Università degli Studi di Pisa - Dipartimento di Matematica

Elementi di teoria degli insiemi

Autore
Alessio Del Vigna
delvigna@mail.dm.unipi.it

Titolare del corso
Prof. Alessandro Berarducci
Università di Pisa

Note dell'omonimo corso tenuto dal Prof. Alessandro Berarducci nell'anno accademico 2010-2011.

Queste note contengono almeno un errore. Se ne trovaste qualcuno, vi pregherei di segnalarmelo all'indirizzo delvigna@mail.dm.unipi.it.

Una precisazione. La frase "Queste note contengono almeno un errore" è un primo esempio di teorema di esistenza. Come ogni teorema che si rispetti, ecco la sua dimostrazione: se ci sono errori, ce ne sono; se non ci sono errori, allora è questa stessa frase a costituire un errore. Così sappiamo che un errore c'è, ma in questo momento non sappiamo dire qual è: questo, del resto, è il prezzo dei teoremi di esistenza! Pertanto, se l'unico errore dovesse essere la frase "Queste note contengono almeno un errore", non segnalatelo: eccezion fatta per questa frase, significherebbe -felicemente- che queste note non contengono altri errori.

Indice

1 Assiomi della teoria degli insiemi di Zermelo–Fraenkel **1**
1.1 Introduzione agli insiemi 1
1.2 Simboli logici e formule 2
1.3 Gli assiomi 4
1.3.1 I numeri naturali 11

2 Relazioni e funzioni **15**
2.1 Coppie ordinate 15
2.2 Relazioni 17
2.3 Funzioni 20
2.4 Relazioni di equivalenza 24
2.5 Relazioni d'ordine 26

3 Assioma della scelta **31**
3.1 Gli ultimi assiomi 31
3.2 L'assioma della scelta 32

4 Numeri naturali e buoni ordini **37**
4.1 Richiami e proprietà dei numeri naturali 37
4.2 Buoni ordini 39

5 Insiemi finiti, numerabili e non numerabili **47**
5.1 Cardinalità degli insiemi 47
5.2 Insiemi finiti 52
5.3 Insiemi numerabili 55
5.4 Insiemi non numerabili 60

6 Numeri cardinali **65**
6.1 Aritmetica dei cardinali 65
6.2 La cardinalità del continuo 68

7 Numeri ordinali **73**
7.1 Richiami sui buoni ordini e induzione transfinita 73
7.2 Segmenti iniziali e isomorfismi 75
7.3 Limiti di buoni ordini 79
7.4 Il teorema di ricursione 82
7.5 Numeri ordinali 85
7.6 Altre proprietà, induzione e ricursione 89
7.7 Aritmetica degli ordinali: addizione 91
7.8 Aritmetica degli ordinali: moltiplicazione e esponenziazione 96
7.8.1 Operazioni tra ordinali e cardinalità 99
7.9 Forma normale 101

8 Ordinabilità e aleph **103**
8.1 Lemma di Zorn e teorema di Zermelo 103
8.2 Ordinali iniziali e numeri di Hartogs 106
8.3 Addizione e moltiplicazione di aleph 111
8.3.1 Un'osservazione sull'assioma della scelta 114

9 Aritmetica cardinale e cofinalità **115**
9.1 Somme e prodotti infiniti 115
9.1.1 L'ipotesi del continuo 120
9.2 Cofinalità 121
9.3 Esponenziazione di cardinali 125

10 L'assioma di fondazione e gli insiemi ben fondati **127**
10.1 Relazioni ben fondate 127
10.2 Gerarchia di von Neumann 129

A L'insieme dei numeri reali **133**
A.1 Gli interi e i razionali 133
A.2 Numeri reali 136

A Esercizi risolti **139**
A.1 Teoria degli insiemi generale 139
A.2 Cardinalità 140
A.2.1 I boreliani di $\mathbb{R}^N$ 144
A.3 Buoni ordini e numeri ordinali 147
A.4 Cardinali 153
A.4.1 La succesione *beth* 154

Capitolo 1

Assiomi della teoria degli insiemi di Zermelo–Fraenkel

1.1 Introduzione agli insiemi

Il concetto centrale di questo libro è che un *insieme* è, almeno in superficie, estremamente semplice. Un insieme è una qualsiasi collezione, gruppo di oggetto. Così abbiamo l'insieme di tutti gli studenti iscritti all'Università di Pisa nel gennaio del 2009, l'insieme di tutti i numeri naturali pari, l'insieme dei punti di un certo piano che distano esattamente 2 cm da un punto dato, l'insieme di tutti gli elefanti rosa. Gli insiemi non sono oggetti del mondo reale, come i tavoli o e stelle; sono creati dalla nostra mente, non dalle nostre mani. Un sacco di patate non è un insieme di patate, l'insieme di tutte le molecole in una goccia di acqua non è lo stesso oggetto che la goccia d'acqua stessa. La mente umana possiede l'abilità di astrarre, di pensare a una variatà di oggetti diversi come messi insieme da una proprietà comune. La proprietà in questione potrebbe essere niente più dell'abilità di pensare questi oggetti insieme. Così è un insieme quello che consiste esattamente dei numeri 2, 7, 12, 13, 29, 34 e 11000, benché non si veda cosa accomuni questi numeri insieme. Georg Cantor, un matematico tedesco che ha fondato la teoria degli insiemi in una serie di articoli pubblicati negli ultimi trent'anni del XIX secolo, espresse questo concetto come segue: "Unter einer Menge verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objecten in unserer Anschauung oder unseres Denkens (welche die Elemente von M genant werden) zu einem ganzen." [Un insieme è una collezione di definiti e distinti oggetti della nostra intuizione o del nostro pensiero. Gli oggetti sono chiamati elementi (membri) dell'insieme].
In questo libro, vogliamo sviluppare la teoria degli insiemi come fondamento per le altre discipline matematiche. Quindi, non ci interesseranno insiemi di molecole, di persone, ma solo insiemi di oggetti matematici, come numeri, punti dello spazio,

funzioni o insiemi stessi. In verità, i primi tre concetti possono essere definiti – nell'ambito della teoria degli insiemi – come insiemi con particolari proprietà, e lo faremo nei prossimi capitoli. Così gli unici oggetti a cui saremo interessati saranno gli insiemi. La teoria degli insiemi di Zermelo–Fraenkel (ZF) è una teoria del primo ordine in un linguaggio che comprende, oltre ai simboli logici e al simbolo di uguaglianza (comuni a tutte le teorie del primo ordine), solamente il simbolo di relazione binaria $\in$. L'idea è che $\in$ rappresenta la relazione di *appartenenza* di cui è probabile che il lettore abbia già qualche idea intuitiva. Tale idea intuitiva ci guiderà nella scelta degli assiomi della teoria. Una volta stabiliti gli assiomi, dobbiamo tuttavia considerare $\in$ come un simbolo indefinito della teoria che siamo liberi di interpretare come vogliamo con la sola condizione che gli assiomi siano verificati. In altre parole nelle dimostrazioni non dobbiamo lasciarci guidare da una qualche precedente intuizione che possiamo avere riguardo alla relazione di appartenza, ma supporre invece che $\in$ sia una qualsiasi relazione binaria tra oggetti che che chiamiamo *insiemi* e di cui l'unica cosa che sappiamo è ciò che viene espresso dagli assiomi.

1.2 Simboli logici e formule

In questa parte della matematica si fa un massiccio uso di formule, un po' più di quanto è consuetudine fare in altri settori. In realtà, uno dei primi compiti della logica matematica è quello di fornire una precisa e rigorosa definizione di formula, ma di questo ci occuperemo solo più avanti. Intanto dobbiamo fornire gli ingredienti necessari alla costruzione di formule. Per dare agli assiomi una forma precisa, come già accennato nell'introduzione, dobbiamo sviluppare la teoria degli insiemi nell'ambito del calcolo dei predicati del primo ordine. Intanto ricordiamo il significato dei *connettivi logici*: questo è quello dettato dalle tavole di verità. Se P e Q sono proposizioni cui si può attribuire uno e un solo valore di verità tra V (vero) e F (falso) allora

P	Q	$\neg P$	$P \vee Q$	$P \wedge Q$	$P \to Q$
V	V	F	V	V	V
V	F	F	V	F	F
F	V	V	V	F	V
F	F	V	F	F	V

.

I simboli che compaiono dalla terza colonna della tabella si dicono rispettivamente *negazione*, *congiunzione*, *disgiunzione* e *implicazione*.
Per giungere a definizioni precise, sono state fatte delle scelte non sempre in accordo con il linguaggio naturale, cioè con il comune linguaggio di tutti i giorni.

Ad esempio la disgiunzione $\vee$ ("o") è *inclusiva*, cioè $P \vee Q$ è vera anche nel caso in cui P e Q siano entrambe vere[1]. Un altro caso non pienamente corrispondente all'uso comune è quello in cui accettiamo come vera l'implicazione $P \to Q$ anche quando P è falsa e Q è vera. Tuttavia le definizioni date sono in pieno accordo con la pratica matematica, come avremo modo di vedere con diversi esempi. Infatti in matematica un enunciato $P \to Q$ viene considerato vero nel caso in cui P sia falso.

Definizione 1.2.1. Due enunciati composti A e B si dicono *logicamente equivalenti*, e si scrive $A \equiv B$, se hanno la stessa tavola di verità.

In questo caso attribuiremo ad A e B lo stesso significato e quindi (a seconda della convenienza) potremo sostituire uno all'altro in ogni ragionamento. A tal fine si definisce la *doppia implicazione* come

$$P \leftrightarrow Q \equiv (P \to Q) \wedge (Q \to P).$$

Nel prossimo esempio sono raccolte le equivalenze logiche più usate nella pratica.

Esempio 1.2.1. Il lettore verifichi, costruendo le tavole di verità, le seguenti equivalenze logiche:
(1) doppia negazione: $\neg(\neg P) \equiv P$;
(2) prima legge di de Morgan: $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$;
(3) seconda legge di de Morgan: $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$;
(4) contronominale: $P \to Q \equiv \neg Q \to \neg P$;
(5) negazione dell'implicazione: $\neg(P \to Q) \equiv P \wedge \neg Q$.

Inoltre esistono i due *quantificatori*: il quantificatore $\forall x$ è da intendersi come "per ogni insieme x" e $\exists x$ come "esiste un insieme x". Attenzione che si può quantificare, come appena detto, solo su insiemi e non su altri oggetti[2]. Adesso siamo pronti per definire induttivamente le formule:

Definizione 1.2.2. Diciamo *formule atomiche* le espressioni del tipo $x \in y$ o $x = y$. Una *formula* della teoria degli insiemi è costruita a partire dalle formule atomiche mediante l'uso dei connettivi logici e dei quantificatori.

Vogliamo ulteriormente precisare cosa intendiamo con la precedente definizione. L'induttività è data dal fatto seguente: se φ e ψ sono formule, allora sono formule

$$\neg\varphi, \quad \varphi \vee \psi, \quad \varphi \wedge \psi, \quad \varphi \to \psi, \quad \forall x\, \varphi, \quad \exists x\, \varphi.$$

[1] è interessante il fatto che questa ambiguità di significato che la disgiunzione ha in italiano, non sussisteva invece nel latino. In quella lingua si usavano infatti due congiunzioni diverse: "vel" per denotare la "o" inclusiva (quella corrispondente al nostro connettivo), e "aut" per la *disgiunzione esclusiva*, dove P aut Q è falsa quando P e Q sono entrambe vere.

[2] logica del primo ordine indica che c'è un insieme di riferimento e i quantificatori possano riguardare solo gli elementi di tale insieme e non i sottoinsiemi infatti.

1.3 Gli assiomi

Dopo questo breve preambolo sui simboli logici, passiamo finalmente ad occuparci degli insiemi, sui quali è incentrato tutto questo libro. Come già anticipato non definiremo cosa sia un insieme, perché si tratta di una nozione primitiva non riconducibile ad altri concetti più elementari. Informalmente, sarà sufficiente pensare ad un *insieme* come ad una collezione di oggetti, priva di ogni struttura. Quegli oggetti che costituiscono un insieme si dicono i suoi *elementi*.
Per vedere un esempio di formula, che non abbiamo avuto modo di specificare nella fine dello scorso paragrafo, definiamo adesso una relazione tra insiemi che ci sarà molto utile:

Definizione 1.3.1. Dati X e Y insiemi, definiamo l'*inclusione* tra insiemi nel modo seguente:

$$X \subseteq Y \leftrightarrow (\forall x)(x \in X \rightarrow x \in Y).$$

La definizione precedente ci dice che un insieme X è incluso in Y se e solo se ogni elemento di X è anche elemento di Y, e tale proprietà viene espressa mediante una formula (nel senso che abbiamo definito).

Osservazione 1.3.1. Ogni volta che scriviamo una formula non ha alcun significato l'utilizzo delle lettere minuscole o maiuscole. Per tradizione gli insiemi vengono denotati con lettere maiuscole, ma in questo ambito della matematica la frase precedente ha poco senso: infatti ogni oggetto è considerato come insieme (in quanto un insieme ha per elementi altri insiemi e così via).

Assioma di estensionalità Due insiemi sono uguali se e solo se contengono gli stessi elementi, ossia

$$X = Y \leftrightarrow (\forall x)(x \in X \leftrightarrow x \in Y).$$

Questo primo assioma non merita particolari commenti, in quanto esprime l'idea base di un insieme: un insieme è determinato dai suoi elementi[3].
Intuitivamente un insieme è una collezione di tutti gli elementi che soddisfano una certa proprietà data e quindi ci aspetteremmo di avere un assioma che esprima questo fatto. Questo è un fatto che il filosofo Frege postulava nel suo sistema di assiomi. Egli cioè considerò il seguente:

Schema di assiomi di comprensione (è falso) Se $P(x)$ è una proprietà allora esiste un insieme $Y = \{x \mid P(x)\}$.

[3]in realtà quello che si dovrebbe postulare è solo $(\forall x)(x \in X \leftrightarrow x \in Y) \rightarrow X = Y$ in quanto l'altra implicazione è vera perché è una proprietà dell'uguaglianza. Quindi avremmo la veridicità di questa formulazione dell'assioma per come è stata definita la doppia implicazione.

Purtruppo però, non ogni proprietà descrive un insieme: questo a dire che l'assioma precedente in realtà conduce a contraddizioni, e quindi è da escludere. Adesso vedremo un tale esempio, molto famoso, e noto come *paradosso di Russell*:

Esempio 1.3.1 (paradosso di Russell)**.** Sia S l'insieme i cui elementi sono tutti e soli gli insiemi che non sono elementi di se stessi; ossia

$$S = \{X \mid X \notin X\}$$ [4]

Ci chiediamo se S appartiene o no a S: se $S \in S$ allora $S \notin S$; ma del resto se $S \notin S$ allora $S \in S$. In entrambi i casi si ottiene una contraddizione.
Adesso un veloce commento su questo esempio potrebbe essere d'aiuto. Innanzitutto non c'è niente di sbagliato nel definire S come insieme di insiemi: gli insiemi i cui elementi sono ancora insiemi sono legittimamente ammessi in matematica e non portano a contraddizioni. Inoltre, non è difficile portare alcuni esempi di elementi di S, basti pensare all'insieme dei numeri naturali: tale insieme è in S in quanto non è elemento di se stesso (non essendo un numero naturale). Però non è semplice dare esempi di insiemi che non stiano in S, ma questo per noi è irrilevante in questo momento. La dimostrazione precedente porterebbe ad una contraddizione anche se non esistessero esempi di insiemi che sono elementi di se stessi[5].

Come risolvere questa contraddizione? Noi assumiamo di avere un insieme S definito come l'insieme di tutti gli insiemi che non sono elementi di se stessi, e deriviamo una contraddizione come immediata conseguenza della definizione di S. Questo può solo voler dire che non esiste alcun insieme che soddisfi la definizione di S. In altre parole, questo argomento prova che non esistono insiemi i cui elementi siano precisamente gli insiemi che non sono elementi di se stessi. La lezione contenuta nel paradosso di Russell e in simili esempi è che semplicemente definendo un insieme non se ne prova l'esistenza. Ci sono proprietà che non definiscono insiemi; cioè, non è possibile raccogliere tutti gli oggetti con tali proprietà in un solo insieme. Questa osservazione lascia i teorici degli insiemi con il desiderio di determinare le proprietà che definiscono insiemi. Sfortunatamente, nessuna strada per fare ciò è conosciuta, e alcuni risultati di logica (come il Teorema di incompletezza scoperto da Kurt Gödel) sembrano indicare che una risposta completa non sia possibile.
Ma allora la difficoltà si supera se postuliamo l'esistenza di un insieme di tutti gli oggetti con una data proprietà solo se già esiste qualche insieme al quale appartengono tutti:

[4] osserviamo che la formula $X \notin X$ equivale per definizione a $\neg(X \in X)$.

[5] un possibile candidato sarebbe l'insieme di tutti gli insiemi: chiaramente tale insieme è elemento di se stesso. Tuttavia l'esistenza di un tale insieme porta ad una contraddizione per conto proprio e per una via molto più sottile, come avremo modo di vedere.

Schema di assiomi di separazione Sia $P(x)$ una prorietà. Per ogni insieme X c'è un insieme Y che contiene gli elementi di X che soddisfano $P(x)$, ossia

$$(\forall X)(\exists Y)(\forall x)(x \in Y \leftrightarrow x \in X \wedge P(x)).$$

Osservazione 1.3.2. Osserviamo che l'insieme Y di cui si postula l'esistenza nel precedente assioma è anche unico. Ad assicurarci questo fatto è l'assioma di estensionalità, e ciò giustifica la definizione che segue l'osservazione.

Definizione 1.3.2. Chiamiamo l'unico insieme Y postulato nell'assioma di separazione l'insieme $Y = \{x \in X \mid P(x)\}$.

Osservazione 1.3.3. Nel testo dell'assioma si legge "schema di assiomi": questo significa che in realtà questo non è un assioma, ma sono infiniti assiomi, uno per ogni proprietà P (anche se non abbiamo ancora definito formalmente cosa sia una proprietà, anche se lo faremo tra poche righe).

A questo punto abbiamo usato il termine "proprietà" più di una volta, ma senza mai averlo definito. Ciò potrebbe avere conseguenze in effetti drammatiche, come mostra il *paradosso di Richard*:

Esempio 1.3.2 (paradosso di Richard)**.** Consideriamo il seguente insieme:

$$A = \{n \in \mathbb{N} \mid x \text{ è descrivibile con meno di 100 lettere}\} \subseteq \mathbb{N}.$$

In effetti A è un insieme finito, in quanto con 100 lettere si possono dire solo un numero finito di frasi. Allora consideriamo

$$m = \min(\mathbb{N} - A) \tag{1.1}$$

che esiste e sta ancora in A. Siamo già arrivati al paradosso: $m \in A$ e quindi non è descrivibile con meno di 100 lettere, ma la (1.1) in effetti lo descrive con meno di 100 lettere.

Come abbiamo fatto per il paradosso di Russell dovremmo vedere dove è il problema ed eliminarlo. A ben vedere il fatto problematico sta nella parola "descrivibile". Per eliminare qualsiasi inconveniente di questo tipo nell'interpretazione della parola "descrivibile" si è drastici. Si prendono come *proprietà descrivibili* solo quelle che fanno uso dei simboli di appartenenza, di uguaglianza, dei connettivi e dei quantificatori.

Osservazione 1.3.4. Un'obiezione a questa definizione potrebbe essere "cosa ci dà la certezza che la proprietà precedente non sia esprimibile con $\in$, $=$, connettivi e quantificatori?" In effetti la domanda è mal posta. La teoria di Zermelo–Fraenkel dimostra i suoi assiomi e tutte le proposizioni che ne discendono. La proprietà di essere descrivibile con meno di 100 lettere non viene neanche presa in considerazione, in quanto non scritta nel linguaggio che la teoria suddetta accetta.

Con gli strumenti a noi in mano in questo momento possiamo già dimostrare un fatto importante. Prima però precisiamo che $(P \to \bot) \leftrightarrow \neg P$ dove con $\bot$ indichiamo l'assurdo: quello appena descritto è lo schema della dimostrazione per assurdo.

Teorema 1.3.1 (inesistenza dell'insieme di tutti gli insiemi)**.** $\neg(\exists \mathbb{V})(\forall x)(x \in \mathbb{V})$.

Dimostrazione. Se esistesse un tale $\mathbb{V}$ allora, per l'assioma di separazione, potremmo costruire l'insieme $R = \{x \in \mathbb{V} \mid x \notin x\}$ (infatti abbiamo vincolato la scelta di x tra gli elementi di $\mathbb{V}$, insieme esistente per quanto appena supposto). Ma allora otteniamo per definizione di $\mathbb{V}$

$$R \in R \leftrightarrow R \in \mathbb{V} \wedge R \notin R,$$

e poiché $R \in \mathbb{V}$ è vero per definizione di $\mathbb{V}$ si ha $R \in R \leftrightarrow R \notin R$, un assurdo. □

Osservazione 1.3.5. Il precedente teorema fa riflettere: intuitivamente un modello della teoria degli insiemi è un *dominio* (o universo) di oggetti, chiamati insiemi, su cui è definita una relazione binaria $\in$ che verifica tutti gli assiomi di Zermelo–Fraenkel. Come vedremo, all'interno di un tale universo possono essere definiti tutti gli usuali oggetti che interessano i matematici (numeri naturali, numeri reali, funzioni...). Tuttavia, fissato un modello, il teorema precedente afferma che il suo universo $\mathbb{V}$ non può esso stesso essere un insieme del modello (simili pseudo–insiemi verranno chiamati *classi*). Può però capitare che $\mathbb{V}$ sia un insieme relativamente ad un universo più grande $\mathbb{V}'$ che verifica anch'esso gli assiomi, ma lo stesso problema si ripresenta poi per $\mathbb{V}'$.

L'osservazione precedente in effetti dà uno spunto interessante per poter definire un concetto più ampio di quello di insieme. Benché lavoriamo in ZFCche ha un solo tipo di oggetto (chiamato insieme) introduciamo la nozione informale di classe. Lo facciamo solo per motivi di comodità: è più facile manipolare classi che formule. Sappiamo che $\{x \mid P(x)\}$ esiste se e solo se $(\exists A)(\forall x)(x \in A \leftrightarrow P(x))$.

Definizione 1.3.3. Sia $P(x)$ una formula. Allora gli $\{x \mid P(x)\}$ si dicono *classi.*

Osservazione 1.3.6. Il fatto che $\mathbb{V}$ non esista non significa che non c'è, sennò non potremmo neanche parlarne: $\mathbb{V}$ non esiste come insieme, ma come classe sì.

Ciò che abbiamo detto appena prima della definizione ci dice che $\{x \in A \mid P(x)\}$ è di più di una classe, ma addirittura un insieme. Questo si può esprimere ricordando che se una classe è inclusa in un insieme allora è essa stessa un insieme.
Ha anche senso definire l'*inclusione* tra classi:

$$\{x \mid P(x)\} \subseteq \{x \mid Q(x)\} \leftrightarrow (\forall x)(P(x) \to Q(x)).$$

Non può verificarsi invece l'appartenza di una classe ad un'altra: se così fosse la classe che appartiene dovrebbe esistere, cioè dovrebbe essere un insieme (in quanto elemento dell'altra classe)[6]. Adesso deve postularsi l'esistenza di un insieme privo di elementi, allora enunciamo:

Assioma dell'insieme vuoto Esiste un insieme che non ha elementi, ossia

$$(\exists X)(\forall y)\neg(y \in X).$$

Osservazione 1.3.7. Esiste un insieme vuoto, e questo è unico. Come già abbiamo avuto modo di osservare, ciò segue dall'assioma di estensionalità. Supponiamo che X_1 e X_2 siano due insiemi privi di elementi, ossia

$$(\forall y)\neg(y \in X_1) \qquad \text{e} \qquad (\forall y)\neg(y \in X_2).$$

Ma allora $(\forall y)(y \in X_1 \to y \in X_2)$ è vera in quanto è un'implicazione con premessa falsa; analogamente si ha che $(\forall y)(y \in X_2 \to y \in X_1)$ è vera. Ma allora per assioma di estensionalità $X_1 = X_2$.

Definizione 1.3.4. L'insieme senza elementi è detto *insieme vuoto* ed è denotato con $\emptyset$.

Esempio 1.3.3. Per ogni A, $\emptyset \subseteq A$ è vera: infatti equivale a $\forall x(x \in \emptyset \to x \in A)$, e dal momento che l'ipotesi dell'implicazione è falsa l'implicazione è vera, come risulta dalla tavola di verità.

Il nostro sistema assiomatico per ora non è molto potente: l'unico insieme di cui sappiamo l'esistenza è l'insieme vuoto, e qualsiasi applicazione dell'assioma di separazione sull'insieme vuoto produce ancora l'insieme vuoto. Infatti si ha che $\{x \in \emptyset \mid P(x)\} = \emptyset$ indipendentemente da quale sia la proprietà P (dimostrare). I prossimi princìpi postulano che alcune delle costruzioni più frequenti in matematica portano in effetti ad insiemi.

Assioma della coppia Per ogni x e y esiste un insieme che contiene esattamente x e y, ossia

$$(\forall x)(\forall y)(\exists C)(\forall c)(c \in C \leftrightarrow c = x \vee c = y).$$

Anche in questo caso l'assioma di estensionalità assicura l'unicità di tale insieme e dunque ha senso dare la seguente definizione:

[6] giusto per riassumere in maniera sintetica l'argomento delle classi precisiamo il seguente fatto. Gli elementi di un insieme sono insiemi, gli elementi di una classe sono insiemi, gli elementi di una classe non possono essere classi.

Definizione 1.3.5. L'unico insieme Z di cui è postulata l'esistenza nell'assioma della coppia si denota con $\{x, y\}$.

Osservazione 1.3.8. Osserviamo che l'assioma precedente permette anche di definire il *singoletto*. Infatti $\{x\} = \{x, x\}$, ossia basta porre $x = y$ nell'assioma che definisce l'insieme coppia.

Osservazione 1.3.9. Come è di immediata verifica dalla definizione dell'insieme coppia data nell'assioma, si ha che $\{x, y\} = \{y, x\}$. Questo ci dice che nell'enumerazione degli elementi di un insieme non conta l'ordine con cui si scrivono.

Adesso veniamo alla costruzione di unioni:

Assioma dell'unione Per ogni X esiste un insieme Y costituito da tutti gli elementi contenuti negli elementi di X; ossia

$$(\forall X)(\exists Y)(\forall y)(y \in Y \leftrightarrow (\exists A)(A \in X \wedge y \in A)).$$

Per come è stato definito l'insieme unione, per ogni X esiste ed è unico (per estensionalità) un insieme

$$Y = \{y \mid (\exists A \in X)(y \in A)\} = \bigcup \{A \mid A \in X\} = \bigcup_{A \in X} A = \bigcup X,$$

l'*unione di* X. L'ultima notazione usata si deve interpetare nel modo descritto subito prima dell'uguaglianza, altrimenti può trarre in inganno (se per esempio si fa riferimento alle notazione che il lettore già conoscerà per l'unione): l'unione di X è l'unione di tutti gli insiemi che appartengono a X.

Osservazione 1.3.10. Osserviamo che l'assioma dell'unione postula l'esistenza di questo insieme:

$$Y = \{y \mid (\exists A \in X)(y \in A)\},$$

come già abbiamo scritto prima. Ma notiamo che la forma con la quale è stato scritto Y è della forma "proibita", quella che abbiamo dovuto scartare per non incorrere in paradossi come quello di Russell: infatti non è specificato da quale insieme già esistente si debba prendere t. In effetti si accettano un numero finito di eccezioni per quello schema di assiomi di comprensione: l'enunciato infatti postulerebbe l'esistenza di un insieme ogni volta che è data una proprietà, e quindi in realtà rappresenta infiniti assiomi. Per alcune proprietà però riteniamo vera l'esistenza dell'insieme $\{x \mid P(x)\}$, e non faremo ciò solo per l'unione, ma anche in altri casi (come ad esempio per l'insieme potenza).

Osservazione 1.3.11. Si osservi che $(\exists x \in A)(P(x))$ è un'abbreviazione: non è possibile quantificare su formule, in quanto si può solo quantificare su insiemi. Allora la notazione appena detta, che abbiamo utilizzato proprio per scrivere più esplicitamente l'unione di X, sta per $(\exists x)(x \in A \wedge P(x))$.
Per completezza, notiamo che scriveremo prima o poi $(\forall x \in A)(P(x))$. Come prima, questa è un'abbreviazione per $(\forall x)(x \in A \to P(x))$.

Grazie all'assiome dell'unione e della coppia possiamo definire anche le *unioni binarie*. Siano X e Y insiemi, allora esiste l'insieme $C = \{X, Y\}$ (assioma della coppia) e quindi possiamo costruire $\bigcup C = \bigcup\{X, Y\}$ (assioma dell'unione). Tale unico insieme viene indicato con $X \cup Y$ e si chiama unione tra X e Y; vale più precisamente

$$X \cup Y = \{a \mid a \in X \vee a \in Y\}.$$

Definizione 1.3.6. Definiamo *unione binaria* di X e Y l'insieme $X \cup Y$ appena scritto.

Analogamente, allora, si definiranno le unioni a tre, a quattro. Infatti grazie alle unioni binarie e all'assioma della coppia si può definire

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

e così via. Da questo segue per esempio $\{a, b, c\} = \{a, b\} \cup \{c\}$, e in generale

$$\{a_1, \ldots, a_n\} = \{a_1\} \cup \cdots \cup \{a_n\}.$$

Quello che seguirà non sarà un assioma: vogliamo parlare e definire l'intersezione tra insiemi, e per fare ciò occorre solo quanto fatto finora.

Definizione 1.3.7. Sia F un insieme non vuoto[7] definiamo l'*intersezione* di F come

$$A = \bigcap F \leftrightarrow (\forall a)(a \in A \leftrightarrow (\forall X)(X \in F \to a \in X)).$$

Osserviamo che per ora dobbiamo ancora dare senso alla definizione: definire un oggetto non significa provarne l'esistenza. In effetti l'ipotesi che F sia non vuoto è necessaria, e in tal caso la definizione data ha sempre senso:

Teorema 1.3.2. $(\forall F \neq \emptyset)(\exists A)(A = \bigcap F)$

Dimostrazione. Visto che $F \neq \emptyset$ esiste un $B \in F$ e quindi

$$\bigcap F = \{b \in B \mid (\forall X \in F)(b \in X)\},$$

che esiste per l'assioma di separazione. □

[7] che va pensato come famiglia di insiemi, tanto ogni suo elemento è un oggetto e tutti gli oggetti sono insiemi

Osservazione 1.3.12. Osserviamo che se $F = \emptyset$ avremmo che la sua intersezione sarebbe $\mathbb{V}$, che in effetti non esiste come insieme.

Adesso affermiamo un fatto ancora poco preciso: finora abbiamo dato assiomi che non ci permettono di costruire insiemi che non siano finiti. L'imprecisione sta nel fatto che non possiamo ancora definire che cosa significhi che un insieme è finito, in quanto non sappiamo cos'è il numero di elementi di un insieme (dal momento che ancora non abbiamo i numeri naturali). L'assioma seguente postula infatti l'esistenza di un insieme che ha delle proprietà che poi ci permetteranno di poter creare diversi tipi di insiemi. È anche chiaro però che la forma dell'assioma può risultare in questo momento artificiosa, ma questo è necessario se non vogliamo menzionare i numeri. L'assioma è il seguente:

Assioma dell'infinito Esiste un insieme che chiameremo *induttivo*, ossia che gode della proprietà espressa nell'assioma:

$$(\exists X)(\emptyset \in X \wedge (\forall y)(y \in X \to y \cup \{y\} \in X)).$$

Questo è l'assioma che ci permette di costruire i numeri naturali. Data l'importanza della costruzione, la presenteremo in una sezione a sé stante.

