Y$ è vuoto o esiste una funzione surgettiva $f$ da $X$ ad $Y$.*

*Dimostrazione del Teorema 18.4.* Un verso richiede l'assioma della scelta: se esiste una funzione surgettiva da $X$ ad $Y$ per l'assioma della scelta ne esiste una iniettiva nel verso opposto (Lemma 17.7), e dunque $|Y| \leq |X|$.

Per l'altro verso assumiamo $|Y| \leq |X|$. Per definizione esiste dunque una funzione iniettiva $g : Y \to X$. Assumendo che $Y$ non sia vuoto, fissiamo un $a \in Y$ e definiamo una funzione $f : X \to Y$ ponendo $f(y) = a$ se $y$ non è nell'immagine di $f$, e $f(y) = x$ se $y = g(x)$. La defizione è ben posta in quanto, per l'iniettività di $g$, ciò può capitare per un solo $x$. Abbiamo così ottenuto una $f : X \to Y$ surgettiva.[7] □

# 19 Teorema di Cantor-Bernstein

Nel prossimo teorema verifichiamo la proprietà antisimmetrica del $\leq$ tra cardinali.

**19.1 Teorema.** *Se due insiemi sono ciascuno in corrispondenza biunivoca con una parte dell'altro, allora si può trovare una corrispondenza biunivoca tra i due. In altre parole se $|A| \leq |B|$ e $|B| \leq |A|$, allora $|A| = |B|$.*

*Dimostrazione.* Siano $f\colon A \to B$ e $g\colon B \to A$ funzioni iniettive. Definiamo induttivamente $A_0 = A$, $B_0 = B$, $A_{n+1} = g(B_n)$ (= l'immagine di $g$ ristretta a $B_n$), $B_{n+1} = f(A_n)$. Otteniamo in tal modo due successioni decrescenti

$$A = A_0 \supseteq A_1 \supseteq A_2 \ldots,$$

$$B = B_0 \supseteq B_1 \supseteq B_2 \ldots$$

come si verifica facilmente per induzione (se decrescono fino ad $n$ decrescono anche al passo successivo). Si vede facilmente (posponiamo per il momento le verifiche) che per ogni $n$ la differenza $A_{2n} \setminus A_{2n+1}$ è in corrispondenza biunivoca, tramite $f$, con $B_{2n+1} \setminus B_{2n+2}$, e analogamente $B_{2n} \setminus B_{2n+1}$ è in corrispondenza biunivoca, tramite $g$, con $A_{2n+1} \setminus A_{2n+2}$. Mettendo insieme queste corrispondenze biunivoche ne otteniamo una da $\bigcup_n (A_n \setminus A_{n+1})$ a $\bigcup_n (B_n \setminus B_{n+1})$. Rimangono da gestire gli eventuali punti di $A$ e $B$ che non appartengono a queste unioni, ovvero i punti di $A_\infty = \bigcap_{n\in\omega} A_n$ e $B_\infty = \bigcap_{n\in\omega} B_n$. Si verifica però facilmente che la restrizione di $f$ a $A_\infty$ è una funzione biunivoca verso $B_\infty$ (e similmente $g$ è una corrispondenza biunivoca da $B_\infty$ in $A_\infty$). Otteniamo in tal modo una corrispondenza biunivoca da $A$ a $B$ definita per casi.

Veniamo ai dettagli: siccome $f$ è iniettiva e $B_{i+1}$ è l'immagine tramite $f$ di $A_i$, abbiamo $x \in A_i \iff x \in B_{i+1}$, e quindi in particolare $x \in A_{2n} \iff f(x) \in B_{2n+1}$. Similmente $x \notin A_{2n+1} \iff x \notin B_{2n+2}$. Quindi $f$ manda $A_{2n} \setminus A_{2n+1}$ biunivocamente in $B_{2n+1} \setminus B_{2n+2}$. Similmente $g$ manda $B_{2n} \setminus B_{2n+1}$ biunivocamente in $A_{2n+1} \setminus A_{2n+2}$. Se ora $x \in A_\infty$ e per assurdo $f(x) \notin B_\infty$, dovremmo avere $f(x) \notin B_n$ per qualche $n > 0$ e quindi $x \notin A_{n-1}$, il che è assurdo in quanto $x \in A_\infty$. □

[7] La possibilià di "scegliere" $a$ non richiede l'assioma della scelta, ma fa parte delle leggi logiche: se so che $\exists y (y \in Y)$ posso immaginare di "scegliere" un tale $y$ e dargli un nome.

Usando il teorema di Cantor-Bernstein si dimostra:

**19.2 Corollario.** *Se in una successione finita di disuguaglianze* $|A_1| \leq |A_2| \leq \ldots \leq |A_n|$ *abbiamo* $|A_n| = |A_1|$*, allora tutti gli* $A_i$ *hanno la stessa cardinalità.*

**19.3 Corollario.** *Se in una successione finita di disuguaglianze* $|A_1| \leq |A_2| \leq \ldots \leq |A_n|$ *c'è almeno una disuguaglianza stretta, allora* $|A_1| < |A_n|$*.*

*Dimostrazione.* Chiaramente $|A_1| \leq |A_n|$ e se avessimo $|A_1| = |A_n|$ per l'esercizio precedente tutti gli $A_i$ avrebbero la stessa cardinalità. □

Anche se ancora non abbiamo definito i numeri reali, propongo il seguente esercizio a chi li conosca già. Esso può essere risolto utilizzando il teorema di Cantor-Bernstein.

**19.4 Esercizio.** Si trovi una corrispondenza biunivoca tra un invervallo aperto e un intervallo chiuso dei numeri reali.

# 20 Insiemi finiti e numerabili

**20.1 Definizione.** Un insieme $X$ è finito se esiste $n \in \omega$ e una funzione biunivoca $f$ da $n$ ad $X$, ovvero $|n| = |X|$ (ricordiamo che $n = \{i : i < n\}$).

**20.2 Esercizio.** Dati $m, n \in \omega$, se $X$ ed $Y$ sono insiemi finiti disgiunti equipotenti ad $m$ ed $n$ rispettivamente, allora $X \cup Y$ è equipotente ad $m + n$.

Per risolvere l'esercizio si ricordi che $m+n$ è stato definito per ricursione sul secondo argomento. Si dovrà quindi procedere per induzione su $n$.

**20.3 Esercizio.** Se $X$ ed $Y$ sono insiemi finiti equipotenti ad $m$ ed $n$ rispettivamente, allora $X \times Y$ è equipotente ad $m \cdot n$.

**20.4 Lemma.** *Se* $X$ *è finito lo sono anche tutti i sottoinsiemi di* $X$*.*

*Dimostrazione.* L'ipotesi dice che $|X| = |n|$ per un certo $n \in \omega$. Posso quindi assumere $X = n$ e considero un sottoinsieme $Y$ di $n = \{i : i < n\}$. Ragiono per induzione su $n$. Il caso $n = 0$ è ovvio. Considero il caso $n = m + 1$. Per ipotesi induttiva $Y \cap m$ è finito. Dunque anche $Y$ è finito in quanto si ottiene da $Y \cap m$ aggiungendo al più un elemento (e posso quindi usare 20.2). □

In modo simile si dimostra:

**20.5 Esercizio.** Se $X$ è finito ed è equipotente ad $n$, allora per ogni $Y \subseteq X$ esiste $n' \leq n$ tale che $Y$ è equipotente ad $n'$.

**20.6 Lemma.** *Se* $X$ *è equipotente a* $n \in \omega$ *e* $Y$ *è un sottoinsieme proprio di* $X$*, allora* $Y$ *è equipotente a qualche* $n' < n$*.*

*Dimostrazione.* Possiamo assumere che $X = n$ e $Y$ sia un sottoinsieme proprio di $n$. Dimostriamo il nostro asserto per induzione su $n$. Se $n = 0$ la tesi vale a vuoto in quanto 0 non ha sottoinsiemi propri. Supponiamo dunque che $n = m+1$. Ci sono due casi. Se $Y = m$ non c'è nulla da dimostrare: la funzione identità è la bigezione cercata. Se invece $Y \neq m$, allora $Y \cap m$ è un sottoinsieme proprio di $m$. In questo secondo caso per ipotesi induttiva $Y \cap m$ è equipotente a qualche $m' < m$. Ma $Y$ si ottiene da $Y \cap m$ aggiungendo al più un elemento, e dunque $Y$ è equipotente ad $m'$ o ad $m'+1$, che in entrambi i casi è $< m+1$. □

Il seguente risultato è il cosiddetto "principio dei cassetti", o della piccionaia. Se $m < n$ e mettiamo $n$ oggetti in $m$ cassetti, almeno un cassetto deve contenere più di un oggetto.

**20.7 Lemma.** *Se $X$ è finito e $Y$ è un sottoinsieme proprio di $X$, allora $|Y| < |X|$.*

*Dimostrazione.* Alla luce del precedente risultato basta mostrare che se $m < n$ sono due elementi di $\omega$, allora non esiste una bigezione da $n$ ad $m$. Consideriamo per assurdo una tale bigezione $f : n \to m$. A meno di comporre $f$ con una permutazione di due elementi di $m$ con $f(m-1))$ possiamo supporre che $f$ mandi il massimo di $n$ nel massimo di $m$ (altrimenti ci riduciamo a questo caso scambiando di posto $f(m-1)$ con $m-1$). Togliendo i massimi di $n$ ed $m$ ci si riconduce al caso $n-1$ e si conclude per induzione. □

Grazie al principio dei cassetti, dato un insieme finito $X$, esiste un unico $n \in \omega$ in corrispondenza biunivoca con $X$, che possiamo chiamare "il numero degli elementi di $X$".

**20.8 Definizione.** Un insieme $X$ è numerabile se esiste una funzione biunivoca da $X$ all'insieme $\omega$ dei numeri naturali.

La cardinalità di un insieme numerabile viene indicata con il simbolo $\aleph_0$. Quindi $|\omega| = \aleph_0$.

Per gli insiemi infiniti non vale il principio dei cassetti:

**20.9 Osservazione.** Esistono sottoinsiemi propri di $\omega$ che hanno la stessa cardinalità di $\omega$, ad esempio i numeri pari.

**20.10 Esercizio.** Se $|X| \leq \aleph_0$, allora $X$ è finito o numerabile.

**20.11 Lemma.** *$\omega \times \omega$ è numerabile.*

*Dimostrazione.* Ordiniamo $\omega \times \omega$ ponendo $(x', y') < (x, y)$ se $\max\{x', y'\} < \max\{x, y\}$ oppure i massimi sono uguali e $y' < y$, oppure i massimi e le seconde componenti sono uguali e $x' < x$. In quest'ordine si vede facilmente l'insieme delle coppie strettamente minori di $(x, y)$ è finito, e per la precisione, posto $n = \max\{x, y\}$, esso è equipotente ad $n \cdot n + x$ se $x < y$, o ad $n \cdot n + x + y$ se $x \geq y$. Associando a $(x, y)$ questo valore, otteniamo una corrispondenza biunivoca da $\omega \times \omega$ ad $\omega$. □

Ci sono molte altre corrispondenze biunivoche che possono darsi da $\omega \times \omega$ ad $\omega$. Quella sopra proposta ha il vantaggio di potersi generalizzare con facilità agli "ordinali iniziali" che vedremo nel seguito.

**20.12 Esercizio.** L'unione e l'intersezione di due insiemi numerabili è numerabile. Il prodotto cartesiano di due insiemi numerabili è numerabile. In particolare $\omega \times \omega$ è numerabile.

In generale il seguente risultato ha bisogno dell'assioma della scelta.

**20.13 Teorema.** *Un'unione numerabile di insiemi di cardinalità $\leq \aleph_0$ ha cardinalità $\leq \aleph_0$.*

*Dimostrazione.* Per ogni $n \in \omega$ sia $A_n$ un insieme di cardinalità $\leq \aleph_0$. Dobbiamo mostrare che l'unione $\bigcup_{n\in\omega} A_n$ ha cardinalità $\leq \aleph_0$. Scegliamo, per ogni $n$, una funzione surgettiva $f_n \colon \omega \to A_n$ (che esiste in quanto $|A_n| \leq \aleph_0$). Consideriamo la funzione $f \colon \omega \times \omega \to \bigcup_n A_n$ che manda $(n, m)$ inf $f_n(m)$. Chiaramente $f$ è surgettiva, e poiché $|\omega \times \omega| = \aleph_0$ ne concludiamo che $|\bigcup_n A_n| \leq \aleph_0$. □

Osserviamo che la funzione $f \colon \omega\times\omega \to \bigcup_n A_n$ dipende dall'intera successione $(f_n : n \in \omega)$, per dimostrare l'esistenza della quale è in generale necessario l'assioma della scelta. La situazione è la seguente. Il fatto che, per ogni $n$, esista una funzione surgettiva $g : \omega \to A_n$ non richiede la scelta (in quanto segue dall'ipotesi che $A_n$ è numerabile). Tuttavia l'assioma della scelta viene usato per dimostrare l'esistenza della successione $(f_n : n \in \omega)$, vista come funzione che associa ad ogni $n \in \omega$ una funzione surgettiva $f_n : \omega \to A_n$. Naturalmente se abbiamo maggiori informazioni sugli $A_n$ (come spesso accade nei casi concreti), possiamo essere in grado di definire la successione $(f_n : n \in \omega)$ senza utilizzare l'assioma della scelta.

Anche per il seguente teorema abbiamo bisogno dell'assioma della scelta.

**20.14 Teorema.** *Ogni insieme infinito $A$ ha un sottoinsieme numerabile. Quindi $\aleph_0$ è minore o uguale di ogni altro cardinale infinito.*

*Dimostrazione.* Possiamo definiamo induttivamente (grazie al teorema di ricursione) una successione $(a_n \mid n \in \omega)$ prendendo come $a_0$ un qualsiasi elemento di $A$, e "scegliendo" come $a_{n+1}$ un elemento dell'insieme non vuoto $A\setminus\{a_i \mid i \leq n\}$. Si noti che l'insieme è effettivamente non vuoto altrimenti $A$ sarebbe finito. Per formalizzare la dimostrazione possiamo supporre che $a_{n+1}$ sia l'elemento dell'insieme $A \setminus \{a_i \mid i \leq n\}$ fornito da una prefissata funzione di scelta $g : \mathcal{P}(A) \setminus \{\emptyset\} \to A$. □

**20.15 Osservazione.** Per essere precisi occorrerebbe definire $a_{n+1}$ distinguendo due casi: se l'insieme $A\setminus\{a_i \mid i \leq n\}$ è non vuoto, poniamo $a_{n+1} = g(A\setminus\{a_i \mid i \leq n\})$, e nel caso contrario definiamo $a_{n+1} = b$ dove $b$ è un qualsiasi oggetto non appartenente ad $A$ fissato all'inizio. In questo modo la successione $(a_n : n \in \omega)$ risulta in ogni caso ben definita (come funzione da $\omega$ ad $A \cup \{b\}$) grazie al teorema di ricursione, e successivamente sarà possibile dimostrare per induzione che in effetti il valore $b$ non è mai assunto. In tal modo evitiamo di mischiare

definizioni e dimostrazioni. Lo stesso problema si porrà altre volte nel seguito, ma una volta capito il trucco possiamo sorvolare su questi dettagli.

**20.16 Esercizio.** Si dimostri, senza usare l'assioma della scelta, che se $(X_i : i \in I)$ è una famiglia di insiemi numerabili parametrizzata da un insieme finito $I$, allora $\bigcup_{i\in I} X_i$ è numerabile.