1.3.1 I numeri naturali

Al fine di sviluppare la matematica entro la teoria assiomatica degli insiemi è necessario definire i numeri naturali. Tutti noi conosciamo i numeri naturali intuitivamente: 0, 1, 2, ..., 17, ..., 324, etc., e possiamo anche dare facilmente esempi di insiemi aventi nessuno, uno, due o tre elementi: basti pensare agli insiemi $\emptyset$, $\{\emptyset\}$ (o in generale $\{a\}$). Lo scopo di questa sezione è di supportare questa visione intuitiva con rigorose definizioni.
Per definire il numero 0 vogliamo scegliere un rappresentante di tutti gli insiemi che non hanno elementi. Ma questo è facile perché esiste un solo insieme di questo tipo. Definiamo $0 = \emptyset$.Procediamo con gli insiemi che hanno un solo elemento (i singoletti): $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\{\emptyset, \{\emptyset\}\}\}$; in generale $\{x\}$. Come possiamo scegliere un rappresentante? Visto che abbiamo già definito un particolare oggetto, chiamato 0, una scelta natuarale è $\{0\}$. Così definiamo

$$1 = \{0\} = \{\emptyset\}.$$

Finora abbiamo definito 0 e 1, e $0 \neq 1$. Grazie a questi possiamo costruire un particolare insieme a due elementi, l'insieme i cui elementi sono i precedentemente definiti 0 e 1:

$$2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}.$$

A questo punto si capisce come sia ovvio che il procedimento continui: l'idea è semplicemente di definire un numero naturale n come l'insieme dei numeri più piccoli precedentemente definiti $\{0, \ldots, n-1\}$ [8].
Questa idea però presenta un difetto di fondo. Abbiamo definito i primi numeri e potremmo facilmente definire 17 e – non così facilmente – 324. Ma nessuna di queste definizioni ci dice cosa sia in generale un numero naturale. Abbiamo bisogno di un'affermazione del tipo: un insieme n è un numero naturale se.... Non possiamo solo dire che un insieme n è un numero naturale se i suoi elementi sono i numeri naturali minori, perché come definizione coinvolgerebbe il concetto stesso. Osserviamo la costruzione dei primi numeri nuovamente. Abbiamo definito $2 = \{0, 1\}$; per avere 3 dobbiamo aggiungere un terzo elemento a 2, chiamato 2 stesso:

$$3 = 2 \cup 2 = \{0, 1\} \cup \{2\}.$$

Similmente si cortuiscono gli altri. Questa considerazione suggerisce la definizione:

Definizione 1.3.8. Il *successore* di un insieme X è $S(X) = X \cup \{X\}$.

Possiamo ora riassumere le considerazioni intuitive sui numeri naturali come segue:
(1) 0 è un numero naturale;
(2) se n è un numero naturale, allora il suo successore lo è;
(3) tutti i numeri naturali sono ottenuti applicando (1) o (2).
Un insieme induttivo contiene 0 e, per ogni elemento, anche il suo successore. Ma allora in accordo con la (3) si ha che l'insieme dei numeri naturali è induttivo e non contiene altri elementi ma solo numeri naturali (ossia è il "minimale"). Sia $Nat(n)$ la proprietà $(\forall X)(X \text{ induttivo} \leftrightarrow n \in X)$, allora definiamo

$$\mathbb{N} = \{n \mid Nat(n)\}.$$

Come sempre è accaduto sinora non sappiamo se l'insieme $\mathbb{N}$ appena definito esiste, perché non ci sono limitazioni per n nell'insieme. Fissiamo allora uno Z induttivo, che esiste per l'assioma dell'infinito, e osserviamo che $Nat(n) \leftrightarrow Nat(n) \wedge n \in Z$: possiamo quindi limitare la scelta degli n a Z. Abbiamo quindi

Definizione 1.3.9. Si definisce *insieme dei numeri naturali* l'insieme $\mathbb{N}$ definito da

$$\mathbb{N} = \{n \in Z \mid Nat(n)\} = \bigcap F,$$

dove $F = \{X \mid \emptyset \in X \vee (\forall y)(y \in X \to y \cup \{y\} \in X)\}$.

Nella definizione precedente abbiamo il primo dei due uguali già discusso prima di darla: abbiamo visto che in effetti la classe definita nel secondo membro è effettivamente un insieme. Poi abbiamo aggiunto anche un terzo membro, nel

[8] tale descrizione dei numeri naturali è dovuta a Von Neumann.

quale consideriamo l'intersezione della classe F definita anch'essa nella definizione, la classe di tutti gli insiemi induttivi: osserviamo che fare l'intersezione di F ha senso perché questa è non vuota per l'assioma dell'infinito.

Osservazione 1.3.13. Alcuni matematici obiettano all'assioma dell'infinito che una collezione di oggetti prodotta da un infinito processo (come $\mathbb{N}$) non dovrebbe essere trattata come un'entità completa. Tuttavia, la maggior parte delle persone con un po' di allenamento non hanno difficoltà a visualizzare l'insieme dei numeri naturali in questo modo. Gli insiemi infiniti sono gli strumenti di base della matematica moderna e l'essenza della teoria degli insiemi. Nessuna contraddizione derivata dal loro uso è stata mai scoperta, a dispetto dell'enorme quantità di risultati fondati su questi. Quindi tratteremo l'assioma dell'infinito alla pari con i nostri altri assiomi.

Abbiamo ora a disposizione l'insieme dei numeri naturali $\mathbb{N}$; prima di procedere oltre, guardiamo che $\mathbb{N}$ è davvero induttivo:

Lemma 1.3.1. *$\mathbb{N}$ è induttivo. Se I è un qualsiasi insieme induttivo, allora $\mathbb{N} \subseteq I$.*

Dimostrazione. Vale che $0 \in \mathbb{N}$ poiché $0 \in I$ per ogni I induttivo. Se $n \in \mathbb{N}$ allora $n \in I$ per ogni I induttivo, quindi $S(n) \in I$ per ogni I induttivo, e conseguentemente $S(n) \in \mathbb{N}$. Questo mostra che $\mathbb{N}$ è induttivo; la seconda parte del teorema segue immediatamente dalla definizione di $\mathbb{N}$. □

Abbiamo definito l'insieme $\mathbb{N}$ dei numeri naturali come il minimo insieme che contiene lo 0 ed è chiuso per successore. Mostriamo ora uno strumento fondamentale per studiare i numeri naturali, il meglio conosciuto principio per le dimostrazioni per induzione.

Teorema 1.3.3 (principio di induzione)**.** *Sia $P(x)$ una proprietà. Assumiamo che*
(1) $P(0)$ vale;
(2) $(\forall n)(P(n) \to P(S(n)))$.
Allora $(\forall n \in \mathbb{N})(P(n))$, ossia la proprietà è valida per ogni numero naturale.

Dimostrazione. Le due assunzioni (1) e (2) dicono semplicemente che l'insieme $A = \{n \in \mathbb{N} \mid P(n)\}$ è induttivo. Segue dunque $\mathbb{N} \subseteq A$. □

Riprendiamo ora con la formulazione degli assiomi. Il seguente assioma postula che tutti i sottoinsiemi di un dato insieme possono essere collezionati in un insieme:

Assioma dell'insieme potenza Per ogni X insieme esiste un insieme Y che ha per elementi i sottoinsiemi di X, ossia

$$(\forall X)(\exists Y)(\forall Z)(Z \in Y \leftrightarrow Z \subseteq X).$$

Osserviamo che l'assioma di estensionalità ci garantisce l'unicità dell'insieme potenza. Allora ha senso la seguente:

Definizione 1.3.10. Dato X insieme, chiamiamo *insieme delle parti* (o insieme potenza) di X, e lo si denota con $\mathcal{P}(X)$, quell'unico insieme che ha per elementi tutti i sottoinsiemi di X. Ossia $\mathcal{P}(X) = \{Z \mid Z \subseteq X\}$.

Osservazione 1.3.14. L'assioma dell'insieme potenza è una delle finite eccezioni che si ammettono all'assioma di Frege secondo cui ogni proprietà definisce un insieme.

Osservazione 1.3.15. Adesso che abbiamo un po' più di assiomi in mano possiamo convincerci meglio del fatto che anche proprietà più complesse ma di frequente utilizzo possono essere interamente espresse mediante il linguaggio dei connettivi, dei quantificatori, di "$=$" e di "$\in$". Ad esempio supponiamo di voler esprimere $\bigcup X \subseteq \mathcal{P}(Y)$ con i soli simboli logici. Inizieremo scrivendo

$$(\exists A)(\exists B)\left(A = \bigcup X \wedge B = \mathcal{P}(Y) \wedge A \subseteq B\right);$$

dopodiché sarà sufficiente caratterizzare ognuna delle tre parti della disgiunzione logica con la rispettiva definizione e abbiamo concluso.

Benché la nostra lista di assiomi non sia completa, posponiamo l'introduzione dei rimenenti postulati finché non ne avremo bisogno. Precisiamo solo che per la teoria ZF all'elenco mancano solo l'assioma di rimpiazzamento e l'assioma di fondazione; infine poi dovremo anche dare l'assioma della scelta per completare la teoria ZFC.

Capitolo 2

Relazioni e funzioni

2.1 Coppie ordinate

In questo capitolo iniziamo il nostro programma di sviluppo della teoria degli insiemi come fondamento della matematica mostrando come i vari concetti matematici generali, come relazioni, funzioni e ordinamenti sono insiemi.
Iniziamo introducendo le coppie ordinate. Se a e b sono insiemi allora esiste (per l'assioma della coppia) l'insieme $\{a, b\}$, che in effetti è una coppia non ordinate. L'ordine con cui a e b sono messi insieme non gioca alcun ruolo: $\{a, b\} = \{b, a\}$. Per molte applicazioni avremo invece bisogna di accoppiare a e b in modo da rendere possibile dire che a "viene prima" di b. Denotiamo con (a, b) la *coppia ordinata* e chiamiamo a e b rispettivamente la prima e la seconda componente o coordinata. Come oggetto del nostro studio, una coppia ordinata deve però essere un insieme. Un coppia ordinata potrebbe essere definita in modo che due coppie ordinate sono uguali se e solo se le loro prime coordinate sono uguali e le loro secondo coordinate anche. Ma questa non è una definizione che classifica come insieme una coppia ordinata, ma dovrà essere una conseguenza della definizione che daremo.

Definizione 2.1.1 (coppia di Kuratowski)**.** Definiamo $(a, b) = \{\{a\}, \{a, b\}\}$.

Adesso dobbiamo provare che la condizione che vogliamo sia soddisfatta da una coppia ordinata in effetti è soddisfatta secondo la nostra definizione:

Teorema 2.1.1. *Vale* $(a, b) = (c, d)$ *se e solo se* $a = c$ *e* $b = d$.

Dimostrazione. ($\Longleftarrow$) Questa implicazione è ovvia per l'assioma di estensionalità. ($\Longrightarrow$) Distinguiamo due casi, e supponiamo dapprima $a = b$, allora $(a, b) = \{\{a\}\}$. Per l'ipotesi di uguaglianza tra le coppie ordinate si ha

$$\{\{a\}\} = \{\{c\}, \{c, d\}\},$$

ma allora $\{c\} \in \{\{a\}\}$ ed anche $\{c,d\} \in \{\{a\}\}$. Dalla prima si ha $\{c\} = \{a\}$, ossia $a = c$; dalla seconda $\{c,d\} = \{a\}$, da cui $c = a = d$. Ma allora $a = b = c = d$. Supponiamo $a \neq b$, allora la coppia (a,b) ha due elementi, quindi anche (c,d) ha due elementi (essendo le due coppie uguali) e quindi $c \neq d$. Per estensionalità $\{a\} = \{c\}$ e $\{a,b\} = \{c,d\}$ oppure $\{a\} = \{c,d\}$ e $\{c\} = \{a,b\}$. In realtà il secondo caso non può darsi perché sennò avremmo $c = a = d$ ma $c \neq d$. Allora $\{a\} = \{c\}$ e quindi $a = c$ sempre per estensionalità; poi da $\{a,b\} = \{c,d\}$ segue che $b = d$, essendo $a = c$. $\square$

In effetti la proprietà che volevamo è verificata dalle coppie di Kuratowski. Adesso vorremmo raccogliere in un insieme tutte le copppie ordinate con le coordinate prese da due insiemi dati, ma non è detto che tale procedimento dia luogo effettivamente ad un insieme. Intanto diamo la definizione:

Definizione 2.1.2. Siano A e B insiemi. Definiamo il *prodotto cartesiano* come l'insieme che ha per elementi tutte le coppie ordinate (a,b) tali che $a \in A$ e $b \in B$; ossia

$$A \times B = \{(a,b) \mid a \in A \wedge b \in B\}.$$

Per come è stata data la definizione non sappiamo se il prodotto cartesiano esiste in effetti perché per ora non si può applicare l'assioma di separazione in quanto non abbiamo una limitazione sulla scelta delle coppie ordinate. Ci sono due modi per dimostrare l'esistenza del prodotto cartesiano, e abbiamo deciso di riportarli entrambi: uno fa uso dell'assioma dell'insieme potenza, mentre l'altro fa uso dell'assioma del rimpiazzamento. Intanto iniziamo dal primo e osserviamo che $(a,b) = \{\{a\},\{a,b\}\} \subseteq \mathcal{P}(A \cup B)$ in quanto gli elementi di (a,b) sono sottoinsiemi dell'unione; ma allora, analogamente, si ha che $(a,b) \in \mathcal{P}(\mathcal{P}(A \cup B))$. A questo punto sarà sufficiente definire

$$A \times B = \{(a,b) \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid a \in A \wedge b \in B\}$$

e osservare che esiste per l'assioma di separazione, essendo $\mathcal{P}(\mathcal{P}(A \cup B))$ un insieme per l'assioma potenza. Adesso presenteremo il secondo metodo, e invitiamo il lettore a rileggerlo non appena sarà stato dato l'assioma del rimpiazzamento.

Osservazione 2.1.1. Il secondo metodo è di seguito descritto. Fissiamo un elemento $b \in B$, tanto $B \neq \emptyset$ e consideriamo la formula $\varphi(b,x,y)$ (con b come parametro) che dice $y = (x,b)$ (si potrebbe scrivere grazie alle formule del linguaggio ma non lo facciamo). Tale formula è funzionale, nel senso che per ogni x esiste un unico y tale che $y = (x,b)$. Adesso prendiamo A e per l'assioma del rimpiazzamento esiste

$$\{(a,b) \mid a \in A\}.$$

Di nuovo per rimpiazzamento, considerando la relazione funzionale $b \mapsto A \times \{b\}$, esiste l'insieme $F = \{A \times \{b\} \mid b \in B\}$. Ma allora $A \times B = \bigcup F$ ed esiste per l'assioma dell'unione.

2.2 Relazioni

I matematici spesso studiano le relazioni tra oggetti matematici. Le relazioni tra oggetti di due tipi accadono molto spesso; possiamo chiamare queste *relazioni binarie*. Per esempio, diciamo che una retta r è in relazione R_1 con un punto P se e solo se r passa per P: R_1 è una relazione binaria tra oggetti chiamati rette e oggetti chiamati punti. Similmente, definiamo una relazione binaria R_2 tra interi positivi e interi positivi dicendo che un numero positivo m è in relazione R_2 con un numero positivo n se e solo se m divide n (senza resto).
Consideriamo ora la relazione R_1' tra rette e punti tale che un retta r è in relazione R_1' con un punto P se e solo se P giace su r: ovviamente una retta r è in relazione R_1 con un punto P esattamente quando il punto P è in relazione R_1' con la retta r. Benché siano state usate diverse proprietà per definire le due relazioni, noi vorremmo considerare R_1 e R_1' come la stessa relazione. In analogia con R_2 possiamo anche dare la relazione R_2' che mette in relazione n e m se e solo se n è un multiplo di m. Ancora, le stesse coppie ordinate (m, n) sono date sia da R_2 che da R_2'.
Quindi determineremo una relazione binaria specificando tutte e sole le coppie di oggetti che sono in relazione; non importa specificare, in questo tipo di concezione, la proprietà dalla quale tale insieme di coppie ordinate è descritto. Siamo giunti (e abbiamo anche giustificato intuitivamente) alla definizione seguente:

Definizione 2.2.1. Un insieme R è una *relazione binaria* se i suoi elementi sono coppie ordinate, ossia se per ogni $z \in R$ esistono x e y tali che $z = (x, y)$. Ossia

$$(\forall z)(z \in R \leftrightarrow (\exists x)(\exists y)(z = (x, y))).$$

Scriveremo xRy per indicare che $(x, y) \in R$, e in tal caso si legge "x è in relazione R con y".

Esempio 2.2.1. Indichiamo con $\mathbb{N}_0 = \mathbb{N} - \{0\}$ l'insieme dei numeri positivi. La relazione R_2 è semplicemente l'insieme $\{(m, n) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid m \mid n\}$. Gli elementi di R_2 sono coppie ordinate

$$\begin{array}{l}(1,1),\ (1,2),\ (1,3),\ \ldots\\ (2,2),\ (2,4),\ (2,6),\ \ldots\\ (3,3),\ (3,6),\ (3,9),\ \ldots\\ \ldots\end{array}$$

Scriveremo ad esempio $3R_26$, $\neg(2R_27)$.

Adesso introdurremo una terminologia per le relazioni:

Definizione 2.2.2. Sia R una relazione binaria:
(1) l'insieme degli x che sono in relazione con qualche y si dice *dominio* di R ed è indicato con $\operatorname{dom} R$. In tal modo $\operatorname{dom} R = \{x \mid (\exists y)((x,y) \in R)\}$;
(2) l'insieme degli y per i quali esiste x in relazione con y si dice *immagine* di R ed è indicato con $\operatorname{imm} R$. In tal modo $\operatorname{imm} R = \{y \mid (\exists x)((x,y) \in R)\}$.

Osservazione 2.2.1. Dobbiamo ancora mostrare che in effetti dominio e immagine di una relazione esistono come insiemi. Infatti quando è assegnata una relazione R, si intende che è assegnato un insieme di coppie ordinate.

Lemma 2.2.1. *Sia R una relazione. Allora esistono sempre dominio e immagine di R.*

Dimostrazione. Mostriamo che esiste $\operatorname{imm} R$, per il dominio $\operatorname{dom} R$ la dimostrazione è analoga. Osserviamo che se $y \in \operatorname{imm} R$ allora esiste un x tale che $(x,y) \in R$ per definizione. Dunque

$$y \in \{x,y\} \in \{\{x\},\{x,y\}\} \in R$$

e quindi $y \in \{x,y\} \in \bigcup R$, da cui infine $y \in \bigcup\bigcup R$. Dunque posto

$$\operatorname{imm} R = \left\{ y \in \bigcup\bigcup R \mid (\exists x)((x,y) \in R) \right\}$$

abbiamo per l'assioma di separazione che l'immagine è un insieme. □

A questo punto prende senso anche la seguente definizione:

Definizione 2.2.3. Siano A e B insiemi. R è una *relazione binaria tra A e B* se $A = \operatorname{dom} R$ e B è un soprainsieme di $\operatorname{imm} R$.

In realtà la definizione di immagine può essere generalizzata come segue:

Definizione 2.2.4. Sia R una relazione binaria tra A e B e siano $A' \subseteq A$ e $B' \subseteq B$:
(1) l'*immagine* di A' secondo R, indicata con $R(A')$ è l'insieme degli $y \in \operatorname{imm} R$ relazionati da R con qualche elemento di A; a dire che

$$R(A') = \{y \in \operatorname{imm} R \mid (\exists x)(x \in A' \wedge (x,y) \in R)\};$$

(2) l'*immagine inversa* di B' secondo R, denotata con $R^{-1}(B')$, è l'insieme di tutti gli $x \in \operatorname{dom} R$ relazionati da R con qualche elemento di B'; ossia

$$R^{-1}(B') = \{x \in \operatorname{dom} R \mid (\exists y)(y \in B' \wedge (x,y) \in R)\}.$$

Vediamo cosa significano questi concetti con qualche esempio riferito alle relazioni R_1 e R_2 definite all'inizio di questo paragrafo.

Esempio 2.2.2. Intanto vale ovviamente $\operatorname{dom} R_2 = \operatorname{imm} R_2 = \mathbb{N}_0$: dato un intero positivo m e scelto $n = m$ si ha che mR_2m e quindi $m \in \operatorname{dom} R_2$ per ogni m; analogamente si dimostra che l'immagine sono tutti gli interi positivi. Invece si ha ad esempio

$$R_2^{-1}(\{3, 8, 9, 12\}) = \{1, 2, 3, 4, 6, 8, 9, 12\},$$

ed anche che $R_2(\{2\})$ è l'insieme di tutti i numeri pari.

Definizione 2.2.5. Sia R una relazione binaria tra A e B. La *relazione inversa* di R, indicata con R^{-1}, è l'insieme

$$R^{-1} = \{z \mid z = (x, y) \wedge (y, x) \in R\} = \{(x, y) \mid (y, x) \in R\}.$$

Osserviamo che nella definizione precedente abbiamo anche introdotto una notazione più stringata per insiemi di coppie ordinate. Ancora una volta utilizziamo la relazione R_2 a esempio per quanto abbiamo appena definito:

Esempio 2.2.3. Vale per definizione che

$$R_2^{-1} = \{(m, n) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid (n, m) \in R\} = \{(m, n) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid n \mid m\},$$

ossia m è multiplo di n. Osserviamo che, nello scrivere la relazione inversa, ci siamo attenuti rigorosamente alla definizione, indicando nuovamente con la lettera m la prima componente e con n la seconda. Generalmente per invertire le relazioni basta scambiare l'ordine delle componenti nelle coppie ordinate, ma nella descrizione insiemistica si deve "rinominare" la prima componente come era prima dello scambio. In questo modo R_2 e R_2^{-1} sono descritte in un modo parallelo: in questo senso, l'inversa della relazione "divide" è la relazione "è un multiplo".

Il lettore avrà notato che il simbolo $R^{-1}(B')$ nella definizione 2.2.4 per l'immagine inversa di B' ora denota anche l'immagine di B' mediante R^{-1}. Fortunatamente i due insiemi ora detti sono uguali:

Lemma 2.2.2. *L'immagine inversa di B' mediante R è uguale all'immagine di B secondo la relazione inversa R^{-1}.*

Dimostrazione. Notiamo intanto che $\operatorname{dom} R = \operatorname{imm} R^{-1}$. Ora, $x \in \operatorname{dom} R$ appartiene all'immagine inversa di B' mediante R se e solo se per qualche $y \in B'$ si ha $(x, y) \in B'$. Ma $(x, y) \in R$ se e solo se $(y, x) \in R^{-1}$. Quindi x appartiene all'immagine inversa di B' mediante R se e solo se per qualche $y \in B'$ si ha $(y, x) \in R^{-1}$; ossia se e solo se x è nell'immagine di B' mediante R^{-1}. □

Nel prossimo paragrafo considereremo particlari relazioni tra insiemi, le funzioni e vedremo a cosa ci serviranno.

2.3 Funzioni

Una funzione, come inteso in matematica, è una procedura, una regola che assegna ad ogni oggetto a del dominio della funzione un unico oggetto b, il valore della funzione in a. Una funzione, quindi, rappresenta un tipo speciale di relazione, una relazione dove *ogni* elemento del dominio è in relazione con *un preciso* oggetto nell'immagine. Prima della definizione precisiamo una notazione che useremo:

Osservazione 2.3.1. Scriveremo $(\exists!\, x)(P(x))$, da leggersi "esiste un unico x tale che $P(x)$", quando $(\exists x)(P(x) \wedge (\forall y)(P(y) \to y = x))$

Definizione 2.3.1. Una relazione binaria F è una *funzione* (o mappa, o corrispondenza) se vale la proprietà seguente:

$$(\forall a)(\forall b_1)(\forall b_2)(((a, b_1) \in F \wedge (a, b_2) \in F) \to b_1 = b_2).$$

Se A e B sono insiemi e $\operatorname{dom} F = A$ e $\operatorname{imm} F \subseteq B$ allora diremo che F è una *funzione tra A e B*, e scriveremo $F : A \to B$, oppure anche $\langle F(a) \mid a \in A\rangle$. È infatti in uso la seguente notazione: scriveremo $F(a) = b$ se e solo se $(a, b) \in F$.

Osservazione 2.3.2. La definzione di funzione è equivalente alla seguente:

$$(\forall a \in \operatorname{dom} F)(\exists! b)((a, b) \in F).$$

Questo unico b si chiama *valore* di F in a e, come detto, lo si indica con $F(a)$.

Osservazione 2.3.3. L'uguale di $F(a) = b$ non è proprio lo stesso che prendiamo nel linguaggio; siccome però b è unico non si entra in conflitto con le proprietà dell'uguale vero e proprio. Infatti $(f(a) = b \wedge f(a) = c) \to b = c$ per definizione di funzione e ciò rispetta la transitività dell'uguaglianza.

Osservazione 2.3.4. Attenzione a non confondere la scrittura $\langle F(a) \mid a \in A\rangle$ con la scrittura $\{F(a) \mid a \in A\}$. Con la prima si intende denotare la funzione F, mentre con la seconda si intende denotare il corrispondente insieme immagine $\operatorname{imm} F$.

L'assioma di estensionalità può essere applicato alle funzioni come segue:

Lemma 2.3.1. *Siano F e G due funzioni. Vale che $F = G$ se e solo se* $\operatorname{dom} F = \operatorname{dom} G$ *e $F(x) = G(x)$ per ogni $x \in \operatorname{dom} F$.*

Dimostrazione. Lasciamo la dimostrazione al lettore. □

Dal momento che le funzioni sono relazioni binarie, i concetti di dominio, immagine, immagine inversa e funzione inversa possono essere applicati a queste. Introduciamo invece qualche altra definizione:

Definizione 2.3.2. Sia F una funzione da A a B:
(1) diciamo che F è *iniettiva* se e solo se porta punti distinti in punti distinti, ossia $(\forall a_1)(\forall a_2)((a_1 \in \operatorname{dom} F \wedge a_2 \in \operatorname{dom} F \wedge a_1 \neq a_2) \to f(a_1) \neq f(a_2))$;
(2) diciamo che F è *suriettiva* se e solo se $\operatorname{imm} F = B$;
(3) diciamo che F è *biunivoca* se e solo se F è iniettiva e suriettiva.

Definizione 2.3.3. La *restrizione* di una funzione F ad $A' \subseteq A$ è la funzione

$$F|_{A'} = \{(a, b) \in F \mid a \in A'\}.$$

Se G è una restrizione di F a qualche A' allora diciamo per contro che F è un'*estensione* di G.

Adesso diamo una definizione che vale per le relazioni e quindi anche per le funzioni. Se abbiamo due relazioni vogliamo definire una nuova relazione:

Definizione 2.3.4. Siano R e S due relazioni binarie. La *composizione* di R e S è la relazione

$$S \circ R = \{(x, z) \mid (\exists y)((x, y) \in R \wedge (y, z) \in S)\}.$$

Adesso supponiamo che R ed S siano funzioni: quello che ci chiediamo è se la proprietà di essere funzione è mantenuta anche dalla composizione. La risposta è sì, come prova il seguente:

Teorema 2.3.1. *Siano F e G funzioni. Allora $G \circ F$ è ancora una funzione e $G \circ F$ è definita su x se e solo se F è definita su x e G è definita su $f(x)$; ossia*

$$\operatorname{dom}(G \circ F) = \operatorname{dom} F \cap F^{-1}(\operatorname{dom} G).$$

Inoltre $(G \circ F)(x) = G(F(x))$ per ogni $x \in \operatorname{dom}(G \circ F)$.

Dimostrazione. Mostriamo dapprima che $G \circ F$ è una funzione. Se $x(G \circ F)z_1$ e $x(G \circ F)z_2$ allora esistono y_1 e y_2 tali che $F(x) = y_1$, $G(y_1) = z_1$ e $F(x) = y_2$, $G(y_2) = z_2$. Dal momento che F è una funzione si ha che $y_1 = y_2$; con questo, e dal momento che G è una funzione si ha anche $z_1 = z_2$.
Adesso vogliamo vedere il dominio di $G \circ F$. Si ha che $x \in \operatorname{dom}(G \circ F)$ se e solo se esiste z tale che $(G \circ F)(x) = z$, ossia se e solo se esiste z ed esiste y tale che $F(x) = y$ e $G(y) = z$. Ma questo accade se e solo se $x \in \operatorname{dom} F$ e $y = F(x) \in \operatorname{dom} G$; quest'ultimo fatto è equivalente a chiedere che $x \in F^{-1}(\operatorname{dom} G)$. □

Se F è una funzione, in particolare è anche una relazione: la sua inversa F^{-1} è in generale una relazione. Quando anche F^{-1} è una funzione diremo che F è una *funzione invertibile*. Adeso daremo condizioni necessarie e sufficienti all'invertibilità di una funzione:

Teorema 2.3.2. *Una funzione è invertibile se e solo se F è iniettiva. Se F è invertibile anche F^{-1} è invertibile e vale anche $(F^{-1})^{-1} = F$.*

Dimostrazione. ($\Longrightarrow$) Supponiamo che F sia invertibile; da questo segue che $F^{-1}(F(a)) = a$ per ogni $a \in \operatorname{dom} F$. Se $a_1, a_2 \in \operatorname{dom} F$ e $F(a_1) = F(a_2)$ abbiamo $F^{-1}(F(a_1)) = F^{-1}(F(a_2))$, ossia $a_1 = a_2$.
($\Longleftarrow$) Supponiamo che F sia iniettiva. Se $F^{-1}(b_1) = a$ e $F^{-1}(b_2) = a$ abbiamo $F(a) = b_1$ e $F(a) = b_2$. Da ciò segue $b_1 = b_2$, e ciò mostra che F^{-1} è una funzione. L'ultima parte a questo punto a banale. Supponendo che F^{-1} sia una funzione segue che anch'essa è invertibile proprio perché $(F^{-1})^{-1} = F$ vale in generale per le relazioni (dimostrare!) ed inoltre F (sua inversa) è una funzione per ipotesi. □

Osservazione 2.3.5 (sulla notazione). Nella pratica matematica è molto comune indicare le funzioni con lettere minuscole. Sino ad ora abbiamo preferito usare lettere maiuscole per mantenere l'analogia con le relazioni; adesso però tenderemo ad usare lettere minuscole.

Esempio 2.3.1. Sia $f = \langle 1/x^2 \mid x \neq 0 \rangle$, vogliamo determinare f^{-1} e sapere se è o meno una funzione. Visto che possiamo scrivere $f = \{(x, 1/x^2) \mid x \neq 0\}$ otteniamo

$$f^{-1} = \{(1/x^2, x) \mid x \neq 0\}.$$

Ma f^{-1} non è una funzione in quanto $(1, -1) \in f^{-1}$ e $(1, 1) \in f^{-1}$; da ciò segue dunque che f non era iniettiva.

Esempio 2.3.2. Sia $g = \langle 3x - 1 \mid x \in \mathbb{R} \rangle$ [1], vogliamo anche ora determinare g^{-1}. Intanto osserviamo che g è iniettiva: infatti se $3x_1 - 1 = 3x_2 - 1$ allora $x_1 = x_2$. Scrivendo $g = \{(x, 3x - 1) \mid x \in \mathbb{R}\}$ abbiamo $g^{-1} = \{(x, y) \mid x = 3y - 1 \wedge x \in \mathbb{R}\}$. Come già osservato in precedenza vorremmo esprimere la seconda componente in funzione della prima:

$$g^{-1} = \left\{ (x, y) \mid y = \frac{x + 1}{3} \wedge x \in \mathbb{R} \right\},$$

ed abbiamo concluso.

Adesso ci chiediamo se, fissati due insiemi, è possibile raccogliere in un insieme tutte le funzioni dal primo di questi nel secondo. La risposta è sì, come ci si aspettava. Prendiamo A e B insiemi allora affermiamo che $\{f \mid f : A \to B\}$, che in generale è una classe, è in realtà un insieme. Per questo è sufficiente osservare che tale insieme è contenuto in $\mathcal{P}(A \times B)$ e quindi possiamo scrivere

$$\{f \in \mathcal{P}(A \times B) \mid f : A \to B\},$$

che è un insieme per l'assioma di separazione. Ha senso quindi la seguente:

[1] non avendo ancora definito i numeri reali il lettore prenda la definizione intuitiva che già avrà.

Definizione 2.3.5. Siano A e B insiemi. L'insieme di tutte le funzioni da A in B è denotato con B^A.

Sia $S = \langle S_i \mid i \in I \rangle$ una funzione con dominio I. Il lettore probabilmente è abiutuato a veder funzioni a valori numerici; ma per noi, i valori S_i sono insiemi arbitrari.

Definizione 2.3.6. La funzione $S = \langle S_i \mid i \in I \rangle$ è detta una *famiglia indiciata di insiemi* o *sequenza di insiemi.*

A questo punto è molto utile definire una nozione più generale di prodotto di insiemi, e possiamo farlo grazie alle funzioni.

Definizione 2.3.7. Sia $S = \langle S_i \mid i \in I \rangle$ una famiglia indiciata di insiemi. Definiamo il *prodotto* della famiglia S come l'insieme

$$\prod S = \left\{ f : I \to \bigcup_{i \in I} S_i \mid (\forall i \in I)(f(i) \in S_i) \right\}.$$

Tra le notazioni usate si incontrano anche $\prod_{i \in I} S_i = \prod \langle S_i \mid i \in I \rangle$.

Probabilmente il lettore sarà curioso di sapere cosa c'entra questa definizione di prodotto con quella data di prodotto cartesiano $A \times B$ precedentemente definito. Ritorneremo su questo problema tecnico più avanti; per ora ci limitiamo a notare che se la famiglia indiciata di insiemi S è quella tale che per ogni $i \in I$ si ha $S_i = B$ allora $\prod S = B^I$. L'"esponenziazione" di insiemi è correlata alla "moltiplicazione" di insiemi così come accade nelle operazioni numeriche.
Concludiamo questo paragrafo con due osservazioni sulla notazione. Sono stati definiti $\bigcup A$ e $\bigcap A$ per ogni famiglia di insiemi A (con $A \neq \emptyset$ nel caso dell'intersezione). Spesso a famiglia A è data come immagine di qualche funzione, ossia è data come una famiglia indiciata di insiemi[2]. Diremo che A è *indicizzata* da S se

$$A = \{S_i \mid i \in I\} = \operatorname{imm} S$$

dove S è una funzione su I. Proprio per questo è molto usato scrivere

$$\bigcup A = \bigcup_{i \in I} S_i \quad \text{e} \quad \bigcap A = \bigcap_{i \in I} S_i.$$

Dopo ciò, sia f una funzione che ha per dominio un sottoinsieme di un prodotto $A \times B$. Denoteremo il valore di f in $(x, y) \in A \times B$ con $f(x, y)$ anziché con la notazione più ridondante $f((x, y))$.

[2] in realtà ogni famiglia A può essere presentata così se si vuole. Basta prendere $I = A$ e $S_i = i$ per ogni $i \in A$.

2.4 Relazioni di equivalenza

Adesso ci occuperemo di relazioni binarie di un insieme in sé, ossia relazioni R in cui dominio e immagine sono un insieme A. Alcuni speciali tipi di relazioni binarie così fatte verranno presi in considerazione molto frequentemente, quindi ci apprestiamo a definirle.

Definizione 2.4.1. Sia R una relazione binaria in A. Allora:
(1) R è *riflessiva* se per ogni $a \in A$ si ha aRa;
(2) R è *simmetrica* se per ogni $a, b \in A$, aRb implica bRa;
(3) R è *transitiva* se per ogni $a, b, c \in A$, aRb e bRc implica aRc;
(4) R è detta *equivalenza* se è riflessiva, simmetrica e transitiva.

Esempio 2.4.1. Sia P l'insieme di tutte le persone che vivono sulla Terra. Diciamo che una persona p è equivalente a una persona q ($p \equiv q$) se p e q vivono entrambi nello stesso stato. Banalmente la relazione definita è riflessiva, simmetrica e transitiva e quindi è una relazione di equivalenza su P. Notiamo che l'insieme P può essere spezzato in classi di elementi reciprocamente equivalenti; tutte le persone che vivono negli Stati Uniti formano una classe, tutte le persone che vivono in Francia sono un'altra classe, eccetera. Tutti i membri di una classe sono equivalenti; membri di classi diverse non sono mai equivalenti. Le classi di equivalenza corrispondono esattamente ai diversi stati.

Esempio 2.4.2. Definiamo una relazione di equivalenza sull'insieme $\mathbb{Z}$ degli interi relativi[3]. Diremo che xRy se e solo se $x-y$ è divisibile per 2. Il lettore può verificare immediatamente che R è una relazione di equivalenza. Ancora, l'insieme $\mathbb{Z}$ risulta partizionato in due classi, che sono quelle dei numeri pari e di quelli dispari.

La situazioni appena vista è abbastanza generale. Ogni relazione di equivalenza su A determina una partizione di A in classi di equivalenza; viceversa, data una partizione di A c'è una relazione di equivalenza su A che ha gli elementi della partizione come classi di equivalenza. Intanto definiamo formalmente cos'è una classe:

Definizione 2.4.2. Sia R una relazione di equivalenza su A. La *classe di equivalenza* di un $a \in A$ secondo R è l'insieme $[a]_R = \{x \in A \mid xRa\}$.

Definizione 2.4.3. Sia R una relazione di equivalenza su A. Il sistema di insiemi di tutte le classi di equivalenza secondo R è denotato con A/R, e si dice *insieme quoziente* di A modulo R. Quindi $A/R = \{[a]_R \mid a \in A\}$.

[3] non abbiamo dato ancora la definizione formale di questo insieme, ma per ora può bastare la definizione intuitiva che il lettore certamente avrà.

Definizione 2.4.4. Un sistema S di insiemi non vuoti è detto una *partizione* di A se valgono:
(1) S è un sistema di insiemi a due a due disgiunti, ossia per ogni $C, D \in S$ con $C \neq D$ si ha $C \cap D = \emptyset$;
(2) l'unione di S è A, ossia $\bigcup S = A$.

Abbiamo fin qui dato alcune definizioni e introdotto alcuni concetti, ma possiamo dire che non abbiamo ancora ottenuto un risultato che abbia una qualche sostanza. Lo facciamo adesso, dimostrando uno dei risultati più importanti sulle relazioni di equivalenza:

Proposizione 2.4.1. *Sia R una relazione di equivalenza su A. Allora A/R è una partizione di A.*

Dimostrazione. Denotiamo con R la relazione di equivalenza su A: dobbiamo mostrare le proprietà (1) e (2) della definizione 2.4.4. Iniziamo dalla seconda: per ogni $a \in A$ si ha $[a]_R \subseteq A$ e quindi vale certamente

$$\bigcup A/R = \bigcup_{a \in A} [a]_R \subseteq A.$$

Viceversa si osserva che per ogni $b \in A$ si ha $b \in [b]_R$ e dunque $b \in \bigcup_{a \in A} [a]_R$ e quindi abbiamo l'altra inclusione, che insieme alla precedente forniscono l'uguaglianza.
Adesso mostreremo la proprietà (1): siano $C, D \in A/R$, ossia $C = [a]_R$ e $D = [b]_R$, con $C \neq D$. Mostriamo che le due classi di equivalenza allora devono essere disgiunte. Supponendo per assurdo che $C \cap D \neq \emptyset$ sia $x \in [a]_R \cap [b]_R$. Essendo $x \in [a]_R$ abbiamo xRa, ossia aRx per la simmetria, ed essendo anche $x \in [b]_R$ abbiamo pure xRb. Per la transitività della relazione abbiamo allora che aRb. Da questo segue che $[a]_R = [b]_R$. Sia infatti $y \in [b]_R$, ossia yRb, allora dal fatto che bRa segue che yRa per la proprietà transitiva; allora $y \in [a]_R$: abbiamo mostrato dunque che $[b] \subseteq [a]$; l'argomentazione utilizzata è simmetrica, e quindi allo stesso modo segue $[b]_R \supseteq [a]_R$. Dalla doppia inclusione segue dunque $[a]_R = [b]_R$. □

Adesso mostreremo, viceversa, che per ogni partizione esiste una corrispondente relazione di equivalenza che la determina. Per esempio, la partizione delle persone nei loro stati di residenza deriva dalla relazione di equivalenza dell'esempio 2.4.1.

Definizione 2.4.5. Sia S una partizione di A. La relazione R_S è definita come segue:

$$R_S = \{(a, b) \in A \times A \mid \exists C \in S \text{ tale che } a, b \in C\}.$$

Gli elementi a e b sono in relazione mediante R_S se e solo se appartengono allo stesso insieme della partizione S. A questo punto non è difficile mostrare che R_S

è una relazione di equivalenza, ed induce proprio la partizione S. Così le relazioni di equivalenza e le partizioni sono due diverse descrizione della stessa realtà matematica. Ogni relazione di equivalenza R determina una partizione $S = A/R$; la relazione di equivalenza R_S determinata da questa partizione è identica all'originale R. Viceversa ogni partizione S determina una relazione di equivalenza R_S, il cui insieme quoziente è ancora S.
Infine una questione di comodità: quando si lavora con relazioni di equivalenza o partizioni è conveniente avere un insieme che contiene esattamente un solo rappresentante da ogni classe di equivalenza:

Definizione 2.4.6. Un insieme $X \subseteq A$ è detto *insieme di rappresentanti* per la relazione di equivalenza R_S se per ogni $C \in S$ si ha $X \cap C = \{a\}$ per qualche $a \in C$.

Sempre nell'esempio 2.4.1 possiamo dire che l'insieme dei capi di stato per ogni stato del mondo è un insieme di rappresentanti per la relazione di equivalenza descritta. Una domanda che potremmo porci adesso è la seguente: ma un insieme di rappresentanti esiste per ogni relazioni di equivalenza assegnata? Intuitivamente la risposta dovrebbe essere sì, ma in realtà con i soli nostri assiomi ciò non può essere provato. Vedremo più avanti che per provare questo fatto è necessario l'assioma della scelta: per chi già sa di cosa si tratta, questo assioma è necessario per poter "scegliere" un elemento da ogni classe di equivalenza, per poi raggruppare questi in un insieme, che sarà l'insieme dei rappresentanti.

2.5 Relazioni d'ordine

Le relazioni d'ordine sono un altro frequente esempio di relazioni in un insieme.

Definizione 2.5.1. Una relazione binaria R su A si dice *antisimmetrica* se per ogni $a, b \in A$, aRb e bRa implica $a = b$.

Definizione 2.5.2. Una relazione binaria R su A che sia riflessiva, antisimmetrica e transitiva è chiamata *relazione d'ordine parziale*. La coppia (A, R) è detta *insieme ordinato*.

La scrittura aRb può essere anche letta come "a è minore o uguale a b", o come "b è maggiore o uguale ad a" (nell'ordine determinato da R). Ed in questo modo possono essere anche rilette le proprietà che deve avere una relazione di ordine.

Esempio 2.5.1. La relazione $\leq$ è d'ordine sull'insieme di tutti i numeri (naturali, razionali, reali).

Esempio 2.5.2. Definiamo in A la relazione $\subseteq_A$ come segue: $x \subseteq_A y$ se e solo se $x \subseteq y$ e $x, y \in A$. In tal modo $\subseteq_A$ è una relazione d'ordine su A.

Esempio 2.5.3. La relazione | di divisibilità tra interi (definita come $n|m$ se e solo se n divide m) è di ordine negli interi positivi.

Vogliamo precisare che i simboli $\leq$ o $\prec$ sono spesso usati per indicare relazioni di ordine generali, quindi non necessariamente solo la relazione $\leq$ definita sugli interi.
Una diversa descrizione degli ordini a volte è conveniente. Per esempio, invece della relazione $\leq$ tra numeri, potremmo voler usare la relazione $<$ (minore stretto). Similmente potremmo voler usare $\subset_A$ (sottoinsieme proprio) invece di $\subseteq_A$. Ogni relazione di ordine può essere descritta in ciascuna di queste due forme intercambiabili.

Definizione 2.5.3. Una relazione S su A è *asimmetrica* se aSb implica che bSa non vale, per ogni $a, b \in A$. Cioè se aSb e bSa non valgono mai insieme.

Definizione 2.5.4. Una relazione S su A che sia asimmetrica e transitiva è detta una *relazione di ordine stretto* (parziale).

Osservazione 2.5.1. Osserviamo che la proprietà di essere asimmetrica implica che a non può essere in relazione di ordine stretto con se stesso. Infatti altrimenti varrebbe aRa, che coincide con la sua simmetrica, e questo è proibito.

Abbiamo detto prima che le due nozioni sono intercambiabili, adesso vediamo cosa significa. Sostanzialmente, dato un ordine parziale si può sempre ricavare un ordine stretto da questo e viceversa dato un ordine stretto si può sempre ricavare un ordine parziale; i due procedimenti inoltre sono in un certo senso uno l'inverso dell'altro, come adesso vedremo meglio. Specifichiamo che nel seguito denoteremo sempre con $\leq$ ordini, mentre con $<$ ordini stretti.

Teorema 2.5.1. *Data $\leq$ una relazione d'ordine su A, la relazione $<$ in A definita da*

$$a < b \leftrightarrow a \leq b \wedge a \neq b$$

è una relazione di ordine stretto su A. Viceversa, data $<$ una relazione d'ordine stretto su A, la relazione $\leq$ in A definita da

$$a \leq b \leftrightarrow a < b \vee a = b$$

è una relazione di ordine su A.

Dimostrazione. (1) Bisogna mostrare che la relazione $<$ definita è asimmetrica. Supponiamo per assurdo che per qualche $a, b \in A$ valga sia $a < b$ che $b < a$. Quindi valgono per definizione $a \leq b$ e $b \leq a$, ma allora, essendo $\leq$ un ordine parziale, si ha $a = b$. Ma ciò è in contraddizione con la definizione di $a < b$. Lasciamo al lettore la verifica che $<$ è transitiva.

(2) Mostriamo che la relazione $\leq$ definita è antisimmetrica. Supponiamo che valga $a \leq b$ e $b \leq a$. Per definizione ciò equivale a

$$(a < b \vee a = b) \wedge (b < a \vee a = b),$$

da cui segue, non potendo valere $a < b \wedge b < a$, che $a = b$. La riflessività e la transitività si verificano in modo simile. $\square$

Definizione 2.5.5. Siano $a, b \in A$ e $\leq$ (rispettivamente $<$) un ordine (stretto) su A. Diciamo che a e b sono *comparabili* se $a \leq b$ o $b \leq a$ (se $a = b$ o $a < b$ o $b < a$), e diremo che sono *incomparabili* se non sono comparabili.

Esempio 2.5.4. Due qualsiasi numeri reali sono comparabili nell'ordine $\leq$; i numeri interi 2 e 3 sono incomparabili mediante l'ordinamento $|$ di divisibilità.

Esempio 2.5.5. Se l'insieme A contiene almeno due elementi allora ci sono elementi incomparabili nell'insieme ordinato $\big(\mathcal{P}(A), \subseteq_{\mathcal{P}(A)}\big)$.

Definizione 2.5.6. Una relazione di ordine parziale (stretto o no) su A si dice *relazione di ordine totale* se, comunque presi due elementi di A, questi sono comparabili. La coppia $(A, \leq)$ è chiamata *insieme totalmente ordinato.*

Dagli esempi che precedono la definizione risulta chiaro che $(\mathbb{R}, \leq)$ è un insieme totalmente ordinato, mentre $(\mathbb{Z}, \mid)$ non lo è.
Un problema che si presenta abbastanza spesso è quello di trovare un elemento più piccolo o più grande tra certi elementi di un insieme ordinato. Un esame più attento rivela che ci sono diverse nozioni di elemento più piccolo e più grande, vediamole:

Definizione 2.5.7. Sia $\leq$ un ordine su A e sia $B \subseteq A$ un suo sottoinsieme. Diamo le seguenti definizioni:
(1) $b \in B$ è il *minimo* di B se $b \leq x$ per ogni $x \in B$;
(2) $b \in B$ è un *elemento minimale* di B se non esistono $x \in B$ tali che $x < b$;
(3) $b \in B$ è il *massimo* di B se $x \leq b$ per ogni $x \in B$;
(4) $b \in B$ è un *elemento massimale* di B se non esistono $x \in B$ tali che $b < x$.

Esempio 2.5.6. Sia $B \subseteq \mathbb{Z}$ l'insieme dei numeri interi positivi ordinati dalla relazione $|$ di divisibilità. Chiaramente 1 è il minimo di B, ma B non contiene massimi. Sia poi $C \subseteq B$ l'insieme di tutti gli interi positivi maggiori di 1, ossia $C = \{2, 3, \ldots\}$. C non ha un minimo se consideriamo la relazione di divisibilità: infatti 2 non è il minimo in quanto $2 \mid 3$ è falso. Però C ha infiniti elementi minimali: i numeri 2, 3, 5 eccetera (esattamente tutti i numeri primi) sono minimali. C, infine, non ha né massimi né elementi massimali.

Nel teorema che segue diamo due semplici proprietà del minimo e degli elementi minimali, e lasciamo la semplice dimostrazione come esercizio.

Teorema 2.5.2. *Sia A un insieme ordinato dalla relazione $\leq$ e sia $B \subseteq A$. Allora*
(1) B ha al massimo un minimo;
(2) il minimo di B (se esiste) è anche minimale.

Il teorema rimane vero se vengono sostituite le parole "minimo" e "minimale" con "massimo" e "massimale" rispettivamente.

Capitolo 3

Assioma della scelta

3.1 Gli ultimi assiomi

Adesso che abbiamo introdotto il concetto di funzione sarà possibile enunciare anche gli ultimi assiomi, tra cui l'assioma della scelta. Intanto dobbiamo concludere l'elenco degli assiomi della teoria ZF (di Zermelo–Fraenkel).

Definizione 3.1.1. Sia $P(x, y)$ una proprietà (una formula) in x e y. Diremo che tale proprietà è *funzionale* se per ogni x esiste un unico y tale che $P(x, y)$ vale, ossia

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

Adesso siamo pronti per presentare l'assioma:

Schema di assiomi di rimpiazzamento Sia $P(x, y)$ una proprietà funzionale, allora per ogni insieme X esiste un insieme Y i cui elementi sono gli z per i quali $P(x, z)$ è verificata da qualche $x \in X$. Più precisamente:

$$(\forall x)(\exists! y)P(x, y) \to (\forall X)(\exists Y)((\forall z)(z \in Y \leftrightarrow (\exists x)(x \in X \wedge P(x, z)))).$$

Così scritto lo schema di assiomi non risulta estremamente chiaro all'intuizione, benché sia stato presentato nella sua veste formale. Un'osservazione che lo presenta in modo informale certamente aiuterà nella comprensione:

Osservazione 3.1.1. A livello di notazioni informali è possibile scrivere l'insieme Y di cui si postula l'esistenza in una maniera più intuitiva. Se $P(x, y)$ è una proprietà funzionale, quando $P(x, y)$ vale possiamo chiamare $y = F(x)$: tale definizione è ben posta per l'ipotesi di unicità su y. Allora avremo che

$$Y = \{F(x) \mid x \in X\} = \operatorname{imm} F|_X.$$

Da notare bene che questa è solo una scrittura intuitiva e in effetti informale: F, infatti, non è una funzione. L'assioma afferma che se X è piccolo abbastanza per essere un insieme allora anche $\operatorname{imm} F|_X$ è piccolo abbastanza per esserlo. Abbiamo già dimostrato che l'immagine di una funzione esiste (bastano l'assioma dell'unione e quello di separazione), quindi è chiaro che l'assioma di rimpiazzamento non può riguardare le funzioni altrimenti sarebbe superfluo.

L'ultimo assioma invece è quello che riguarda la fondatezza degli insiemi:

Assioma di fondazione Per ogni insieme X non vuoto esiste un suo elemento che non contiene altri elementi di X: un tale x è detto $\in$–minimale. Più precisamente la formulazione dell'assioma è la seguente:

$$(\forall X \neq \emptyset)(\exists x)(x \in X \wedge (\neg(\exists y)(y \in X \wedge y \in x))).$$

Osservazione 3.1.2. Una formulazione equivalente dell'assioma di fondazione è la seguente: per ogni X non vuoto esiste $Y \in X$ tale che $X \cap Y \neq \emptyset$, ossia

$$(\forall X \neq \emptyset)(\exists Y)(Y \in X \wedge X \cap Y \neq \emptyset).$$

Un risultato che segue da questo assioma è il seguente:

Teorema 3.1.1. *Nessun insieme è un elemento di se stesso, ossia* $\neg(\exists A)(A \in A)$.

Dimostrazione. Supponiamo per assurdo che esista A insieme tale che $A \in A$ e definiamo l'insieme $B = \{A\}$, che esiste per l'assioma della coppia. Affermiamo che B non soddisfa l'assioma di regolarità: infatti deve esistere in B un elemento $\in$–minimale e questo deve necessariamente essere A. L'assioma allora ci dice che non esiste alcun $y \in B$ tale che $y \in A$, ma ciò è contraddetto dal fatto che $A \in B$ e $A \in A$ per ipotesi di assurdo. □

Sostanzialmente l'assioma serve evitare cicli di appartenenze come i seguenti: $x \in y \in z \in x$ oppure $x = \{x\}$, come abbiamo appena mostrato. L'assioma di fondazione è forse l'assioma meno utile della teoria degli insiemi di Zermelo–Fraenkel, dal momento che tutti i risultati nelle branche della matematica basate sulla teoria degli insiemi valgono anche in assenza di fondatezza. Oltre ad omettere l'assioma di fondazione, le teorie degli insiemi non standard hanno addirittura postulato l'esistenza di insiemi che sono elementi di se stessi.

3.2 L'assioma della scelta

L'assioma della scelta è classicamente l'ultimo assioma della teoria assiomatica degli insiemi, il decimo quindi, essendo abbastanza particolare per molti aspetti.

Anzitutto è un assioma per il quale fin dall'inizio si è sospettato si trattasse di un teorema, ma poi a tutti gli effetti è stato dimostrato che si tratta di un assioma, per giunta coerente con il resto della teoria assiomatica. Nel 1938 Kurt Gödel ha dimostrato che se il sistema assiomatico di Zermelo–Fraenkel è consistente allora rimane consistente anche con l'aggiunta dell'assioma della scelta: tale sistema viene quindi denotato con l'acronimo ZFC (Zermelo–Fraenkel with Choice). Il risultato di Gödel è stato ottenuto costruendo un modello per la teoria degli insiemi in cui l'assioma della scelta era valido (il modello è noto come "universo degli insiemi costruibili"). Tuttavia l'assioma della scelta non si può dimostrare a partire dagli altri assiomi, come è stato dimostrato da Cohen nel 1963. La dimostrazione di Cohen si basa sulla costruzione di un modello alternativo alla teoria degli insiemi mediante la tecnica del *forcing*: nel modello di Cohen tutti gli assiomi di ZF sono veri e l'assioma della scelta è falso.
Detto in parole povere, l'assioma della scelta afferma che dato un insieme esiste una funzione che associa ad ogni sottoinsieme non vuoto un elemento del sottoinsieme stesso; ovvero, tradotto, è sempre possibile effettuare una "scelta" di elementi di un dato insieme.

Esempio 3.2.1 (di Russell)**.** Un tipico esempio con cui si spiega il senso dell'assioma è il seguente, dovuto a Bertrand Russell. Supponiamo di avere un numero infinito di paia di scarpe e di voler definire un insieme che contiene una (e una sola) scarpa di ogni paio; possiamo farlo senza problemi considerando ad esempio l'insieme delle scarpe destre. I problemi nascono se abbiamo un numero infinito di paia di calzini, e vogliamo considerare come prima un insieme che contenga un calzino per ognuno di essi: non possiamo più parlare dell'insieme dei "calzini destri" e non abbiamo in effetti nessun modo di distinguere i due elementi di un paio, cioè di avere una funzione di scelta che ci assicuri di poterne scegliere contemporaneamente uno da ogni insieme. Per poter dire che tale insieme esiste ci serve l'assioma della scelta.

Tale assioma trova contro i matematici costruttivisti, per i quali un insieme ha senso solo se costruito mediante proprietà di specificazione esplicite a partire da insiemi noti. In effetti l'assioma della scelta postula l'esistenza di un insieme (l'immagine di quella funzione di scelta) astratto, per il quale non sappiamo come siano fatti gli elementi: essi non vengono selezionati mediante specificazione di una loro proprietà. Però rifiutare l'assioma della scelta comporta parecchie perdite di risultati sostanziali in matematica. Ad esempio sull'assioma della scelta è fondata l'esistenza di un insieme non misurabile secondo Lebesgue e comunque l'assioma della scelta è alla base della dimostrazione di molti teoremi dell'analisi matematica o anche di algebra lineare: in effetti è proprio grazie a tale assioma se si può dimostrare che ogni spazio vettoriale ammette una base: per quelli finiti non è richiesto, ma per quelli infiniti sì. Va anche detto però che se da un lato l'assioma

della scelta consente di dimostrare dei risultati importanti, dall'altro porta anche alla costruzione di oggetti matematici controintuitivi, come insiemi non misurabili (l'insieme di Vitali) o come partizioni finite della sfera che riassemblate opportunamente diventano due sfere di uguale dimensione[1]. Dopo questa introduzione storica informale veniamo alla matematica e enunciamo l'assioma della scelta. Esistono molte forme equivalenti, ma a seguito di tutta l'introduzione fatta ci pare naturale darlo così:

Assioma di scelta Per ogni sistema non vuoto di insiemi non vuoti esiste una funzione di scelta che da ognuno degli insiemi del sistema sceglie uno e un solo elemento. In modo formale:

$$(\forall S \neq \emptyset)(\exists f)(\operatorname{dom} f = S \wedge (\forall X \in S - \{\emptyset\})(f(X) \in X)).$$

Osservazione 3.2.1. Se S è tale che esiste una "regola" per scegliere da ogni X un elemento allora l'esistenza di una funzione di scelta f è dimostrabile in base agli altri assiomi senza far ricorso all'assioma della scelta. Ad esempio se S è l'insieme di tutti i sottoinsiemi non vuoti di $\mathbb{N}$, allora per mostrare l'esistenza di una funzione di scelta si può definire $f(X) = \min X$ per ogni $X \in S$.

Come già anticipato nel caso di un insieme finito non è richiesto l'assioma di scelta: quando il numero di scelte da fare è finito si dimostra che esiste una funzione di scelta senza dover ricorrere all'assioma della scelta.

Teorema 3.2.1. *Ogni sistema finito di insiemi ha una funzione di scelta.*

Dimostrazione. Procediamo per induzione sulla cardinalità $n \in \mathbb{N}$ del sistema S. Se $|S| = 0$ allora bisogna prendere come funzione di scelta la funzione vuota. Supponiamo che ogni sistema di n insiemi abbia una funzione di scelta e sia S un sistema tale che $|S| = n + 1$. Fissiamo $X \in S$; l'insieme $S - \{X\}$ ha n elementi e dunque per ipotesi induttiva ha una funzione di scelta g_X. Se $X = \emptyset$ allora $g = g_X \cup \{(X, \emptyset)\}$ è una funzione di scelta per S. Se invece $X \neq \emptyset$ allora $g^x = g_X \cup \{(X, x)\}$ è una funzione di scelta per S (per ogni $x \in X$). □

Adesso presentiamo le principali formulazioni equivalenti dell'assioma della scelta:

[1] questo è il famoso *paradosso di Banach–Tarski* sul raddoppiamento della sfera. Questo stabilisce che, usando l'assioma di scelta, è possibile prendere S^2 come sottospazio di $\mathbb{R}^3$, suddividerla in un insieme finito di pezzi (che saranno non misurabili) e, utilizzando solo rotazioni e traslazioni, riassemblarli insieme in modo da ottenere due copie identiche di S^2. Banach e Tarski intendevano confutare l'assioma della scelta con questo argomento, ma la natura della dimostrazione ha portato altri matematici ad assumere che l'assioma di scelta produca semplicemente dei risultati controintuitivi.

Teorema 3.2.2. *Assumendo ZF, sono proprietà equivalenti le seguenti:*
(1) ogni sistema di insiemi non vuoti ammette una funzione di scelta;
(2) per ogni $g : A \to B$ suriettiva esiste $f : B \to A$ iniettiva e tale che $g \circ f = id_B$;
(3) per ogni sequenza non vuota $\langle A_i \mid i \in I \rangle$ di insiemi non vuoti si ha $\prod_{i \in I} A_i \neq \emptyset$.

Dimostrazione. ((1) $\implies$ (2)) Osserviamo che se $g : A \to B$ è surgettiva allora per ogni $b \in B$ si considera l'insieme $g^{-1}(b) \in \mathcal{P}(A) - \{\emptyset\}$. Ma essendo A non vuoto e $\mathcal{P}(A) - \{\emptyset\}$ un sistema di insiemi non vuoti esiste una funzione di scelta $h : \mathcal{P}(A) - \{\emptyset\} \to A$ che permette di scegliere un elemento da ciascun sottoinsieme di A non vuoto. Per ogni $b \in B$ si pone $f(b) = h\left(g^{-1}(b)\right)$ e abbiamo concluso.
((2) $\implies$ (3)) Ricordiamo innanzitutto che

$$\prod_{i \in I} A_i = \left\{ f : I \to \bigcup_{i \in I} A_i \mid (\forall i \in I)(f(i) \in A_i) \right\}.$$

Sia $A'_i = A_i \times \{i\}$ e sia $g : \bigcup_{i \in I} A'_i \to I$ definita da $g(x, i) = i$. g è suriettiva perché per ogni $i \in I$ si ha $A_i \neq \emptyset$, ma allora per ipotesi ha come inversa a destra la funzione f, che soddisfa $f(i) = A'_i$ per ogni $i \in I$. Detta $p : \bigcup_{i \in I} A'_i \to \bigcup_{i \in I} A_i$ la proiezione $p(x, i) = x$, si pone

$$h : I \to \bigcup_{i \in I} A_i \quad \text{tale che } h(i) = p(f(i))$$

e abbiamo un elemento di $\prod_{i \in I} A_i$.
((3) $\implies$ (1)) Sia $S = \{S_i \mid i \in I\}$ una famiglia di insiemi non vuoti. Allora per ipotesi vale che $\prod_{i \in I} S_i \neq \emptyset$, ossia esiste una funzione

$$f : I \to \bigcup_{i \in I} S_i$$

tale che $f(i) \in S_i$ per ogni $i \in I$. Inoltre esiste una funzione $p : S \to I$ tale che $p(S_i) = i$ (si associa ad ogni insieme il suo indice). L'applicazione $f \circ p : S \to \bigcup_{i \in I} S_i$ è tale che $(f \circ p)(S_i) \in S_i$ per ogni $S_i \in S$, ossia è una funzione di scelta per S. □

Osservazione 3.2.2. Osserviamo che la proposizione inversa della (2) del teorema 3.2.2 non richiede l'assioma della scelta. Supponiamo che esista una funzione iniettiva $f : A \to B$ allora affermiamo che esiste una funzione $g : B \to A$ surgettiva. Visto che $A \neq \emptyset$ sia $a \in A$. Definiamo la funzione

$$g(x) = \begin{cases} a & \text{se } x \notin \operatorname{imm} f \\ y & \text{se } f(y) = x \end{cases}.$$

Più formalmente definiamo

$$g = \{(u, v) \in B \times A \mid (v, u) \in f \vee (u \notin \operatorname{imm} f \wedge v = a)\}.$$

Infine vale $(g \circ f)(a) = a$ per ogni $a \in A$.

Quando abbiamo introdotto l'assioma della scelta avevamo detto che questo diceva che dato un insieme non vuoto era sempre possibile scegliere un elemento da ciascun sottoinsieme non vuoto. Bene, mostriamo che la nostra formulazione equivale a quella appena richiamata:

Teorema 3.2.3. *Sono equivalenti le seguenti due affermazioni:*
(1) ogni sistema non vuoto di insiemi non vuoti ammette una funzione di scelta;
(2) per ogni $A \neq \emptyset$ esiste $f : \mathcal{P}(A) - \{\emptyset\} \to A$ tale che $f(X) \in X$ per ogni $X \neq \emptyset$.

Dimostrazione. ((1) $\implies$ (2)) Osserviamo che se A è non vuoto allora $\mathcal{P}(A) - \{\emptyset\}$ è un sistema di insiemi non vuoto. Dunque per ipotesi esiste una funzione di scelta $f : \mathcal{P}(A) - \{\emptyset\} \to A$ tale che per ogni $X \in \mathcal{P}(A)$ non vuoto si ha $f(X) \in X$.
((2) $\implies$ (1)) Osserviamo che la (2) implica la (2) del precedente teorema. Infatti avevamo detto che potevamo scegliere un elemento da ogni $g^{-1}(b)$ perché $\mathcal{P}(A) - \{\emptyset\}$ era un sistema di insiemi non vuoti. Con la nostra nuova ipotesi però, l'esistenza della funzione di scelta dipende subito dal fatto che A è non vuoto. Quindi dalla (2) del precedente teorema segue la (1) del precedente teorema, che è la nostra tesi. □

Capitolo 4

Numeri naturali e buoni ordini

Adesso riprenderemo la definizione dei numeri naturali che abbiamo dato nel primo capitolo, e definiremo una relazione di ordine totale su $\mathbb{N}$ e le operazioni aritmetiche. Passeremo infine a trattare i buoni ordinamenti.

4.1 Richiami e proprietà dei numeri naturali

Abbiamo definito l'insieme $\mathbb{N}$ dei numeri naturali come il può piccolo contenente l'insieme vuoto e chiuso per successore. Se si preferisce, ma è la stessa cosa, $\mathbb{N}$ è l'intersezione della famiglia degli insiemi induttivi, che è non vuota per l'assioma dell'infinito. Adesso vogliamo definire una relazione di ordine su $\mathbb{N}$:

Definizione 4.1.1. Per ogni $n, m \in \mathbb{N}$ diciamo $n < m$ se e solo se $n \in m$.