Suggerimento: si proceda per induzione sul numero di elementi di $I$.

# 21 Teorema di Cantor

**21.1 Teorema** (Cantor)**.** *Per ogni insieme $X$, $|\mathcal{P}(X)| > |X|$.*

*Dimostrazione.* Per dimostrare $|X| \leq \mathcal{P}(X)$ basta considerare la funzione iniettiva che associa ad ogni $x \in X$ il suo singoletto $\{x\} \in \mathcal{P}(X)$. Rimane da dimostrare che non esiste una funzione biunivoca da $X$ a $\mathcal{P}(X)$. Mostreremo che non ne esiste neppure una che sia semplicemente surgettiva. Supponiamo dunque di avere una funzione che associa ad ogni elemento $a \in X$ un sottoinsieme $X_a$ di $X$. Basta mostrare che la famiglia degli $X_a$ non esaurisce tutte le parti di $X$. Per ogni $a \in X$ possiamo chiederci se $a$ appartenga o no ad $X_a$. Consideriamo l'insieme $D = \{a \in X : a \notin X_a\}$. Tale $D$ è un sottoinsieme di $X$. Se appartenesse alla famiglia $\{X_a : a \in X\}$ ci sarebbe un $u \in X$ tale che $D = X_u$. Ma $u \in D$ se e solo se $u \notin X_u$. Assurdo. □

Dal teorema di Cantor segue in particolare che $\mathcal{P}(\omega)$ non è numerabile.

# 22 Operazioni sui numeri cardinali

**22.1 Lemma.** *Dati due insiemi $A$ e $B$, la classe $\{f \mid f : A \to B\}$ delle funzioni da $A$ a $B$, è un insieme.*

*Dimostrazione.* Tale classe è inclusa in $\mathcal{P}(A \times B)$. □

**22.2 Definizione.** Dati due insiemi $A$ e $B$ definiamo la loro unione disgiunta $A \sqcup B$ come $A \times \{0\} \cup B \times \{1\}$. Definiamo somma, prodotto, ed esponenziazione tra cardinali nel modo seguente:

1. $|A| + |B| = |A \sqcup B|$;
2. $|A| \cdot |B| = |A \times B|$;
3. $|A|^{|B|} = |\{f \mid f : B \to A\}|$.

**22.3 Esercizio.** Si dimostri che le definizioni sono ben poste. Ad esempio nel caso della somma occorre dimostrare che se $A'$ è equipotente ad $A$ e $B'$ è equipotente a $B$, allora $A \sqcup B$ è equipotente a $A' \sqcup B'$.

Il seguente esercizio mostra che in generale non è possibile definire la sottrazione di cardinali, sebbene si possa fare per i cardinali finiti.

**22.4 Esercizio.** Si dimostri che $|A| + |B| = |A| + |C|$ non implica in generale $|B| = |C|$.

**22.5 Proposizione.** $|\mathcal{P}(X)| = 2^{|X|}$ *dove qui* 2 *indica la cardinalità dell'insieme* $2 = \{0, 1\}$.

*Dimostrazione.* Dobbiamo trovare una corrispondenza biunivoca tra $\mathcal{P}(X)$ e l'insieme $\{f : f : X \to 2\}$. A tal fine basta associare a ciascun sottoinsieme $A$ di $X$ la sua funzione caratteristica $\chi_A : X \to 2$ definita da: $\chi_A(x) = 0$ se $x \notin A$ e $\chi_A(x) = 1$ se $x \in A$. □

Dal teorema di Cantor otteniamo:

**22.6 Corollario.** $2^{|X|} > |X|$.

In particolare $2^{\aleph_0} > \aleph_0$. Una dimostrazione diretta di quest'ultimo risultato si può ottenere come segue. Data una famiglia di funzioni $f_n : \omega \to 2$ parametrizzata da numeri naturali $n \in \omega$, basta dimostrare che esiste una funzione $f : \omega \to 2$ diversa da tutte le $f_n$. Basta a tal fine considerare la funzione diagonale $\delta : \omega \to 2$ definita da $\delta(n) = 0$ se $f_n(n) = 1$ e $\delta(n) = 1$ se $f_n(n) = 0$. Tale $\delta$ differisce da $f_n$ almeno per l'argomento $n$, e quindi è diversa da ciascuna $f_n$.

**22.7 Esercizio.** Si dimostri che valgono le seguenti proprietà trovando le opportune corrispondenze biunivoche.

1. (proprietà distributiva) $|C| \cdot (|A| + |B|) = |C| \cdot |A| + |C| \cdot |B|$,
2. $|A|^{|B|+|C|} = |A|^{|B|} \cdot |A|^{|C|}$,
3. $|A|^{|B|\cdot|C|} = (|A|^{|B|})^{|C|}$.

*Dimostrazione.* (Cenno) Scriviamo $Fun(X, Y)$ per indicare l'insieme delle funzioni da $X$ ad $Y$. Per il punto 3 osserviamo che, data una funzione binaria $g : B \times C \to A$, possiamo scrivere $g(b, c) = h(c)(b)$ dove $h$ è una funzione unaria che applicata a $c \in C$ fornisce in output una funzione $h(c) : B \to A$, che a sua volta applicata a $b \in B$ fornisce in output $g(b, c) \in A$. La corrispondenza $g \mapsto h$ è una bigezione da $Fun(B \times C, A)$ a $Fun(C, Fun(B, A))$, come richiesto per il punto 3. □

# 23 Relazioni di equivalenza

**23.1 Definizione.** Una relaziona di equivalenza $E$ su un insieme $X$ è una relazione binaria $E \subseteq X \times X$ tale che per ogni $x, y, z \in X$ si ha: $xEy \wedge yEz \to xEz$ (transitività); $xEy \leftrightarrow yEx$ (simmetria); $xEx$ (riflessività). La classe di equivalenza di $x \in X$ è l'insieme $[x]_E = \{y \in X : xEy\}$. L'insieme quoziente $X/E$ è l'insieme $\{[x]_E : x \in X\}$ delle classi di equivalenza.

Esiste una funzione surgettiva $f : X \to X/E$ che manda ciascun $x \in X$ nella sua classe $[x]_E$, e dunque per l'assioma di rimpiazzamento $X/E$ è un insieme. Lo stesso ragionamento mostra che $|X/E| \leq |X|$.

**23.2 Esercizio.** Si dimostri che $X/E$ è un insieme senza usare l'assioma di rimpiazzamento, ma usando in suo luogo l'assioma delle parti.

**23.3 Definizione.** Una partizione di un insieme $X$ è una famiglia di insiemi a due a due disgiunti la cui unione è $X$.

**23.4 Esercizio.** Data una relazione di equivalenza $E$ su $X$ le classi di equivalenza $\{[x]_E : x \in X\}$ formano una partizione di $X$. Viceversa, data una partizione $P$ di $X$, esiste una ed una sola relazione di equivalenza $E$ su $X$ tale che $P$ sia la famiglia delle classi di equivalenza di $E$.

# 24 Numeri interi e razionali

**24.1 Definizione.** A partire dai numeri naturali $\mathbb{N}$ costruiamo i numeri interi $\mathbb{Z}$ come segue. Sia $E$ la relazione di equivalenza su $\mathbb{N} \times \mathbb{N}$ così definita: $(n, m)E(n', m')$ se e solo se $n + m' = m + n'$, e si definisca $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/E$. L'idea è che $[(n, m)]_E$ corrisponde al numero intero $n - m$. Possiamo mandare iniettivamente $\mathbb{N}$ in $\mathbb{Z}$ associando ad $n \in \mathbb{N}$ la classe $[(n, 0)]_E \in \mathbb{Z}$. In questo modo $\mathbb{Z}$ non include letteralmente $\mathbb{N}$, ma solo la sua immagine tramite la funzione suddetta. Tuttavia per abuso di notazione quando si parla di $\mathbb{Z}$ si identifica $\mathbb{N}$ con la sua immagine in $\mathbb{Z}$. Come esercizio si definiscano la somma e il prodotto e l'ordine in $\mathbb{Z}$ in modo che valgano le usuali proprietà.

**24.2 Definizione.** Definiamo l'insieme $\mathbb{Q}$ dei numeri razionali nel modo seguente. Sia $E$ la relazione di equivalenza su $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ così definita: $(n, m)E(n', m')$ se e solo se $n \cdot m' = m \cdot n'$. Si definisca $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/E$. L'idea è che $[(n, m)]_E$ corrisponde al numero razionale $n/m$. Come esercizio si definiscano la somma e il prodotto e l'ordine in $\mathbb{Q}$ in modo che valgano le usuali proprietà. Si può immergere $\mathbb{Z}$ in $\mathbb{Q}$ tramite la funzione iniettiva che manda $z \in \mathbb{Z}$ in $[(z, 1)]_E \in \mathbb{Q}$.

**24.3 Lemma.** $|\,\mathbb{Q}\,| = |\,\mathbb{Z}\,| = |\,\mathbb{N}\,| = \aleph_0$.

*Dimostrazione.* Tutto segue facilmente dal fatto che l'unione e il prodotto cartesiano di due insiemi numerabili è numerabile e che un quoziente di un insieme numerabile è numerabile (se non è finito). □

# 25 Numeri reali

Diamo per nota la nozione di campo ordinato. La definizione si può trovare in ogni testo introduttivo di algebra (o sul web). Definiremo i numeri reali in termini insiemistici in modo che si abbia:

**25.1 Fatto.** *I numeri reali costituiscono un campo ordinato $\mathbb{R}$ che contiene $\mathbb{Q}$ come sottocampo e verifica le seguenti proprietà.*

1. *(Assioma di Archimede) Il sottoinsieme $\mathbb{Q}$ dei numeri razionali è denso in $\mathbb{R}$, ovvero tra due elementi di $\mathbb{R}$ c'è sempre un elemento di $\mathbb{Q}$.*
2. *(Assioma di continuità) Ogni insieme $X \subseteq \mathbb{R}$ limitato superiormente ha un estremo superiore (ovvero tra gli elementi maggiori di ogni elemento di $X$ ve ne è uno minore di tutti gli altri).*

Usiamo le seguenti abbreviazioni: $\aleph_0 = |\omega|$, $\mathbf{c} = |\mathbb{R}|$. Dall'assioma di Archimede otteniamo:

**25.2 Lemma.** $\mathbf{c} \leq 2^{\aleph_0}$.

*Dimostrazione.* Consideriamo la funzione $f\colon \mathbb{R} \to \mathcal{P}(\mathbb{Q})$ che associa ad ogni $r \in \mathbb{R}$ l'insieme $\{x \in \mathbb{Q} \mid x < r\}$. La funzione $f$ è iniettiva perché i razionali sono densi in $\mathbb{R}$. Ne segue che $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})| = 2^{\aleph_0}$. □

Dall'assioma di continuità otteniamo:

**25.3 Lemma.** $2^{\aleph_0} \leq \mathbf{c}$.

*Dimostrazione.* Data una successione binaria $a = (a_i | i \in \mathbb{N})$ (con $a_i \in \{0, 1\}$ per ogni $i$) associamo ad $a$ il numero reale $x_a = \Sigma_{i \in \mathbb{N}} a_i 1/10^i$ (definito come l'estremo superiore al variare di $n$ delle somme parziali finite $\Sigma_{i \leq n} a_i 1/10^i$). La funzione che manda $a$ in $x_a$ è iniettiva. Siccome la cardinalità dell'insieme delle successioni binarie è $2^{\aleph_0}$, otteniamo la disuguaglianza cercata (attenzione: in generale un numero reale può avere due sviluppi decimali diversi, ma questo può capitare solo se uno degli sviluppi finisce con un 9 periodico, mentre noi ci siamo limitati a sviluppi in cui compaiono solo le cifre 0 ed 1). □

Mettendo insieme le due disuguaglianze otteniamo:

**25.4 Teorema.** $\mathbf{c} = 2^{\aleph_0}$.

Vogliamo dimostrare che nel nostro universo di insiemi $V$ esiste effettivamente un campo ordinato $\mathbb{R}$ che verifica gli assiomi di continuità e di Archimede.

**25.5 Definizione.** Definiamo $\mathbb{R}$ in termini insiemistici come segue. Diciamo che un sottoinsieme $X$ di $\mathbb{Q}$ è un taglio di Dedekind se verifica le seguenti proprietà: i) ogniqualvolta $X$ contiene un dato razionale contiene anche tutti quelli minori di lui; (ii) $X$ è limitato superiormente, ovvero esiste un razionale $q$ (dipendente da $X$) tale che tutti gli elementi di $X$ sono minori di $q$; (iii) $X$ non ha un massimo. Definiamo $\mathbb{R}$ come l'insieme dei tagli di Dedekind di $\mathbb{Q}$. Definiamo l'ordine $\leq$ tra numeri reali come l'inclusione tra tagli di Dedekind. L'idea è la seguente: visto che vogliamo che una copia isomorfa di $\mathbb{Q}$ sia inclusa in $\mathbb{R}$, identifichiamo $q \in \mathbb{Q}$ con il taglio di Dedekind dei numeri razionali $< q$. Chiamiamoli "tagli razionali". I numeri irrazionali di $\mathbb{R}$ sono i tagli di Dedekind che non sono razionali. Ad esempio $\sqrt{2}$ sarà il taglio costituito da tutti i razionali

negativi e da tutti quelli positivi il cui quadrato è $< 2$. La somma $X + Y$ di due tagli di Dedekind è il taglio costituito da tutte le somme $x + y$ al variare di $x \in X$ e $y \in Y$. Lasciamo al lettore l'esercizio di definire il prodotto su $\mathbb{R}$: occorrerà distinguere alcuni casi a seconda che i numeri siano positivi o negativi.

A rigore l'$\mathbb{R}$ costruito con i tagli di Dedekind non include $\mathbb{Q}$ ma solo la sua immagine tramite la funzione iniettiva che manda $q \in \mathbb{Q}$ in $q_{\mathbb{R}} = \{x \in \mathbb{Q} : x < q\} \in \mathbb{R}$. Tuttavia potremmo ridefinire $\mathbb{R}$ in modo che contenga letteralmente $\mathbb{Q}$. Basta sostituire ciascun $q_{\mathbb{R}} \in \mathbb{R}$ con il corrispondente $q \in \mathbb{Q}$. Questo rende però le definizioni più complicate. Risulta più comodo, quando si parla di $\mathbb{R}$, pensare a $\mathbb{Q}$ come all'insieme dei $q_{\mathbb{R}}$, con le operazioni definite copiando quelle di $\mathbb{Q}$. Stessi ragionamenti valgono per le "inclusioni" $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

**25.6 Esercizio.** I numeri reali $\mathbb{R}$ definiti come sopra, e dotati delle operazioni di somma e prodotto, sono un campo ordinato che verifica gli assiomi di archimede e di continuità.