Adesso è compito della prossima parte mostrare che in effetti quella appena definita è una relazione che si comporta esattamente come ci aspettiamo.

Lemma 4.1.1. *Definito $n \leq m$ come $n < m$ o $n = m$, valgono le due proprietà:*
(1) $0 \leq n$ per ogni $n \in \mathbb{N}$;
(2) per ogni $k, n \in \mathbb{N}$, $k < n + 1$ se e solo se $k < n$ o $k = n$.

Dimostrazione. (1) Dimostriamo questa proprietà $P(n)$ per induzione. Sicuramente per $n = 0$ la proprietà è vera perché $0 = 0$. Adesso supponiamo che $P(n)$ valga e mostriamo che allora vale $P(n + 1)$. Dalla definizione di $<$, la proprietà $P(n)$ equivale a $0 = n$ o $0 \in n$: da questo segue $0 \in n \cup \{n\}$, ossia $0 < n + 1$ e quindi vale $P(n + 1)$.
(2) Questa parte non richiede l'induzione. Infatti basta osservare che $k < n + 1$ se e solo se $k \in n + 1 = n \cup \{n\}$, e questo se e solo se $k \in n$ o $k = n$. □

Osservazione 4.1.1. Il punto (2) del precedente lemma afferma che $k < n + 1$ è equivalente a $k \leq n$, come ci aspettiamo, essendo $n + 1$ il successore di n.

La dimostrazione del seguente importante teorema è un altro esempio, più complicato, di dimostrazione per induzione. Vediamo:

Teorema 4.1.1. $(\mathbb{N}, <)$ *è un insieme totalmente ordinato.*

Dimostrazione. Ricordiamo ciò che dobbiamo mostrare: (1) $<$ è una relazione transitiva, (2) $<$ è una relazione asimmetrica e (3) $<$ è un ordine totale. Procediamo con ciascuno di essi separatamente.
(1) Siamo $k, m, n \in \mathbb{N}$ tali che $k < m$ e $m < n$: dobbiamo mostrare che $k < n$. Abbiamo pert ipotesi che $k \in m \in n$, e quindi $k \in \bigcup n$. Ma $\bigcup n = n - 1$ e quindi $k < n - 1$, e allora per il lemma precedente si ha $k < n$, e abbiamo concluso[1].
(2) Supponiamo che valga contemporaneamente $n < k$ e $k < n$. Per la transitività questa implica $n < n$, quindi dobbiamo solo mostrare che ciò è impossibile. Procediamo per induzione: ovviamente $0 < 0$ non è possibile (vorrebbe dire $\emptyset \in \emptyset$). Supponiamo ora che $n < n$ sia impossibile e mostriamo che lo è anche $n+1 < n+1$. Se $n+1 < n+1$ fosse vera avremmo per la (2) del lemma che $n+1 < n$ o $n+1 = n$. La seconda è chiaramente falsa, e la prima conduce ad un assurdo in quanto si contraddice l'ipotesi induttiva: infatti, essendo $n < n+1$ e $n+1 < n$ si concluderebbe $n < n$.
(3) Dobbiamo mostrare ora che per ogni $m, n \in \mathbb{N}$ vale o $m = n$ o $m < n$ o $n < m$. Procediamo per induzione su n. Se $n = 0$ è ovvio che per ogni $m \in \mathbb{N}$ si ha $m < 0$ o $m = 0$ o $m > 0$: il primo caso non si dà mai e poi sappiamo dal primo punto del lemma che $0 \leq m$ per ogni $m \in \mathbb{N}$, che corrisponde alle altre due condizioni. Adesso supponiamo che per ogni $m \in \mathbb{N}$ valga $m = n$ o $m < n$ oppure $m > n$, dobbiamo mostrare che allora $m = n + 1$ o $m > n + 1$ o $m < n + 1$. Se $m < n$ allora, essendo $n < n + 1$ per il lemma, segue che $m < n + 1$ per transitività. Similmente, se $m = n$ allora segue $m < n + 1$ sempre per il lemma. Infine, se $n < m$ vorremmo concludere che $n + 1 \leq m$ in quanto ciò mostrerebbe $m = n + 1$ o $m > n + 1$. Mostriamo questo fatto con un'induzione su $m \in \mathbb{N}$ (si osservi che ora n è un parametro fissato). Se $m = 0$ l'affermazione "se $n < 0$ allora $n + 1 \leq 0$" è vero (in quanto è un'implicazione con premessa falsa). Supponiamo adesso che valga "se $n < m$ allora $n + 1 \leq m$"; supponiamo $n < m + 1$, dobbiamo mostrare $n + 1 \leq m + 1$. L'ipotesi $n < m + 1$ equivale per il lemma a $n < m$ o $n = m$. Se $n < m$ segue che $n + 1 \leq m$ per ipotesi induttiva, e quindi per il lemma si ha $n + 1 < m + 1$. Se invece $n = m$ allora ovviamente $n + 1 = m + 1$, ed abbiamo concluso. L'induzione su m è finita e con questa si conclude quella su n. □

[1] potevamo anche procedere per induzione su n, ossia dimostriamo la proprietà $P(x)$ "per ogni $k, m \in \mathbb{N}$ se $k < m$ e $m < x$ allora $k < x$". Sicuramente $P(0)$ è vera: infatti se $k < m$ e $m < 0$ allora $k < 0$ in quanto non esistendo nessun $m < 0$ per il lemma precedente la condizione è banalmente vera. Supponiamo che valga $P(n)$, e sia $k < m$ e $m < n+1$: per il lemma precedente si ha che la seconda di queste equivale a $m < n$ o $m = n$. Se $m < n$ allora si conclude per ipotesi induttiva; se invece $m = n$ allora si ha $k < n$ e quindi per il lemma precedente si ha $k < n + 1$.

Osservazione 4.1.2. Il lettore dovrebbe studiare con attenzione la precedente dimostrazione, specialmente la parte (3), che è un esempio di doppia induzione. Con lo scopo di dimostrare una proposizione che dipende da due parametri m e n si procede per induzione su uno di essi (n) e nella dimostrazione del passo induttivo di questa si deve iniziare un'induzione sulla variabile m (per n fissato).

Prima di proseguire oltre, dimostreremo un'altra versione dell'induzione, che spesso è più conveniente dell'altra.

Teorema 4.1.2 (principio di induzione, seconda versione)**.** *Sia $P(x)$ una proprietà (possibilmente con parametro). Supponiamo che per ogni $n \in \mathbb{N}$ valga*

$$\text{se per ogni } P(k) \text{ vale per ogni } k < n \text{ allora } P(n). \tag{4.1}$$

Allora $P(n)$ vale per ogni $n \in \mathbb{N}$.

Dimostrazione. Supponiamo che la proprietà (4.1) valga. Consideriamo la proprietà $Q(n)$: "$P(k)$ vale per ogni $k < n$". La proprietà $Q(0)$ è banalmente vera, in quanto è un'implicazione con premessa falsa. Supponiamo che $Q(n)$ valga, allora mostriamo che vale anche $Q(n+1)$. Dire che $Q(n)$ vale significa dire che vale $P(k)$ per ogni $k < n$, e quindi per la (4.1), vale anche $P(n)$. Grazie al lemma possiamo concludere che $P(k)$ vale per ogni $k < n + 1$, ossia vale $Q(n + 1)$. Quindi per induzione $Q(n)$ vale per ogni $n \in \mathbb{N}$: visto che per ogni $k \in \mathbb{N}$ esiste un $n > k$ (per esempio $n = k + 1$) si ha che $P(k)$ è vera per ogni $k \in \mathbb{N}$. □

4.2 Buoni ordini

Adesso, dopo le prime proprietà dei numeri naturali possiamo parlare di buoni ordinamenti. Abbiamo deciso di trattare questo argomento in questo capitolo poiché mostreremo subito un esempio di insieme ben ordinato, i numeri naturali stessi. Il concetto di buon ordine è molto importante, e distingue l'ordine dei numeri naturali per esempio da quello dei numeri razionali. Iniziamo dunque con la seguente definizione:

Definizione 4.2.1. Un ordine totale $\prec$ su un insieme A si dice *buon ordine* se ogni sottoinsieme non vuoto di A ha un elemento minimo. La coppia $(A, \prec)$ si dice *insieme ben ordinato.*

Osservazione 4.2.1. Se $(A, \prec)$ è un insieme ben ordinato allora ogni sottoinsieme non vuoto X di A può essere ben ordinato mettendo su X l'ordine di A ristretto agli elementi di X.

Come annunciato mostriamo che la proprietà di buon ordinamento caratterizza i numeri naturali:

Teorema 4.2.1. $(\mathbb{N}, <)$ *è un insieme ben ordinato.*

Dimostrazione. Sia X un sottoinsieme non vuoto di $\mathbb{N}$, dobbiamo mostrare che X ha un elemento minimo. Supponiamo che X non abbia un minimo e consideriamo $\mathbb{N} - X$. Il passo cruciale è osservare che se $k \in \mathbb{N} - X$ per ogni $k < n$ allora $n \in \mathbb{N} - X$: infatti altrimenti n sarebbe l'elemento minimo di X. Ma allora grazie alla seconda versione dell'induzione appena mostrata segue che $n \in \mathbb{N} - X$ per ogni $n \in \mathbb{N}$. Ma allora $X = \emptyset$ e ciò è assurdo. □

Adesso vediamo modi di ben ordinare unioni e prodotti di due buoni ordini. Vediamo subito di cosa si tratta:

Proposizione 4.2.1. *Siano* $(A_1, \leq_1)$ *e* $(A_2, \leq_2)$ *due insiemi ben ordinati e tali che* $A_1 \cap A_2 = \emptyset$. *La relazione* $\leq$ *definita su* $A_1 \cup A_2$ *come segue:*

$$a \leq b \iff a, b \in A_1 \text{ e } a \leq_1 b \quad o \quad a, b \in A_2 \text{ e } a \leq_2 b \quad o \quad a \in A_1 \text{ e } b \in A_2$$

è un buon ordine.

Dimostrazione. Dobbiamo mostrare tre fatti: (1) la relazione $\leq$ è di ordine su $A_1 \cup A_2$, (2) l'ordine è totale e infine (3) l'ordine è buono.
(1) Il fatto che $\leq$ sia riflessiva è banale in quanto sono riflessivi sia $\leq_1$ che $\leq_2$. Ora siano $u, v \in A_1 \cup A_2$ con $u \leq v$ e $v \leq u$, dobbiamo mostrare che $u = v$. Le due relazioni scritte danno, distribuendo la disgiunzione logica sulle congiunzioni, nove distinti casi: in questi o si giunge ad un caso che non si dà oppure si conclude grazie all'antisimmetria di $\leq_1$ e $\leq_2$. Infine la transitività si mostra in modo del tutto analogo.
(2) Siano $u, v \in A_1 \cup A_2$. Se $u, v \in A_1$ allora sarà $u \leq_1 v$ oppure $v \leq_1 u$ per la totalità di $\leq_1$: nei due casi si ha rispettivamente $u \leq v$ oppure $v \leq u$. Se $u, v \in A_2$ il caso è esattamente analogo al precedente. Se invece $u \in A_1$ e $v \in A_2$ allora segue per definizione che $u \leq v$; il caso $u \in A_2$ e $v \in A_1$ è analogo.
(3) Sia $X \subseteq A_1 \cup A_2$ un sottoinsieme non vuoto dell'unione. Se $X \subseteq A_1$ allora, essendo $\leq_1$ un buon ordine, si ha che esiste $x \in X$ tale che $x \leq_1 a_1$ per ogni $a_1 \in X$, ossia per definizione $x \leq a_1$ per ogni $a_1 \in X$. Se invece $X \subseteq A_2$ si procede analogamente. Se invece $X \cap A_1$ e $X \cap A_2$ sono entrambi non vuoti basta prendere il minimo x di $X \cap A_1 \subseteq A_1$ secondo la relazione $\leq_1$. Questo è anche il minimo di X secondo $\leq$. □

Osservazione 4.2.2. La costruzione precedente può anche essere generalizzata a due insiemi non disgiunti A_1 e A_2. Basta prendere $A_1 \times \{0\}$ e $A_2 \times \{1\}$ e ordinare questi due insiemi che ora sono disgiunti.

Definizione 4.2.2. L'insieme ben ordinato $(A_1 \cup A_2, \leq)$ definito nella proposizione è detto *somma* degli ordini $(A_1, \leq_1)$ e $(A_2, \leq_2)$, e lo indicheremo con $(A_1 \oplus A_2, \leq)$.

Proposizione 4.2.2. *Siano $(A_1, \leq_1)$ e $(A_2, \leq_2)$ due insiemi ben ordinati. La relazione $\leq$ definita su $A_1 \times A_2$ come segue:*

$$(a_1, a_2) \leq (b_1, b_2) \Longleftrightarrow a_2 <_2 b_2 \ o \ (a_2 = b_2 \ e \ a_1 \leq_1 b_1)$$

è un buon ordine.

Dimostrazione. Ancora una volta dobbiamo mostrare tre fatti: (1) la relazione $\leq$ è di ordine su $A_1 \times A_2$, (2) l'ordine è totale e infine (3) l'ordine è buono.
(1) Il fatto che $\leq$ sia riflessiva è banale in quanto in particolare con lo stesso elemento vale l'uguaglianza. Adesso mostriamo che è antisimmetrica: supponiamo che $(a_1, a_2) \leq (b_1, b_2)$ e $(b_1, b_2) \leq (a_1, a_2)$. Questo significa formalmente che

$$[a_2 <_2 b_2 \text{ o } (a_2 = b_2 \text{ e } a_1 \leq_1 b_1)] \quad \text{e} \quad [b_2 <_2 a_2 \text{ o } (a_2 = b_2 \text{ e } b_1 \leq_1 a_1)]\,;$$

distribuendo la disgiunzione logica "e", ricordando che $<$ è asimmetrica e che $\leq_1$ è antisimmetrica si conclude $b_1 = b_2$ e $a_1 = a_2$, che è ciò che volevamo. La transitività è analoga.
(2) Siano (a_1, a_2) e (b_1, b_2) elementi di $A_1 \times A_2$. Per il fatto che $\leq_1$ e $\leq_2$ sono ordini totali si ha che uno dei seguenti casi deve presentarsi: $a_1 <_1 b_1$; $b_1 <_1 a_1$; $a_1 = b_1$ e $a_2 <_2 b_2$; $a_1 = b_1$ e $b_2 <_2 a_2$; $a_1 = b_1$ e $a_2 = b_2$. In ciascuno di questi casi segue che (a_1, b_1) e (b_1, b_2) sono comparabili secondo la relazione $\leq$.
(3) Mostriamo adesso che $\leq$ è un buon ordinamento. Sia $X \subseteq A_1 \times A_2$ sottoinsieme non vuoto. Consideriamo

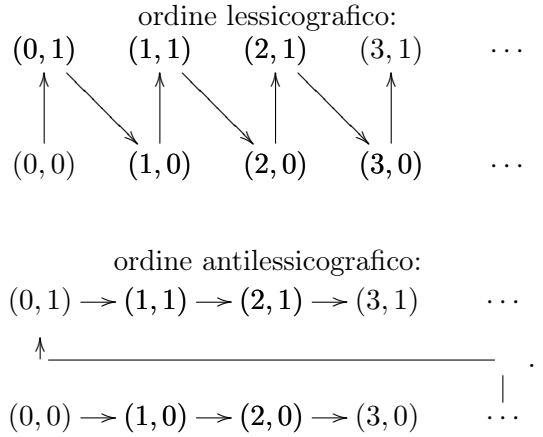
$$X_1 = \{a_1 \in A_1 \mid \exists a_2 \in A_2 \text{ tale che } (a_1, a_2) \in X\} \subseteq A_1;$$

questo è un sottinsieme non vuoto di A_1 (in quanto X è non vuoto) e pertanto ammette un minimo secondo l'ordinamento $\leq_1$, sia $m_1 = \min X_1$. Analogamente considerando l'insieme $X_2 = \{a_2 \in A_2 \mid \exists a_1 \in A_1 \text{ tale che } (a_1, a_2) \in X\}$ sottoinsieme non vuoto di A_2 si pone $m_2 = \min X_2$ secondo la relazione $\leq_2$. Affermiamo che $(m_1, m_2) \in X$ è il minimo di X: la verifica è molto semplice. □

Potevamo scegliere anche di ordinare il prodotto confrontando le prime coordinate prima di confrontare le seconde: questo è quello che si chiama *ordine lessicografico* in quanto nel caso in cui $A_1 = A_2 = \{a, b, c, \ldots, z\}$ è l'insieme delle lettere e $\leq_1 = \leq_2$ è l'ordine alfabetico $a <_1 b <_1 \cdots <_1 z$ allora $\leq$ definito su $A_1 \times A_2$ ordina gli elementi come questi lo sarebbero in un dizionario. L'ordinamento sul prodotto che invece abbiamo definito nella proposizione 4.2.2 è quello che si dice *ordine antilessicografico.*

Definizione 4.2.3. L'insieme ben ordinato $(A_1 \times A_2, \leq)$ con l'ordine antilessicografico è detto *prodotto* degli ordini $(A_1, \leq_1)$ e $(A_2, \leq_2)$, e lo indicheremo con $(A_1 \odot A_2, \leq)$.

I due ordinamenti proposti sono in generale piuttosto diversi: compariamo per esempio l'ordinamento lessicografico e quello antilessicografico sul prodotto $\mathbb{N} \times \{0, 1\}$. I due ordinamenti sono di seguito mostrati:



Il primo ordinamento è simile a $(\mathbb{N}, <)$ e il secondo tipo no, anzi è la somma di due identiche copie di $(\mathbb{N}, <)$.
Visto che quello su $\mathbb{N}$ è il primo buon ordinamento che abbiamo incontrato possiamo collegare un buon ordine su un qualsiasi insieme e osservare che questo è collegato in modo molto stretto all'insieme $\mathbb{N}$. Prima di vedere questo fatto dobbiamo però enunciare un teorema importante, che mostreremo nei succesivi paragrafi per non perdere il filo del discorso sui buoni ordini, ed è il seguente:

Teorema 4.2.2 (di ricorsione numerabile)**.** *Siano A un insieme, $a \in A$ e $h : A \to A$ una funzione. Allora esiste un'unica funzione $f : \mathbb{N} \to A$ tale che $f(0) = a$ e $f(n + 1) = h(f(n))$.*

Questo sostanzialmente è il teorema che ci permette di poter dare le definizioni per induzione, definendo la funzione f su 0 e poi per successore[2]. Adesso possiamo vedere il risultato sui buoni ordini:

Teorema 4.2.3. *Sia $(A, \leq)$ un insieme totalmente ordinato. La relazione $\leq$ è un buon ordine se e solo se non esiste in A alcuna successione $\langle a_n \mid n \in \mathbb{N} \rangle$ strettamente decrescente, ovvero tale che $a_{n+1} < a_n$ per ogni $n \in \mathbb{N}$.*

[2]la forma data del teorema di ricorsione non è la più generale in assoluto. Infatti, anziché prendere $\mathbb{N}$ come dominio della funzione f da definire, si può anche prendere un qualsiasi buon ordine: quello sarà il *teorema di ricursione transfinita* che mostreremo più avanti, quando ritorneremo a parlare di buoni ordinamenti.

Dimostrazione. ($\Longrightarrow$) Sia $(A, \leq)$ un buon ordine e supponiamo che esista una successione $\langle a_n \mid n \in \mathbb{N} \rangle$ con le proprietà indicate. Per costruzione si ha che l'immagine della sequenza $\langle a_n \mid n \in \mathbb{N} \rangle$ è non vuoto ma non ha minimo, e questo è assurdo.
($\Longleftarrow$) Supponiamo che A non sia ben ordinato, e sia $X \subseteq A$ non vuoto e che non ha minimo. Mostriamo che allora si riesce a trovare una funzione $f : \mathbb{N} \to A$ tale che $f(n+1) < f(n)$ per ogni $n \in \mathbb{N}$, e dunque $\langle f(n) \mid n \in \mathbb{N} \rangle$ sarà la successione cercata: questa parte richiede l'assioma della scelta nella forma seguente: per ogni insieme non vuoto A esiste una funzione di scelta

$$f_S : \mathcal{P}(A) - \{\emptyset\} \to A$$

tale che $f_S(X) \in X$ per ogni $X \neq \emptyset$. A questo punto definiamo ricorsivamente la nostra funzione f come segue:

$$f(0) = f_S(X), \quad f(n+1) = f_S\left(\{x \in X \mid x < f(n)\}\right).$$

Definita $h : A \to A$ come $h(u) = f_S\left(\{x \in X \mid x < u\}\right)$ possiamo applicare il teorema di ricorsione numerabile con $a = f_S(X) \in A$ e h la funzione appena definita: in questo modo abbiamo definito univocamente una funzione f. La proprietà $f(n+1) < f(n)$ per ogni $n \in \mathbb{N}$ a questo punto si fa per induzione. □

Corollario 4.2.1. *Sia $(A, \leq)$ un insieme totalmente ordinato. Se A è finito allora $\leq$ è un buon ordinamento.*

Dimostrazione. Per il teorema precedente A deve essere bene ordinato in quanto, essendo finito, non può esistere una successione strettamente decrescente. □

Osservazione 4.2.3. Si poteva dare anche una dimostrazione diretta, che però deve presuporre una definizione precisa di "numero di elementi di un insieme", che però il lettore avrà già in maniera intuitiva. Per dimostrare che si tratta di un buon ordine dobbiamo mostrare che ogni sottoinsieme non vuoto di A ammette minimo: visto che A è finito, diciamo con n elementi, anche un qualsiasi suo sottoinsieme $B \subseteq A$ lo è. Se B ha un elemento allora quello deve essere il suo minimo. Supponiamo che la tesi valga per tutti i $B \subseteq A$ con $m < n$ elementi, dimostriamo che vale per un B con $m+1$ elementi. Tale B si scriverà

$$B = \{b\} \cup B',$$

dove $b \notin B'$: allora B' ammette minimo b' perché ha m elementi (ipotesi induttiva), e vale $b < b'$ o $b' < b$ o $b = b'$ per la totalità di $<$. In ogni caso B ha minimo.

Osservazione 4.2.4. Una parte del teorema ci garantisce che se un insieme è ben ordinato allora non può esistere una successione strettamente decrescente di suoi elementi. Questo vuol dire che se una successione è decrescente non può esserlo in senso stretto, da un certo punto in poi dovrà stabilizzarsi per esempio: nulla viene detto sul comportamento di tali successioni, che in effetti può essere vario. Consideriamo $\mathbb{N} \times \mathbb{N}$ ordinato con l'ordinamento antilessicografico e sia

$$\langle a_n \mid n \in \mathbb{N} \rangle$$

una successione in $\mathbb{N} \times \mathbb{N}$. Immaginiamo $\mathbb{N} \times \mathbb{N}$ come una successione di infinite righe con infiniti elementi per riga, o se vogliamo esemplificare come un albergo con infiniti piani ed infinite stanze per piano (questo è quello che si chiama *albergo di Russell*). Avremo ovviamente che a_0 sarà una certa di stanza del piano k–esimo: se la successione deve essere decrescente sappiamo che prima o poi arriverà a stabilizzarsi ad una stanza precisa: stanza precedente se sullo stesso piano, o stanza qualsiasi ma su un piano più basso. In ogni caso, scendendo di piano, per esempio, si può scegliere qualsiasi stanza e le scelte sono infinite: pertanto non possiamo prevedere la lunghezza della successione di stanze. Invece se consideriamo $\mathbb{N}$ con il suo buon ordinamento se $a_0 = n$ allora la successione decrescente al massimo assumerà n valori, cioè dopo al più n passi dovrà stabilizzarsi.

La domanda che ci possiamo porre adesso è la seguente: è possibile ben ordinare $\mathbb{R}$? Sicuramente il naturale ordinamento su $\mathbb{R}$ non è buono: infatti esiste ad esempio il sottoinsieme

$$\{x \in \mathbb{R} \mid x \leq 0\}$$

che non ha minimo. Ma Zermelo enunciò nel 1904 il seguente teorema:

Teorema 4.2.4 (di Zermelo)**.** *Ogni insieme è ben ordinabile.*

Georg Cantor considerava che questo enunciato fosse un "fondamentale principio del pensiero". Molti matematici, tuttavia, trovarono difficile visualizzare un buon ordinamento di insiemi come $\mathbb{R}$. Nello stesso anno König annunciò di avere dimostrato che tale buon ordinamento non può esistere, ma successivamente Hausdorff trovò un errore nella sua dimostrazione. Zermelo in seguito per dimostrare il teorema del buon ordinamento introdusse l'assioma della scelta ritenendolo un "principio logico non sottoponibile ad obiezioni". Oggi sappiamo che si può dire di più: il teorema del buon ordinamento è equivalente all'assioma della scelta. Il fatto che dall'assioma della scelta discenda il teorema di Zermelo può essere mostrato non molto difficilmente grazie al lemma di Zorn, forma equivalente all'assioma della scelta: non avendolo ancora trattato però, rimandiamo la dimostrazione. Però qui possiamo mostrare che se vale il teorema di Zermelo allora deve valere l'assioma di scelta.

Teorema 4.2.5. *Se ogni insieme è ben ordinabile allora è valido l'assioma della scelta.*

Dimostrazione. Sia S un sistema non vuoto di insiemi non vuoti, allora vorremmo una funzione

$$f : S \longrightarrow \bigcup S = \bigcup_{X \in S} X$$

tale che $f(X) \in X$ per ogni $X \in S$. Visto che vale il teorema di Zermelo allora $\bigcup_{X \in S} X$ è bene ordinabile mediante una relazione d'ordine. Allora, per la definizione di buon ordine, dato un insieme $X \in S$, che sarà sottoinsieme di $\bigcup_{X \in S} X$, possiamo trovare un elemento minimo. Ponendo $f(X) = \min X$ per ogni $X \in S$ abbiamo una funzione f ben definita. $\square$

Capitolo 5

Insiemi finiti, numerabili e non numerabili

5.1 Cardinalità degli insiemi

Dal punto di vista della teoria degli insiemi, il problema di base riguardo a un insieme è chiedersi quanti elementi abbia. È importante osservare che noi potremmo definire (come faremo) il fatto che due insiemi "hanno lo stesso numero di elementi" senza sapere niente sui numeri. Per spiegare meglio questo fatto ricorriamo ad un esempio. Se proviamo a chiedere a un bambino che non conosce ancora cosa siano i numeri se le dita della mano destra sono tante quante quelle della mano sinistra, lui risponderà certamente di sì: come lo ha stabilito? Semplicemente accostando le due mani e verificando che nell'accostamento ogni dito della mano destra si toccava con un solo dito della mano sinistra e che nessun dito rimaneva fuori. Ciò è stato fatto senza sapere che le dita sono cinque per ogni mano: il bambino ha stabilito una corrispondenza biunivoca tra le dita delle due mani.

Definizione 5.1.1. Due insiemi A e B si dicono *equipotenti* (hanno *la stessa cardinalità*) se esiste una funzione $f : A \to B$ biunivoca. Indichiamo questo fatto con $|A| = |B|$.

Esempio 5.1.1. Gli insiemi $\{\emptyset, \{\emptyset\}\}$ e $\{\{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}\}$ sono equipotenti. Infatti basta definire

$$f(\emptyset) = \{\{\emptyset\}\} \quad \text{e} \quad f(\{\emptyset\}) = \{\{\{\emptyset\}\}\}.$$

Esempio 5.1.2. Gli insiemi $\{\emptyset\}$ e $\{\emptyset, \{\emptyset\}\}$ non sono equipotenti.

Esempio 5.1.3. L'insieme dei numeri reali positivi è equipotente a quello dei numeri reali negativi. Basta definire per ogni $x \in \{x \in \mathbb{R} \mid x > 0\}$ l'immagine $f(x) = -x$.

Il prossimo passo è dimostrare che l'equipotenza gode delle proprietà di una relazione di equivalenza. Non possiamo però propriamente parlare dell'equipotenza come una relazione di equivalenza perché si tratterebbe di una relazione sull'intero universo di tutti gli insiemi, la cui esistenza come insieme porta a contraddizioni, come abbiamo visto. Comunque mostriamo le proprietà dell'equipotenza, che in un certo senso giustificano la notazione con l'uguale che abbiamo usato:

Teorema 5.1.1. *Valgono le seguenti tre proprietà:*
(1) A è equipotente ad A;
(2) se A è equipotente a B allora B è equipotente ad A;
(3) se Aé equipotente a B e B è equipotente a C allora A è equipotente a C.

Dimostrazione. (1) Basta prendere $f : A \to A$ tale che $f(a) = a$ per ogni $a \in A$.
(2) Per ipotesi esiste $f : A \to B$ biunivoca. Essendo f iniettiva e surgettiva abbiamo che anche $f^{-1} : B \to A$ è iniettiva e surgettiva.
(3) Per ipotesi esistono $f : A \to B$ e $g : B \to C$ entrambe biunivoche. Allora $g \circ f : A \to C$ è una funzione biunivoca. □

Osservazione 5.1.1. Non abbiamo definito cos'è la cardinalità di A, ma solo cosa vuol dire che due insiemi hanno la stessa cardinalità. Chiaramente si può definire la cardinalità di A, ma lo vedremo più in avanti. La difficoltà sta in questo fatto: vorremo dire che la cardinalità di A è la classe $\{B \mid |A| = |B|\}$ ma vedremo anche che l'assunzione che tale classe sia un insieme porta a contraddizioni.

Analogamente a prima anche la seguente definizione è molto intuitiva:

Definizione 5.1.2. La cardinalità di A è minore o uguale alla cardinalità di B, e si scrive $|A| \leq |B|$, se esiste una funzione iniettiva da A in B.

Osservazione 5.1.2. La definizione precedente equivale a dire che esiste una funzione biunivoca $f : A \to C$ per un opportuno sottoinsieme $C \subseteq B$. Infatti se vale $|A| = |B|$ abbiamo $f : A \to B$ funzione iniettiva ed è sufficiente prendere $C = \operatorname{imm} f$. Viceversa se abbiamo una funzione biunivoca $f : A \to C$ con $C \subseteq B$ questa è anche una funzione iniettiva $f : A \to B$.

Definizione 5.1.3. La cardinalità di A è minore della cardinalità di B, e si scrive $|A| < |B|$ se $|A| \leq |B|$ e $|A| \neq |B|$.

Osservazione 5.1.3. Come prima, questa definizione equivale a dire che esiste una funzione iniettiva da A in un sottoinsieme di B ma non ne esiste una su B.

Il teorema 5.1.1 mostra che l'equipotenza di comporta come una relazione di equivalenza: è riflessiva, simmetrica e transitiva. Adesso mostriamo che la relazione $|A| \leq |B|$ si comporta come una relazione di ordine sulle "classi di equivalenza" secondo l'equipotenza.