**25.7 Lemma.** *Sia $X$ un insieme infinito. Allora $|X| + \aleph_0 = |X|$.*

*Dimostrazione.* Siccome $X$ è infinito, $\aleph_0 \leq |X|$ (per 20.14). Possiamo dunque scrivere $X = A \cup N$ con $N$ numerabile e disgiunto da $A$. Chiaramente $|X| = |A| + \aleph_0$. Ne segue che $|X| + \aleph_0 = (|A| + \aleph_0) + \aleph_0 = |A| + (\aleph_0 + \aleph_0) = |A| + \aleph_0 = |X|$. □

**25.8 Teorema.** *L'insieme dei numeri irrazionali ha cardinalità* $\mathbf{c}$.

*Dimostrazione.* L'insieme $\mathbb{R} \setminus \mathbb{Q}$ dei numeri irrazionali è infinito in quanto contiene $\{\sqrt{2} + q : q \in \mathbb{Q}\}$. Per il Lemma 25.7 $|\,\mathbb{R} \setminus \mathbb{Q}\,| + \aleph_0 = |\,\mathbb{R} \setminus \mathbb{Q}\,|$. D'altra parte $|\,\mathbb{R} \setminus \mathbb{Q}\,| + \aleph_0 = |\,\mathbb{R} \setminus \mathbb{Q}\,| + |\,\mathbb{Q}\,| = |\,\mathbb{R}\,|$. □

In modo analogo si dimostra:

**25.9 Lemma.** *Se da un insieme $X$ più che numerabile togliamo un insieme numerabile $N \subseteq X$, otteniamo un insieme $X \setminus N$ della stessa cardinalità di $X$.*

*Dimostrazione.* $X \setminus N$ è infinito, altrimenti $X = (X \setminus N) \cup N$ sarebbe numerabile. D'altra parte $|X| = |X \setminus N| + |N| = |X \setminus N| + \aleph_0$ e per il Lemma 25.7 possiamo concludere che $|X| = |X \setminus N|$. □

**25.10 Esercizio.** L'insieme dei numeri reali algebrici è numerabile (un numero reale si dice algebrico se è uno zero di un polinomio a coefficienti in $\mathbb{Q}$). L'insieme dei numeri reali trascendenti (=non algebrici) ha cardinalià $\mathbf{c}$.

*Dimostrazione.* Un polinomio a coefficienti di $\mathbb{Q}$ di grado $\leq n$ è determinato dalla successione finita dei suoi coefficienti, che sono $n+1$. Ne segue che l'insieme dei polinomi di grado $n$ ha cardinalità $|\,\mathbb{Q}^{n+1}\,| = \aleph_0$. Al variare di $n$ otteniamo un'unione numerabile di insiemi numerabili, quindi i polinomi sono in quantità numerabile. D'altra parte ogni polinomio ha un numero finito di zeri. I numeri algebrici si ottengono dunque come unione numerabile di insiemi finiti e formano quindi un insieme numerabile. Il complemento è pertanto della cardinalità del continuo per il Lemma 25.9. □

Il seguente esercizio fornisce una seconda dimostrazione del fatto che $|\mathbb{R}| \geq 2^{\aleph_0}$ che non usa gli sviluppi decimali ma solo la completezza dell'ordine $<$ su $\mathbb{R}$.

**25.11 Esercizio.** Sia $(X, \leq)$ un insieme totalmente ordinato tale che tra ogni due punti ce ne é sempre un terzo e ogni sottoinsieme $A \subseteq X$ limitato superiormente ha un estremo superiore. Si dimostri che, se $X$ ha almeno due elementi, allora $|X| \geq 2^{\aleph_0}$.

*Dimostrazione.* (Suggerimento) Si costruisca entro $X$ una sorta di "insieme di Cantor" (sul quale non dovrebbe essere difficile documentarsi), e si trovi una funzione iniettiva dall'insieme delle funzioni $f : \omega \to 2$ verso l'insieme di Cantor. □

# 26 Buoni ordini

**26.1 Definizione.** Una relazione binaria $\leq$ su un insieme (o una classe) $A$ si dice un ordine parziale se per ogni $x, y, z \in A$ si ha $x \leq x$ (proprietà riflessiva), $x \leq y \wedge y \leq z \to x \leq z$ (proprietà transitiva), $x \leq y \wedge y \leq x \to x = y$ (proprietà antisimmetrica). Un ordine totale è un ordine parziale tale che per ogni $x, y \in A$ si ha $x \leq y \vee y \leq x$.

**26.2 Esempio.** L'inclusione $\subseteq$ tra insiemi è un ordine parziale, mentre la relazione d'ordine $\leq$ sui numeri naturali è un ordine totale. La relazione di appartenenza $\in$ tra insiemi non è un ordine parziale perché ad esempio non verifica la proprietà transitiva.

Dato un ordine parziale $(A, \leq)$ e dati $x, y \in A$ definiamo una relazione $<$ (minore stretto) come segue

$$x < y \iff x \leq y \wedge x \neq y. \tag{1}$$

Osserviamo che

$$x \leq y \iff x < y \vee x = y \tag{2}$$

Quindi da $\leq$ possiamo ottenere $<$ e viceversa.

Si verifica che $<$ gode della proprietà transitiva $x < y \wedge y < z \to x < z$ e antiriflessiva $x \not< x$. Diciamo che $(A, <)$ è un ordine parziale stretto (o irriflessivo) quando verifica queste proprietà. Si ha che $(A, \leq)$ è un ordine totale se e solo se per l'ordine stretto $(A, <)$ ad esso associato vale la proprietà $x < y \vee x = y \vee y < x$. In tal caso diciamo che $(A, <)$ è un ordine stretto totale.

Talvolta ometteremo la parola "stretto" lasciando che sia la scelta del simbolo $\leq$ oppure $<$ a chiarire se si tratti di un ordine o di un ordine stretto.

**26.3 Definizione.** Un ordine totale $(A, \leq)$ si dice un buon ordine, o un insieme bene ordinato, se ogni sottoinsieme non vuoto $X$ di $A$ ha un minimo, ovvero un elemento $a$ tale $\forall x \in A\ a \leq x$.

Se $(A, \leq)$ è un buon ordine e $<$ è la relazione d'ordine stretto corrispondente a $\leq$ diremo che $(A, <)$ è un buon ordine stretto, o irriflessivo.

**26.4 Definizione.** Dato un ordine totale $(A, \leq)$, un sottoinsieme $J$ di $A$ si dice un *segmento iniziale* se ogni elemento di $A$ che sia minore di qualche elemento di $J$ appartiene esso stesso a $J$. Equivalentemente, $J$ è un segmento iniziale di $A$ se ogni elemento di $A$ che non appartiene a $J$ è maggiore di tutti gli elementi di $J$. Un segmento iniziale proprio di $A$ è un segmento iniziale che non coincide con $A$.

**26.5 Esercizio.** Se $(A, \leq)$ è un buon ordine e $J$ è un suo segmento proprio, allora esiste un $a \in A$ tale che $J = \{x \in A : x < a\}$. Ciò non è in generale vero se $(A, \leq)$ è un ordine totale che non sia un buon ordine (si consideri un insieme di numeri razionali senza un estremo superiore razionale).

Per ora gli unici buoni ordini che abbiamo incontrato sono i numeri naturali (con l'usuale ordine) e gli ordini totali con un numero finito di elementi. Per trovare altri esempi diamo le seguenti definizioni.

**26.6 Definizione.** (Somma di ordini) Dati due ordini totali $(A, \leq_A)$ e $(B, \leq_B)$ definiamo un nuovo ordine totale $(A + B, \leq) = (A, \leq_A) + (B, \leq_B)$ come segue. Il dominio $A+B$ è definito come $A \times \{0\} \cup B \times \{1\}$. L'ordine su $A+B$ è definito stabilendo che $(a, 0) < (b, 1)$ per ogni $a \in A$ e $b \in B$, mentre per coppie con la stessa seconda componente si segue l'ordine delle prime componenti rispetto agli ordini $\leq_A$ e $\leq_B$ (cioè $(a, 0) \leq (a', 0)$ se $a \leq_A a'$ e $(b, 1) \leq (b', 1)$ se $b \leq_B b'$).

**26.7 Esercizio.** Si mostri che se $(A, \leq_A)$ e $(B, \leq_B)$ sono buoni ordini anche $(A, \leq_A) + (B, \leq_B)$ lo è.

**26.8 Definizione.** (Prodotto lessicografico) Dati due ordini totali $(A, \leq_A)$ e $(B, \leq_B)$ definiamo un nuovo ordine $(A \times B, \leq) = (A, \leq_A) \times (B, \leq_B)$ come segue. Il dominio $A \times B$ è il prodotto cartesiano costituito da tutte le coppie $(a, b)$ con $a \in A$ e $b \in B$. Ordiniamo tali coppie confrontando innanzitutto le seconde componenti secondo l'ordine di $B$, e a parità di seconde componenti confrontando le prime componenti secondo l'ordine di $A$. Formalmente: $(a, b) < (a', b')$ se $b <_B b'$ oppure se $b = b'$ e $a <_A a'$.

**26.9 Esercizio.** Si mostri che se $(A, \leq_A)$ e $(B, \leq_B)$ sono buoni ordini, anche il loro prodotto lessicografico $(A \times B, \leq)$ lo è.

**26.10 Definizione.** Sia $(A, \leq)$ un buon ordine e siano $x, y \in A$. Diciamo che $y$ è il successore immediato di $x$ se $x < y$ e non esiste alcun $z \in A$ con $x < z < y$. In questo caso diciamo anche che $x$ è il precedessore immediato di $y$. Gli elementi di $A$ sono di tre tipi: 1) Il minimo di $A$; 2) Gli elementi successore, definiti come quelli che hanno un predecessore immediato; 3) Gli elementi limite, ovvero quelli diversi dal minimo che non hanno predecessore immediato.

**26.11 Osservazione.** Dato un buon ordine $(A, \leq)$ senza un massimo, ogni elemento ha un successore immediato; basta infatti considerare il minimo elemento tra quelli maggiori di $x$. Si noti anche che se $x \in A$ è un elemento limite, allora $x$ è l'estremo superiore dell'insieme degli elementi strettamente minori di $x$.

**26.12 Esercizio.** In $(\mathbb{N}, \leq) + (\mathbb{N}, \leq)$ ogni elemento ha un successore immediato, e ci sono esattamente due elementi che non hanno predecessore immediato, di cui uno è il minimo e l'altro è un elemento limite.

In $(\mathbb{N}, \leq) \times (\mathbb{N}, \leq)$, con l'ordine lessicografico, vi sono infiniti elementi limite.

# 27 Tipi d'ordine

**27.1 Definizione.** Dati due insiemi totalmente ordinati $(A, \leq_A)$ e $(B, \leq_B)$, una funzione $f\colon A \to B$ si dice crescente se $x < y$ implica $fx < fy$ per ogni $x, y \in A$. Se $f$ è anche biunivoca diremo che $f$ è un isomorfismo.

Si noti che una funzione crescente è necessariamente iniettiva e che nella definizione di funzione crescente possiamo equivalentemente richiedere la doppia implicazione: $x < y$ se e solo se $fx < fy$.

**27.2 Definizione** (Tipo d'ordine)**.** Se esiste un isomorfismo $f : (A, \leq_A) \to (B, \leq_B)$, diremo che $(A, \leq_A)$ e $(B, \leq_B)$ hanno lo stesso tipo d'ordine.

Ad esempio i numeri naturali con l'usuale ordinamento hanno lo stesso tipo d'ordine del sottoinsieme dei numeri pari.

**27.3 Lemma.** *Se $(W, \leq)$ è un buon ordinamento e $f\colon W \to W$ è una funzione crescente (cioè $x < y$ implica $fx < fy$), allora $f(x) \geq x$ per ogni $x \in W$.*

*Dimostrazione.* Supponiamo che $fx < x$ per qualche $x$ e sia $z$ il minimo di tali $x$. In particolare $fz < z$. Poichè $f$ è crescente, $ffz < fz$. Ma allora l'elemento $w = fz$ contraddice la minimalità di $z$. □

**27.4 Lemma.** *Sia $(A, \leq)$ un buon ordine e sia $B \subseteq A$ un sottoinsieme superiormente limitato di $A$. Allora $(A, \leq)$ non è isomorfo a $(B, \leq\restriction_B)$.*

*Dimostrazione.* Sia $a$ un elemento di $A$ maggiore di tutti gli elementi di $B$. Se $f : (A, \leq) \to (B, \leq\restriction_B)$ fosse un isomorfismo, allora in particolare $f$ sarebbe una funzione crescente da $A$ ad $A$, e quindi per il Lemma 27.3 $f(a) \geq a$. Questo è assurdo perché $f(a) \in B$ e gli elementi di $B$ sono tutti minori di $a$. □

**27.5 Definizione.** Dati due insieme bene ordinati $(A, \leq_A)$ e $(B, \leq_B)$, Se esiste un isomorfismo da $(A, \leq_A)$ ad un segmento iniziale proprio di $(B, \leq_B)$, diremo che il tipo d'ordine di $(A, \leq_A)$ è strettamente minore di quello di $(B, \leq_B)$.

Per il lemma precedente, il tipo d'ordine di un insieme bene ordinato $(A, \leq_A)$ non è mai strettamente minore di se stesso, quindi la terminologia è coerente. Nel seguito dimostreremo che i tipi d'ordine di insiemi bene ordinati sono sempre confrontabili: due insiemi bene ordinati o sono isomorfi o uno dei due è isomorfo ad un segmento iniziale proprio dell'altro.

Possiamo provvisoriamente definire i numeri ordinali come i tipi d'ordine degli insiemi bene ordinati, dove il tipo d'ordine di un insieme bene ordinato $(X, \leq)$ è la classe di equivalenza di tutti i buoni ordini isomorfi ad $(X, \leq)$.

Nel seguito definiremo dei particolari buoni ordini chiamati "ordinali di von Neumann" e vedremo che ve ne è esattamente uno in ogni classe di equivalenza. Potremo allora ridefinire il tipo d'ordine di $(X, \leq)$ come l'unico ordinale di von Neumann isomorfo ad $(X, \leq)$.

# 28 Insiemi transitivi

Per definire gli ordinali di von Neumann abbiamo bisogno della nozione di insieme transitivo.

**28.1 Definizione.** Un insieme $\alpha$ si dice transitivo se per ogni $x, y$ con $x \in y \in \alpha$ si ha $x \in \alpha$. Equivalentemente $\alpha$ è transitivo se $x \in \alpha \to x \subseteq \alpha$. Un'altra definizione equivalente è: $\alpha$ è transitivo se $\bigcup \alpha \subseteq \alpha$.

**28.2 Teorema.** *Sia $X$ un insieme. Allora esiste un insieme transitivo $Y$ con $X \subseteq Y$. Inoltre tra tutti gli insiemi transitivi che contengono $X$ ne esiste uno più piccolo di tutti (rispetto all'inclusione) che viene chiamato* chiusura transitiva *di $X$.*

*Dimostrazione.* Definiamo grazie al teorema di ricursione una successione di insiemi $(X_n : n \in \omega)$ ponendo $X_0 = X$ ed $X_{n+1} = \bigcup X_n$. Sia $Y = \bigcup_{n \in \omega} X_n$ e mostriamo che $Y$ è transitivo. A tal fine supponiamo $x \in y \in Y$. Allora esiste $n \in \omega$ con $y \in X_n$ e siccome $x \in y$ si ha $x \in \bigcup X_n = X_{n+1} \subseteq Y$. Quindi $Y$ è transitivo. Mostriamo che l'insieme $Y$ così costruito è in effetti il più piccolo insieme transitivo contenente $X$. A tal fine prendiamo un altro insieme transitivo $Y'$ che include $X$ e dimostriamo che $Y \subseteq Y'$. È sufficiente mostrare, per induzione su $n \in \omega$, che $X_n \subseteq Y'$. Il caso $n = 0$ è ovvio. Supponendo per ipotesi induttiva che $X_n \subseteq Y'$. Allora $\bigcup X_n \subseteq \bigcup Y' \subseteq Y'$, dove la seconda inclusione segue dal fatto che $Y'$ è transitivo. Per induzione $X_n \subseteq Y'$ per ogni $n \in \omega$ e quindi $Y \subseteq Y'$. □

# 29 Ordinali di von Neumann

**29.1 Definizione.** Un insieme $\alpha$ è un ordinale se è transitivo (Definizione 28.1) e $\alpha$ è bene ordinato dall'appartenenza, nel senso che $(\alpha, \in \restriction_\alpha)$ è un buon ordine stretto.

Il fatto che $\in$ sia un buon ordine stretto sugli elementi di $\alpha$ implica in particolare che se $x, y, z$ sono elementi di $\alpha$ con $x \in y \in z$, allora $x \in z$, ovvero $\in \restriction_\alpha$ è una relazione transitiva. Inoltre se $\alpha$ è un ordinale ed $x \in \alpha$, non può essere che $x \in x$ (in quanto $\in \restriction_\alpha$ è un ordine stretto). Quindi in particolare non può capitare che $\alpha \in \alpha$.

**29.2 Proposizione.** *Per ogni ordinale $\alpha$ abbiamo $\alpha \notin \alpha$.*

Nel seguito introdurremo un assioma, chiamato assioma di fondazione, che implica che la stessa proprietà vale per tutti gli insiemi, non solo per gli ordinali, ma per il momento non ne abbiamo bisogno.

**29.3 Esempio.** I seguenti insiemi sono ordinali: $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$ etc. Anche $\omega$ è un ordinale.

**29.4 Lemma.** *Se $\alpha$ è un ordinale e $x \in \alpha$ allora $x$ è un ordinale.*

*Dimostrazione.* Per mostrare che $x$ è transitivo supponiamo che $z \in y \in x$. Applicando la transitività di $\alpha$ vediamo che $x, y, z$ sono tutti elementi di $\alpha$ (prima mostro che $y \in \alpha$, poi usando questo fatto anche $z \in \alpha$). Ora poiché tra elementi di $\alpha$ la relazione $\in$ gode della proprietà transitiva (essendo un ordine stretto), otteniamo $z \in x$. Quindi $x$ è transitivo.

Resta da dimostrare che $(x, \in)$ è un buon ordine stretto. A tal fine basta osservare che da $x \in \alpha$ segue $x \subseteq \alpha$ (essendo $\alpha$ transitivo) e che un sottoinsieme di un buon ordine è un buon ordine (con l'ordine indotto). □

**29.5 Lemma.** *Siano $\alpha$ e $\beta$ due ordinali. Sono equivalenti:*

1. *$\alpha \in \beta$,*
2. *$\alpha \subset \beta$ (inclusione stretta),*
3. *$\alpha$ è un segmento iniziale proprio di $\beta$ (rispetto all'ordine stretto dato da $\in$).*

*Dimostrazione.* Per la transitività degli ordinali, 1) implica 2) (l'inclusione deve essere stretta altrimenti $\alpha \in \alpha$) e 2) è equivalente a 3). Mostriamo che 3) implica 1). Sia $\alpha$ un segmento iniziale proprio di $\beta$. Allora $\alpha$ si può scrivere nella forma $\alpha = \{x \in \beta \mid x < \gamma\}$ per un certo $\gamma \in \beta$. Ricordando che $<$ è l'appartenenza $\in$, abbiamo $\alpha = \{x \in \beta \mid x \in \gamma\} = \gamma$, dove l'ultima uguaglianza segue dal fatto che gli elementi di $\gamma$ sono automaticamente anche elementi di $\beta$, essendo $\beta$ transitivo. Abbiamo così dimostrato che $\alpha = \gamma \in \beta$. □

**29.6 Lemma.** *Se $\alpha$ e $\beta$ sono ordinali, allora $\alpha \subseteq \beta$ oppure $\beta \subseteq \alpha$.*

*Dimostrazione.* Sia $\gamma = \alpha \cap \beta$. Chiaramente $\gamma$ è un ordinale, e $\gamma \subseteq \alpha$, $\gamma \subseteq \beta$. Basta mostrare che $\gamma = \alpha$ oppure $\gamma = \beta$. Se così non fosse, $\gamma$ sarebbe incluso strettamente sia in $\alpha$ che in $\beta$ e quindi per il lemma precedente apparterrebbe sia ad $\alpha$ che a $\beta$: $\gamma \in \alpha$, $\gamma \in \beta$. Ma allora $\gamma \in \alpha \cap \beta = \gamma$, e quindi $\gamma \in \gamma$ contraddicendo il fatto che $\gamma$ è un ordinale. □

**29.7 Lemma.** *Dati due ordinali $\alpha$ e $\beta$, se $(\alpha, \in)$ è isomorfo a $(\beta, \in)$ allora $\alpha = \beta$.*

*Dimostrazione.* Se $\alpha \neq \beta$ allora in base ai Lemmi 29.6 e 29.5 $\alpha$ è un segmento iniziale proprio di $\beta$ o viceversa. Ora basta ricordare che, per il Lemma 27.4, un buon ordine non è mai isomorfo ad un suo segmento iniziale proprio. □

**29.8 Definizione.** Se $\alpha$ e $\beta$ sono ordinali scriviamo $\alpha \leq \beta$ se $\alpha \subseteq \beta$ e $\alpha < \beta$ se $\alpha \in \beta$.

Per il Lemma 29.5 $x < y$ se e solo se $x \leq y$ e $x \neq y$. Inoltre $\leq$ è un ordine totale sulla classe degli ordinali (la totalità è data dal Lemma 29.6)

**29.9 Osservazione.** Ogni ordinale coincide con l'insieme degli ordinali minori di lui. Quindi in particolare $\{x \mid x < \alpha\}$ è un insieme (in quanto coincide con $\alpha$).

**29.10 Teorema.** *(Principio del minimo per gli ordinali) Ogni classe non vuota $X$ di ordinali ha un minimo elemento.*

*Dimostrazione.* Fissiamo un elemento $\alpha$ di $X$. Se $\alpha$ non è il minimo di $X$ consideriamo l'insieme $\{\beta < \alpha \mid \beta \in X\}$. Questo è un sottoinsieme non vuoto dell'insieme bene ordinato $\alpha$ e pertanto ha un minimo, che deve coincidere con il minimo di $X$. □

**29.11 Corollario.** *La classe $ON$ degli ordinali non è un insieme.*

*Dimostrazione.* Poiché gli elementi di un ordinale sono ordinali, $ON$ è una classe transitiva. Inoltre è bene ordinata da $\leq$ per il principio del minimo sopra dimostrato. Se $ON$ fosse un insieme, sarebbe dunque un ordinale, ovvero $ON \in ON$. Ma questo è assurdo in quanto un ordinale non appartiene mai a se stesso. □

**29.12 Lemma.** *Sia $X$ un insieme transitivo di ordinali. Allora $X$ è un ordinale.*

*Dimostrazione.* Un insieme di ordinali è sempre bene ordinato dall'appartenenza. Se è anche transitivo, allora per definizione è un ordinale. □

**29.13 Teorema.** *Consideriamo la classe ordinata $(ON, \leq)$ degli ordinali.*

1. *$\emptyset$ è il minimo ordinale (lo zero).*
2. *Se $\alpha$ è un ordinale, allora $\alpha \cup \{\alpha\}$ è un ordinale, ed è il minimo ordinale strettamente maggiore di $\alpha$. Lo chiamiamo $\alpha + 1$.*
3. *Se $X$ è un insieme di ordinali, allora $\bigcup X$ è un ordinale, ed è il minimo ordinale maggiore o uguale a tutti gli ordinali di $X$, cioè $\bigcup X = \sup X$.*

*Dimostrazione.* Verifichiamo che $\bigcup X$ è un ordinale. Poiché gli elementi di $X$ sono transitivi (essendo ordinali), $\bigcup X$ è transitivo (l'unione di una famiglia di insiemi transitivi è transitiva). Poichè gli elementi di un ordinale sono ordinali, $\bigcup X$ è l'unione di un insieme $X$ i cui elementi sono insiemi di ordinali, e pertanto $\bigcup X$ è un insieme di ordinali. Essendo anche transitivo, è un ordinale.

Similmente si verifica che $\alpha \cup \{\alpha\}$ è un ordinale.

Gli altri punti seguono facilmente dal fatto che tra ordinali l'inclusione coincide con l'ordine e quindi l'unione coincide con l'estremo superiore. □

Sono dunque ordinali i numeri naturali $0, 1, 2, \ldots$, il loro sup $\omega = \bigcup \omega$, e poi $\omega + 1 = \omega \cup \{\omega\}$, $\omega + 2 = \omega + 1 + 1$, eccetera.

**29.14 Corollario.** *Ogni insieme $X$ di ordinali è limitato superiormente.*

*Dimostrazione.* Basta prendere $\sup(X) + 1$. □

**29.15 Corollario.** *Ogni classe di ordinali non limitata superiormente non è un insieme.*

**29.16 Esercizio.** La classe degli ordinali è la più piccola classe contenente 0 e chiusa per successore e unione di sottoinsiemi.

# 30 Induzione e ricursione sugli ordinali

**30.1 Teorema.** *(Induzione sugli ordinali) Sia $P(x)$ una proprietà ben definita sugli ordinali. Supponiamo che:*

1. *valga $P(0)$.*
2. *per ogni ordinale $\alpha$ se vale $P(\alpha)$ vale $P(\alpha+1)$.*
3. *per ogni insieme $X$ di ordinali, se per ogni $\beta \in X$ vale $P(\beta)$, allora allora vale $P(\sup X)$.*

*Allora tutti gli ordinali $x$ verificano $P(x)$.*

*Dimostrazione.* Altrimenti si consideri il minimo ordinale che non verifica $P(x)$ e si raggiunga una contraddizione distinguendo i casi in cui tale ordinale è 0, il successore di un altro ordinale, o il sup degli ordinali minori di lui. □

Analogamente si dimostra un teorema di ricursione transfinita per definire funzioni su ordinali.

**30.2 Teorema.** *(Ricursione su ordinali) Sia $H : ON \times V \to V$ una funzione classe. Allora esiste una ed una sola funzione $F : ON \to V$ tale che per ogni $a \in ON$ si ha*

$$F(a) = H(a, F\restriction_{\{x:x<a\}})$$

*Dimostrazione.* Diciamo che una funzione $g$ è buona se esiste $\alpha \in ON$ tale che $\mathrm{dom}(g) = \alpha$ e $g$ verifica l'equazione ricorsiva

$$g(\beta) = H(n, g\restriction_{\{i:i<\beta\}})$$

per ogni $\beta$ nel suo dominio. Per induzione è facile vedere che due funzioni buone coincidono sull'intersezione dei loro domini, e quindi ve ne al massimo una su un dato dominio. Definiamo ora $F$ come l'unione di tutte le funzioni buone. L'equazione ricorsiva permette di estendere una funzione buona $g$ con dominio $\beta = \{i : i < \beta\}$ ad una funzione buona $g'$ con dominio $\beta + 1 = \beta \cup \{\beta\}$, ponendo $g'(\beta) = H(n, g\restriction_{\{i:i<\beta\}})$. Se $\lambda$ è un ordinale limite, e supponendo che per ogni $\beta < \lambda$ esista una funzione buona $g_\beta$ con dominio $\beta$ (necessariamente unica), possiamo ottenere una funzione buona $g_\lambda$ con dominio $\lambda$ ponendo $g_\lambda = \bigcup_{\beta<\lambda} g_\beta$ (qui dobbiamo usare l'assioma di rimpiazzamento per assicurarci che la classe $\{g_\beta : \beta < \lambda\}$ di cui prendiamo l'unione sia un insieme). Per induzione ne segue che per ogni ordinale $\alpha$ esiste una funzione buona con dominio $\alpha$. Ne segue che l'unione $F$ di tutte le funzioni buone è una funzione da $ON$ ad $V$ che verifica l'equazione ricorsiva. □

Applicando il teorema di ricursione possiamo definire la somma tra ordinali nel modo seguente.

**30.3 Definizione.** Definiamo la somma di due numeri ordinali per ricursione sul secondo argomento:

1. $\alpha + 0 = \alpha$,
2. $\alpha + S(\beta) = S(\alpha + \beta)$, dove $S(x) = x + 1$,
3. $\alpha + \lambda = \sup_{\beta<\lambda} \alpha + \beta$ se $\lambda$ è un ordinale limite.

**30.4 Definizione.** Definiamo il prodotto di due numeri ordinali per induzione sul secondo argomento:

1. $\alpha \cdot 0 = 0$,
2. $\alpha \cdot S(\beta) = \alpha \cdot \beta + \alpha$,
3. $\alpha \cdot \lambda = \sup_{\beta<\lambda} \alpha \cdot \beta$, se $\lambda$ è un ordinale limite.

**30.5 Definizione.** Definiamo l'esponenziazione di due numero ordinali per induzione sul secondo argomento:

1. $\alpha^0 = 1$,
2. $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$,
3. $\alpha^\lambda = \sup_{\beta<\lambda} \alpha^\beta$, se $\lambda$ è un ordinale limite.

**30.6 Osservazione.** Se $(\beta_i : i \in I)$ è una famiglia di ordinali, allora

$$\alpha + \sup_{i\in I} \beta_i = \sup_{i\in I}(\alpha + \beta_i).$$

Per dimostrarlo si distinguono due casi. Se la famiglia ha un massimo elemento $\beta_j$, allora entrambi i membri dell'uguaglianza da dimostrare coincidono con $\alpha + \beta_j$ (dopo aver verificato che $\alpha + x$ è una funzione crescente di $x$). Se invece la famiglia non ha un massimo allora il sup è un ordinale limite e possiamo applicare la terza clausola nella definizione di somma. Analogamente $\alpha \cdot \sup_{i\in I} \beta_i = \sup_{i\in I}(\alpha \cdot \beta_i)$ e $\alpha^{\sup_{i\in I} \beta_i} = \sup_{i\in I} \alpha^{\beta_i}$.

**30.7 Esercizio.** Se $\alpha$ e $\beta$ sono ordinali numerabili, anche $\alpha^\beta$ lo è.

**30.8 Esercizio.** Valgono le leggi associative del $+$ e del $\cdot$, e la legge distributiva a destra $x \cdot (y + z) = x \cdot y + x \cdot z$. Non valgono le leggi commutative, e neppure la distributività a sinistra.

**30.9 Esercizio.** Abbiamo:

1. (Sottrazione) Se $\alpha$ e $\beta$ sono ordinali, ed $\alpha \leq \beta$, allora esiste un unico ordinale $\gamma$ con $\alpha + \gamma = \beta$.

2. (Divisione con resto) Se $\alpha$ e $\beta$ sono ordinali, con $\beta \neq 0$, allora esiste una unica coppia di ordinali $\xi$ e $\rho$ tale che $\alpha = \beta\xi + \rho$, con $\rho < \beta$.

3. (Rappresentazione in base $\gamma$) Dato un ordinale $\gamma \neq 0$ possiamo rappresentare ogni ordinale $\alpha \neq 0$ in modo unico nella forma $\alpha = \gamma^{\alpha_1} t_1 + \ldots + \gamma^{\alpha_k} t_k$ con $k \in \omega$, $t_1, \ldots, t_k < \gamma$, $\alpha_1 > \ldots > \alpha_k$.

4. (Forma normale di Cantor) In particolare se $\alpha$ è un ordinale diverso da zero, allora esiste un'unica scrittura della forma $\alpha = \omega^{\alpha_1} n_1 + \ldots + \omega^{\alpha_k} n_k$ con $k \in \omega$, $n_1, \ldots, n_k < \omega$, $\alpha_1 > \ldots > \alpha_k$.