Teorema 5.1.2. *Valgono le seguenti proprietà:*
(1) se $|A| \leq |B|$ *e* $|A| = |C|$ *allora* $|C| \leq |B|$*;*
(2) se $|A| \leq |B|$ *e* $|B| = |C|$ *allora* $|A| \leq |C|$
(3) $|A| \leq |A|$*;*
(4) se $|A| \leq |B|$ *e* $|B| \leq |C|$ *allora* $|A| \leq |C|$*.*

Dimostrazione. La dimostrazione è ovvia e quindi la lasciamo per esercizio. □

Abbiamo appena visto che $\leq$ è riflessiva e transitiva. Rimane da stabilirne l'antisimmetria, e questa va enunciata in un teorema in quanto è di importanza miliare nella teoria degli insiemi. Intanto però premettiamo un lemma che riguarda le funzioni:

Lemma 5.1.1. *Se* $f : A \to B$ *è una funzione iniettiva allora valgono i seguenti due fatti:*
(1) $f(U \cap V) = f(U) \cap f(V)$*;*
(2) $f(U - V) = f(U) - f(V)$*.*

Dimostrazione. (1) L'inclusione $\subseteq$ è immediata: infatti se $y \in f(U \cap V)$ allora $y = f(x)$ per qualche $x \in U \cap V$. Ma essendo quindi $x \in U$ e $x \in V$ segue che $y = f(x) \in f(U)$ e $y = f(x) \in f(V)$, ossia $y \in f(U) \cap f(V)$. Per l'altra sia $y \in f(U)$ e $y \in f(V)$, allora esistono $u \in U$ e $v \in V$ tali che $y = f(u)$ e $y = f(v)$. Ma allora $f(u) = f(v)$, e visto che f è iniettiva si ha $u = v \in U \cap V$.
(2) La seconda proprietà a questo punto è semplice. Basta osservare che $U - V = U \cap V^C$ e si utilizza di nuovo la dimostrazione sopra. □

Abbiamo già citato, ma non ancora dimostrato, un teorema che ci servirà ancora una volta, ossia il teorema di ricursione numerabile. Tale teorema sostanzialmente afferma che si possono dare le definizioni per induzione. Abbiamo scelto di non mostrarlo a questo punto e voglimo farlo più avanti non per problemi di difficoltà tecniche nella dimostrazione, ma solo perché lo inseriremo in contesto più ampio, entro il quale capiremo veramente la sua potenza. Infatti daremo una dimostrazione a se stante del teorema come lo abbiamo enunciato, però poi lo generalizzeremo più volte a altri insiemi che non siano $\mathbb{N}$ ma saranno buoni ordini e poi addirittura ordinali. Per adesso però ci basta sapere che si possono definire gli insiemi per ricorsione:

Teorema 5.1.3 (di Cantor–Bernstein)**.** *Se* $|X| \leq |Y|$ *e* $|Y| \leq |X|$ *allora* $|X| = |Y|$*.*

Dimostrazione. Per ipotesi esistono $f : X \to Y$ iniettiva e $g : Y \to X$ iniettiva. Per il teorema di ricorsione numerabile si definisce la seguente successione di insiemi:

$$\begin{cases} X_0 = X, \quad Y_0 = Y \\ X_{n+1} = g(Y_n), \quad Y_{n+1} = f(X_n) \quad n \geq 0 \end{cases}.$$

Più precisamente, volendo usare alla lettera il teorema di ricorsione in questo caso si ha $a = (X_0, Y_0) = (X, Y)$ come punto iniziale e

$$\begin{array}{rccc} r: & \mathcal{P}(X) \times \mathcal{P}(Y) & \longrightarrow & \mathcal{P}(X) \times \mathcal{P}(Y) \\ & (A, B) & \longmapsto & (g(B), f(A)) \end{array}.$$

Data la funzione F dal teorema di ricorsione numerabile poniamo per semplicità $(X_n, Y_n) = F(n)$ per ogni $n \in \mathbb{N}$.
Intanto affermiamo che per ogni $n \in \mathbb{N}$ vale

$$X_n \supseteq X_{n+1} \quad \text{e} \quad Y_n \supseteq Y_{n+1},$$

dimostriamo questo fatto per induzione. Se $n = 0$ vale certamente che $X = X_0 \supseteq X_1 = g(Y)$ perché g è iniettiva, e analogamente vale $Y = Y_0 \supseteq Y_1 = f(X)$ perché f è iniettiva. Supponiamo adesso che la proprietà valga fino al numero naturale n e mostriamo anche che vale per il successore. Per ipotesi induttiva vale $X_n \supseteq X_{n+1}$ e $Y_n \supseteq Y_{n+1}$: dalla prima segue $f(X_n) \supseteq f(X_{n+1})$, ossia $Y_{n+1} \supseteq Y_{n+2}$, e applicando g si ottiene $X_{n+1} \supseteq X_{n+2}$.
Adesso dobbiamo costruire una funzione biunivoca da X a Y. Grazie a quanto visto finora abbiamo che X risulta partizionato dagli insiemi

$$X_n - X_{n+1} \ \text{ con } n \in \mathbb{N} \quad \text{e} \quad \bigcap_{n=0}^{\infty} X_n,$$

e analogo per Y. Essendo f iniettiva, per il lemma 5.1.1 vale che $f(X_0 - X_1) = f(X_0) - f(X_1) = Y_1 - Y_2$ e inoltre la restrizione $f|_{X_0 - X_1}$ è biunivoca perché è iniettiva ed è surgettiva sull'immagine. Ma non possiamo proseguire così su ogni insieme $X_n - X_{n+1}$ perché sennò gli elementi di $Y_0 - Y_1$ non vengono raggiunti. Invece osserviamo che, essendo g iniettiva, vale anche $g(Y_0 - Y_1) = g(Y_0) - g(Y_1) = X_1 - X_2$ e inoltre $g|_{Y_0 - Y_1}$ è biunivoca. Quindi esiste la funzione inversa $g|^{-1}_{Y_0 - Y_1}$. Con questa idea costruiamo l'applicazione seguente:

$$\begin{array}{rccc} h: & X & \longrightarrow & Y \\ & x & \longmapsto & \begin{cases} f(x) & \text{se } x \in X_n - X_{n+1} \text{ e } n \text{ è pari} \\ g^{-1}(x) & \text{se } x \in X_n - X_{n+1} \text{ e } n \text{ è dispari} \\ f(x) = g^{-1}(x) & \text{se } x \in \bigcap_{n=0}^{\infty} X_n \end{cases} \end{array}$$

Dobbiamo mostrare che in effetti h è biunivoca: è un'unione di applicazioni biunivoche con domini e immagini a due a due disgiunti. Questo è ovvio negli insiemi $X_n - X_{n+1}$, ma anche in $\bigcap_{n=0}^{\infty} X_n$ lo è: infatti siccome f è iniettiva si ha che

$$f\left(\bigcap_{n=0}^{\infty} X_n\right) = \bigcap_{n=0}^{\infty} f(X_n) = \bigcap_{n=0}^{\infty} Y_{n+1} = \bigcap_{n=0}^{\infty} Y_n,$$

dove l'ultimo passaggio è giustificato dal fatto che $Y_0 \supseteq Y_n$ per ogni $n \in \mathbb{N}$. $\square$

Abbiamo visto che la relazione $\leq$ gode delle proprietà di una relazione di ordine. Una domanda naturale a questo punto è chiedersi se tale ordine è, come si dice, *totale* ossia se per ogni A e B insiemi vale sempre una delle due relazioni $|A| \leq |B|$ o $|A| \geq |B|$. È noto che la prova di questo fatto richiede l'assioma della scelta.
Per ora abbiamo dunque determinate le proprietà della cardinalità, senza in realtà definire cosa la cardinalità sia. In principio è possibile continuare lo studio delle proprietà $|A| = |B|$ e $|A| \leq |B|$, senza mai definire $|A|$: si può vedere $|A| = |B|$ solo come un'abbreviazione per dire che A è equipotente a B. Tuttavia, è più conveniente sia concettualmente che a livello di notazioni, definire cosa sia $|A|$, "il numero degli elementi dell'insieme A", e di definirlo come un oggetto della nostra teoria, ossia un insieme. Quindi prendiamo la seguente assunzione:

Assunzione. Ci sono insiemi chiamati *numeri cardinali* (o *cardinali*) con la proprietà che per ogni insieme X c'è un unico cardinale $|X|$, detto *cardinalità* di X, tale che gli insiemi X e Y sono equipotenti se e solo se $|X|$ è uguale a $|Y|$.

In effetti, stiamo assumendo l'esistenza di un rappresentante per ogni classe di insiemi reciprocamente equipotenti. L'assunzione è innocua nel senso che la useremo solo per convenienza e potremmo formulare e dimostrare tutti i nostri teoremi senza di essa. In realtà, l'assunzione può essere provata con l'aiuto dell'assioma della scelta, e lo faremo più avanti. Inoltre, per certe classi di insiemi i numeri cardinali possono essere definiti, e l'assunzione provata, senza l'assioma della scelta. Uno di questi casi, e forse il più importante, è il caso degli insiemi finiti.
Prima di proseguire però vogliamo mostrare come una definizione elementare della cardinalità fallisca nella teoria ZF:

Teorema 5.1.4. *Per ogni $A \neq \emptyset$ si ha che*

$$E = \{B \mid |B| = |A|\}$$

non è un insieme.

Dimostrazione. Supponiamo che E sia un insieme, mostriamo che però $\bigcup E = \mathbb{V}$. Sia $a \in A$, che esiste in quanto A è non vuoto. Definiamo i seguenti insiemi, per ogni x sia

$$B_x = \begin{cases} (A - \{a\}) \cup \{x\} & \text{se } x \notin A \\ A & \text{se } x \in A \end{cases}.$$

È immediato mostrare che $|B_x| = |A|$, e dunque che $B_x \in E$. Ma allora per ogni x si ha $x \in B_x \in E$ e dunque $x \in \bigcup E$; ciò mostra che $\bigcup E = \mathbb{V}$, assurdo perché $\mathbb{V}$ non è un insieme. $\square$

5.2 Insiemi finiti

Come detto alla fine dello scorso paragrafo, gli insiemi finiti sono il caso più interessante di insiemi per i quali la definizione dei numeri cardinali non richiede l'assioma della scelta. Intanto iniziamo con la definizione di insieme finito:

Definizione 5.2.1. Un insieme S si dice *finito* quando è equipotente a un certo numero naturale $n \in \mathbb{N}$.[1] Definiamo inoltre $|S| = n$ a diremo che S ha n elementi. Un insieme si dice *infinito* se non è finito.

Secondo la nostra definizione i numeri cardinali degli insiemi finiti sono i numeri naturali. Ovviamente i numeri naturali sono essi stessi insiemi finiti e $|n| = n$ per ogni $n \in \mathbb{N}$. Tuttavia, come detto nell'assunzione, ci resta da verificare che il numero cardinale di un insieme finito è unico. Questo segue dal prossimo lemma:

Lemma 5.2.1. *Se $n \in \mathbb{N}$ allora non esiste alcuna funzione biunivoca da n in un suo sottoinsieme proprio $X \subset n$.*

Dimostrazione. Questo lemma si dimostra per induzione su n. Se $n = 0$ la tesi è banalmente vera. Assumiamo che essa sia vera per n e mostriamola per $n+1$. Se l'affermazione fosse falsa per $n+1$ allora esisterebbe una funzione biunivoca f da $n+1$ in un suo sottoinsieme $X \subset n+1$. Ci sono due casi: o $n \in X$ o $n \notin X$.
Se $n \notin X$ allora $X \subseteq n$, e $f|_n$ mappa biunivocamente n in un suo sottoinsieme proprio, che è $X - \{f(n)\}$, e ciò è assurdo per ipotesi induttiva.
Se $n \in X$ allora $n = f(k)$ per qualche $k \leq n$. Consideriamo la funzione g definita come segue

$$g(i) = \begin{cases} f(i) & \text{per ogni } i \neq k \text{ e } i < n \\ f(n) & \text{se } i = k < n \end{cases} .$$

La funzione g è biunivoca e porta n in $X - \{n\}$, che è un suo sottoinsieme proprio, e questo è assurdo per ipotesi induttiva. □

Corollario 5.2.1. *Valgono i seguenti fatti:*
(1) se $n \neq m$ allora non esiste alcuna funzione biunivoca da n in m;
(2) se $|S| = n$ e $|S| = m$ allora $n = m$;
(3) $\mathbb{N}$ è infinito.

Dimostrazione. (1) Se $n \neq m$ sappiamo che o $n \subset m$ o $m \subset n$, e quindi non può esistere una funzione biunivoca da uno nell'altro per il lemma precedente.
(2) Segue immediatamente dal primo punto.
(3) Questo punto è vero in quanto la funzione successore definita nel precedente capitolo dà una bigezione tra $\mathbb{N}$ e il suo sottoinsieme proprio $\mathbb{N} - \{0\}$. □

[1] ricordiamoci che i numeri naturali sono insiemi, come ha introdotto Von Neumann. Infatti $0 = \emptyset$ e $n = \{0, \ldots, n-1\}$.

Un'altra osservazione degna di nota è che se $n, m \in \mathbb{N}$ e $m < n$ allora $m \subset n$, ed in tale modo $m = |m| < |n| = n$ (dove questo $<$ rappresenta l'ordinaento tra cardinali introdotto in questo capitolo). Questa stessa osservazione però mostra anche che è superfluo fare la distinzione tra il $<$ di ordinamento su $\mathbb{N}$ e il $<$ riferito alle cardinalità. Nel resto del paragrafo ci occuperemo delle proprietà degli insiemi finiti e delle loro cardinalità in dettaglio. Iniziamo con qualche proprietà banale, ma che deve essere dimostrata:

Teorema 5.2.1. *Se X è un insieme finito e $Y \subseteq X$ allora Y è finito. Inoltre $|Y| \leq |X|$.*

Dimostrazione. Essendo X finito sappiamo che esiste $f : X \to n$ per un certo $n \in \mathbb{N}$. Adesso consideriamo $f|_Y : Y \to n$: questa è un'applicazione iniettiva e mostra quindi che $|Y| \leq n = |X|$. Questo mostra che Y è finito e che vale la relazione tra le cardinalità. □

Teorema 5.2.2. *Sia $f : A \to B$ una funzione e $X \subseteq A$ sottoinsieme finito. Allora $f(X) \subseteq B$ è finito.*

Dimostrazione. Si consideri la funzione $f|_X : X \to f(X)$: tale funzione è chiaramente surgettiva e dunque segue che $|f(X)| \leq |X|$. □

Adesso vogliamo vedere modi di ottenere insiemi finiti a partire da insiemi finiti: in effetti tutte le costruzioni possibili ottenibili con gli assiomi di comprensione quando sono applicate a insiemi finiti danno luogo a insiemi finiti. Adesso mostreremo che se X è finito allora $\mathcal{P}(X)$ è finito, e che se X è una collezione finita di insiemi finiti allora $\bigcup X$ è finito. Proprio per questo motivo, come ora possiamo precisare, l'assioma dell'infinito è necessario per ottenere insiemi infiniti.

Lemma 5.2.2. *Siano X e Y due insiemi finiti, allora $X \cup Y$ è finito. Inoltre, $|X \cup Y| \leq |X| + |Y|$ e se X e Y sono disgiunti allora $|X \cup Y| = |X| + |Y|$.*

Dimostrazione. Sia

$$X = \{x_0 \ldots, x_{n-1}\} \quad \text{e} \quad Y = \{y_0 \ldots, y_{m-1}\},$$

dove $\langle x_0, \ldots, x_{n-1}\rangle$ e $\langle y_0, \ldots, y_{m-1}\rangle$ sono sequenze biunivoche. Costruiamo adesso la sequenza finita $z = \langle x_0, \ldots, x_{n-1}, y_0, \ldots, y_{m-1}\rangle$ di lunghezza $n + m$, ossia più precisamente poniamo

$$z_i = x_i \quad \text{per } 0 \leq i < n, \qquad z_i = y_{i-n} \quad \text{per } n \leq i < n + m.$$

Chiaramente z mappa $n + m$ in $X \cup Y$ suriettivamente e quindi $X \cup Y$ è finito e vale $|X \cup Y| \leq |X| + |Y|$ per il teorema 5.2.2. Se X e Y sono disgiunti e allora z risulta iniettiva e quindi vale l'uguaglianza. □

Teorema 5.2.3. *Se S è finito e se ogni $X \in S$ è finito allora $\bigcup S$ è finito.*

Dimostrazione. Procederemo per induzione sul numero degli elementi di S. La tesi è certamente vera se $|S| = 0$. Quindi assumiamo che la tesi sia vera per tutti gli S con $|S| = n$. Sia $S = \{X_0, \ldots, X_{n-1}, X_n\}$ insieme con $n+1$ elementi con $X_i \in S$ per ogni i. Per l'ipotesi induttiva si ha che $\bigcup_{i=1}^{n-1} X_i$ è finita. Quindi abbiamo

$$\bigcup S = \left(\bigcup_{i=0}^{n} X_i \right) \cup X_n,$$

che è finita per il lemma 5.2.2. □

Teorema 5.2.4. *Se X è finito allora $\mathcal{P}(X)$ è finito.*

Dimostrazione. Procediamo per induzione su $|X|$. Se $|X| = 0$ allora $X = \emptyset$ e dunque $\mathcal{P}(X) = \{\emptyset\}$, che è finito. Si supponga che $\mathcal{P}(X)$ sia finito ogni volta che $|X| = n$ e sia Y un insieme con $n+1$ elementi: $Y = \{y_0, \ldots, y_n\}$. Sia $X = \{y_0, \ldots, y_{n-1}\}$. Notiamo che $\mathcal{P}(Y) = \mathcal{P}(X) \cup P$, dove

$$P = \{U \mid U \subseteq Y \wedge y_n \in P\}.$$

Immediatamente osserviamo che $|P| = |\mathcal{P}(X)|$ in quanto possiamo costruire una funzione $f : P \to \mathcal{P}(X)$ biunivoca: basta prendere $f(U) = U - \{y_n\}$ per ogni $U \in P$. Quindi $\mathcal{P}(Y)$ è unione finita di due insieme finiti e quindi è finito. □

Teorema 5.2.5. *Se X è infinito allora $|X| > n$ per ogni $n \in \mathbb{N}$.*

Dimostrazione. Dovendo mostrare la proprietà per ogni $n \in \mathbb{N}$ sarà sufficiente mostrare $|X| \geq n$ per ogni $n \in \mathbb{N}$. Anche questo può essere mostrato per induzione. Certamente $0 < |X|$. Supponiamo che $|X| \geq n$, allora esiste una funzione iniettiva $f : x \to X$. Dal momento che X è infinito esiste $x \in X - \operatorname{imm} f$. Definiamo $g = f \cup \{(n, x)\}$; g è una funzione iniettiva di $n+1$ in X, e questo permette di concludere $|X| \geq n+1$. □

Infine, consideriamo un'altra definizione di insieme finito. Segue dal lemma 5.2.1 che se X è un insieme finito, allora non esiste una funzione biunivoca da X in un suo sottoinsieme proprio. Dall'altro lato, gli insiemi infiniti (come l'insieme dei numeri naturali $\mathbb{N}$) ammettono una mappa biunivoca da loro in un loro sottoinsieme proprio (ad esempio $f(n) = n+1$ per $\mathbb{N}$). Uno sarebbe tentato di definire gli insiemi finiti come quegli insiemi che non sono equipotenti a nessuno sottoinsieme proprio. Tuttavia non è possibile provare l'equivalenza della definizione detta con quella data a inizio pargrafo senza usare l'assioma della scelta.

5.3 Insiemi numerabili

L'assioma dell'infinito ci fornisce un esempio di insieme infinito, l'insieme dei numeri naturali $\mathbb{N}$. In questo paragrafo siamo interessati alla cardinalità di $\mathbb{N}$, ossia a insiemi che a $\mathbb{N}$ sono equipotenti.

Definizione 5.3.1. Un insieme S si dice *numerabile* se $|S| = |\mathbb{N}|$. Un insieme S si dice *al più numerabile* se $|S| \leq |\mathbb{N}|$.

Così un insieme S è numerabile se esiste una mappa biunivoca tra $\mathbb{N}$ e S, ossia se S è l'immagine di una sequenza biunivoca infinita. Adesso vogliamo mostrare che ogni insieme infinito ammette un sottoionsieme numerabile:

Proposizione 5.3.1. *Se A è un insieme infinito allora esiste $\sigma : \mathbb{N} \to A$ iniettiva.*

Dimostrazione. Sia $S = \mathcal{P}(A) - \{\emptyset\}$: questa è una famiglia di insiemi non vuoti. Prendiamo $f : \mathcal{P}(A) - \{\emptyset\} \to A$ funzione di scelta: questo significa che $f(X) \in X$ per ogni $X \in \mathcal{P}(A)$ e $X \neq \emptyset$. Definiamo per ricorsione numerabile

$$\begin{cases} \sigma(0) = f(A) \\ \sigma(n) = f\left(A - \{\sigma(0), \ldots, \sigma(n-1)\}\right) \end{cases}.$$

Osserviamo che questa è una buona definizione in quanto $A - \{\sigma(0), \ldots, \sigma(n-1)\}$ non è mai vuoto perché sennò $A = \{\sigma(0), \ldots, \sigma(n-1)\}$ e quindi sarebbe finito perché in bigezione con n. Adesso affermiamo che in efftti σ è iniettiva: questo fatto è quasi ovvio per costruzione. Sia $n < m$ e mostriamo che $\sigma(n) \neq \sigma(m)$. Infatti

$$\begin{aligned} &\sigma(n) \in A - \{\sigma(0), \ldots, \sigma(n-1)\} = A_{n-1} \\ &\sigma(m) \in A - \{\sigma(0), \ldots, \sigma(m-1)\} = A_{n-1} - \{\sigma(n), \ldots, \sigma(m-1)\} \end{aligned}.$$

Se fosse $\sigma(n) = \sigma(m)$ avremmo $\sigma(n) \in A_{n-1} - \{\sigma(n), \ldots, \sigma(m-1)\}$, assurdo. □

Corollario 5.3.1. *Un sottoinsieme infinito di un insieme numerabile è numerabile.*

Dimostrazione. Sia S un insieme numerabile e $A \subseteq S$ un suo sottoinsieme infinito. Visto che $A \subseteq S$ avremo che $|A| \leq |S|$ (c'è l'applicazione di inclusione) ed inoltre si ha $|S| \leq |A|$ perché A è infinito e quindi esiste un'applicazione iniettiva da $\mathbb{N}$ in A. Ma allora per il teorema di Cantor–Bernstein si ha $|S| = |A|$. □

Vogliamo far notare che le proprietà che usualmente siamo abituati a vedere nel caso degli insiami finiti possono cessare di valere se si passa anche solo agli insiemi numerabili. Per esempio se S è un insieme numerabile, allora può essere decomposta in due sottinsiemi disgiunti A e B anch'essi numerabili, che è inconcepibile

nel caso finito (tranne quando $S = \emptyset$). Basta infatti notare che se S è numerabile allora è in bigezione con $\mathbb{N}$, ma $\mathbb{N}$ contiene i sottoinsiemi dei numeri pari e dispari, che in effetti soddisfano le richieste per A e B. Ma potremmo fare ancora di più trovando un sottoinsieme di $\mathbb{N}$ che si decompone in una quantità numerabile di insiemi numerabili e disgiunti.

Esempio 5.3.1. Come è noto i numeri primi sono infiniti[2], e quindi per il corollario precedente i numeri primi sono una quantità numerabile. Denotiamo con p_n l'n–esimo numero primo per ogni $n \in \mathbb{N}$ e poniamo

$$S_n = \{p_n^k \mid k \in \mathbb{N}\} \quad \text{per ogni } n \in \mathbb{N}.$$

Gli insiemi S_n sono disgiunti a due a due e sono numerabili (perché sottoinsiemi infiniti di un numerabile). Così abbiamo

$$\bigcup_{n=0}^{\infty} S_n \subseteq \mathbb{N},$$

come volevamo.

I prossimi teoremi mostreranno che semplici operazioni su insiemi numerabili conducono ad insiemi numerabili. Vedremo nelle sezioni successive che invece occorreranno altri tipi di operazioni per passare da insiemi numerabili a insiemi più che numerabili.

Teorema 5.3.1. *L'unione di due insiemi numerabili è numerabile.*

Dimostrazione. Questo è un risultato molto semplice. Siano

$$A = \{a_n \mid n \in \mathbb{N}\} \quad \text{e} \quad B = \{b_n \mid n \in \mathbb{N}\}$$

due insiemi numerabili. Costruiamo una sequenza $\langle c_n \mid n \in \mathbb{N}\rangle$ come segue:

$$c_{2k} = a_k \quad \text{e} \quad c_{2k+1} = b_k, \quad \text{per ogni } k \in \mathbb{N}.$$

Adesso basta osservare che $A \cup B = \{c_n \mid n \in \mathbb{N}\}$ e abbiamo così mostrato che $A \cup B$ è numerabile. □

[2] il lettore già dovrebbe conoscere la dimostrazione che dette Euclide di questo fatto. Si suppone che i numeri primi siano finiti e siano $p_1, \ldots, p_k$ e si prende poi il numero

$$N = p_1 p_2 \cdots p_k + 1.$$

Tale N è primo in quanto nessuno dei p_i è suo divisore, altrimenti p_i dividerebbe sia N che $N-1$ e avremmo dunque che $p_i = 1$; ma tale N è anche maggiore strettamente di ciascun p_i per costruzione e dunque avremmo l'assurdo.

Corollario 5.3.2. *L'unione di un numero finito di insiemi numerabili è numerabile.*

Dimostrazione. È una semplice prova per induzione. □

Abbiamo già parlato dell'albergo di Russell nel capitolo precedente: questo è un albergo con un'infinità numerabile di piani e con un'infinita numerabile di stanze per ogni piano. Chiaramente l'albergo di Russell altro non è che $\mathbb{N} \times \mathbb{N}$; ebbene, quello che vogliamo mostrare è che in realtà tutto l'albergo ha ancora un'infinità numerabile di stanze (!).

Teorema 5.3.2. *Se A e B sono insiemi numerabili allora $A \times B$ è numerabile.*

Dimostrazione. Per questo teorema è sufficiente mostrare che $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, e quindi costruiremo una funzione biunivoca da $\mathbb{N} \times \mathbb{N}$ a $\mathbb{N}$. L'idea è quella di procedere per diagonali discendenti. Definiamo $\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tale che

$$\varphi(n, m) = \sum_{i=1}^{m+n} i + n = \frac{(m+n)(m+n+1)}{2} + n.$$

Potremmo subito mostrare che φ definisce una corrispondenza biunivoca, però prima vogliamo spiegare un attimo perché abbiamo scelto proprio quella. La prima somma viene fuori perché si somma il numero di elementi di ogni diagonale fino alla $(m + n - 1)$–esima diagonale: la diagonale numero 0 ha un elemento, la prima due elementi, la seconda tre elementi, fino alla $(m+n-1)$–esima che ne ha $m+n$. Gli n che sono stati aggiunti dopo sono quelli sulla $(m+n)$–esima diagonale e che hanno numero di stanza minore di n, che sono n. Al lettore il compito che si tratta di una corrispondenza biunivoca (o direttamente o, ragionando con l'albergo di Russell, scrivendone un'inversa). □

Dimostrazione. Un altro modo è prendere la funzione

$$\varphi(n, m) = 2^n(2m + 1) - 1.$$

Tralasciando la traslazione per 1 si vede che abbiamo una funzione biunivoca tra $\mathbb{N}\times\mathbb{N}$ e $\mathbb{N}-\{0\}$. Descriviamo la funzione inversa: prendiamo k e scriviamolo come $k = 2^a b$ con $a = \max\{i \mid 2^i \mid k\}$ e quindi con b dispari; basterà porre $\psi(k) = (a, b)$ e abbiamo che $\varphi \circ \psi$ e $\psi \circ \varphi$ sono le due identità. □

Corollario 5.3.3. *Il prodotto cartesiano di un numero finito di insiemi numerabili è un insieme numerabile.*

Dimostrazione. Semplice dimostrazione per induzione sul numero di insiemi. □

Adesso vediamo come questi due risultati si applicano per il calcolo della cardinalità di qualche insieme numerico (nonostante $\mathbb{Z}$ e $\mathbb{Q}$ non li abbiamo ancore definiti formalmente).

Teorema 5.3.3. *L'insieme $\mathbb{Z}$ è numerabile.*

Dimostrazione. $\mathbb{Z}$ è numerabile perché si può scrivere come unione di due insiemi numerabili, che sono

$$\mathbb{Z} = \{0, 1, \ldots\} \cup \{-1, -2, \ldots\},$$

ed abbiamo concluso. □

Teorema 5.3.4. *L'insieme $\mathbb{Q}$ è numerabile (!).*

Dimostrazione. La tesi vale perché esiste una funzione iniettiva $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$: è quella tale che prende una frazione ridotta ai minimi termini $\frac{k}{m}$ con $k \in \mathbb{Z}$ e $m \in \mathbb{N} - \{0\}$ e la manda nella coppia (k, m), ossia

$$\frac{k}{m} \longmapsto (k, m).$$

Quindi $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$. Grazie all'inclusione $i : \mathbb{N} \to \mathbb{Q}$ si ha l'altra disuguaglianza $|\mathbb{N}| \leq |\mathbb{Q}|$; si conclude per il teorema di Cantor–Bernstein. □

Per rimanere nell'ambito degli insiemi numerabili per ora ci limitiamo solo a far presente che invece l'insieme $\mathbb{R}$ dei numeri reali è più che numerabile.

Definizione 5.3.2. Poniamo $Fin(\mathbb{N}) = \{A \subseteq \mathbb{N} \mid A \text{ è finito}\}$ l'insieme dei *sottoinsiemi finiti* di $\mathbb{N}$. Poniamo anche $Seq(\mathbb{N}) = \{\langle \sigma(1), \ldots, \sigma(n) \rangle \mid \sigma : \{1, 2, \ldots, n\} \to \mathbb{N} \text{ e } n \in \mathbb{N}\}$, l'insieme delle *sequenze finite* di $\mathbb{N}$.

Teorema 5.3.5. *Si ha $|Fin(\mathbb{N})| = |Seq(\mathbb{N})| = |\mathbb{N}|$.*

Dimostrazione. Mostreremo che $|\mathbb{N}| \leq |Fin(\mathbb{N})| \leq |Seq(\mathbb{N})| \leq |\mathbb{N}|$ e si conclude grazie al teorema di Cantor–Bernstein.
(1) La prima disuguaglianza è di facile dimostrazione perché basta considerare l'applicazione iniettiva che manda $n \mapsto \{n\}$.
(2) Sia A un sottoinsieme finito di $\mathbb{N}$, allora può essere scritto in modo ordinato[3] come $A = \{a_i \mid 0 \leq i \leq n \text{ e } a_i < a_{i+1}\}$. Allora basta considerare l'applicazione che manda A nella sequenza $(a_0, \ldots, a_n)$.

[3]non abbiamo mai mostrato questo fatto: se $A \subseteq \mathbb{N}$ è finito allora può essere ordinato. Se si procede per induzione il caso base è banale; il passo si mostra osservando che A ammette un massimo (provarlo a sua volta per induzione), e dunque tolto il massimo a avremo che $A - \{a\}$ è ordinabile.

(3) Facciamo la terza disuguaglianza. Sia $\langle a_n \mid n \in \mathbb{N}\rangle$ la sequezna crescente degli infiniti numeri primi. Allora si manda la sequenza $(a_0, \ldots, a_n)$ in $p_0^{a_0+1}p_1^{a_1+1}\cdots$ e otteniamo un'applicazione biunivoca (gli uno all'esponente servono a distinguere distinguere $(0,0)$ da $(0,0,0)$). $\square$

Adesso, come avevamo accennato, occupiamoci dell'unione di una quantità numerabile di insiemi numerabili. Per questo, però, serve l'assioma della scelta.

Teorema 5.3.6. *Unione numerabile di insiemi non vuoti e numerabili è numerabile.*

Dimostrazione. Sia $\langle A_n \mid n \in \mathbb{N}\rangle$ una sequenza di insiemi non vuoti dove $|A_n| = |\mathbb{N}|$. Per ogni $n \in \mathbb{N}$ esiste allora una sequenza la cui immagine è A_n. Per l'assioma di scelta possiamo scegliere una tale sequenza per ogni $n \in \mathbb{N}$. Spieghiamo meglio: per ogni $n \in \mathbb{N}$ sia S_n l'insieme di tutte le sequenza che hanno A_n come immagine. Sia F una funzione di scelta per $\{S_n \mid n \in \mathbb{N}\}$, e si ponga $s_n = F(S_n)$ per ogni $n \in \mathbb{N}$.
Avendo scelto una $s_n = \langle a_n(k) \mid k \in \mathbb{N}\rangle$ per ogni $n \in \mathbb{N}$ otteniamo una mappa f di $\mathbb{N}\times\mathbb{N}$ in $\bigcup_{n=0}^{\infty} A_n$ ponendo

$$f(n,k) = a_n(k).$$

Visto che f è surgettiva si ha che $|\mathbb{N}\times\mathbb{N}| \geq |\bigcup_{n=0}^{\infty} A_n|$; l'altra disuguaglianza è ovvia, quindi si conclude per il teorema di Cantor–Bernstein. $\square$

Come corollario possiamo riottenere il risultato sulle sequenze finite:

Corollario 5.3.4. *L'insieme delle sequenze finite di $\mathbb{N}$ è numerabile.*

Dimostrazione. Posto $\mathbb{N}^0 = \emptyset$ vediamo che esiste una corrispondenza biunivoca tra $Seq(\mathbb{N})$ e $\bigcup_{k=0}^{\infty}\mathbb{N}^k$: basta mandare

$$\langle a_1, a_2, \ldots, a_n\rangle \longmapsto (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n.$$

Visto che $\mathbb{N}^k$ è numerabile per ogni $k \in \mathbb{N}_0$ si ha che l'unione $\bigcup_{k=0}^{\infty}\mathbb{N}^k$ è numerabile, e ciò conclude. $\square$

Concludiamo definendo il numero cardinale degli insiemi numerabili (ricordiamoci l'assunzione fatta qualche paragrafo addietro, secondo la quale ad ogni insieme è possibile associare un numero cardinale, rappresentante della classe di equipotenza dell'insieme):

Definizione 5.3.3. Chiamiamo "aleph–zero" il cardinale di $\mathbb{N}$, ossia $|\mathbb{N}| = \aleph_0$.