*Dimostrazione.* (1) Procedo per induzione su $\beta$. Per $\beta < \alpha$ non c'è nulla da dimostrare e per $\beta = \alpha$ l'unico possibile $\gamma$ è zero. Se $\alpha+\gamma = \beta$, allora $\alpha+\gamma+1 = \beta+1$ (dando per buona l'associatività). Rimane da trattare il caso in cui $\beta$ è limite. Per ipotesi induttiva possiamo supporre che per ogni $x < \beta$ con $\alpha \leq x$ esiste un unico ordinale $\gamma_x$ tale che $\alpha + \gamma_x = x$. Sia $\gamma = \sup_{x<\beta} \gamma_x$. Allora $\alpha + \gamma = \alpha + \sup_{x<\beta} \gamma_x = \sup_{x<\beta}(\alpha + \gamma_x) = \sup_{x<\beta} x = \beta$.

(2) Considero il massimo ordinale $\xi$ tale che $\beta \cdot \xi \leq \alpha$ e prendo come $\rho$ la differenza tra $\alpha$ e $\beta \cdot \xi$, ovvero l'unico ordinale tale che $\alpha = \beta \cdot \xi + \rho$. Dobbiamo però dimostrare che il massimo esiste e che $\rho < \beta$. Per mostrare che il massimo esiste osserviamo che la classe $C$ degli ordinali $x$ tali che $\beta \cdot x \leq \alpha$ è un insieme (essendo ciascun $x$ necessariamente $< \alpha + 1$). Posto $\xi$ l'estremo superiore di $C$, dobbiamo avere $\beta \cdot \xi \leq \alpha$ in quanto la moltiplicazione è continua nel secondo argomento (nel senso che commuta con i sup). Abbiamo così dimostrato che $\xi$ è in effetti un massimo. Ora se per assurdo $\rho$ fosse maggiore di $\beta$, potremmo sostituire $\rho$ con $\rho - \beta$ e $\xi$ con $\xi + 1$, ottenendo $\alpha = \beta \cdot (\xi + 1) + (\rho - \beta)$, e contraddicendo la massimalità di $\xi$.

(3) Considero il massimo ordinale $\alpha_1$ tale che $\gamma^{\alpha_1} \leq \alpha$ (dimostrate che esiste). Ora per il teorema di divisione con resto scrivo $\alpha = \gamma^{\alpha_1} t_1 + \rho$ con $\rho < \gamma^{\alpha_1}$. Osservo che $t_1 < \gamma$ altrimenti avrei $\gamma^{\alpha_1} \leq \alpha$ contraddicendo la massimalità di $\alpha_1$. Per induzione posso supporre che $\rho$, se non è zero, si scriva nella forma $\gamma^{\alpha_2} t_2 + \ldots + \gamma^{\alpha_k} t_k$ con $\alpha_2 > \ldots > \alpha_k$ e $t_i < \gamma$ per ogni $i$, e concludo osservando che $\alpha_1 > \alpha_2$ altrimenti riarrangiando i termini contraddirei la massimalità di $\alpha_1$. □

**30.10 Esercizio.** Se $\alpha$ e $\beta$ sono ordinali, $\alpha+\beta$ è isomorfo a $\alpha \times \{0\} \cup \beta \times \{1\}$ con l'unico ordine in cui tutti gli elementi di $\alpha \times \{0\}$ sono minori di quelli di $\beta \times \{1\}$ e in ciascuno di questi due insiemi si segue l'ordine delle prime componenti in $\alpha$ e $\beta$ rispettivamente.

*Dimostrazione.* L'isomorfismo $f : \alpha + \beta \to \alpha \times \{0\} \cup \beta \times \{1\}$ è il seguente. Dato $x < \alpha + \beta$, distinguiamo due casi. Se $x < \alpha$, poniamo $f(x) = x \times \{0\}$. Se invece $\alpha \leq x$ possiamo scrivere $x = \alpha + y$ e poniamo $f(x) = y \times \{1\}$. □

**30.11 Esercizio.** Se $\alpha$ e $\beta$ sono ordinali, $\alpha \cdot \beta$ è isomorfo a $\alpha \times \beta$ con l'ordine lessicografico: prima si confrontano le seconde componenti delle coppie, poi a parità si confrontano le prime.

*Dimostrazione.* Dato $u < \alpha \cdot \beta$, posso usare il teorema di divisione con resto per scrivere $u = \alpha y + x$ con $x < \alpha$. L'isomorfismo cercato manda $u$ nella coppia $(x, y)$ (osserviamo che $y$ è necessariamente $< \beta$). L'isomorfismo inverso manda $(x, y)$ in $\alpha y + x$. □

**30.12 Esercizio.** Se $\alpha$ e $\beta$ sono ordinali, $\alpha^\beta$ è il tipo d'ordine dell'insieme bene ordinato $(S, <)$ così definito: $S$ è l'insieme delle funzioni $f : \beta \to \alpha$ con supporto finito, ovvero con $f(x) = 0$ per tutti gli $x \in \beta$ al di fuori di un insieme finito; date $f_1 \neq f_2$ in $S$, poniamo $f_1 < f_2$ se per il massimo $x$ tale che $f_1(x) \neq f_2(x)$, si ha $f_1(x) < f_2(x)$. Si noti che il massimo esiste perché i supporti sono finiti.

*Dimostrazione.* (Cenno) Data $f : \beta \to \alpha$ con supporto finito $\mathrm{supp}(f) \subseteq \beta$, associamo ad $f$ l'ordinale $\alpha^{x_1} \cdot f(x_1) + \ldots + \alpha^{x_k} \cdot f(x_k)$ dove $x_1 > \ldots > x_k$ sono gli elementi del supporto di $f$ (conveniamo che se il supporto è vuoto associamo ad $f$ l'ordinale 0). Questa corrispondenza definisce l'isomorfismo cercato. □

**30.13 Lemma.** *Sia $f : ON \to ON$ una funzione crescente e continua, dove continua significa che $f(\lambda) = \sup_{\alpha<\lambda} f(\alpha)$ per ogni ordinale limite $\lambda$. Allora esistono ordinali $x$ arbitrariamente grandi tali che $f(x) = x$.*

*Dimostrazione.* (Cenno) Dato $x_0 \in ON$ definiamo induttivamente $x_{n+1} = f(x_n)$ e poniamo $x = \sup_{n\in\omega} x_n$. Allora $f(x) = x$ ed $x \geq x_0$. □

**30.14 Esercizio.** Si dimostri che esistono ordinali $\alpha$ arbitrariamente grandi tali che $\alpha = \omega^\alpha$. Sia $\varepsilon_0$ il minimo ordinale tale che $\varepsilon_0 = \omega^{\varepsilon_0}$. Si dimostri che $\varepsilon_0$ è numerabile.

# 31 Relazioni ben fondate

**31.1 Definizione.** Una relazione binaria $R$ su un insieme (o una classe) $A$ si dice ben fondata se ogni sottoinsieme non vuoto $X$ di $A$ ha un elemento $a \in X$ tale che non esiste alcun $x \in A$ con $xRa$. Tale $a$ si dice un elemento $R$-minimale di $X$. Si noti che in generale può esistere più di un elemento $R$-minimale di $X$.

**31.2 Esercizio.** Sia $R$ la relazione binaria su $\mathbb{N}$ così definita: $xRy$ se $S(x) = y$. Si dimostri che $R$ è ben fondata.

La relazione $\leq$ sui numeri naturali non è ben fondata in quanto vale la proprietà riflessiva $x \leq x$ e una relazione riflessiva non è mai ben fondata. Tuttavia abbiamo:

**31.3 Esercizio.** La relazione di ordine stretto $<$ su $\mathbb{N}$ è ben fondata.

**31.4 Esempio.** La relazione di inclusione stretta $\subset$ tra sottoinsiemi di $\omega$ non è ben fondata. Infatti sebbene vi sia un sottoinsieme di $\omega$ minimale rispetto all'inclusione (l'insieme vuoto) esistono famiglie di sottoinsiemi di $\omega$ all'interno delle quali non vi sono elementi minimali. Un esempio è dato dalla famiglia di tutte le semirette $\{x : x \geq n\}$ al variare di $n$ in $\omega$.

**31.5 Proposizione.** *Una relazione $R$ su $A$ è ben fondata se e solo se non esistono successioni $(a_n \mid n \in \mathbb{N})$ con $a_{n+1}Ra_n$ per ogni $n \in \mathbb{N}$.*

*Dimostrazione.* Se esiste $(a_n \mid n \in \mathbb{N})$ come sopra, allora $\{a_n \mid n \in \mathbb{N}\}$ non ha elementi $R$-minimali, e quindi $R$ non è ben fondata. Viceversa supponiamo che $R$ non sia ben fondata. Esiste dunque un insieme non vuoto $B \subseteq A$ senza elementi $R$-minimali. Definiamo ricorsivamente $a_n$ prendendo come $a_0$ un arbitrario elemento di $B$ e come $a_{n+1}$ un qualsiasi elemento $x$ di $B$ tale che $xRa_n$. Più formalmente, usando l'assioma della scelta, fissiamo una funzione $f$ che, dato $b \in B$, restituisce un elemento $f(b) \in B$ con $f(b)Rb$ (tale elemento esiste visto che $B$ non ha elementi $R$-minimali), e definiamo induttivamente $a_{n+1} = f(a_n)$. □

**31.6 Esercizio.** Un ordine totale $(A, \leq)$ è un buon ordine se e solo se la corrispondente relazione di ordine stretto $<$ è ben fondata.

# 32 Induzione e ricursione su relazioni ben fondate

**32.1 Proposizione.** *(Induzione ben fondata) Se $R$ è una relazione ben fondata su un insieme $X$ e sia $P$ una proprietà ben definita. Supponiamo che, dato un qualsiasi $x \in X$, sia possibile dimostrare $P(x)$ assumendo "come ipotesi induttiva", che $P(y)$ valga per ogni $y \in X$ con $yRx$. Detto più formalmente supponiamo che valga l'enunciato*

$$(\forall x \in X)\big((\forall y \in X)(yRx \to P(y)) \to P(x)\big)$$

*(detto "passo induttivo"). Allora, per ogni $x \in X$, vale $P(x)$.*

*Dimostrazione.* Se vi fosse un $a \in X$ tale che $\neg P(a)$, consideriamo un elemento $R$-minimale $a$ tale che $\neg P(a)$. Allora per tutti gli $y \in X$ con $yRa$ vale $P(y)$, e dunque per il passo induttivo vale anche $P(a)$. Assurdo. □

**32.2 Osservazione.** Nel caso in cui $R$ sia la relazione $<$ sui numeri naturali $\mathbb{N}$, l'induzione ben fondata coincide con "induzione forte". Si noti che non abbiamo bisogno di un "caso base" dell'induzione, in quanto il "passo induttivo"

$$(\forall x \in \mathbb{N})\big((\forall y \in \mathbb{N})(y < x \to P(y)) \to P(x)\big)$$

già include il caso base, come già visto nel caso dell'induzione forte sui numeri naturali.

Diamo qui sotto una versione molto generale del teorema di ricursione, che permette definizioni ricorsive non solo sui numeri naturali, ma su qualunque insieme dotato di una relazione ben fondata $R$.

**32.3 Teorema.** *(Teorema di ricursione per relazioni ben fondate) Sia $R$ una relazione ben fondata su un insieme $A$. Sia $H : A \times V \to V$ una funzione. Esiste una ed una sola funzione $F : A \to V$ tale che per ogni $a \in A$ si ha*

$$F(a) = H(a, F\restriction_{\{x:xRa\}})$$

*L'ipotesi che $A$ sia un insieme può essere rilassata. Possiamo permettere ad $A$ di essere una classe, ma in questo caso abbiamo bisogno di una ipotesi in più su $R$, ovvero che per ogni $a \in A$ la classe $\{x : xRa\}$ sia un insieme (altrimenti $F\restriction_{\{x:xRa\}}$ sarebbe una classe e non potrebbe essere fornita in input ad $H$).*

*Dimostrazione.* (Unicità) Supponiamo che $G$ sia una funzione che verifica la stessa equazione di $F$, ovvero per ogni $a \in A$ si abbia

$$G(a) = H(a, G\restriction_{\{x:xRa\}}).$$

Vogliamo dimostrare che $G(a) = F(a)$ per ogni $a \in A$. Se per assurdo così non fosse, consideriamo un elemento $R$-minimale $a \in A$ tale che $G(a) \neq F(a)$. Per tale $a$ dobbiamo allora avere $F\restriction_{\{x:xRa\}} = G\restriction_{\{x:xRa\}}$. Ciò è assurdo in quanto $F(a) = H(a, F\restriction_{\{x:xRa\}}) = G(a, G\restriction_{\{x:xRa\}}) = G(a)$.

(Esistenza) Dato un sottoinsieme $B$ di $A$ diciamo che $B$ è buono se esiste una funzione $g$ con $\mathrm{dom}(g) = B$ e tale che $\forall a \in B$ si abbia $\{x : xRa\} \subseteq B$ e

$$g(a) = H(a, g\restriction_{\{x|xRa\}}).$$

La restrizione di $R$ a $B$ è ben fondata, e quindi per la prima parte del teorema se una tale $g$ esiste essa è unica. Ad ogni $B$ buono possiamo quindi associare un'unica funzione $g = g_B$ (tramite una funzione classe che manda $B$ in $g_B$). Lo stesso ragionamento mostra che se $B$ e $B'$ sono entrambi buoni allora $B \cap B'$ è buono e $g_B$ coincide con $g_{B'}$ su $B \cap B'$. Consideriamo la classe $\{g_B \mid B \text{ è buono}\}$ e la sua unione

$$F = \bigcup_{B \text{ buono}} g_B.$$

Tale $F$ è una funzione classe (in quanto unione di una classe di funzioni che coincidono a due a due sul dominio comune) e ha come dominio l'unione di tutti i sottoinsiemi buoni. Inoltre $F$ estende ogni $g_B$ e pertanto verifica ancora l'equazione ricorsiva $F(b) = H(b, F\restriction_{\{x|xRb\}})$ per ogni $b \in \mathrm{dom}(F)$. (Basta infatti, dato $b \in \mathrm{dom}(F)$, considerare un $B$ buono con $b \in B$ ed usare la condizione per $g_B$.)

Resta da dimostrare che $\mathrm{dom}(F) = A$. Consideriamo per assurdo un elemento $R$-minimale $a \in A$ tale che $a \notin \mathrm{dom}(F)$. Per ogni $b$ con $bRa$ esiste dunque una funzione $g$ con dominio buono tale che $b \in \mathrm{dom}(g)$. Di tali funzioni ne possono esistere più di una, ma possiamo prendere quella con il dominio più piccolo possibile, chiamiamola $g_b$, che sicuramente esiste perché basta prendere l'intersezione di tutti gli insiemi buoni che contengono $b$. Siccome $\{b : bRa\}$ è un insieme per le nostre ipotesi, la classe $\{g_b : bRa\}$ è un insieme per l'assioma di rimpiazzamento, e pertanto l'unione $g = \bigcup\{g_b : bRa\}$ è ancora un insieme.

Poichè le $g_b$ coincidono a due a due sul dominio comune (per la parte sull'unicità), $g$ è una funzione, e verifica ancora l'equazione ricorsiva. Pertanto il dominio di $g$ è buono, ed include $\{b : bRa\}$. Possiamo estendere $g$ ad una funzione $f$ il cui dominio include anche $a$ definendo $f(a) = H(a, g\restriction_{\{b:bRa\}})$ e ponendo $f = g$ sugli elementi del dominio di $g$. Siccome anche $f$ verifica l'equazione ricorsiva, abbiamo dimostrato che $a$ appartiene ad un insieme buono, e dunque $a \in \mathrm{dom}(F)$, contro l'ipotesi. Questo assurdo mostra che $\mathrm{dom}(F) = A$. □

**32.4 Esercizio.** (Funzione di Ackermann) Si dimostri che esiste una e una sola funzione $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tale che:

$$f(m,n) = \begin{cases} n+1 & \text{se } m = 0 \\ f(m-1,1) & \text{se } m > 0 \text{ and } n = 0 \\ f(m-1, f(m,n-1)) & \text{se} m > 0 \text{ and } n > 0. \end{cases}$$

La funzione di Ackermann cresce molto velocemente: si provi a calcolarne alcuni valori, come ad esempio $f(2,2)$ o $f(3,2)$.

*Dimostrazione.* (Suggerimento) Si definisca una relazione ben fondata $R$ su $\mathbb{N} \times \mathbb{N}$ nel modo seguente: $(x,y)R(x',y')$ se $x < x'$ oppure $x = x'$ e $y < y'$. Si applichi il teorema di ricursione con questa relazione ben fondata. □

# 33 Rango di una relazione ben fondata

**33.1 Teorema.** *Una relazione binaria $R$ su un insieme $A$ è ben fondata se e solo se esiste una funzione $\rho : A \to ON$ tale che per ogni $x, y \in A$ con $xRy$ si ha $\rho(x) < \rho(y)$.*

*Dimostrazione.* Se $\rho$ esiste, $R$ deve essere ben fondata, altrimenti esisterebbe una successione infinita decrescente $a_{n+1}Ra_n$ di elementi $a_n \in A$ che darebbe luogo ad una successione infinita descrescente $\rho(a_n)$ di ordinali (cosa impossibile).

Viceversa, supponendo $R$ ben fondata, definiamo per ricursione transfinita una funzione $\rho : A \to V$ ponendo, per ogni $a \in A$,

$$\rho(a) = \bigcup \{\rho(b) + 1 : bRa\},$$

dove $x + 1 = x \cup \{x\}$. Verifichiamo che $\rho$ fa il lavoro richiesto. Innanzitutto mostriamo che per ogni $a \in A$ $\rho(a)$ è un ordinale. Dato $a \in A$, per induzione ben fondata possiamo supporre che per ogni $b$ con $bRa$ l'insieme $\rho(b)$ sia un ordinale. Ma allora lo è anche $\rho(b)+1$ e pertanto anche $\rho(a)$, essendo un'unione di un insieme di ordinali. Il resto è chiaro: $\rho(a) = \sup\{\rho(b) + 1 : bRa\}$, e quindi $\rho(a) > \rho(b)$ per ogni $bRa$. □

**33.2 Esercizio.** Sia $R$ la relazione su $\mathbb{N}$ definita da $xRy$ se e solo se $x$ divide $y$ ed $x \neq y$. Si definisca $\rho$ come sopra e si calcoli $\rho(72)$.

**33.3 Esercizio.** L'immagine della funzione $\rho$ sopra definita è un insieme transitivo di ordinali, e pertanto è un ordinale.

*Dimostrazione.* Sia $a \in A$ e sia $\beta < \rho(a)$ un ordinale. Dobbiamo mostrare che esiste $c \in A$ con $\rho(c) = \beta$. Lo dimostriamo per induzione ben fondata su $a$. Siccome $\beta < \rho(a) = \sup\{\rho(b) + 1 : bRa\}$, esiste un $b$ con $bRa$ tale che $\beta < \rho(b)+1$. Se $\beta = \rho(b)$ abbiamo concluso. Nel caso contrario $\beta < \rho(b)$ e visto che $bRa$ per induzione esiste $c \in A$ con $\rho(c) = \beta$. □

**33.4 Definizione.** La funzione $\rho$ sopra definita si dice funzione rango associata a $(A, R)$. La sua immagine è un ordinale, detto il rango di $(A, R)$.

**33.5 Esercizio.** Se $(A, R)$ è un buon ordine, la $\rho$ è iniettiva.

**33.6 Esercizio.** Sia $R$ la relazione binaria su $\omega \times \omega$ definita come segue. $(x, y)R(x', y')$ se $x \leq x', y \leq y'$ e almeno una delle due disuguaglianze è stretta. Si dimostri che $R$ è ben fondata e si calcoli il rango di $(\omega \times \omega, R)$.

# 34 Ordinale associato ad un buon ordine

**34.1 Teorema.** *Dato un buon ordine $\leq_A$ su un insieme $A$, esiste uno ed uno solo ordinale $\alpha$ tale che $(A, <_A)$ è isomorfo ad $(\alpha, \in)$. Tale $\alpha$ viene chiamato il tipo d'ordine di $(A, \leq_A)$ (secondo von Neumann).*

*Dimostrazione.* L'unicità segue dal Lemma 29.7. Mostriamo l'esistenza. Definiamo $F : A \to V$ per ricursione transfinita come segue:

$$F(a) = \{F(b) : b <_A a\}.$$

Sia $\alpha = \mathrm{im}(F)$. Dobbiamo verificare che $\alpha$ è un ordinale e che $F : (A, <_A) \to (\alpha, \in)$ è un isomorfismo.

Mostriamo che $\alpha$ è transitivo: se $x \in y \in \alpha$, allora $y = F(a)$ per qualche $a \in A$, e siccome tutti gli elementi di $F(a)$ sono della forma $F(b)$ per qualche $b \in A$, abbiamo $x \in \mathrm{im}(F) = \alpha$.

Un ragionamento simile mostra che, per ogni $a \in A$, $F(a)$ è transitivo. Infatti se $x \in y \in F(a)$, abbiamo $y = F(b)$ per qualche $b <_A a$ e quindi $x = F(c)$ per qualche $c <_A b$. Ma essendo $<_A$ transitiva otteniamo $c <_A a$ e quindi $x \in F(a)$.

Per induzione su $a$ mostriamo ora che $F(a)$ è un ordinale. Per ipotesi induttiva se $bRa$ allora $F(b)$ è un ordinale. Ne segue che $F(a) = \{F(b) : b <_A a\}$ è un insieme transitivo di ordinali, e pertanto è un ordinale.

Osserviamo ora che se vale $b <_A a$, per definizione di $F$ deve valere $F(b) \in F(a)$, ovvero $F(b) < F(a)$ come ordinali. Abbiamo quindi dimostrato che $F$ è una funzione crescente da $(A, <_A)$ ad $\alpha = \mathrm{im}(F)$, e pertanto è un isomorfismo d'ordine. □

**34.2 Esercizio.** La $F$ nella dimostrazione appena data non è altro che la funzione rango: $F(a) = \sup\{F(b) + 1 : b <_A a\}$.

**34.3 Esercizio.** Dati due buoni ordini $(A, \leq_A)$ e $(B, \leq_B)$ con tipi d'ordine $\alpha$ e $\beta$ rispettivamente, si ha che $(A, \leq_A)$ è isomorfo ad un segmento iniziale di $(B, \leq_B)$ se e solo se $\alpha \leq \beta$.

**34.4 Corollario.** *Dati due buoni ordini, uno dei due è isomorfo ad un segmento iniziale dell'altro.*

*Dimostrazione.* Siccome ogni buon ordine è isomorfo ad un ordinale, possiamo ricondurci al caso in cui i due buoni ordini siano due ordinali. Ma già sappiamo che dati due ordinali uno dei due è uguale (non solo isomorfo) ad un segmento iniziale dell'altro. □

**34.5 Esercizio.** Dato un buon ordine $(X, \leq)$ indichiamo con $ot(X, <) \in ON$ il tipo d'ordine di $(X, <)$, ovvero l'unico ordinale isomorfo a $(X, <)$. Si dimostri che se $X = \bigcup_{i \in I} X_i$ e gli $X_i$ sono segmenti iniziali di $X$, allora $ot(X, <) = \sup_{i \in I} ot(X_i, <)$.

# 35 Teorema di Zermelo

**35.1 Teorema.** *(Zermelo) Ogni insieme $X$ può essere bene ordinato.*

*Dimostrazione.* Basta dimostrare che $X$ può essere messo in corrispondenza biunivoca con un ordinale. Per l'assioma della scelta esiste una funzione $h$ che associa a ciascun sottoinsieme non vuoto $A$ di $X$ un suo elemento $h(A) \in A$ e chiamiamo $h(A)$ l'elemento selezionato di $A$. Fissiamo un elemento $a \notin X$ e definiamo $F : ON \to X \cup \{a\}$ per ricursione sugli ordinali ponendo $F(\alpha)$ come l'elemento selezionato tra gli elementi di $X$ che non appartengono all'immagine di $F$ ristretta agli ordinali minori di $\alpha$, ovvero

$$F(\alpha) = h(X \setminus \{F(\beta) : \beta < \alpha\}),$$

sempre che l'insieme sia non vuoto. Se invece $X \setminus \{F(\beta) : \beta < \alpha\}$ è vuoto diamo ad $F(\alpha)$ il valore convenzionale $a$. Per l'assioma di rimpiazzamento $F$ non può essere iniettiva (altrimenti, considerando l'inversa, $ON$ sarebbe un insieme per l'assioma di rimpiazzamento). D'altra parte se $F$ non assumesse mai il valore $a$ sarebbe iniettiva in quanto per definizione $F(\alpha)$ è scelto tra gli elementi di $X$ diversi da $F(\beta)$ per ogni $\beta < \alpha$. Quindi esiste un minimo ordinale $\alpha$ tale che $F(\alpha) = a$. Per definizione di $F$ ciò può capitare solo se $X \setminus \{F(\beta) : \beta < \alpha\}$ è vuoto, ovvero $X = \{F(\beta) : \beta < \alpha\} = \mathrm{im}(F \restriction_\alpha)$. Per la minimalità di $\alpha$, $F \restriction_\alpha : \alpha \to X$ è iniettiva, e dunque biunivoca. □

Abbiamo anche dimostrato:

**35.2 Teorema.** *Ogni insieme può essere messo in corrispondenza biunivoca con un ordinale.*

**35.3 Corollario.** *Dati due insiemi $X$ ed $Y$, abbiamo $|X| \leq |Y|$ o $|Y| \leq |X|$.*

*Dimostrazione.* Per il teorema precedente e il fatto che due ordinali sono l'uno incluso nell'altro. □

# 36 Lemma di Zorn

**36.1 Definizione.** Sia $(A, \leq)$ un ordine parziale. Sia $B \subseteq A$. Diciamo che $B$ è una catena se per ogni coppia di elementi distinti $x, y \in B$ sia ha $x \leq y$ o $y \leq x$. In altre parole $B$ è una catena se è un ordine totale rispetto all'ordine indotto da $(P, \leq)$. Un elemento $a \in A$ viene detto un maggiorante della catena $B \subseteq A$ se per ogni $b \in B$ sia ha $b \leq a$ (tale $a$ può appartenere o no alla catena). Diciamo che $x \in A$ è un elemento massimale di $(A, \leq)$ se non esiste alcun $y \in A$ con $x < y$.

Un ordine parziale può avere o non avere un elemento massimale (ad esempio $\mathbb{N}$ non ne ha) e nel caso ne abbia può averne più di uno. Non bisogna confondere massimale con massimo: un elemento $x$ di un insieme ordinato $(A, \leq)$ è un massimo se per ogni $y \in A$ si ha $y \leq x$. Di elementi massimi ce ne può essere al più uno e se esiste un massimo esso è anche massimale. Se $(A, \leq)$ è un ordine totale il concetto di massimo e di massimale coincidono.

**36.2 Teorema.** *(Lemma di Zorn) Sia $P$ un insieme e $\leq$ un ordine parziale su $P$ tale che ogni catena ha un maggiorante. Allora esiste almeno un elemento $x \in P$ massimale.*

*Dimostrazione.* (Usando l'assioma di Scelta) Supponiamo che non esista alcun elemento massimale e definiamo $x_\alpha \in P$ per ricursione su $\alpha \in ON$ prendendo come $x_0$ un qualsiasi elemento di $P$, come $x_{\alpha+1}$ un elemento maggiore di $x_\alpha$ (esiste perché stiamo assumendo che non vi sia un elemento massimale), e come $x_\lambda$, per $\lambda$ limite, un maggiorante della catena degli $x_\beta$ per $\beta < \lambda$. Per scegliere questi elementi tra le varie possibilità usiamo una funzione di scelta. In tal modo otteniamo una funzione iniettiva da ON a P, il che è assurdo in quanto ON è una classe propria e P è un insieme (considerando la funzione inversa risulta violato l'assioma di rimpiazzamento). □

Il lemma di Zorn viene spesso usato nelle dimostrazioni di esistenza non costruttive in matematica. Ad esempio può essere usato per dimostrare che ogni spazio vettoriale, anche di dimensione infinita, ha una base. In particolare può essere usato per dimostrare che esiste una base di $\mathbb{R}$ come spazio vettoriale su $\mathbb{Q}$.

A partire dal Lemma di Zorn possiamo dare una nuova dimostrazione del teorema di Zermelo.

**36.3 Teorema.** *Il lemma di Zorn implica il teorema di Zermelo: ogni insieme $X$ può essere bene ordinato.*

*Dimostrazione.* Vogliamo dimostrare l'esistenza di un buon ordinamento su $X$. Sia $P$ l'insieme di tutte le coppie della forma $(A, \leq)$ dove $A$ è un sottoinsieme di $X$ e $\leq$ è un buon ordine su $A$. Chiaramente $P$ è non vuoto in quanto ad esempio ogni sottoinsieme finito di $X$ può essere bene ordinato. Mettiamo su $P$ il seguente ordine parziale $\preceq$: diciamo che $(A, \leq) \preceq (A', \leq')$ se e solo se $(A, \leq)$ è un segmento iniziale di $(A', \leq')$ (cioè $A$ è un segmento iniziale di $(A', \leq')$ e $\leq$

coincide con la restrizione di $\leq'$ ad $A$). Ogni catena in $(P, \leq)$ ha un maggiorante data dall'unione dei buoni ordini della catena (verificate!), e quindi per il lemma di Zorn esiste un elemento massimale $(M, \leq)$ in $P$. Per finire dimostriamo che $M = X$. Nel caso contrario sia $a \in X \setminus M$, e definiamo un buon ordinamento $\leq'$ su $M \cup \{a\}$ mantenendo su $M$ il precedente ordinamento $\leq$ e stabilendo che $a$ è maggiore rispetto ad $\leq'$ di ogni elemento di $M$. Evidentemente $(M, \leq)$ è un segmento iniziale di $(M \cup \{a\}, \leq')$, contraddicendo la massimalità di $(M, \leq)$ in $P$. □

Per chiudere il cerchio dimostriamo l'assioma della scelta a partire dal teorema di Zermelo.

**36.4 Teorema.** *Il teorema di Zermelo implica l'assioma di scelta.*

*Dimostrazione.* Dato un insieme $X$ per trovare una funzione di scelta $f : \mathcal{P}(X) \setminus \{\emptyset\} \to X$ basta bene ordinare $X$ e, per ogni sottoinsieme non vuoto $Y$ di $X$, definire $f(Y)$ come il minimo di $Y$. □

# 37 Cardinali come ordinali iniziali

**37.1 Definizione.** Un buon ordine $(A, \leq)$ si dice iniziale se e solo se ogni suo segmento iniziale proprio ha cardinalià inferiore a quella di $A$. Un ordinale $\alpha$ si dice iniziale se è il tipo d'ordine di un buon ordine iniziale.