Riformulando alcuni risultati dimostrati or ora in termini di $\aleph_0$ abbiamo:
(1) $\aleph_0 > n$ per ogni $n \in \mathbb{N}$ e se $\kappa \leq \aleph_0$ per qualche cardinale κ allora o $\kappa = \aleph_0$ o $\kappa = n$ per qualche $n \in \mathbb{N}$;
(2) $|\mathbb{N} \times \mathbb{N}| = |Fin(\mathbb{N})| = |Seq(\mathbb{N})| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$;
(3) se $0 \neq |A_n| \leq \aleph_0$ per ogni $n \in \mathbb{N}$ allora $|\bigcup_{n=0}^{\infty} A_n| = \aleph_0$.

5.4 Insiemi non numerabili

Tutti gli insiemi infiniti la cui cardinalità è stat determinata sinora sono numerabili. Ovviamente, una lecità domanda è se esistono insiemi più che numerabili: se la risposta fosse no il libro si sarebbe chiuso al precedente paragrafo. Invece la scoperta rivoluzionaria che Georg Cantor fece è che insiemi più che numerabili in effetti esistono. Questa scoperta comportò un notevole sviluppo alla teoria degli insiemi e divenne fonte dei suoi aspetti più profondi e ricchi.
Non abbiamo ancora definito formalmente l'insieme dei numeri reali, cosa che faremo più avanti, però per adesso basterà la nozione che tutti hanno. Vediamo allora la prova che Cantor dette del fatto che $\mathbb{R}$ sia più che numerabile, esempio di un tipico procedimento detto "diagonale", di cui il nome sarà chiaro fra un attimo:

Teorema 5.4.1. *L'insieme dei numeri reali è più che numerabile.*

Dimostrazione. Supponiamo per assurdo che $\mathbb{R}$ sia numerabile: ciò significa che $\mathbb{R}$ dovrebbe essere immagine di una sequenza infinita $\langle r_n \rangle_{n=1}^{\infty}$. Sia

$$r_n = a_0^{(n)}, a_1^{(n)} a_2^{(n)} a_3^{(n)} \cdots$$

l'espansione decimale di r_n per ogni $n \in \mathbb{N}$ [4]. Sia adesso

$$b_n = \begin{cases} 1 & \text{se } a_n^{(n)} = 0 \text{ [5]} \\ 0 & \text{altrimenti} \end{cases} .$$

Sia r il numero reale la cui espansione è $0.b_1 b_2 b_3 \cdots$: ma per costruzione $b_n \neq a_n^{(n)}$ per ogni $n \in \mathbb{N}_0$ e dunque $r \neq r_n$ per ogni $n \in \mathbb{N}_0$. Dunque r è un numero reale che però non appartiene all'immagine della sequenza $\langle r_n \rangle_{n=0}^{\infty}$, assurdo. □

Adesso presentiamo un altro importantissimo teorema della teoria delle cardinalità, che è il teorema di Cantor. In un certo senso tale teorema, che non presenta una dimostrazione difficile, risponde alla delicata questione se, comunque preso un certo insieme, ne esista un altro che abbia cardinalità strettamente superiore. La risposta è affermativa:

[4] assumiamo che nessuna espansione decimale contenga la cifra 9 ripetuta definitivamente, in modo tale che ogni numero reale abbia un'*unica* rappresentazione decimale.

Teorema 5.4.2 (di Cantor)**.** *Sia $X \neq \emptyset$. Allora $|X| < |\mathcal{P}(X)|$.*

Dimostrazione. Per mostrare la disuguaglianza stretta tra le cardinalità mostriamo $|X| \leq |\mathcal{P}(X)|$ e $|X| \neq |\mathcal{P}(X)|$. Per la disuguaglianza larga basta considerare l'applicazione da X in $\mathcal{P}(X)$ tale che $x \longmapsto \{x\}$, e questa è chiaramente iniettiva. Adesso dobbiamo mostrare la diversità; supponiamo per assurdo che esista una funzione $f : X \to \mathcal{P}(X)$ biunivoca (anche se basterebbe supporla surgettiva). Allora potremmo costruire

$$R = \{x \in X \mid x \notin f(x)\}.$$

La proprietà ha senso perché $x \in X$ e $f(x) \subseteq X$. Ora, R è un sottoinsieme di X, dunque $R \in \mathcal{P}(X)$, ed essendo f è surgettiva deve esistere $y \in X$ tale che $f(y) = R$. Ma per definizione di R si ha allora

$$y \in R \iff y \notin f(y) = R,$$

e ciò è un assurdo. □

Osservazione 5.4.1. Dal teorema di Cantor segue un'altra dimostrazuione dell'inesistenza di $\mathbb{V}$: infatti se l'insieme di tutti gli insiemi esistesse, allora dovrebbe avere la cardinalità massima, ma le sue parti hanno cardinalità più alta.

Grazie al teorema di Cantor si ha in particolare che $|\mathcal{P}(\mathbb{N})| > |\mathbb{N}|$: le parti di $\mathbb{N}$, dunque, hanno cardinalità strettamente maggiore di $\aleph_0$ e, così come fatto per $\aleph_0$, diamo un nome anche a questa cardinalità:

Definizione 5.4.1. Si denota con $\mathbf{c}$ la cardinalità di $\mathcal{P}(\mathbb{N})$. Talvolta quando un insieme ha cardinalità $\mathbf{c}$ viene detto avere la *cardinalità del continuo.*

Uno studio più dettagliato sugli insiemi non numerabili sarà fatto nel prossimo capitolo, dove definiremo formalmente le operazioni tra cardinali. Qui ci limitiamo a provare che l'insieme $2^{\mathbb{N}} = \{0,1\}^{\mathbb{N}}$ di tutte le sequenze binarie ha cardinalità $\mathbf{c}$, e che tale cardinalità è anche quella di $\mathbb{R}$. Procediamo per gradi:

Teorema 5.4.3. *Si ha $|\mathcal{P}(\mathbb{N})| = |2^{\mathbb{N}}|$.*

Dimostrazione. Ricordiamo che

$$2^{\mathbb{N}} = \{f \text{ funzione} \mid f : \mathbb{N} \to \{0,1\}\}.$$

Adesso costruiamo la corrispondenza con $\mathcal{P}(\mathbb{N})$: vista la presenza dei soli numeri 0 o 1 utilizzeremo le funzioni caratteristiche. Per ogni $S \subseteq \mathbb{N}$ sia $\chi_S : \mathbb{N} \to \{0,1\}$ la funzione caratteristica

$$\chi_S(n) = \begin{cases} 0 & \text{se } n \in S \\ 1 & \text{se } n \notin S \end{cases}.$$

È ora facile mostrare che la corrispondenza $S \mapsto \chi_S$ è una mappa biunivoca. □

Talvolta, proprio in virtù del precedente teorema, la cardinalità delle parti di $\mathbb{N}$ viene denotata con $2^{\aleph_0}$: per ora si prenda questa solo come una notazione, poi vedremo nel prossimo capitolo che l'esponenziazione fra numeri cardinali è un'operazione ben definibile e corrisponde proprio a prendere la cardinalità dell'insieme delle funzioni da un insieme in un altro.
Adesso verifichiamo che $\mathbb{R}$ ha proprio la cardinalità del continuo, da cui peraltro $\mathbf{c}$ prende il nome. Diamo soltanto per buono che $\mathbb{R}$ è un campo ordinato completo e che $\mathbb{Q}$ è un sottoinsieme denso di $\mathbb{R}$.

Teorema 5.4.4. *Si ha* $|\mathbb{R}| = \mathbf{c} = |\mathcal{P}(\mathbb{N})|$.

Dimostrazione. Mostreremo che $|\mathbb{R}| \leq \mathbf{c}$ e che $|\mathbb{R}| \geq \mathbf{c}$, dopodiché la tesi seguirà dal teorema di Cantor–Bernstein.
(1) Per la prima disuguaglianza costruiremo un'applicazione $f : \mathbb{R} \to \mathcal{P}(\mathbb{Q})$, tanto $|\mathcal{P}(\mathbb{Q})| = |\mathcal{P}(\mathbb{N})|$, essendo $|\mathbb{N}| = |\mathbb{Q}|$ (il lettore lo mostri ora o attenda più avanti). Basta definire

$$r \longmapsto f(r) = \{q \in \mathbb{Q} \mid q < r\}.$$

Mostriamo che l'applicazione f è iniettiva: se $r \neq r'$, diciamo $r < r'$ possiamo considerare un razionale q compreso tra questi due (ad esempio la loro media); vale che $q \in f(r')$ ma $q \notin f(r)$.
(2) Adesso costruiamo un'applicazione $g : 2^{\mathbb{N}} \to \mathbb{R}$ che prende una sequenza binaria e gli associa un unico numero reale e che sia iniettiva. Basta infatti definire

$$s = \langle a_k \rangle_{k=0}^{\infty} \longmapsto g(s) = \sum_{k=0}^{\infty} a_k \cdot 10^{-k},$$

e questa g è in effetti iniettiva. Abbiamo così provato che $|2^{\mathbb{N}}| \leq |\mathbb{R}|$. □

Adesso mostriamo dei fatti che possono apparire sorprendenti, ma che saranno solo i primi di una serie di risultati che appaiono quasi paradossali.

Proposizione 5.4.1. *Il segmento chiuso* $[0, 1]$ *ha la stessa cardinalità di* $\mathbb{R}$.

Dimostrazione. Questo fatto è quasi una conseguenza del precedente, in quanto parte della dimostrazione è analoga. Sia $I = [0, 1]$: intanto vale ovviamente, grazie all'inclusione, che $|I| \leq |\mathbb{R}|$. Per mostrare che $|\mathbb{R}| \leq |I|$ faremo vedere che $|2^{\mathbb{N}}| \leq |I|$. Basterà prendere infatti l'applicazione

$$s = \langle a_k \rangle_{k=0}^{\infty} \longmapsto g(s) = \sum_{k=0}^{\infty} a_k \cdot 10^{-k-1},$$

che è chiaramente iniettiva. □

Proposizione 5.4.2. *Il segmento unitario chiuso* $[0,1]$ *e il segmento unitario aperto* $(0,1)$ *hanno la stessa cardinalità.*

Dimostrazione. La prima dimostrazione che vogliamo dare di questo fatto consiste nell'osservare che $(0,1)$ ha la stessa cardinalità di $\mathbb{R}$ e che dunque ha la stessa cardinalità di $[0,1]$ per la proposizione precedente. Adesso dobbiamo mostrare che $|(0,1)| = |\mathbb{R}|$, intuitivamente si procede così: si identifica il segmento aperto con una semicirconferenza e la si proietta su $\mathbb{R}$ mediante proiezione stereografica.
I dettagli sono i seguenti: identifichiamo $\mathbb{R}$ con

$$A = \{(x,y) \mid y = 0\} \subseteq \mathbb{R}^2$$

in modo naturale, in modo che $|A| = |\mathbb{R}|$. Identifichiamo $(0,1)$ con

$$B = \{(x,y) \mid y = -\sqrt{1-x^2} + 1 \text{ e } x \in (-1,1)\},$$

in modo che $|B| = |(0,1)|$. Adesso consideriamo la proiezione su A di centro $(0,1)$: questa è un'applicazione iniettiva da B ad A (come si vede facilmente esplicitandone l'equazione). □

Dimostrazione. La seconda prova consta di due passi: prima mostriamo che $|[0,1]| = |[0,1)|$ e poi per simmetria del ragionamento avremo che $|[0,1)| = |(0,1)|$.
Si consideri

$$\left\{ a_n = \frac{1}{n} \mid n \in \mathbb{N}^+ \right\} \subseteq [0,1].$$

Consideriamo poi l'applicazione $f : [0,1] \to [0,1)$ tale che

$$x \longmapsto f(x) = \begin{cases} a_{n+1} & \text{se } x = a_n \text{ per qualche } n \in \mathbb{N}+ \\ x & \text{altrimenti} \end{cases} .$$

Questa è una mappa biunivoca e quindi si ha la tesi. □

Capitolo 6

Numeri cardinali

6.1 Aritmetica dei cardinali

I numeri cardinali sono stati introdotti nel capitolo precedente. Questo capitolo è dedicato allo studio delle loro proprietà generali, con particolare enfasi sulla cardinalità del continuo $2^{\aleph_0}$. In questa sezione definiremo le operazioni aritmetiche (addizione, moltiplicazione e esponenziazione) sui numeri cardinali e ne vedremo le principali proprietà.
Per definire la somma di due numeri cardinali usiamo un'analogia con gli insiemi finiti. Se l'insieme A ha a elementi B ne ha b e $A \cap B = \emptyset$ allora $A \cup B$ avrà $a + b$ elementi. Dunque possiamo dare la seguente:

Definizione 6.1.1. Sia $|A| = \kappa$ e $|B| = \lambda$. Se $A \cap B = \emptyset$ allora poniamo $\kappa + \lambda = |A \cup B|$.

Osservazione 6.1.1. La definizione precedente può essere anche data nel caso di insiemi non disgiunti. In tal caso si pone infatti $\kappa + \lambda = |(A \times \{0\}) \cup (B \times \{1\})|$.

In realtà per rendere la definizione precedente ben definita dobbiamo mostrare che $\kappa + \lambda$ non dipende dalla scelta degli insiemi A e B. Questo è il contenuto del prossimo:

Lemma 6.1.1. *Se A, B, A', B' sono insiemi tali che $|A| = |A'|$, $|B| = |B'|$ e $A \cap B = A' \cap B' = \emptyset$, allora $|A \cup B| = |A' \cup B'|$.*

Dimostrazione. Siano f e g due funzioni biunivoche rispettivamente da A in A' e B in B'. La funzione $f \cup g$ è una funzione biunivoca da $A \cup B$ in $A' \cup B'$. □

Non solo l'addizione tra cardinali coincide con l'ordinaria addizione dei numeri naturali nei casi dei cardinali finiti, ma molte delle usuali leggi della somma rimangono valide. Per esempio, la somma di cardinali è commutativa e associativa

Teorema 6.1.1. *Siano κ, λ e μ numeri cardinali. Valgono le seguenti proprietà:*
(1) $\kappa + \lambda = \lambda + \kappa$*;*
(2) $\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$*;*
(3) $\kappa + 0 = \kappa$*, dove* $0 = |\emptyset|$.

Dimostrazione. Le proprietà sulla somma sono molto semplici e seguono subito dalla definizione. □

Tuttavia non tutte le proprietà dell'addizione tra numeri valgono anche per l'addizione di cardinali. In particolare, le disuguaglianze strette nelle formule sono rare nel caso di cardinali infiniti e, come vedremo più avanti (col teorema di König), quelle che valgono sono molto difficili da stabilire. Come esempio si prenda il semplice fatto che se $n \neq 0$ allora $n+n > n$. Se κ è infinito, questo non è sempre vero: abbiamo visto che $\aleph_0 + \aleph_0 = \aleph_0$, e l'assioma della scelta implica che $\kappa + \kappa = \kappa$ per ogni cardinale infinito.
La moltiplicazione di cardinali è ancora motivata dalle proprietà della moltiplicazione tra numeri. Se A e B sono insiemi con a e b elementi allora il prodotto $A \times B$ ha ab elementi.

Definizione 6.1.2. Sia $|A| = \kappa$ e $|B| = \lambda$. Allora poniamo $\kappa \cdot \lambda = |A \times B|$.

Anche in questo caso dobbiamo vedere se la moltiplicazione di cardinali è ben definita. In effetti è così, come mostra il lemma seguente:

Lemma 6.1.2. *Se A, B, A', B' sono insiemi tali che $|A| = |A'|$, $|B| = |B'|$ allora $|A \times B| = |A' \times B'|$.*

Dimostrazione. Siano $f : A \to A'$ e $g : B \to B'$ le due funzioni biunivoche che danno l'equipotenza. Dobbiamo definire una funzione $h : A \times B \to A' \times B'$, e abbiamo un modo privilegiato per farlo, avendo a disposizione f e g. Definiamo

$$h(a, b) = (f(a), g(b)),$$

e la biunivocità di h segue direttamente da quella di f e g. □

Ancora, la moltiplicazione ha alcune proprietà che ci aspettiamo: in particolare è commutativa e associativa e valgono anche le leggi distributive con la somma.

Teorema 6.1.2. *Siano κ, λ e μ cardinali. Allora valgono:*
(1) $\kappa \cdot \lambda = \lambda \cdot \kappa$*;*
(2) $\kappa \cdot (\lambda \cdot \mu) = (\kappa \cdot \lambda) \cdot \mu$*;*
(3) $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$.

Dimostrazione. Anche in questo caso la dimostrazione è elementare conseguenza delle definzioni. Ci limitiamo solo ad osservare che la (3) discende dall'uguaglianza $A \times (B \cup C) = (A \times B) \cup (A \times C)$ e abbiamo concluso. □

Per completare l'analogia tra moltiplicazioni di cardinali e moltiplicazioni tra numeri dimostriamo il seguente semplice fatto:

Lemma 6.1.3. *Sia κ un cardinale. Allora $\kappa + \kappa = 2 \cdot \kappa$.*

Dimostrazione. Supponiamo $|A| = \kappa$, allora $2 \cdot \kappa$ è la cardinalità di $\{0,1\} \times A$. Osserviamo che

$$\{0,1\} \times A = (\{0\} \times A) \cup (\{1\} \times A),$$

e che $|\{0\} \times A| = |\{1\} \times A| = \kappa$. Essendo l'unione disgiunta si ha la tesi. □

A questo punto non ci resta altro che definire l'esponenziazione tra numeri cardinali, e nuovamente partiamo dall'osservare il caso finito. Se abbiamo due insiemi A e B finiti con cardinalità rispettivamente a e b, allora l'insieme delle funzioni da B ad A in effetti consta di a^b elementi. Prenderemo proprio questa come definizione:

Definizione 6.1.3. Sia $|A| = \kappa$ e $|B| = \lambda$. Definiamo $\kappa^\lambda = |A^B|$.

Al solito, prima di proseguire studiando le proprietà dell'esponenziazione, dobbimo verificare che quella appena data è una buona definizione.

Lemma 6.1.4. *Siano A, B, A', B' insiemi tali che $|A| = |A'|$ e $|B| = |B'|$. Allora si ha che $|A^B| = |A'^{B'}|$.*

Dimostrazione. Siano $f : A \to A'$ e $g : B \to B'$ le due funzioni biunivoche che danno l'equipotenza. Dobbiamo definire una funzione $F : A^B \to A'^{B'}$. Sia $k : B \to A$, dobbiamo associargli una funzione $h = F(k)$: osserviamo il diagramma sottostante

$$\begin{array}{ccc} B & \xrightarrow{\ g\ } & B' \\ {\scriptstyle k}\downarrow & & \downarrow{\scriptstyle F(k)} \\ A & \xrightarrow[\ f\ ]{} & A' \end{array}.$$

L'unico modo sensato di costruire $F(k)$ è quello di porre $F(k) = f \circ k \circ g^{-1}$. Verificare che F è biunivoca è, a questo punto, un semplice esercizio. □

Teorema 6.1.3. *Siano κ, λ e μ cardinali. Allora valgono:*
(1) $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$;
(2) $(\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}$;
(3) $(\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu$.

Dimostrazione. Assumiamo che $|A| = \kappa$, $|B| = \lambda$ e $|C| = \mu$. (1) Intanto supponiamo B e C disgiunti, allora vale per definizione che

$$\kappa^{\lambda+\mu} = |\{f : B \cup C \to A\}| \quad \text{e} \quad \kappa^\lambda \cdot \kappa^\mu = |\{g : B \to A\} \times \{h : C \to A\}|.$$

Adesso dobbiamo costruire una corrispondenza biunivoca $F : A^{B\cup C} \to A^B \times A^C$. Definiamo

$$F(f) = (f|_Y, f|_Z) \quad \forall\, f \in A^{B\cup C}.$$

La biunivocità di F si dimostra più facilmente se costruiamo l'applicazione inversa. È data una coppia di applicazioni $(g, h) \in A^B \times A^C$ e vogliamo associargli una funzione di $A^{B\cup C}$. Costruiamo $G : A^B \times A^C \to A^{B\cup C}$ tale che

$$G(g,h) = g \cup h = \begin{cases} g(u) & \text{se } u \in B \\ h(u) & \text{se } u \in C \end{cases},$$

e in effetti vale che le composizioni di F e G danno le rispettiva identità.
(2) Come prima iniziamo a scrivere che

$$(\kappa^\lambda)^\mu = |\{g : C \to A^B\}| \quad \text{e} \quad \kappa^{\lambda\cdot\mu} = |\{f : B \times C \to A\}|.$$

Adesso dobbiamo trovare una corrispondenza biunivoca $F : A^{B\times C} \to (A^B)^C$ e allora si pone $F(f) = g$ per ogni $f \in A^{B\times C}$, dove $g \in (A^B)^C$ è la funzione seguente:

$$g(c) = h_c \in A^B \ \forall c \in C, \quad \text{e} \quad h_c(b) = f(b,c) \ \forall b \in B.$$

Anche in questo caso si vede facilmente che F è una corrispondenza biunivoca. A questo punto anche la (3) risulta semplice. □

6.2 La cardinalità del continuo

Nello scorso capitolo ci siamo soffermati sulla cardinalità $\aleph_0$ dei numeri naturali e abbiamo mostrato alcune proprietà di tale cardinale. Adesso che abbiamo dato le definizioni delle operazioni tra cardinali possiamo esprimere i risultati del precedente capitolo in formula:
(1) $\kappa < \aleph_0$ se e solo se $\kappa \in \mathbb{N}$;
(2) $n + \aleph_0 = \aleph_0 + \aleph_0 = \aleph_0$ per $n \in \mathbb{N}$ (questo esprime che l'unione di due insiemi numerabili è numerabile);
(3) $n \cdot \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0$ per $n \in \mathbb{N}$ (questo invece è il fatto che il prodotto cartesiano di insiemi numerbaili è numerabile).
Nell'ultimo paragrafo dello scorso capitolo abbiamo poi mostrato che l'insieme $\mathbb{R}$ è equipotente a $\mathcal{P}(\mathbb{N})$, e che entrambi hanno cardinalità strettamente superiore ad $\aleph_0$. Abbiamo mostrato che

$$|\mathcal{P}(\mathbb{N})| = |2^{\mathbb{N}}|,$$

e adesso con la definizione di esponenziazione possiamo scrivere $|\mathcal{P}(\mathbb{N})| = 2^{|\mathbb{N}|} = 2^{\aleph_0}$. Quindi possiamo scriovere adesso

$$\mathbf{c} = 2^{\aleph_0}.$$

Ripetendo la stessa dimostrazione del teorema 5.4.3 con X al posto di $\mathbb{N}$ possiamo formulare il seguente teorema:

Teorema 6.2.1. *Per ogni X insieme vale $|\mathcal{P}(X)| = 2^{|X|}$.*

Il teorema di Cantor può essere dunque ora espresso in termine di cardinali come segue: per ogni κ cardinale

$$\kappa < 2^\kappa.$$

Adesso invece vogliamo concentrarci sulla cardinalità del continuo $\mathbf{c} = 2^{\aleph_0}$, la cardinalità dell'insieme dei numeri reali.

Teorema 6.2.2. *Valgono le seguenti uguaglianze:*
(1) $n + 2^{\aleph_0} = \aleph_0 + 2^{\aleph_0} = 2^{\aleph_0} + 2^{\aleph_0} = 2^{\aleph_0}$ *per* $n \in \mathbb{N}$*;*
(2) $n \cdot 2^{\aleph_0} = \aleph_0 \cdot 2^{\aleph_0} = 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0}$ *per* $n > 1$*;*
(3) $(2^{\aleph_0})^n = (2^{\aleph_0})^{\aleph_0} = n^{\aleph_0} = \aleph_0^{\aleph_0} = 2^{\aleph_0}$ *per* $n > 1$.

Dimostrazione. Per (1) e (2) si conclude per il teorema di Cantor–Bernstein da

$$2^{\aleph_0} \leq n + 2^{\aleph_0} \leq \aleph_0 + 2^{\aleph_0} \leq 2^{\aleph_0} + 2^{\aleph_0} = 2 \cdot 2^{\aleph_0} = 2^{1+\aleph_0} = 2^{\aleph_0}.$$

La seconda parte è del tutto analoga.
(3) Per questa basta notare che valgono sia

$$2^{\aleph_0} \leq (2^{\aleph_0})^n \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$$

e anche

$$2^{\aleph_0} \leq n^{\aleph_0} \leq \aleph_0^{\aleph_0} \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0}.$$

Il teorema è così provato. □

Osserviamo che il teorema appena provato, benché sia un'immediata conseguenza del teorema di Cantor–Bernstein, porta a delle conseguenze inaspettate. Per esempio $2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0}$ significa che $\mathbb{R} \times \mathbb{R}$ è equipotente ad $\mathbb{R}$. Cioè, esiste una mappa biunivoca dalla retta nel piano (!); ma di più anche lo spazio $\mathbb{R}^n$, spazio n–dimensionale, è equipotente ad $\mathbb{R}$. Questo risultato (dovuto a Cantor) stupì i contemporanei di Cantor tanto era controintuitivo: questo era quello che però la teoria, a partire da assiomi intuitivi, dimostrava.

Corollario 6.2.1. *L'insieme dei numeri complessi, delle sequenze infinite di numeri naturali e delle sequenze infinite di numeri reali hanno cardinalità $2^{\aleph_0}$.*

Dimostrazione. Per i numeri complessi basta osservare che $\mathbb{C}$ è isomorfo a $\mathbb{R}^2$, quindi ha cardinalità del continuo. Poi, l'insieme delle sequenze infinite di numeri naturali altri non è che $\mathbb{N}^{\mathbb{N}}$, quindi $|\mathbb{N}^{\mathbb{N}}| = \aleph_0^{\aleph_0} = 2^{\aleph_0}$. L'insieme delle sequenze infinite di numeri reali è $\mathbb{R}^{\mathbb{N}}$, e vale $|\mathbb{R}^{\mathbb{N}}| = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0}$. □

Adesso mostriamo un risultato che a prima vista sembra intuitivo, ma che necessita di una rigorosa dimostrazione:

Teorema 6.2.3. *Sia A un insieme numerabile e B un insieme di cardinalità $2^{\aleph_0}$. Allora $B - A$ ha sempre cardialità $2^{\aleph_0}$.*

Dimostrazione. Assumiamo senza perdere di generalità che $B = \mathbb{R} \times \mathbb{R}$ e $A \subseteq B$. Sia ora

$$P = \{x \in \mathbb{R} \mid \exists y \text{ tale che } (x, y) \in A\};$$

visto che $|A| = \aleph_0$ allora $|P| \leq \aleph_0$. Così esiste $x_0 \in \mathbb{R}$ tale che $x_0 \notin P$ e dunque l'insieme $X = \{x_0\} \times \mathbb{R}$ è disgiunto da A, ossia $X \subseteq (\mathbb{R} \times \mathbb{R}) - A$. Ovviamente X ha cardinalità $2^{\aleph_0}$. e allora $|(\mathbb{R} \times \mathbb{R}) - A| \geq 2^{\aleph_0}$. □

Corollario 6.2.2. *L'insieme dei numeri irrazionali ha cardinalità $2^{\aleph_0}$.*

Dimostrazione. Segue dal teorema precedente essendo i numeri irrazionali l'insieme $\mathbb{R} - \mathbb{Q}$ e $\mathbb{Q}$ è numerabile. □

Adesso occupiamoci dei numeri algebrici e dei numeri trascendenti: essendo abituati a lavorare più con numeri algebrici che con numeri trascendenti saremmo portati a dire che i primi sono di più dei secondi: in realtà è esattamente il contrario. Intanto ricordiamo le loro definizioni:

Definizione 6.2.1. Un numero reale si dice *algebrico* se è radice di un polinomio non nullo a coefficienti interi. Un nero numero reale si dice *trascendente* se non è algebrico.

Teorema 6.2.4. *I numeri algebrici sono una quantità numerabile, mentre i trascendenti hanno cardinalità $2^{\aleph_0}$.*

Dimostrazione. Mostrato che gli algebrici sono numerabili seguirà immediatamente che i trascendenti sono $2^{\aleph_0}$ per il teorema precedente. Dapprima mostriamo che l'anello $\mathbb{Z}[x]$ ha una quantità numerabile di elementi. Possiamo identificare ogni polinomio di $\mathbb{Z}[x]$ con il vettore dei suoi coefficienti, di modo che

$$\mathbb{Z}[x] \text{ è isomorfo a } \bigcup_{k=1}^{\infty} \mathbb{Z}^k.$$

Adesso l'unione a destra è l'unione numerabile di insiemi numerabili e dunque ha cardinalità $\aleph_0$. Adesso mostrare che gli algebrici sono numerabili è molto semplice: infatti ogni polinomio, per il teorema fondamentale dell'algebra, ha un numero finito di radici basterà unire tutte le radici reali di tutti tali polinomi. Queste saranno numerabili perché unione numerabile di insiemi finiti. □

Infine vogliamo calcolare la cardinalità di alcuni insiemi significativi, come quello delle funzioni continue, delle funzioni in generale e degli aperti di $\mathbb{R}$.

Teorema 6.2.5. *L'insieme $C^0(\mathbb{R})$ delle funzioni continue su $\mathbb{R}$ e l'insieme degli aperti di $\mathbb{R}$ ha cardinalità $2^{\aleph_0}$.*

Dimostrazione. Dal corso di analisi è noto che ogni funzione continua è univocamente determinata dalle immagini di ogni punto di un insieme denso in $\mathbb{R}$, per esempio sull'insieme $\mathbb{Q}$ dei razionali. Consideriamo allora la mappa da $C^0(\mathbb{R})$ in $\mathbb{R}^{\mathbb{Q}}$ che manda f in $f|_{\mathbb{Q}}$. Per quanto appena detto tale corrispondenza deve essere iniettiva e dunque

$$|C^0(\mathbb{R})| \leq |\mathbb{R}^{\mathbb{Q}}| = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0}.$$

Dall'altro lato è ovvio che $|C^0(\mathbb{R})| \geq 2^{\aleph_0}$, basta considerare le funzioni costanti.
Per la seconda parte invece usiamo un fatto noto dal corso di topologia: ogni aperto di $\mathbb{R}$ può essere scritto come unione di un sistema intervalli aperti con estremi razionali. Ci sono dunque $\aleph_0$ intervalli siffatti e pertanto $2^{\aleph_0}$ sistemi di intervalli. Questo mostra che ci sono al massimo $2^{\aleph_0}$ aperti. Dall'altro lato però, per ogni $a, b \in \mathbb{R}$ distinti $(a, \infty) \neq (b, \infty)$, e quindi ci sono almento $2^{\aleph_0}$ aperti. □

In effetti se adesso consideriamo le funzioni da $\mathbb{R}$ in sé, queste superano la cardinalità del continuo. Infatti vale il seguente:

Lemma 6.2.1. *L'insieme di tutte le funzioni da $\mathbb{R}$ in sé ha cardinalità strettamente superiore a $2^{\aleph_0}$.*

Dimostrazione. Si ha semplicemente

$$|\mathbb{R}^{\mathbb{R}}| = (2^{\aleph_0})^{2^{\aleph_0}} = 2^{\aleph_0 \cdot 2^{\aleph_0}} = 2^{2^{\aleph_0}},$$

che supera certamente $2^{\aleph_0}$ per il teorema sull'insieme delle parti. □

Capitolo 7

Numeri ordinali

Quando abbiamo introdotto i numeri naturali, eravamo motivati dall'esigenza di formalizzare il processo di "contare": i numeri naturali iniziano con 0 e sono generati mediante successivi incrementi di una unità: 0, 1, 2, ..., e così via. Abbiamo definito l'operatore di *successore* mediante $S(x) = x \cup \{x\}$, e introdotto i numeri naturali come il più piccolo degli insiemi contenenti 0 e chiusi per successore.
Quello che vogliamo fare in questo capitolo è di continuare il processo di enumerazione altre oltre i numeri naturali. L'idea è che possiamo immaginare di definire un numero infinito ω che viene "dopo" tutti i numeri naturali e quindi continuare il processo di conta nel transfinito: ω, $\omega + 1$, $(\omega + 1) + 1$, e così via. In questo capitolo formalizzeremo questi concetti e introdurremo i *numeri ordinali* come una generalizzazione dei numeri naturali. Molto importante sarà che generalizzeremo i teoremi di induzione e di ricorsione numerabile che abbiamo enunciato (in questo capitolo dovremo anche dimostrare la ricorsione numerabile) ai teoremi di induzione e ricursione transfinita.

7.1 Richiami sui buoni ordini e induzione transfinita

Adesso riprendiamo in maniera più sistematica lo studio dei buoni ordini e ci svincoliamo da un'impostazione più concreta e rivolta verso il primo esempio di insieme ben ordinato che abbimo visto, ossia i numeri naturali. La teoria che svilupperemo qui in generale porterà poi verso la definizione dei numeri ordinali, così come dicevamo qui sopra. Ricordiamo i seguenti fatti:

(1) un insieme totalmente ordinato $(A, \leq)$ si dice un insieme bene ordinato se ogni sottoinsieme non vuoto di A ammette un minimo;

(2) dire $(A, \leq)$ è un insieme ben ordinato equivale a dire che non esistono successioni strettamente descrescenti in A;

(3) la somma (unione) e il prodotto di buoni ordini è ancora un buon ordine.

Dopo questi richiami anticipiamo che generalizzeremo la proprietà (3) al caso di unioni di una famiglia qualsiasi di buoni ordini con certe proprietà in più, ma lo vedremo più avanti. Adesso il nostro obiettivo sarà quello di dimostrare l'induzione transfinita. Per fare ciò occorre però ancora qualche nozione e qualche risultato sui buoni ordini, vediamo di cosa si tratta:

Definizione 7.1.1. Sia $(A, <)$ un insieme ben ordinato e $a, b \in A$. Diciamo che b è il *successore immediato* di a se vale $a < b$ e non esiste alcun $c \in A$ tale che $a < c$ e $c < b$: quando ciò accade si scriverà $b = S(a)$. In tal caso si dice anche che a è il *predecessore immediato* di b.

Definizione 7.1.2. Sia $(A, <)$ un insieme ben ordinato. Diremo che $a \in A$ è un *successore* quando esiste $b \in A$ tale che $S(b) = a$.

Lemma 7.1.1. *Sia $(A, <)$ un insieme bene ordinato. Ogni elemento di A tranne l'eventuale massimo ammette un successore immediato.*

Dimostrazione. Sia $a \in A$ un elemento: se A ha massimo allora supponiamo anche che a non sia il massimo. Si considera l'insieme $M = \{x \in A \mid a < x\}$ dei *maggioranti* di a: visto che a non è l'eventuale massimo segue che M non è vuoto. Di conseguenza possiamo prendere $b = \min M$: ebbene, tale b si verifica facilmente essere il successore immediato di a. □

Osservazione 7.1.1. Si osservi che il viceversa del lemma è falso. Basta pensare a $\mathbb{Z}$ con l'usuale ordinamento: ogni elemento (tranne lo 0) ammette un successore immediato, ma $\mathbb{Z}$ stesso non ha minimo per esempio.

Definizione 7.1.3. Sia $(A, <)$ un insieme bene ordinato. Un elemento $a \in A$ diverso dal minimo di A si dice un *limite* se non esiste alcun $b \in A$ tale che a sia il suo successore immediato, ossia tale che $S(b) = a$.

Osservazione 7.1.2. Si può vedere facilmente che se $(A, <)$ è un insieme ben ordinato allora gli elementi di A sono ripartiti tra il minimo, i successori e i limiti. Infatti se un elemento non è un successore significa che non ha predecessore immediato, ma allora o è il minimo oppure è un limite (per definizione).

Quelli dati sinora sono gli ingredienti fondamentali per poter mostrare il teorema di induzione transfinita, che è dato di seguito:

Teorema 7.1.1 (di induzione transfinita)**.** *Sia $(A, <)$ un insieme ben ordinato e sia $P \subseteq A$ una proprietà identificata con un sottoinsieme di A. Supponiamo che:*
(1) $\min A \in P$*;*
(2) per ogni $a \in A$, se $a \in P$ allora $S(a) \in P$;
(3) per ogni $a \in A$ elemento limite, se per ogni $x < a$ vale $x \in P$ allora $a \in P$.
Allora $P = A$.

Dimostrazione. Supponiamo per assurdo che $P \neq A$, ossia $A - P \neq \emptyset$. Essendo A un buon ordine esisterà $a = \min(A - P) \in A - P$. Valendo le proprietà (1) e (2) tale a non può essere né il minimo di A, nè il successore di un certo elemento: se infatti fosse $a = S(b)$ tale $b \in P$ per minimalità di a, ma allora anche $a \in P$ per la (2). Inoltre valendo la (3) a non può essere neanche un elemento limite. Ma ciò è assurdo perché $a \in A$ e dunque deve essere di uno dei tipi detti per l'osservazione 7.1.2. □

7.2 Segmenti iniziali e isomorfismi

Per rendere più chiaro il percorso annunciamo già qual è il nostro obiettivo. Ogni coppia di insiemi ben ordinati può essere confrontata, cioè esiste sempre una ben precisa correlazione tra uno e l'altro; per il momento di più non possiamo dire, nel senso che ci mancano ancora le nozioni fondamentali per poter andare avanti. Intanto apprestiamoci a definire questi concetti:

Definizione 7.2.1. Siano $(A, <)$ e $(B, \prec)$ due insiemi ben ordinati. Un *isomorfismo* di buoni ordini è un'applicazione biunivoca $\varphi : A \to B$ tale che per ogni $a_1, a_2 \in A$

$$a_1 < a_2 \iff \varphi(a_1) \prec \varphi(a_2). \tag{7.1}$$

In tal caso $(A, <)$ e $(B, \prec)$ si dicono *isomorfi*.

Quando l'applicazione φ rispetta la proprietà (7.1) diremo che preserva l'ordine. Adesso mostreremo un semplice risultato che è molto utile: del "se e solo se" della proprietà (7.1) quando si ha a che fare con insiemi totalmente ordinati è sufficiente mostrare una sola implicazione.

Lemma 7.2.1. *Siano $(A, <)$ e $(B, \prec)$ due insiemi totalmente ordinati. Sia φ un'applicazione biunivoca $\varphi : A \to B$ tale che $\varphi(a_1) \prec \varphi(a_2)$ se $a_1 < a_2$. Allora φ è un isomorfismo di ordini.*

Dimostrazione. Dobbiamo mostrare che se $a_1, a_2 \in A$ e $\varphi(a_1) \prec \varphi(a_2)$ allora $a_1 < a_2$. Supponiamo per assurdo che a_1 non sia minore di a_2: essendo l'ordine totale dovrà essere o $a_1 = a_2$ o $a_2 < a_1$. In entrambi i casi però si ha l'assurdo perché seguirebbe $\varphi(a_1) = \varphi(a_2)$ o $\varphi(a_2) < \varphi(a_1)$, contro l'ipotesi. □

Visto che un buon ordine in particolare è un ordine totale, il lemma precedente varrà anche nel caso di insiemi ben ordinati. L'altra nozione di cui abbiamo bisogno è quella di segmento iniziale, che ci apprestiamo a dare:

Definizione 7.2.2. Sia $(A, <)$ un insieme ben ordinato. Diciamo che $S \subseteq X$ è un *segmento iniziale* di A se e solo se per ogni $s \in S$ si ha $s' \in S$ per ogni $s' < s$. Un segmento iniziale si dice *proprio* se non coincide con tutto A.

Osservazione 7.2.1. La notazione usata per i segementi iniziali può essere (e in effetti a volte ne faremo uso) $S \subseteq_i A$, ma parlando di buoni ordini è inutile, visto che adesso mostreremo che ogni segmento iniziale proprio è determinato univocamente da un $a \in A$: in questo modo potremo denotare S con A_a.

Osservazione 7.2.2. Dalla definizione segue subito che se $x \notin S$ allora $x > s$ per ogni $s \in S$.

Proposizione 7.2.1. *Sia $(A, <)$ un insieme ben ordinato. Ogni segmento iniziale proprio $S \subset_i A$ è generato da un elemento $a \in A$, cioè $S = \{x \in A \mid x < a\}$.*

Dimostrazione. Ricordando che $A - S$ è non vuoto visto che S è proprio basta prendere

$$a = \min(A - S) = \min\{a \in A \mid a \notin S\} = \min\{a \mid a > s \text{ per ogni } s \in S\}$$

e verificare che in effetti è ciò che ci serve affinché $S = \{x \in A \mid x < a\}$. Se $x < a$ allora $x \in S$ per la definizione di a come minimo di $A - S$; se $x \geq a$ si ha che $x \notin S$ perché se $x \in S$ allora anche $a \in S$ perché S è segmento iniziale. □

Come già detto nell'enunciato del teorema e nell'osservazione precedente, ogni segemento iniziale proprio S di A diremo che è *generato* da un certo $a \in A$ quando $S = \{x \in A \mid x < a\}$, e denoteremo $S = A_a$.

Osservazione 7.2.3. L'ipotesi che $(A, <)$ sia ben ordinato e non che semplicemente sia un ordine totale è necessaria. Consideriamo l'insieme totalmente ordinato $(\mathbb{Q}, \leq)$: ebbene questo insieme – che con l'ordinamento usuale non è ben ordinato – ha dei segementi iniziali propri che non sono della forma $\mathbb{Q}_q$ per nessun $q \in \mathbb{Q}$. Ad esempio sia

$$S = \{q \in \mathbb{Q} \mid q^2 < 2\};$$

S è chiaramente un segmento iniziale proprio, ma non può essere espresso come $\mathbb{Q}_q$ perché tale q dovrebbe essere $\sqrt{2}$, che non è razionale. Già che abbiamo in mano questo esempio possiamo osservare che $\mathbb{Q}$, nonostante sia numerabile, ammette una quantità più che numerabile di segmenti iniziali propri: basta prendere infatti l'insieme

$$\{q \in \mathbb{Q} \mid q < r\}$$

per ogni $r \in \mathbb{R}$ (dove $<$ è l'ordine in $\mathbb{R}$).

Adesso quelli che seguono sono tutti risultati intorno a segmenti iniziali e isomorfismi d'ordine, che serviranno poi per il teorema di confrontabilità. Nei prossimi risultati $(A, <)$ sarà sempre un insieme ben ordinato e $\varphi : A \to A$ un isomorfismo di ordine.

Proposizione 7.2.2. *Per ogni $a \in A$ vale $\varphi(a) \geq a$.*

Dimostrazione. Se per assurdo fosse $X = \{a \mid \varphi(a) < a\} \neq \emptyset$, prendiamo $\tilde{a} = \min X$; anche per $\tilde{a}$ varrà la proprietà $\varphi(\tilde{a}) < \tilde{a}$. Ma allora visto che φ preserva l'ordine si avrebbe $\varphi(\varphi(\tilde{a})) < \varphi(\tilde{a})$ e allora $\varphi(\tilde{a}) \in X$ e questo è assurdo, contro il fatto che $\tilde{a}$ è il minimo. □

Corollario 7.2.1. *Se $\varphi : A \to A$ è un isomorfismo allora $\varphi = id_A$.*

Dimostrazione. Vale $\varphi(a) \geq a$. Ma $\varphi^{-1}(b) \geq b$ per ogni $b \in A$: preso $b = \varphi(a)$ si ottiene l'altra disuguaglianza.[1] □

Corollario 7.2.2. *Sia $\varphi : A \to B$ un isomorfismo di buoni ordini. Allora questo è unico.*

Dimostrazione. Sia $\psi : A \to B$ un altro isomorfismo di buoni ordini, allora $\varphi \circ \psi^{-1}$ è un isomorfismo tra B e B. Ma allora, per quandto appena dimostrato si ha che $\varphi \circ \psi^{-1} = id_B$, ossia φ e ψ coincidono. □

Corollario 7.2.3. *Ogni segmento iniziale proprio non può essere isomorfo a tutto l'insieme A.*

Dimostrazione. Per la proposizione 7.2.1 si ha che $X = A_a$ per un certo $a \in A$. Supponiamo per assurdo che esista $\psi : A \to A_a$ isomorfismo di ordini. Allora $\psi(a) \geq a$ per la proposizione 7.2.2 precedente. Ma si ha l'assurdo osservando che se $\psi(a) \geq a$ allora $\psi(a) \notin A_a$. □

Osservazione 7.2.4. Detto ancora a livello intuitivo, il corollario precedente ci dice il seguente fatto: se abbiamo un insieme ben ordinato $(A, <)$ e consideriamo l'insieme ben ordinato $(A', <)$ ottenuto dal precedente aggiungendo un elemento (quindi $A' = A \cup \{b\}$) e estendendo l'ordine all'unione, i due insiemi ottenuti non possono essere isomorfi.

Osservazione 7.2.5. Se $(A, <)$ è un insieme ben ordinato si può sempre ordinare ogni suo sottoinsieme. Ogni segmento iniziale proprio non è isomorfo a tutto A, ma è vero che neanche un sottoinsieme proprio può esserlo? In effetti la risposta è no: basta prendere i numeri pari dentro $\mathbb{N}$, questi hanno lo stesso tipo d'ordine di $\mathbb{N}$ (l'isomorfismo è $n \mapsto 2n$).

[1] si poteva anche dimostrare per assurdo. Se $\varphi \neq id_A$ prendiamo $\tilde{a} = \min\{a \in A \mid \varphi(a) \neq a\}$. Per la proposizione 7.2.2 avremmo $\varphi(\tilde{a}) > \tilde{a}$, ma allora $\tilde{a} \notin \operatorname{imm} \varphi$. Infatti

Corollario 7.2.4. *Siano $(A, <_A)$ e $(B, <_B)$ due insiemi ben ordinati. Se φ è un isomorfismo da A a un segmento iniziale di B e ψ è un isomorfismo tra A e un segmento iniziale di B (possibilmente diverso) allora $\varphi = \psi$.*

Dimostrazione. Innanzitutto $\operatorname{imm}\varphi$ e $\operatorname{imm}\psi$ sono due segmenti iniziali di B tra loro isomorfi, perché entrambi isomorfi ad A. Quindi per il corollario 7.2.3 si ha $\operatorname{imm}\varphi = \operatorname{imm}\psi$, perché sennò uno sarebbe segmento iniziale dell'altro e sarebbero isomorfi. Quindi φ e ψ sono isomorfismi con lo stesso dominio e la stessa immagine, e quindi per il corollario 7.2.2 si ha la tesi. □

Corollario 7.2.5. *Sia $\varphi : A \to B$ un isomorfismo di buoni ordini e sia A_a un segmento iniziale di A. Allora $\varphi|_{A_a}$ è un isomorfismo da A_a a $B_{\varphi(a)}$.*

Dimostrazione. La semplice dimostrazione è lasciata come esercizio al lettore. □

Adesso possiamo finalmente enunciare la proprietà più importante dei buoni ordini: due qualsiasi buoni ordini possono sempre essere confrontati, nel senso che o sono isomorfi oppure potremmo dire che "uno va più avanti dell'altro". Il teorema è il seguente:

Teorema 7.2.1 (di confrontabilità)**.** *Dati due insiemi ben ordinati $(A, <_A)$ e $(B, <_B)$, uno dei due è isomorfo ad un segmento iniziale dell'altro, non necessariamente proprio. Più precisamente accade una e una sola delle seguenti condizioni: o A è isomorfo a B, o A è isomorfo ad un segmento iniziale di B, o B è isomorfo ad un segmento iniziale di A.*

Dimostrazione. Sia P l'insieme seguente:

$$P = \{g : A' \to B' \mid g' \text{ isomorfismo e } A' \subseteq A \text{ e } B' \subseteq B \text{ segmenti iniziali}\}.$$

Intanto osserviamo che P è non vuoto: infatti c'è la mappa che manda $\min A$ in $\min B$, che esistono in quanto siamo in insiemi ben ordinati. Dobbiamo mostrare che in P c'è una funzione f il cui dominio è tutto A, nel qual caso A è isomorfo mediante f ad un segmento iniziale di B, oppure la cui immagine sia tutto B, nel qual caso invece è B ad essere isomorfo mediante f^{-1} ad un segemento iniziale di A. Definiamo allora

$$f = \bigcup_{g \in P} g,$$

dobbiamo verificare che in effetti tale f ha le proprietà richieste, ossia è una funzione, è un elemento di P e il suo dominio è A o la sua immagine è B.
Per mostrare che f è una funzione mostreremo che per ogni $g, h \in P$ esse coincidono sull'intersezione dei loro domini. Visto che $\operatorname{dom} g$ e $\operatorname{dom} h$ sono entrambi segmenti iniziali di A abbiamo che uno deve essere incluso nell'altro, supponiamo

ad esempio $\operatorname{dom} g \subseteq \operatorname{dom} h$. Ma in tal caso, grazie al corollario 7.2.4 applicato a g e a $h|_{\operatorname{dom} g}$, segue che $g = h|_{\operatorname{dom} g}$. Questo dimostra che f è una funzione, ed inoltre abbiamo anche mostrato che P è totalmente ordinato per inclusione.
Adesso mostriamo che $f \in P$, ossia che è un isomorfismo tra un segmento iniziale di A e uno di B. Intanto osserviamo che

$$\operatorname{dom} f = \bigcup_{g \in P} \operatorname{dom} g \quad \text{e} \quad \operatorname{imm} f = \bigcup_{g \in P} \operatorname{imm} g$$

sono segmenti iniziali rispettivamente di A e di B. Verifichiamo che effettivamente f è un isomorfismo tra questi due segmenti. Essendo P totalmente ordinato per inclusione esisterà $g \in P$ tale che $x, y \in \operatorname{dom} g$ e per tale g abbiamo

$$x < y \iff g(x) < g(y) \iff f(x) < f(y);$$

la prima equivalenza è dovuta al fatto che g è un isomorfismo, mentre la seconda dipende dal fatto che f estende g.
Infine dobbiamo mostrare che $\operatorname{dom} f = A$ o $\operatorname{imm} f = B$. Se per assurdo $\operatorname{dom} f \neq A$ e $\operatorname{imm} f \neq B$, allora questi sono due segmenti iniziali propri il primo di A e il secondo di B. Per raggiungere una contraddizione costruiremo un elemento $h \in P$ che estende propriamente f: la contraddizione nasce dal fatto che invece f è il massimo elemento di P rispetto all'inclusione, perché appartiene a P e è l'unione di tutti gli elementi di P. Detti $x = \min(A - \operatorname{dom} f)$ e $y = \min(B - \operatorname{imm} f)$ basta porre $h = f \cup \{(x, y)\}$ ed abbiamo concluso. □

7.3 Limiti di buoni ordini

Adesso occupiamoci dei limiti di buoni ordini, il problema è il seguente. Sia F una famiglia di buoni ordini, ovvero un insieme i cui elementi sono insiemi ben ordinati, ossia coppie $(A, <_A)$. Ci chiediamo in quali casi esista un buon ordine $(X, <)$ tale che tutti i buoni ordini di F siano segmenti iniziali di $(X, <)$. Chiaramente una condizione necessaria affinché ciò avvenga è la seguente:

$(*)$ dati due insiemi ben ordinati $(A, <_A)$ e $(B, <_B)$ nella famiglia F, uno dei due è un segmento iniziale dell'altro.

Con ciò intendiamo dire che o A è un segmento iniziale di $(B, <_B)$ e $<_A$ è la restrizione di $<_B$ ad A, ossia

$$<_A = <_B \cap (A \times A),$$

oppure il viceversa. Questa è anche una condizione sufficiente a garantire l'esistenza del buon ordine detto, come mostreremo tra poco; tuttavia per avere la sola totalità dell'ordine si può anche usare una condizione più debole di quella espressa. La proposizione che intanto enunciamo è dunque la seguente:

Proposizione 7.3.1. *Sia F una famiglia di insiemi totalmente ordinati tale che per ogni $(A, \leq_A)$ e $(B, \leq_B)$ in F si ha o $A \subseteq B$ o $B \subseteq A$ (dove i rispettivi ordini sono le rispettive restrizioni). Allora esiste un insieme totalmente ordinato $(X, \leq)$ tale che ogni elemento $(A, \leq_A)$ della famiglia F è un suo sottoinsieme e $\leq_A$ è la restrizione di $\leq$ ad A.*

Dimostrazione. Definiamo

$$X = \bigcup_{(A, \leq_A) \in F} A,$$

ossia $x \in X$ se e solo se esiste un $(A, <_A) \in F$ tale che $x \in A$. Ora definiamo la relazione $\leq$ su X ponendo

$$\leq = \bigcup_{(A, \leq_A) \in F} \leq_A,$$

ossia $x \leq y$ se e solo se esiste un $(A, \leq_A) \in F$ tale che $x, y \in A$ e $x \leq_A y$. Intanto compiamo un'osservazione: siano $(A, \leq_A)$ e $(B, \leq_B)$ due insiemi ben ordinati in F tali che $x, y \in A$ e $x, y \in B$, allora in base alla $(*)$ si ha

$$x \leq_A y \iff x \leq_B y.$$

Questo ci dice che nella definizione dell'ordine $\leq$ su X non importa quale insieme $(A, \leq_A) \in F$ si sceglie per confrontare x e y; la precedente definizione equivale alla seguente: $x \leq y$ se e solo se per ogni A tale che $x, y \in A$ si ha $x \leq_A y$. Quindi $x \leq_A y$ se e solo se $x \leq y$, ossia $\leq_A$ coincide con la restrizione di $\leq$ ad A.
Dobbiamo mostrare la proprietà riflessiva. Sia $x \in X$, allora $x \in A$ per un certo A tale che $(A, \leq_A) \in F$. Essendo $\leq_A$ un ordine totale si ha $x \leq_A x$, e questo se e solo se $x \leq x$.
Siano $x, y \in X$ tali che $x \leq y$ e $y \leq x$, vogliamo mostrare che $x = y$. Avremo che $x \in A$ e $y \in B$ per certi A e B tali che $(A, \leq_A)$ e $(B, \leq_B)$ sono in F; per ipotesi varrà $A \subseteq B$ o $B \subseteq A$. Per fissare le idee supponiamo ad esempio $A \subseteq B$, allora $x, y \in B$. Per ipotesi $x \leq_B y$ e $y \leq_B x$ e dunque, visto che $\leq_B$ è un ordine totale, si ha $x = y$.
In modo analogo si dimostra la proprietà transitiva: ciò che ci consente di dimostrare ogni proprietà è che, presi un certo numero di elementi, allora questi staranno tutti in un certo A comune tale che $(A, \leq_A) \in F$. □

Come dicevamo, se tutti gli elementi della famiglia sono insiemi ben ordinati la sola condizione espressa nelle ipotesi del precedente teorema non è sufficiente a garantire che X sia un insieme ben ordinato. Vediamo un controesempio: si prenda la famiglia

$$F = \{(\{-n, \ldots, 0\}, <) \mid n \in \mathbb{N}\};$$

F è formata da insiemi bene ordinati perché sono ordini totali finiti. Ma l'unione degli insiemi di F è

$$\bigcup F = \bigcup_{n\in\mathbb{N}} \{-n, \ldots, 0\} = \mathbb{Z}^-,$$

l'insieme dei numeri interi non positivi, che in effetti non è ben ordinato, in quanto neanche l'insieme tutto non ammette minimo.
Quella che serve per garantire che X sia un insieme ben ordinato è proprio la condizione $(*)$ che abbiamo espresso:

Teorema 7.3.1. *Sia F una famiglia di insiemi ben ordinati che soddisfano la condizione $(*)$. Allora esiste un insieme ben ordinato $(X, <)$ tale che ogni insieme ben ordinato di F è segmento iniziale di X.*

Dimostrazione. Definito X e $\leq$ come nella proposizione precedente abbiamo che $(X, \leq)$ è un insieme totalmente ordinato. Quello che dobbiamo mostrare è che $\leq$ è un buon ordine e che ogni segmento iniziale di X è uno degli A tali che $(A, \leq_A) \in F$.
Sia $(A, \leq_A) \in F$, mostriamo che allora $A \subseteq X$ è un segmento iniziale di X. Siano dunque $a \in A$ e $b \in X$ con $b < a$, dobbiamo mostrare che $b \in A$. Ciò che sappiamo è che $b \in B$ per un certo $(B, \leq_B) \in F$. Se $B \subseteq A$ abbiamo finito; sennò per la condizione $(*)$ si ha che A è un segmento iniziale di B e quindi essendo $b \in B$ e minore di $a \in A$ ne concludiamo che $b \in A$.
Adesso possiamo mostrare che $\leq$ è un buon ordine su X. Sia $Y \subseteq X$ sottoinsieme non vuoto, dobbiamo mostrare che Y ha un minimo in $(X, \leq)$. Sicuramente esiste $(A, \leq_A) \in F$ tale che $A \cap Y \neq \emptyset$ (basta prendere $y \in Y$, che in particolare starà in un certo A). Essendo non vuoto, avremo che $A \cap Y$ ammette un minimo nell'ordine di $(A, \leq_A)$ (che è buono); sia a tale minimo. Affermiamo che

$$a = \min_A(A \cap Y) = \min_X Y.$$

Supponiamo per assurdo esista $b \in Y$ con $b < a$: essendo $A \subset_i X$ avremo che gli elementi di X minori di a stanno in A, quindi $b \in A$. Ma allora $b \in A \cap Y$, e ciò è assurdo perché $b < a$ ma a è anche il minimo di $A \cap Y$. □

Il teorema precedente giustifica la seguente:

Definizione 7.3.1. Il buon ordine $(X, <)$ costruito nella dimostrazione precedente viene detto il *limite*, o l'unione, della famiglia di buoni ordini di F.

Esempio 7.3.1. L'insieme $\mathbb{N}$, con l'usuale ordinamento, può essere visto come limite della famiglia F dei suoi segmenti iniziali finiti.

7.4 Il teorema di ricursione

L'induzione non è solo uno strumento per dimostrare, ma anche per definire. Presentiamo un esempio semplice: la funzione fattoriale è definita induttivamente ponendo $0! = 1$ e $(n+1)! = (n+1) \cdot n!$. L'idea è che per definire il valore della funzione in un certo n si può supporre di averlo già definito per i valori minori di n. Le definizioni per induzione vengono anche dette ricorsive. Un analogo principio vale per definire funzioni f che hanno come dominio un qualunque insieme bene ordinato $(A, <_A)$ (nel caso del fattoriale $A = \mathbb{N}$).
Esistono varie versioni sempre più generali del teorema di ricursione. Visto che in un capitolo precedente già avevamo citato il teorema di ricorsione numerabile (ossia con $A = \mathbb{N}$) intanto mostreremo quello, per poi vedere altre versioni più generali. Il teorema di ricursione è una pietra miliare della teoria degli insiemi elementare, e quindi vederne più versioni e diverse dimostrazioni ci sembra istruttivo.

Teorema 7.4.1 (di ricorsione numerabile)**.** *Siano A un insieme, $a \in A$ e $H : A \to A$ una funzione. Allora esiste un'unica funzione $f : \mathbb{N} \to A$ tale che $f(0) = a$ e $f(n+1) = H(f(n))$.*

Dimostrazione. Diciamo che B è *buono* se B è un segemento iniziale di $\mathbb{N}$ ed esiste $g : B \to A$ tale che $g(0) = a$ e $g(n+1) = H(g(n))$ per ogni n tale che $n+1 \in B$; inoltre chiameremo g una funzione buona per B.
Intanto affermiamo che, fissato B buono, la funzione g è unica. Supponiamo che ci sia un'altra funzione buona per B, diciamo $g' : B \to A$ e consideriamo

$$n_0 = \min\{n \in B \mid g(n) \neq g'(n)\},$$

che esiste perché stiamo lavorando in un buon ordine. Per definizione vale che $g(n_0) \neq g'(n_0)$, ma $g(n_0) = H(g(n_0 - 1)) = H(g'(n_0 - 1)) = g'(n_0)$ e ciò è assurdo. Quindi se B è buono allora è unica la g che esiste per definizione, che pertanto verrà denotata con g_B. Definiamo quindi

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

La definizione è ben posta, in quanto f è un insieme: la classe $\{g_B \mid B \text{ è buono}\}$ è un insieme per rimpiazzamento. Inoltre f è una funzione e vogliamo mostrare che $\operatorname{dom} f = \mathbb{N}$. Supponiamo per assurdo che ciò non sia vero, visto che siamo in un buon ordine esisterà $\bar{n} = \min(\mathbb{N} - \operatorname{dom} f)$. Vogliamo adesso far vedere che ciò permette di costruire una funzione buona che però estende propriamente f, il che è assurdo in quanto f è l'unione di tutte. Detto $\overline{B} = \operatorname{dom} f \cup \{\bar{n}\}$ possiamo definire una funzione $\bar{f} : \overline{B} \to A$ come $\bar{f} = f \cup \{(\bar{n}, H(f(\bar{n}-1)))\}$. Ora, $\bar{B}$ è buono e $\bar{f}$ è buona per B, ma questo è assurdo perché $\bar{B} \supset \operatorname{dom} f$ che però era l'unione di tutti i domini $\operatorname{dom} g_B$. □

Osservazione 7.4.1. L'analogo del teorema precedente vale anche se $f(n+1)$, oltre a dipendere da $f(n)$, dipende anche dal numero n. Un esempio di questo tipo di funzione è proprio il fattoriale che abbiamo definito prima del teorema: la definizione di $(n+1)!$ dipende da $n!$ ma anche da n. Dunque H viene definita su n e su $f(n)$, e così $f(n+1) = H(n, f(n))$.

Vediamo adesso il teorema di ricursione in generale.

Teorema 7.4.2 (di ricursione su buoni ordini)**.** *Sia $(A, <)$ un insieme ben ordinato e H una funzione. Allora esiste ed è unica una funzione con dominio A e tale che per ogni $a \in A$ vale $f(a) = H\left(a, f|_{A_a}\right)$.*

Dimostrazione. Sia B il codominio di H e chiamiamo *a–approssimazione* una

$$\varphi : A_a \cup \{a\} \to B$$

tale che $\varphi(x) = H(x, \varphi|_{A_x})$ per ogni $x \leq a$. Detto $0 = \min A$, osserviamo che la 0–approssimazione esiste sempre ed è determinata da $\varphi(0) = H(0, \emptyset)$. Per rendere più chiara l'esposizione mostriamo tre fatti importanti ai fini della dimostrazione separatamente in un lemma:

Lemma 7.4.1. *Valgono i seguenti fatti:*
(1) se φ e ψ sono due a–approssimazioni allora $\varphi = \psi$;
(2) se $a < b$ e φ è una b–approssimazione allora $\varphi|_{A_a \cup \{a\}}$ è una a–approssimazione;
(3) per ogni $a \in A$ esiste una a–approssimazione.