**37.2 Esempio.** $0, 1, 2, 3, \ldots$, $\omega$ sono ordinali iniziali. $\omega + 1$, $\omega + 2$, $\omega + \omega$ non lo sono. Attenzione: qui il simbolo $+$ indica la somma ordinale, non cardinale.

**37.3 Esercizio.** Tutti gli ordinali iniziali infiniti sono ordinali limite, ma non è vero il viceversa: ad esempio $\omega + \omega$ è un ordinale limite non iniziale.

**37.4 Teorema.** *Per ogni insieme $X$ esiste uno ed un solo ordinale iniziale $\alpha$ della stessa cardinalità di $X$.*

*Dimostrazione.* Bene ordiniamo $X$ e sia $\beta$ il tipo d'ordine di $X$ con il dato buon ordine. Ora sia $\alpha$ il minimo ordinale della stessa cardinalià di $\beta$. □

Possiamo ora ridefinire $|X|$ come segue.

**37.5 Definizione.** $|X|$ = l'unico ordinale iniziale della stessa cardinalità di $X$. Identifichiamo quindi gli ordinali iniziali con i numeri cardinali.

Abbiamo in questo modo due definizioni di $|X|$. Quella di Frege, secondo cui $|X|$ è la classe di equivalenza tutti gli insiemi equipotenti a $X$, e quella di von Neumann secondo cui $|X|$ è l'unico ordinale iniziale equipotente ad $X$. Le due definizioni non sono in conflitto. Secondo entrambe le definizioni si ha che $|X| \leq |Y|$ se e solo se esiste una funzioni iniettiva da $X$ ad $Y$, e ciò equivale al fatto che $|X|$, visto come ordinale iniziale, è minore o uguale (ovvero incluso) a $|Y|$ visto come ordinale iniziale.

Il fatto che i cardinali possano essere identificati con una una sottoclasse degli ordinali (quelli iniziali) implica che anche per i cardinali valga un principio del minimo.

**37.6 Corollario.** *Ogni classe non vuota di cardinali ha un minimo elemento.*

Aver identificato i cardinali con gli ordinali iniziali non significa però che la somma che abbiamo definito sui cardinali coincida con la somma definita sugli ordinali. Ad esempio nonostante il cardinale $\aleph_0$ coincida con l'ordinale iniziale $\omega$, abbiamo $\aleph_0 + 1 = \aleph_0$ (aggiungere un elemento ad un insieme numerabile non cambia la cardinalità), ma $\omega + 1 \neq \omega$ (aggiungere un elemento in fondo ad un buon ordine ne cambia il tipo d'ordine). Il punto è che nei due casi il $+$ ha un significato diverso. Quando usiamo la notazione $\aleph_0$ usiamo le operazioni cardinali, quando usiamo la notazione $\omega$ usiamo le operazioni ordinali.

**37.7 Esercizio.** Se $\alpha \in Ord$, $|\alpha| \leq \alpha$. Ad esempio $|\omega + \omega| = \omega < \omega + \omega$.

# 38 La funzione aleph

**38.1 Lemma.** *Per ogni cardinale $\alpha$ esiste un cardinale $\alpha^+$ più grande di $\alpha$ tale che non cè nessun cardinale tra $\alpha$ e $\alpha^+$.*

*Dimostrazione.* Sicuramente esiste un cardinale più grande di $\alpha$ (ad esempio $2^\alpha$). Quindi esiste un minimo cardinale più grande di $\alpha$. □

La dimostrazione appena data usa l'assioma della scelta per dimostrare che $2^\alpha$ è ben definito come ordinale iniziale (occorre trovare un ordinale iniziale in bigezione con l'insieme delle funzioni da $\alpha$ a 2, e per far ciò occorre bene ordinare tale insieme). Il seguente esercizio fornisce una nuova dimotrazione che non usa l'assioma della scelta.

**38.2 Esercizio.** Senza usare l'assioma della scelta, si dimostri che per ogni ordinale iniziale $\alpha$ esiste un ordinale $\beta$ di cardinalità strettamente più grande.

*Dimostrazione.* (Cenno) Fissiamo $\alpha$ e supponiamo per assurdo che non vi siano ordinali di cardinalità superiore. Ne segue che per ogni ordinale $\beta$ esiste una funzione iniettiva da $\beta$ ad $\alpha$ (perché?). Dunque ogni tipo d'ordine può essere realizzato da un buon ordinamento su $\alpha$. Ma la classe di tutti gli ordinamenti su $\alpha$ è un insieme (in quanto una relazione binaria su $\alpha$ è un elemento di $\mathcal{P}(\alpha \times \alpha)$), mentre $ON$ è una classe propria. □

In base al lemma possiamo definire $\aleph_1 = \aleph_0{}^+$, $\aleph_2 = \aleph_1{}^+$ e così via. Si noti che $\aleph_0 < \aleph_1 \leq 2^{\aleph_0} = |\,\mathbb{R}\,|$. Dai lavori di Gödel (1941) e Cohen (1963) sappiamo che non si può determinare in base agli assiomi se valga l'uguaglianza $\aleph_1 = 2^{\aleph_0}$.

**38.3 Teorema.** *Se $X$ è un insieme di ordinali iniziali,* $\sup X$ *è un ordinale iniziale.*

*Dimostrazione.* Se $\sup X$ non è iniziale esiste un ordinale iniziale $\kappa < \sup X$ della stessa cardinalità di $\sup X$. Per definizione di sup, esiste $\beta \in X$ con $\kappa < \beta \leq \sup X$. Visto che la relazione $\leq$ tra ordinali coincide con l'inclusione $\subseteq$, e visto che $\kappa$ e $\sup X$ hanno la stessa cardinalità, ne segue che anche $\beta$,

essendo compreso tra i due, ha la stessa cardinalità. Questo è assurdo in quanto $\beta$ è iniziale, e non può pertanto avere la stessa cardinalità di un ordinale più piccolo. □

**38.4 Definizione.** Definiamo per ricursione transfinita:

$$\begin{array}{lcl} \aleph_0 & = & |\,\mathbb{N}\,|, \\ \aleph_{\alpha+1} & = & \aleph_\alpha^+, \\ \aleph_\alpha & = & \sup\{\aleph_\beta \mid \beta < \alpha\} \text{ se } \alpha \text{ è un ordinale limite .} \end{array}$$

**38.5 Esercizio.** Se $\alpha < \beta$, allora $\aleph_\alpha < \aleph_\beta$.

**38.6 Teorema.** *La funzione $\alpha \mapsto \aleph_\alpha$ è una bigezione dalla classe ON degli ordinali verso la classe dei cardinali infiniti.*

*Dimostrazione.* Sia $\kappa$ un cardinale infinito. Dobbiamo mostrare che esiste un ordinale $\alpha$ tale che $\kappa = \aleph_\alpha$. Sia $\alpha$ l'estremo superiore dell'insieme $X$ degli ordinali $\beta$ tali che $\aleph_\beta \leq \kappa$. In base alle definizioni, distinguendo i due casi in cui $X$ ha un massimo e il caso in cui non lo ha, si deve in ogni caso avere $\aleph_\alpha = \aleph_{\sup(X)} = \sup_{\beta\in X} \aleph_\beta \leq \kappa$. Se fosse $\aleph_\alpha < \kappa$ avremmo $\aleph_{\alpha+1} \leq \kappa$ contraddicendo la definizione di $\alpha$. Ne segue che $\aleph_\alpha = \kappa$. □

**38.7 Definizione.** L'ordinale iniziale $\aleph_\alpha$ viene anche indicato con la notazione $\omega_\alpha$. Usiamo la prima notazione quanto lo pensiamo come cardinale, e la seconda quanto lo pensiamo come ordinale. Ad esempio se scriviamo $\aleph_\alpha + \aleph_\beta$ intendiamo la somma cardinale (che, come vedremo, fornisce come risultato $\max\{\aleph_\alpha, \aleph_\beta\}$), mentre se scriviamo $\omega_\alpha + \omega_\beta$ intendiamo la somma ordinale, che è definita per ricursione sul secondo argomento. Analoghe convenzioni valgono per la moltiplicazione e l'esponenziazione. Se scriviamo $\omega^\omega$ intendiamo l'esponenziazione tra ordinali e otteniamo un ordinale numerabile, mentre se scriviamo $\aleph_0^{\aleph_0}$ otteniamo il cardinale non numerabile $2^{\aleph_0} = |\,\mathbb{R}\,|$. Un altro esempio è: $\aleph_0 + 1 = \aleph_0$ mentre $\omega_0 + 1 = \omega + 1 > \omega$.

# 39 Somma e prodotto di alephs

**39.1 Teorema.** *Per ogni insieme infinito $X$ si ha $|X \times X| = |X|$.*

*Dimostrazione.* Sia $X$ un insieme di cardinalità $\aleph_\theta$. Dobbiamo trovare una corrispondenza biunivoca tra $X \times X$ ed $X$. Possiamo supporre per ipotesi induttiva che la tesi $|Y \times Y| = |Y|$ valga per insiemi infiniti $Y$ di cardinalità strettamente inferiore a quella di $X$. (Se no ci si riduca a questo caso considerando il minimo cardinale per cui non valga il teorema.) Fissiamo su $X$ un buon ordine $<$ iniziale (ovvero di tipo d'ordine $\aleph_\theta$), in modo che i segmenti iniziali propri di $X$ abbiamo cardinalità strettamente minore a quella di $X$. L'idea ore è quella di cercare di definire un buon ordine $\prec$ su $X \times X$ in modo che la corrispondenza biunivoca cercata sia un isomorfismo d'ordine. Ordiniamo le coppie $(\alpha, \beta) \in X \times X$ nel modo seguente: $(\alpha, \beta) \prec (\gamma, \delta)$ se e solo se $\max(\alpha, \beta) < \max(\gamma, \delta)$ oppure a

parità di massimi $\alpha < \gamma$, oppure a parità di massimi e prime componenti $\beta < \delta$ (i massimi sono presi rispetto all'ordine $<$). Chiaramente $\prec$ è un buon ordine, e per il teorema di confrontabilità dei buoni ordini abbiamo che o $(X \times X, \prec)$ e $(X, <)$ sono isomorfi oppure uno dei due è un segmento iniziale proprio dell'altro. Poichè certamente $|X \times X| \geq |X|$, e i segmenti iniziali propri di $X$ hanno cardinalità minore di $|X|$, una delle tre alternative si esclude subito: $X \times X$ non può essere isomorfo ad un segmento iniziale di $X$. Resta quindi da escludere che $X$ sia isomorfo ad un segmento proprio $J$ di $X \times X$, e a tal fine è sufficiente dimostrare che ogni tale $J$ ha cardinalità $< |X|$. Per verificare quest'ultima affermazione notiamo prendiamo un elemento $(u, v)$ in $X \times X \setminus J$. Poiché $J$ è un segmento iniziale, $(u, v)$ è maggiore o uguale a tutti gli elementi di $J$. Ne segue che $J \subseteq Y \times Y$, dove $Y = \{x \in X \mid x \leq \max(u, v)\}$, e dunque $|J| \leq |Y \times Y|$. Ma $Y$ è un segmento iniziale proprio di $X$ (non può essere uguale ad $X$ in quanto un buon ordine iniziale infinito non può avere un massimo elemento), e pertanto per le nostre ipotesi $|Y \times Y| = |Y| < |X|$, da cui la tesi. □

**39.2 Teorema.** *Dati due cardinali infiniti $\alpha, \beta$ si ha $\alpha + \beta = \alpha \cdot \beta = \max\{\alpha, \beta\}$.*

*Dimostrazione.* Sia $\alpha \leq \beta$. Abbiamo $\beta \leq \alpha + \beta \leq \beta + \beta = \beta \cdot 2 \leq \beta \cdot \beta = \beta$. □

# 40 Teorema di König

**40.1 Definizione.** Per $i \in I$, sia $\alpha_i$ un cardinale. Definiamo la somma $\Sigma_{i \in I} \alpha_i$ come la cardinalità di $\bigcup_{i \in I} A_i$ dove gli $A_i$ sono insiemi disgiunti con $|A_i| = \alpha_i$. Equivalentemente, senza assumere che gli $A_i$ siano disgiunti, $\Sigma_{i \in I} |A_i| = |\bigcup_{i \in I} A_i \times \{i\}|$.

**40.2 Lemma.** *Data una famiglia $(A_i : i \in I)$ di insiemi $A_i$, non necessariamente disgiunti, abbiamo* $\sup_{i \in I} |A_i| \leq |\bigcup_{i \in I} A_i| \leq \Sigma_{i \in I} |A_i|$.

*Dimostrazione.* La prima disuguaglianza è ovvia. Per la seconda basta considerare la funzione surgettiva da $\bigcup_{i \in I} A_i \times \{i\}$ in $\bigcup_{i \in I} A_i$ che manda $(x, i)$ in $x$. □

**40.3 Definizione.** Per $i \in I$, sia $\beta_i$ un cardinale. Definiamo il prodotto $\Pi_{i \in I} \beta_i$ come la cardinalità del prodotto cartesiano infinito $\Pi_{i \in I} B_i$ dove i $B_i$ sono insiemi con $|B_i| = \kappa_i$.

**40.4 Teorema** (Teorema di König)**.** *Per ogni $i \in I$ siano $\alpha_i$ e $\beta_i$ cardinali tali che $\alpha_i < \beta_i$. Allora $\Sigma_{i \in I} \alpha_i < \Pi_{i \in I} \beta_i$.*

*Dimostrazione.* Per ogni $i \in I$ fissiamo degli insiemi $A_i \subset B_i$ con $|A_i| = \alpha_i$ e $|B_i| = \beta_i$, e definiamo $A'_i := A_i \times \{i\}$. Basta mostrare che non esistono funzioni surgettive $g$ da $\bigcup_{i \in I} A'_i$ a $\Pi_{i \in I} B_i$ (quindi in particolare non esistono funzioni biunivoche). Data $g \colon \bigcup_{i \in I} A'_i \to \Pi_{i \in I} B_i$, occorre dunque trovare un elemento $(c_i \mid i \in I)$ di $\Pi_{i \in I} B_i$ che non è nell'immagine di $g$. Per $j \in I$, consideriamo la funzione $g_j \colon A_j \to B_j$ ottenuta come composizione delle funzioni $A_j \xrightarrow{\iota_j} \bigcup_{i \in I} A'_i \xrightarrow{g} \Pi_{i \in I} B_i \xrightarrow{\pi_j} B_j$, dove $\iota_j(a) = (a, j)$ e $\pi_j((c_i \mid i \in I)) = c_j$.

Poiché $|A_j| < |B_j|$, la $g_j$ non è surgettiva. Possiamo dunque scegliere $(c_i \mid i \in I) \in \Pi_{i\in I} B_i$ in modo che per ogni $j \in I$ $c_j \notin \mathrm{im}(g_j)$. Se per assurdo $(c_i \mid i \in I) = g(x)$ per qualche $x \in \bigcup_{i\in I} A'_i$, sia $j \in I$ tale che $x \in A'_j$, e scriviamo $x$ nella forma $(a, j)$ con $a \in A_j$. Per definizione di $g_j$ dobbiamo avere $g_j(a) = c_j$, ma questo è assurdo in quanto $c_j$ era stato scelto fuori dall'immagine di $g_j$. □

Come corollario otteniamo una seconda dimostrazione del teorema di Cantor:

**40.5 Corollario.** *Per ogni cardinale $\kappa$ abbiamo $\kappa < 2^\kappa$.*

*Dimostrazione.* $\kappa = \Sigma_{i\in\kappa} 1 < \Pi_{i\in\kappa} 2 = 2^\kappa$. □

In base agli assiomi di GB non riusciamo a stabilire se $|\,\mathbb{R}\,|$ sia $\aleph_1$, tuttavia abbiamo:

**40.6 Corollario.** $|\,\mathbb{R}\,| \neq \aleph_\omega$.

*Dimostrazione.* Supponiamo per assurdo che $|\,\mathbb{R}\,| = \aleph_\omega$. Ne segue che, per ogni $n \in \omega$, $\aleph_n \leq \aleph_\omega = |\,\mathbb{R}\,| = 2^{\aleph_0}$ e quindi per il teorema di König $\Sigma_{n<\omega}\aleph_n < \Pi_{n<\omega} 2^{\aleph_0}$. Questo è assurdo in quanto $\Pi_{n<\omega} 2^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0\cdot\aleph_0} = 2^{\aleph_0} = |\,\mathbb{R}\,|$, e d'altra parte $|\,\mathbb{R}\,| = \aleph_\omega = \sup_{n<\omega} \aleph_n \leq \Sigma_{n<\omega}\aleph_n$. □

# 41 Cofinalità

**41.1 Definizione.** Siano $(A, \leq_A)$ e $(B, \leq_B)$ due insiemi ordinati. Una funzione $f : A \to B$ si dice cofinale o illimitata se l'immagine di $f$ non ha maggioranti stretti in $B$. La cofinalità di $(B, \leq_B)$ è il minimo ordinale $\alpha$ tale che esiste una funzione cofinale $f\colon \alpha \to (B, \leq_B)$.

**41.2 Esempio.** L'inclusione di $\mathbb{N}$ in $\mathbb{R}$ è cofinale (rispetto all'usuale ordine di $\mathbb{R}$). Siccome $\mathbb{N}$ ha tipo d'ordine $\omega$, ne segue che la cofinalità di $\mathbb{R}$ è minore o uguale ad $\omega$, e visto che un insieme finito non può essere cofinale in $\mathbb{R}$ essa è esattamente $\omega$.

**41.3 Esercizio.** La cofinalità di $(A, \leq_A)$ è uguale ad 1 se e solo se $(A, \leq_A)$ ha un massimo. Se la cofinalità di un ordine totale è maggiore di 1 essa deve essere almeno $\omega$ (ad esempio non può essere 2).

**41.4 Definizione.** Identificando un ordinale con l'insieme ordinato degli ordinali minori di lui, abbiamo che una funzione tra due ordinali $f\colon \alpha \to \beta$ è cofinale se per ogni $\gamma < \beta$ esiste $\delta < \alpha$ tale che $f(\delta) \geq \gamma$. La cofinalità $cf(\beta)$ di $\beta$ è il minimo ordinale $\alpha$ tale che esiste una funzione cofinale $f\colon \alpha \to \beta$.

**41.5 Esercizio.**

1. Se $\beta$ è un ordinale successore, $cf(\beta) = 1$.
2. $cf(\omega + \omega) = \omega$ (dove + indica la somma ordinale).

**41.6 Lemma.** *$\alpha \leq cf(\beta)$ se e solo se esiste una funzione cofinale da $\beta$ ad $\alpha$.*

*Dimostrazione.* Se esiste una funzione cofinale da $\beta$ ad $\alpha$, allora il minimo ordinale $\delta$ per cui esiste una funzione cofinale da $\delta$ ad $\alpha$ è ovviamente minore o uguale a $\beta$, ovvero $cf(\alpha) \leq \beta$. Viceversa supponiamo che $cf(\alpha) \leq \beta$ e sia $f : cf(\alpha) \to \alpha$ cofinale. Estendiamo $f$ in modo arbitrario ad una funzione $g : \beta \to \alpha$. Visto che $g$ estende $f$, è ancora cofinale. □

**41.7 Lemma.** *Per ogni ordinale $\alpha$ abbiamo $cf(\alpha) \leq |\alpha| \leq \alpha$.*

*Dimostrazione.* Per definizione $|\alpha|$ è il minimo ordinale tale che esiste una funzione biunivoca da $|\alpha|$ ad $\alpha$. Ora basta osservare che ogni funzione biunivoca (o anche solamente surgettiva) è ovviamente cofinale. □

**41.8 Definizione.** Un ordinale $\beta$ si dice regolare se $cf(\beta) = \beta$.

**41.9 Lemma.** *Ogni ordinale regolare è un cardinale (ordinale iniziale).*

*Dimostrazione.* Ovvio dalle disuguaglianze $cf(\alpha) \leq |\alpha| \leq \alpha$ e dal fatto che $\alpha$ è un cardinale se e solo se $|\alpha| = \alpha$. □

**41.10 Definizione.** Un cardinale successore è un cardinale della forma della forma $\kappa^+$ dove $\kappa^+$ è il minimo cardinale maggiore di $\kappa$. Equivalentemente i cardinali successori sono i cardinali finiti e i cardinali della forma $\aleph_{\alpha+1}$ per qualche ordinale $\alpha$.

**41.11 Lemma.** *Ogni cardinale successore $\kappa^+$ è regolare. In particolare $\aleph_1$ è regolare.*

*Dimostrazione.* Supponiamo per assurdo che $cf(\kappa^+) < \kappa^+$. Ogni cardinale strettamente minore di $\kappa^+$ è minore o uguale a $\kappa$, e visto che $cf(\kappa^+)$ è un cardinale otteniamo $cf(\kappa^+) \leq \kappa$, ovvero esiste una funzione cofinale $f : \kappa \to \kappa^+$. Ciò ci permette di scrivere $\kappa^+ = \sup_{\alpha<\kappa} f(\alpha) = \bigcup_{\alpha<\kappa} f(\alpha)$, dove $\alpha$ varia tra gli ordinali minori di $\kappa$ (non necessariamente iniziali). Per ogni $\alpha < \kappa$, $f(\alpha) \in \kappa^+$, e visto che $\kappa^+$ è iniziale, $|f(\alpha)| < \kappa^+$, ovvero $|f(\alpha)| \leq \kappa$ (sebbene possa accadere che $f(\alpha) > \kappa$). Poiché la cardinalità dell'unione è minore o uguale alla somma delle cardinalità, abbiamo $\kappa^+ \leq \Sigma_{\alpha<\kappa}|f(\alpha)| \leq \kappa \cdot \kappa = \kappa$, il che è assurdo. □

**41.12 Esempio.** $\aleph_\omega$ e $\aleph_{\omega+\omega}$ hanno cofinalità $\omega$, quindi non sono regolari.

*Dimostrazione.* Basta considerare le funzioni cofinali $n \mapsto \aleph_n$ e $n \mapsto \aleph_{\omega+n}$. □

**41.13 Esercizio.** Un cardinale $\kappa$ è regolare se e solo se per ogni famiglia $(A_i \mid i \in I)$ di insiemi $A_i$ tali che $|A_i| < \kappa$ e $|I| < \kappa$, si ha $|\bigcup_{i\in I} A_i| < \kappa$.

**41.14 Teorema.** *Per ogni ordinale $\alpha$, $cf(2^{\aleph_\alpha}) > \aleph_\alpha$.*

*Dimostrazione.* Sia $\theta = cf(2^{\aleph_\alpha})$. Possiamo allora scrivere $2^{\aleph_\alpha} = \Sigma_{\nu<\theta}\kappa_\nu$ dove $\kappa_\nu$ è un cardinale minore di $2^{\aleph_\alpha}$. Per il teorema di König $\Sigma_{\nu<\theta}\kappa_u < \Pi_{\nu<\theta}2^{\aleph_\alpha} = (2^{\aleph_\alpha})^\theta$. Se fosse $\theta \leq \aleph_\alpha$, avremmo l'assurdo $2^{\aleph_\alpha} < (2^{\aleph_\alpha})^\theta = 2^{\aleph_\alpha \cdot \theta} = 2^{\aleph_\alpha}$. □

**41.15 Corollario.** *La cofinalità di $2^{\aleph_0}$ è diversa da $\omega$. Quindi in particolare $2^{\aleph_0}$ è diverso sia da $\aleph_\omega$ (già lo sapevamo) che da $\aleph_{\omega+\omega}$ (ma non si può stabilire, in base agli assiomi, se sia più grande o più piccolo).*

# 42 Gerarchia di von Neumann

**42.1 Assioma.** L'assioma di fondazione dice che ogni insieme non vuoto $X$ contiene un elemento $a$ che è disgiunto da $X$ (ricordiamo che stiamo assumendo che non vi siano urelementi, ovvero ogni oggetto è un insieme).

**42.2 Esercizio.** L'assioma di fondazione equivale al fatto che la relazione di appartenenza su $V$ sia ben fondata.

*Dimostrazione.* Assumiamo la fondazione. Se per assurdo $\in$ non è ben fondata su $V$ esiste un sottoinsieme non vuoto $X$ di $V$ senza elementi $\in$-minimali, ovvero per ogni $a \in X$ esiste $b \in X$ con $b \in a$. Questo significa in particolare che $a \cap X \neq \emptyset$ (in quanto $b$ vi appartiene) e quindi $X$ non ha elementi disgiunti da $X$ stesso, contraddicendo l'assioma di fondazione.

Viceversa, se $\in$ è ben fondata su $V$, dato un insieme non vuoto $X$ e considerato un suo elemento $a \in V$ che sia $\in$-minimale, dobbiamo necessariamente avere $a \cap X = \emptyset$, altrimenti un eventuale elemento $b \in a \cap X$ contraddirrebbe la minimalità di $a$. □

**42.3 Definizione.** La gerarchia di von Neumann è definita per ricursione transfinita nel modo seguente:

$$\begin{array}{lcl} V_0 & = & \emptyset \\ V_{\alpha+1} & = & \mathcal{P}(V_\alpha) \\ V_\lambda & = & \bigcup_{\alpha<\lambda} V_\alpha \text{ per } \lambda \text{ ordinale limite.} \end{array}$$

**42.4 Esercizio.** Ogni $V_\alpha$ è transitivo e per $\beta < \alpha$ si ha $V_\beta \subseteq V_\alpha$.

*Dimostrazione.* Per induzione su $\alpha$. Se $\alpha$ è limite $V_\alpha$ include ogni $V_\beta$ con $\beta < \alpha$ essendo l'unione di tali insiemi. Inoltre $V_\alpha$ è transitivo essendo l'unione di insiemi che per ipotesi induttiva sono transitivi. Se $\alpha = \gamma + 1$ per ipotesi induttiva $V_\gamma$ è transitivo, e quindi $x \in V_\gamma \to x \subseteq V_\gamma$, ovvero $V_\gamma \subseteq \mathcal{P}(V_\gamma) = V_{\gamma+1}$. Rimane da dimostrare la transitività di $V_{\gamma+1}$. Se $x \in y \in V_{\gamma+1}$, allora $x \in y \subseteq V_\gamma$, e quindi $x \in V_\gamma$. Ma sappiamo che $V_\gamma \subseteq V_{\gamma+1}$ e pertanto $x \in V_{\gamma+1}$. □

Assumendo l'assioma di fondazione possiamo definire il rango di un insieme per ricursione sulla relazione ben fondata $\in$.

**42.5 Definizione.** Il rango $\rho(x)$ di un insieme $x$ è definito da

$$\rho(x) = \sup\{\rho(y) + 1 : y \in x\}.$$

**42.6 Lemma.** *$x \in V_\alpha$ se e solo se $\rho(x) < \alpha$.*

*Dimostrazione.* Per induzione su $\alpha$. Assumiamo $x \in V_\alpha$ e dimostriamo $\rho(x) < \alpha$. Se $\alpha$ è limite allora $x \in V_\beta$ per qualche $\beta < \alpha$, e per ipotesi induttiva $\rho(x) < \beta < \alpha$. Se $\alpha = \gamma + 1$, allora $V_\alpha = \mathcal{P}(V_\gamma)$ e $x \subseteq V_\gamma$. Per ipotesi induttiva gli elementi $y \in x$ hanno $\rho(y) < \gamma$, e quindi $\rho(y) + 1 \leq \gamma$. Per definizione di $\rho(x)$ ne segue che $\rho(x) \leq \gamma < \alpha$.

Viceversa assumiamo $\rho(x) < \alpha$ e dimostriamo $x \in V_\alpha$. Se $\alpha$ è limite $\rho(x) < \beta$ per qualche $\beta < \alpha$ per ipotesi induttiva $x \in V_\beta \subseteq V_\alpha$. Supponiamo allora

$\alpha = \gamma + 1$. Per ogni $y \in x$ si ha $\rho(y) < \rho(x) < \gamma + 1$ e pertanto $\rho(y) < \gamma$. Per ipotesi induttiva $y \in V_\gamma$, e visto che ciò vale per tutti gli elementi di $x$ ne segue che $x \in \mathcal{P}(V_\gamma) = V_\alpha$. □

**42.7 Osservazione.** Anche senza assumere l'assioma di fondazione, per ogni $\alpha$ la relazione di appartenenza ristretta a $V_\alpha$ è ben fondata e per ogni $x \in V_\alpha$ $\rho(x) < \alpha$. La dimostrazione è analoga alla precedente.

**42.8 Corollario.** *L'assioma di fondazione equivale all'affermazione che ogni insieme $x$ appartiene a qualche $V_\alpha$, ovvero $V = \bigcup_{\alpha \in ON} V_\alpha$.*

*Dimostrazione.* Dato $x \in V$, se vale la fondazione $\alpha = \rho(x)$ è ben definito e abbiamo $x \in V_\alpha$. Viceversa se $V = \bigcup_{\alpha \in ON} V_\alpha$ non possono esserci successioni decrescenti infinite $x_{n+1} \in x_n$ altrimenti, supponendo $x_0 \in V_\alpha$, per la transitività di $V_\alpha$ l'intera successione apparterrebbe a $V_\alpha$, contraddicendone la ben fondatezza. □

**42.9 Corollario.** *Se $x \subseteq y \in V_\alpha$, allora $x \in V_\alpha$.*

*Dimostrazione.* Se $x \subseteq y$, in base alla definizione di $\rho$ si ha immediatamente $\rho(x) \leq \rho(y)$, e la tesi segue dal risultato precedente. □

Assumendo l'assioma di fondazione abbiamo un semplice criterio per distinguere gli insiemi dalle classi proprie.

**42.10 Lemma.** *Una classe $X \subseteq V$ è un insieme se e solo se appartiene a $V_\alpha$ per qualche $\alpha \in ON$.*

*Dimostrazione.* Se $X$ è un insieme, possiamo definire $\alpha = \rho(X)$ e abbiamo $X \in V_\alpha$. Viceversa se $X \in V_\alpha$ allora ovviamente $X$ è un insieme. □

**42.11 Definizione.** Definiamo $\beth_0 = \aleph_0$, $\beth_{\alpha+1} = 2^{\beth_\alpha}$ e $\beth_\lambda = \sup_{\alpha<\lambda} \beth_\alpha$ per $\lambda$ limite.

**42.12 Esercizio.** Per ogni $\alpha$, $|V_{\omega+\alpha}| = \beth_\alpha \geq \aleph_\alpha$.