Dimostrazione. (1) Se fosse $\varphi \neq \psi$ allora sia $x = \min\{y \geq a \mid \varphi(y) \neq \psi(y)\}$, che esiste per ipotesi di assurdo. Allora $\varphi|_{A_x} = \psi|_{A_x}$ e quindi

$$\varphi(x) = H(x, \varphi|_{A_x}) = H(x, \psi|_{A_x}) = \psi(x).$$

(2) È ovvia per definizione.
(3) Dimostriamo tale punto per induzione sui buoni ordini. Chiaramente $0 = \min A$ ha una approssimazione, come detto prima. Supponiamo adesso che a sia un successore, ossia che $a = S(a')$, dove a' ammette una a'–approssimazione φ'. Posto

$$\varphi = \varphi' \cup \left\{(a, H(a, \varphi'))\right\}$$

otteniamo una a–approssimazione (il lettore verifichi i dettagli). Supponiamo infine che a sia un limite, allora A_a non ha massimo: per ogni $x < a$ sia ψ_x una x–approssimazione, allora definiamo

$$\varphi' = \{(x, \psi_x(x)) \mid x < a\} \quad \text{e} \quad \varphi = \varphi' \cup \left\{(a, H(a, \varphi'))\right\}.$$

Affinché la definizione precedente abbia senso dobbiamo assicurarci che φ' sia un insieme: in effetti basta osservare che $\varphi' \subseteq A \times B$ e usare l'assioma di separazione. A questo punto anche φ è un insieme ed è una a–approssimazione. □

A questo punto basta definire $f(a) = \varphi_a(a)$ per ogni $a \in A$, dove φ_a è una a–approssimazione. La buona definizione come funzione segue dal lemma, in quanto due a–approssimazioni coincidono ed ogni elemento ne ammette una. □

Teorema 7.4.3 (di ricursione transfinita)**.** *Sia $(A, \leq_A)$ un insieme ben ordinato e H una "funzione classe" definita da una formula $\varphi(x, y)$. Allora esiste ed è unica una funzione f con dominio A tale che $f(a) = H(a, f|_{A_a})$ per ogni $a \in A$.*

Osservazione 7.4.2. Prima di iniziare la dimostrazione vogliamo fare un osservazione sulle "funzioni classe". Dire intanto che H come funzione classe è determinata da una formula $\varphi(x, y)$ significa dire che

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

Intanto si ha $\operatorname{dom} H = \{x \mid (\exists y)(\varphi(x, y))\}$, che in generale è una classe. Quello che vogliamo notare è che si può sempre estendere $\varphi(x, y)$ in modo che $\operatorname{dom} H = \mathbb{V}$, cioè in modo che $\operatorname{dom} H$ sia la classe che contiene tutti gli insiemi. Basta infatti prendere la formula

$$\varphi'(x, y) : \varphi(x, y) \vee ((\forall z)(\neg\varphi(x, z)) \wedge y = \emptyset).$$

Dimostrazione. La dimostrazione consiste esattamente degli stessi passi della precedente tranne che nell'esistenza delle a–approssimazioni. Dimostravamo questa parte per induzione e quando arrivavamo al caso in cui a è un limite dicevamo di prendere una x–approssimazione ψ_x e si formava l'insieme

$$\{(x, \psi_x(x)) \mid x < a\},$$

che era un insieme perché contenuto in $A \times B$, dominio e immagine di H. Il problema è che H in questo caso non è una vera e propria funzione e quindi B può non essere un insieme, dunque dobbiamo cambiare strategia. Consideriamo per ogni $x < a$ una x–approssimazione ψ_x. Visto che $x \mapsto \psi_x$ è una corrispondenza funzionale (in quanto la x–approssimazione è unica) la classe

$$\{\psi_x \mid x < a\}$$

diventa un insieme grazie all'assioma di rimpiazzamento. Allora possiamo considerare l'unione di questa famiglia di funzioni, che è

$$\varphi' = \bigcup_{x<a} \psi_x,$$

ed è un insieme. A questo si può procedere come prima definendo $\varphi = \varphi' \cup \{(a, \varphi')\}$, che è una a–approssimazione. □

7.5 Numeri ordinali

Nei capitoli precedenti abbiamo introdotto i numeri naturali per rappresentare sia la cardinalità che il tipo di ordine degli insiemi finiti, e li abbiamo usati per provare i teoremi sull'induzione e sulla ricursione. Adesso generalizzeremo questa definizione introducendo i numeri ordinali.
I numeri ordinali altro non fanno che continuare il processo di generazione di numeri sempre più grandi entro il transfinito. Come nel caso dei numeri naturali, vorremmo che gli ordinali siano ben ordinati dalla relazione $\in$ di appartenenza. Di più, la collezione di tutti i numeri ordinali (che infatti mostreremo non essere un insieme) è essa stessa ben ordinata da $\in$, e contiene i numeri naturali come segmento iniziale. Ma la proprietà più importante dei numeri ordinali è che sono rappresentanti canonici per ogni insieme ben ordinato: ogni insieme ben ordinato è isomorfo ad un unico ordinale. In questo modo possono essere visti come i *tipi d'ordine* degli insiemi ben ordinati.

Definizione 7.5.1. Un insieme T si dice *transitivo* se ogni elemento di T è un sottoinsieme di T. Ossia, per ogni u e v, $u \in v \in T$ implica $u \in T$.

Osservazione 7.5.1. Si osservi che la transitività di T può essere anche riformulata in un modo equivsalente come segue: per ogni $u \in T$ si ha che $T_u = u$ (il lettore provi a mostrare l'equivalenza).

Definizione 7.5.2. Un insieme α si dice *numero ordinale* se è transitivo e $(\alpha, \in)$ è un insieme ben ordinato.

È ormai pratica comune denotare gli ordinali con le lettere greche minuscole, e inoltre il termine *ordinale* è utilizzato al posto di numero ordinale per semplicità. Per quanto detto all'inizio del paragrafo vorremmo che tutti i numeri naturali siano ordinali, e in effetti è così:

Teorema 7.5.1. *Ogni numero naturale è un ordinale.*

Dimostrazione. Sia m un numero naturale e sia $k \in l \in m$, ossia $k < l < m$: allora sappiamo che $k < m$, ossia $k \in m$. Questo significa che m è un insieme transitivo. Inoltre ogni numero m è anche ben ordinato da $\in$ in quanto ogni $n \in \mathbb{N}$ è anche un sottoinsieme di $\mathbb{N}$, ed $\mathbb{N}$ è ben ordinato da $\in$. $\square$

Inoltre è facile vedere che $\mathbb{N}$ è transitivo, e abbiamo appena detto che è ben ordinato da $\in$. Dunque anche $\mathbb{N}$ è un ordinale:

Definizione 7.5.3. Poniamo $\omega = \mathbb{N}$.

Non abbiamo fatto altro che dare un nuovo nome all'insieme $\mathbb{N}$, che come ordinale si chiama ω. Adesso mostriamo che la proprietà di essere ordinale passa al successore di un insieme:

Lemma 7.5.1. *Sia α un ordinale. Allora $S(\alpha) = \alpha \cup \{\alpha\}$ è un ordinale.*

Dimostrazione. È ovvio che $S(\alpha)$ sia transitivo (basta distinguere nella dimostrazione se gli elementi che si prendono sono in $\alpha \subseteq S(\alpha)$ o in $S(\alpha)$). Inoltre $S(\alpha)$ è ben ordinato da $\in$, essendo α il massimo elemento e $\alpha \subseteq \alpha \cup \{\alpha\}$ il segmento iniziale generato da α. □

Definizione 7.5.4. Denotiamo l'ordinale successore di α con $\alpha + 1$.

Definizione 7.5.5. Un ordinale α è detto *ordinale successore* se esiste un ordinale β tale che $\alpha = \beta + 1$. Altrimenti, se non è il minimo, è chiamato *ordinale limite*.

Adesso l'obiettivo che vogliamo raggiungere è quello di dimostrare che ad ogni insieme ben ordinato è possibile associare in modo unico (a meno di isomorfismo) un numero ordinale. Prima di tutto questo, però, vogliamo dimostrare alcune proprietà caratteristiche dei numeri ordinali:

Proposizione 7.5.1. *Sia α un ordinale. Se $\beta \in \alpha$ allora β è un ordinale.*

Dimostrazione. Se $\beta \in \alpha$ allora per la trasitività di α si ha che $\beta \subseteq \alpha$, e allora $(\beta, \in)$ è ben ordinato perché sottoinsieme di un ben ordinato.
Ora dobbiamo mostrare che β è transitivo. Supponiamo che $\delta \in \gamma \in \beta$, dobbiamo mostrare che $\delta \in \beta$. Visto che α è transitivo si ha che $\gamma \in \alpha$, ma allora da $\delta \in \gamma \in \alpha$ segue che $\delta \in \alpha$. Adesso $\delta \in \gamma \in \beta$ è una relazione che vale in α, e per il fatto che $\in$ gode della proprietà transitiva segue $\delta \in \beta$.[2] □

Lemma 7.5.2. *Se α è un ordinale allora $\alpha \notin \alpha$.*

Dimostrazione. Se così non fosse non varrebbe la proprietà antiriflessiva di $\in$. □

Proposizione 7.5.2. *Siano α e β ordinali. Sono proprietà equivalenti:*
(1) $\alpha \in \beta$;
(2) α è un segmento iniziale proprio di β;
(3) $\alpha \subset \beta$.

Dimostrazione. ((1) $\Longrightarrow$ (2)) Visto che β è transitivo sappiamo che ciò equivale a dire che $\beta_\alpha = \alpha$, e dunque α è segmento iniziale di β.
((2) $\Longrightarrow$ (3)) Questa implicazione è del tutto ovvia.
((3) $\Longrightarrow$ (1)) Visto che $\alpha \subseteq \beta$ abbiamo che l'insieme $\beta - \alpha$ è non vuoto, e quindi possiamo considerarne il minimo. Sia dunque $\gamma = \min(\beta - \alpha) \in \beta$. Allora per costruzione $\beta_\gamma = \alpha$, e dunque $\gamma = \alpha$ per la proprietà di cui godono gli ordinali. □

[2] potevamo anche ragionare come segue. Arrivati a dire che $\delta, \beta \in \alpha$ entrambi, allora visto che $\in$ è totale in α si ha o $\delta = \beta$ o $\delta \in \beta$ o $\beta \in \delta$. Ma se $\delta = \beta$ avremmo $\beta \in \gamma \in \beta$ il che è assurdo in α; se $\beta \in \delta$ si ha $\beta \in \delta \in \gamma \in \beta$ e ciò è assurdo perché sennò $\beta \in \delta$.

Proposizione 7.5.3. *Siano α e β ordinali. Se $\alpha \cong \beta$ allora $\alpha = \beta$.*

Dimostrazione. Sia $\psi : \alpha \to \beta$ un isomorfismo d'ordine tra α e β; vogliamo dimostrare che $\psi = id$. Se così non fosse prendiamo

$$\xi = \min\{x \mid \psi(x) \neq x\}.$$

Ma allora sappiamo che $\psi|_{\alpha_\xi} : \alpha_\xi \to \beta_{\psi(\xi)}$ è un isomorfismo, e per costruzione di ξ si ha $\psi|_{\alpha_\xi} = id_{\alpha_\xi}$, e dunque $\alpha_\xi = \beta_{\psi(\xi)}$. Ma ciò significa, dalla trasitività, che $\xi = \psi(\xi)$, e ciò è assurdo. □

Proposizione 7.5.4 (tricotomia degli ordinali)**.** *Siano α e β ordinali. Allora vale una ed una sola delle seguenti: $\alpha \in \beta$, $\alpha = \beta$ o $\beta \in \alpha$.*

Dimostrazione. Dal teorema di confrontabilità dei buoni ordini sappiamo che ci sono tre possibilità: o $\alpha \cong \beta$ o $\alpha \cong \beta_\gamma$ o $\beta \cong \alpha_\delta$. Queste implicano, grazie alla proposizione 7.5.3, che $\alpha = \beta$, $\alpha = \beta_\gamma = \gamma \in \beta$ o $\beta = \alpha_\delta = \delta \in \alpha$, rispettivamente; ciò conclude. □

Corollario 7.5.1. *I numeri naturali sono tutti e soli gli ordinali di cardinalità finita.*

Dimostrazione. Sappiamo già che i numeri naturali sono ordinali e che la loro cardinalità è finita, dobbiamo mostrare che non ce ne sono altri, ossia che se α è un ordinale e $\alpha \notin \omega$ allora non è finito. Visto che $\alpha \notin \omega$ avremo $\alpha \ni \omega$ o $\omega = \alpha$, e quindi $\alpha \supseteq \omega$ per la transitività di α. Ma allora α contiene un sottoinsieme infinito e dunque deve essere infinito. □

Con le precedenti abbamo esaurito gran parte delle proprietà degli ordinali che volevamo presentare. Eccoci adesso giunti al teorema tanto preannunciato riguardo agli ordinali: dimostreremo che ad ogni buon ordine è possibile associare in modo unico un ordinale. In questo modo potremmo dire che gli ordinali sono i *tipi d'ordine* degli insiemi bene ordinati. Ma veniamo al teorema:

Teorema 7.5.2. *Ogni insieme ben ordinato è isomorfo a un unico ordinale.*

Dimostrazione. Sia $(A, <)$ un insieme ben ordinato, definiamo per ricursione la funzione di dominio A tale che

$$R(a) = \{R(b) \mid b < a\},$$

che chiameremo *funzione rango*. Osserviamo che per poter applicare il teorema di ricursione abbiamo utilizzato la corrispondenza funzionale $H(a, R|_{A_a}) = \operatorname{imm} R|_{A_a}$; osserviamo inoltre che $R(\min A) = \emptyset$. L'obiettivo è di dimostrare che $\operatorname{imm} R$ è l'ordinale cui $(A, <)$ è isomorfo.

Osserviamo che per ogni $a \in A$ vale $R(a) \notin R(a)$. Se così non fosse prendiamo

$$b = \min\{a \in A \mid R(a) \in R(a)\};$$

un tale b soddisfa $R(b) \in R(b) = \{R(c) \mid c < b\}$ e dunque $R(b) = R(c)$ per qualche $c < b$, e tale c contraddice la minimalità di b perché avremmo $R(c) \in R(c)$. Ora possiamo mostrare che R è iniettiva: sia $R(a) = R(b)$, allora facciamo vedere che $a = b$. Se per assurdo avessimo $a < b$ allora $R(a) \in R(b) = R(a)$, e ciò contraddice l'osservazione precedente[3]; analogamente si procede nel caso $a > b$.
Abbiamo che R è un'applicazione iniettiva, e sarà dunque biunivoca sulla sua immagine $\operatorname{imm} R$. Mostriamo che $\operatorname{imm} R$ è un insieme ben ordinato dalla relazione di appartenenza $\in$. Intanto la relazione è transitiva: supponiamo che $R(a) \in R(b)$ e $R(b) \in R(c)$, allora $a < b$ e $b < c$.Visto che $<$ è transitivo segue che $a < c$ e dunque che $R(a) \in R(c)$. Inoltre la relazione è asimmetrica, infatti se fosse $R(a) \in R(b)$ e $R(b) \in R(a)$ avremmo per la transitività che $R(a) \in R(a)$, e ciò è assurdo. Sempre dalla totalità dell'ordine $<$ su A segue anche la totalità di $\in$ in modo analogo a sopra, e sempre in questo modo si dimostra anche che $(\operatorname{imm} R, \in)$ è un buon ordine (il lettore completi i dettagli).
Per stabilire che R è un isomorfismo di ordine tra $(A, <)$ e $(\operatorname{imm} R, \in)$ dobbiamo mostrare che R preserva l'ordine, ossia

$$a < b \iff R(a) \in R(b).$$

L'implicazione diretta è vera per definizione, mentre quella inversa segue dall'iniettività. Infatti Se $R(a) \in R(b)$ significa che $R(a) = R(c)$ per qualche $c < b$, ma allora $a = c < b$. Ciò che ci rimane da dimostrare per concludere è che $(\operatorname{imm} R, \in)$ è un ordinale e che è unico. Il fatto che sia ben ordinato l'abbiamo già trattato, dobbiamo solo mostrare che $\operatorname{imm} R$ è un insieme transitivo, ma a questo punto è molto semplice. Sia $r \in s \in \operatorname{imm} R$, allora $s = R(a)$ per qualche $a \in A$, e il fatto che $r \in s$ significa che $r = R(b)$ per qualche $b < a$, e dunque $r = R(b) \in \operatorname{imm} R$. L'unicità è diretta conseguenza della proposizione 7.5.3: se avessimo $A \cong \alpha$ e $A \cong \beta$ allora $\alpha \cong \beta$, da cui $\alpha = \beta$. □

Definizione 7.5.6. Se $(A, <)$ è un insieme ben ordinato, allora il *tipo d'ordine* di A è l'unico ordinale isomorfo ad A.

Ciò che di più importava per questa parte è concluso, l'ultimo problema che ci vogliamo porre è il seguente: esiste l'insieme di tutti gli ordinali? Intanto vediamo quando una raccolta di ordinali continua ad essere un ordinale:

[3] volendo potevamo omettere l'osservazione che per ogni $a \in A$ vale $R(a) \notin R(a)$ e dire a questo punto che $R(a) \in R(a)$ contraddice l'assioma di fondazione.

Proposizione 7.5.5. *Sia X un insieme di numeri ordinali. X è un ordinale se e solo se X è transitivo.*

Dimostrazione. ($\Longrightarrow$) L'implicazione è vera per definizione.
($\Longleftarrow$) Dobbiamo mostrare che $(X, \in)$ è un buon ordine. È un ordine totale per il teorema di tricotomia, adesso mostriamo che vale la proprietà del minimo. Sia $Y \subseteq X$ non vuoto e sia $\gamma \in Y$: se γ è il minimo abbiamo finito, altrimenti si prende l'insieme

$$Z = \{\delta \in Y \mid \delta \in \gamma\},$$

che è dunque non vuoto. Visto che Z è un buon ordine con $\in$, il minimo di Z esiste, ed è ovvio che $\min Y = \min Z$. □

La proposizione precedente basta per dimostrare che non può esistere l'insieme di tutti gli ordinali. Questo fatto è noto come *paradosso di Burali–Forti*. Infatti se esistesse l'insieme di tutti gli ordinali allora, essendo transitivo, sarebbe esso stesso un ordinale. Ma allora sarebbe un elemento di se stesso, e ciò non è consentito dal lemma 7.5.2. Denotiamo con Ord la classe degli ordinali; possiamo scrivere:

Teorema 7.5.3. *Non esiste l'insieme di tutti gli ordinali.*

Dimostrazione. È data dal paradosso di Burali–Forti scritto prima. □

7.6 Altre proprietà, induzione e ricursione

In questo paragrafo vogliamo completare le proprietà degli ordinali rimaste e poi vedere come si possa fare l'induzione e la ricursione sugli ordinali, nonostante la classe di tutti gli ordinali non sia un insieme.

Definizione 7.6.1. Siano α e β ordinali. Scriveremo $\alpha < \beta$ quando $\alpha \in \beta$.

Abbiamo detto nello scorso paragrafo (proposizione 7.5.1) che ogni elemento di un ordinale è esso stesso un ordinale. Questo porta a scoprire una proprietà molto particolare che caratterizza i numeri ordinali, ossia che ogni ordinale è l'insieme degli ordinali a lui minori, ossia

$$\alpha = \{\beta \mid \beta \text{ è ordinale e } \beta < \alpha\}.$$

Tutte queste proprietà in effetti, così come anche la definizione di $<$ tra ordinali che abbiamo dato, estendono quanto già avevamo detto per i numeri naturali.
Abbiamo anticipato all'inizio del paragrafo che nonstante la classe di tutti gli ordinali non sia un insieme (paradosso di Burali–Forti) possiamo fare induzione e rircursione sugli ordinali. Prima però ci serve qualche risultato:

Proposizione 7.6.1 (principio del minimo)**.** *Sia $P(x)$ una formula. Se esiste un ordinale α che verifica P, allora esiste un minimo tale α.*

Dimostrazione. Supponiamo che valga $P(\alpha)$. Se α è il minimo abbiamo concluso; se non lo è basta considerare $\{\beta \mid \beta \text{ è ordinale, } \beta < \alpha \text{ e } P(\beta)\} \subseteq \alpha$, che è un insieme non vuoto. Essendo sottoinsieme di un ben ordinato è anch'esso ben ordinato con l'ordine indotto e pertanto ammette minimo. □

Proposizione 7.6.2. *Sia X un insieme di ordinali. Allora $\bigcup X$ è un ordinale, ed è il minimo ordinale maggiore o uguale a tutti gli ordinali di X.*

Dimostrazione. Per il teorema 7.3.1 l'unione $\bigcup X = \bigcup_{\alpha \in X} \alpha$ è un ordinale: il teorema garantisce che tale unione è ben ordinata da $\in$ e la transitività si verifica facilmente. Se $x \in y \in \bigcup X$ allora vorrà dire che esiste $\alpha \in X$ tale che $y \in \alpha$; ma essendo α un ordinale abbiamo che $y \subseteq \alpha$ e dunque $x \in \alpha$.
Per mostrare che è il minimo ordinale maggiore o uguale a tutti gli ordinali di X dobbiamo mostrare i seguenti due fatti: (1) se $\alpha \in X$ allora $\alpha \leq \bigcup X$; e (2) se $\alpha \in \gamma$ per ogni $\alpha \in X$ allora $\bigcup X \leq \gamma$. Per il primo abbiamo semplicemente

$$\alpha \in X \Longrightarrow \alpha \subseteq \bigcup X \Longrightarrow \alpha \leq \bigcup X,$$

dove la seconda implicazione vale perché se fosse $\alpha > \bigcup X$ avremmo $\bigcup X \in \alpha$. Per la seconda invece basta osservare che se γ è un ordinale allora

$$(\forall \alpha \in X)(\alpha \in \gamma) \Longrightarrow (\forall \alpha \in X)(\alpha \subseteq \gamma) \Longrightarrow \bigcup X \subseteq \gamma \Longrightarrow \bigcup X \leq \gamma,$$

con analoghe motivazioni alle precedenti. □

Definizione 7.6.2. L'ordinale $\bigcup X$ della proposizione precedente è detto *estremo superiore* di X, e viene denotato talvolta con $\sup X$.

Osservazione 7.6.1. Se l'insieme X ha un elemento massimo β rispetto all'ordine $<$ allora $\sup X = \beta$. Altrimenti $\sup X > \alpha$ per ogni $\alpha \in X$ (e questo è il minimo tale ordinale).

Osservazione 7.6.2. Abbiamo mostrato che ogni insieme di ordinali ammette un estremo superiore; questo fatto può essere anche utilizzato per mostrare l'inesistenza dell'insieme di tutti gli ordinali. Se tale insieme esistesse avrebbe un estremo superiore γ; preso allora $S(\gamma) = \gamma + 1$ avremmo trovato un ordinale che non appartiene all'insieme, e ciò è assurdo.

Ciò è quanto bastava per poter dare i risultati di induzione e ricursione sugli ordinali, che presentiamo di seguito:

Teorema 7.6.1 (induzione transfinita per ordinali)**.** *Sia $P(x)$ una proprietà possibilmente dotata di parametri. Supponiamo che per ogni ordinale α valga il seguente fatto:*

$$\text{se } P(\beta) \text{ per ogni } \beta < \alpha \text{ allora } P(\alpha). \tag{7.2}$$

Allora $P(\alpha)$ vale per ogni α ordinale.

Dimostrazione. Supponiamo per assurdo che esista un ordinale γ che non verifica P, allora consideriamo $\{\beta \mid \beta \leq \gamma \text{ e } \neg(P(\beta))\}$. Tale insieme è non vuoto e quindi ammette un minimo α. Ma tutti gli ordinali minori di α verificano P e dunque per ipotesi vale $P(\alpha)$, assurdo. □

A volte risulta utile utilizzare il principio di induzione transfinita in una forma che ricorda anche la versione per i numeri naturali. Tale forma è quella che distingue gli ordinali successori dagli ordinali limite:

Teorema 7.6.2 (induzione transfinita per ordinali, seconda versione)**.** *Sia $P(x)$ una proprietà possibilmente dotata di parametri. Supponiamo che valgano i seguenti fatti:*
(1) vale $P(0)$;
(2) $P(\alpha)$ implica $P(\alpha + 1)$ per tutti gli ordinali α;
(3) per ogni ordinale limite α, se $P(\beta)$ vale per ogni $\beta < \alpha$ allora vale $P(\alpha)$.
Allora $P(\alpha)$ vale per ogni α ordinale.

Dimostrazione. Basta osservare che le condizioni (1), (2) e (3) implicano la (7.2) e si ha la tesi. □

Adesso generalizziamo il teorema di ricursione nella forma seguente:

Teorema 7.6.3 (teorema di ricursione)**.** *Sia $H : \mathrm{Ord} \to \mathrm{Ord}$ una funzione classe. Allora esiste ed è unica una funzione classe $f : \mathrm{Ord} \to \mathbb{V}$ tale che per ogni ordinale α si ha $f(\alpha) = H(f|_\alpha)$.*

Non daremo la prova di questo teorema in quanto è una immediata generalizzazione del teorema di ricursione già dato precedentemente.

7.7 Aritmetica degli ordinali: addizione

Il teorema di ricursione transfinita sugli ordinali dato nel precedente paragrafo ci serve adesso per definire addizione, moltiplicazione e esponenziazione di numeri ordinali. Queste definizioni sono date come generalizzazione delle definzioni sui numeri naturali, come anche in altri ambiti è già successo. La definizione della somma è data per ricursione sul secondo argomento:

Definizione 7.7.1. Per ogni ordinale β:
(1) $\beta + 0 = \beta$;
(2) $\beta + (\alpha + 1) = (\beta + \alpha) + 1$ per ogni ordinale α;
(3) $\beta + \alpha = \bigcup_{\gamma<\alpha}(\beta + \gamma)$ per ogni ordinale limite α.

Osserviamo che se si pone $\alpha = 0$ nella (2) otteniamo $\beta + 1 = \beta + 1$: il primo membro denota la somma tra l'ordinale β e l'ordinale 1, mentre il secondo denota il successore di β.

Esempio 7.7.1. Come conseguenza della definizione abbiamo, per ogni β ordinale

$$(\beta + 1) + 1 = \beta + 2, \quad (\beta + 2) + 1 = \beta + 3,$$

e più in generale $(\beta + n) + 1 = \beta + (n + 1)$ per ogni $n \in \mathbb{N}$.

Esempio 7.7.2. Consideriamo adesso alcune somme che coinvolgono l'ordinale limite ω. Intanto

$$1 + \omega = \bigcup_{n<\omega}(1 + n) = \omega;$$

Geometricamente, la somma che abbiamo eseguito potrebbe essere immaginata come segue: possiamo mettere 0 all'inizio e poi fargli seguire una copia di $\mathbb{N}$ (ossia ω), e allora vediamo che in effetti è come ordinare ω. In generale $n + \omega = \omega$ per ogni $n \in \mathbb{N}$.
Consideriamo ora $\omega+1$: questo è un ordinale diverso da ω perché è il suo successore, ossia $\omega + 1 = \omega \cup \{\omega\}$. Questi due esempi mostrano che $\omega + 1 \neq 1 + \omega$, ossia che la somma di ordinali non è commutativa.

Esempio 7.7.3. Inoltre si può notare che, nonostante $1 \neq 2$ si ha $1 + \omega = 2 + \omega = \omega$. Dunque la somma di ordinali non gode della legge di cancellazione a destra; tuttavia vedremo fra poco che la somma è associativa gode della legge di cancellazione *solo a sinistra*.
Questo stesso esempio ci mostra che non vale una legge di cancellazione a destra neanche per disuguaglianze, infatti $1 < 2$ ma $1 + \omega = 2 + \omega$. Analogamente però mostreremo che vale una legge di cancellazione per disuguaglianza ma che vale solo a sinistra.

Esempio 7.7.4. Dimostriamo formalmente che tra ordinali $2 + 3 = 5$. Si ha

$$\begin{aligned} 2 + 3 &= 2 + (2 + 1) = (2 + 2) + 1 = (2 + (1 + 1)) + 1 = \\ &= ((2 + 1) + 1) = (3 + 1) + 1 = 4 + 1 = 5, \end{aligned}$$

e abbiamo concluso.

Osservazione 7.7.1 (elemento neutro). L'operazione di addizione di numeri ordinali ha anche un elemento neutro, che è l'ordinale 0. Infatti vale $\alpha + 0 = \alpha$ per definizione, e affermiamo che vale anche

$$0 + \alpha = \alpha.$$

per ogni ordinale α. Quest'ultimo asserto può essere facilmente provato per induzione su α, lasciamo i dettagli al lettore.

Nel capitolo 4 abbiamo dato la definizione di somma di buoni ordini A_1 e A_2, e avevamo visto che tale somma (denotata con $A_1 \oplus A_2$) può essere ben ordinata. In effetti se α e β sono gli ordinali associati agli ordini addendo abbiamo che l'ordinale associato a $A_1 \oplus A_2$ è proprio $\alpha + \beta$.

Teorema 7.7.1. *Siano $(A_1, <_1)$ e $(A_2, <_2)$ due insiemi ben ordinati isomorfi agli ordinali α e β, e sia $A = A_1 \oplus A_2$ l'ordine somma. Allora $(A_1 \oplus A_2, <)$ è isomorfo a $\alpha + \beta$.*

Dimostrazione. Senza perdere di generalità possiamo supporre $A_1 \cap A_2 = \emptyset$.[4] Proviamo il teorema per induzione su β.
Se $\beta = 0$ allora $A_2 = \emptyset$ e allora $A = A_1$, e dunque $A = A_1 \cong \alpha = \alpha + \beta$. Adesso supponiamo che $\beta = \beta' + 1$, questo significa che A_2 ha un elemento massimo a e A_a è isomorfo a $\alpha + \beta'$. L'isomorfismo si estende ad un isomorfismo tra A e $\alpha + \beta = (\alpha + \beta') + 1$.
Infine supponiamo che β sia un ordinale limite e che per ogni $\gamma < \beta$ esista un isomorfismo f_γ tra $\alpha + \gamma$ e A_{α_γ}, dove $\alpha_\gamma \in A_2$. Inoltre f_γ è unico, α_γ è il γ–esimo elemento di A_2 e se $\gamma < \delta$ allora $f_\gamma \subset f_\delta$. Sia adesso

$$f = \bigcup_{\gamma<\beta} f_\gamma.$$

Visto che $\alpha + \beta = \bigcup_{\gamma<\beta}(\alpha + \gamma)$ segue che f è un isomorfismo tra $\alpha + \beta$ e A. □

Adesso vogliamo presentare, come promesso, alcune proprietà della somma di ordinali, che proponiamo nelle seguenti proposizioni:

Proposizione 7.7.1. *Siano α_1, α_2 e β ordinali. Allora $\alpha_1 < \alpha_2$ se e solo se $\beta + \alpha_1 < \beta + \alpha_2$.*

Dimostrazione. ($\Longrightarrow$) Useremo l'induzione transfinita su α_2 per mostrare questa implicazione. Non c'è da mostrare niente se $\alpha_2 = 0$ in quanto la premessa dell'implicazione è falsa e quindi l'implicazione risulta vera a vuoto. Supponiamo

[4] come abbiamo già osservato ciò è possibile perché sennò basta ordinare analogamente gli insiemi disgiunti $A_1 \times \{0\}$ e $A_2 \times \{1\}$.

$\alpha_1 < \alpha_2$ e che α_2 sia un successore e poniamo $\alpha_2 = \delta + 1$. Allora deve essere $\delta \geq \alpha_1$ (altrimenti se $\delta < \alpha_1$ allora $\delta + 1 \leq \alpha_1$). Per ipotesi induttiva nel caso $\delta > \alpha_1$, e banalmente nel caso $\delta = \alpha_1$, otteniamo

$$\beta + \alpha_1 \leq \beta + \delta < (\beta + \delta) + 1 = \beta + (\delta + 1) = \beta + \alpha_2.$$

Adesso invece supponiamo che α_2 sia un ordinale limite. Si ha allora $\alpha + 1 < \alpha_2$ e possiamo scrivere

$$\beta + \alpha_1 < (\beta + \alpha_1) + 1 = \beta + (\alpha_1 + 1) \leq \bigcup_{\gamma < \alpha_2} (\beta + \gamma) = \beta + \alpha_2.$$

($\Longleftarrow$) Per provare questa implicazione faremo uso della precedente. Supponiamo che $\beta + \alpha_1 < \beta + \alpha_2$; se per assurdo fosse $\alpha_2 < \alpha_1$ la parte appena provata mostrerebbe $\beta + \alpha_2 < \beta + \alpha_1$ e quindi avremmo l'assurdo; se $\alpha_2 = \alpha_1$ avremmo ovviamente $\beta + \alpha_2 = \beta + \alpha_1$, assurdo. □

Corollario 7.7.1 (legge di cancellazione a sinistra)**.** *Siano α_1, α_2 e β numeri ordinali. Allora $\alpha_1 = \alpha_2$ se e solo se $\beta + \alpha_1 = \beta + \alpha_2$.*

Dimostrazione. L'implicazione verso destra è banale, mostriamo quella verso sinistra. Se per assurdo fosse $\alpha_1 \neq \alpha_2$ allora abbiamo solo le due possibilità $\alpha_1 < \alpha_2$ e $\alpha_1 > \alpha_2$ (per la totalità di $<$). Per la proposizione precedente, in ciascuno di questi due casi si raggiunge l'assurdo. □

L'operazione di somma tra ordinali, per quanto come abbiamo visto possa apparire distante dall'usuale concetto di addizione, preserva lo stesso alcune delle proprietà che ci aspettiamo. Ad esempio è associativa, come mostreremo adesso, ed inoltre vedremo che il prodotto si distribuisce (solo da sinistra) sulla somma.

Proposizione 7.7.2 (legge associativa)**.** *Siano α, β e γ ordinali. Allora*

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$$

Dimostrazione. Dimostriamo la proprietà per induzione su γ. Se $\gamma = 0$ la proprietà risulta banale perché si ha

$$(\alpha + \beta) + 0 = \alpha + \beta = \alpha + (\beta + 0),$$

per definizione. Supponiamo adesso che γ sia un successore, ossia $\gamma = \delta + 1$, allora

$$\begin{aligned} (\alpha + \beta) + (\delta + 1) &= ((\alpha + \beta) + \delta) + 1 = (\alpha + (\beta + \delta)) + 1 = \\ &= \alpha + ((\beta + \delta) + 1) = \alpha + (\beta + (\delta + 1)), \end{aligned}$$

dove nella seconda uguaglianza abbiamo utilizzato l'ipotesi induttiva. Supponiamo infine che γ sia un limite,

$$(\alpha + \beta) + \gamma = \bigcup_{\delta<\gamma}((\alpha + \beta) + \delta) = \bigcup_{\delta<\gamma}(\alpha + (\beta + \delta)).$$

Affermiamo che $\beta + \gamma$ è un ordinale limite: infatti se $\xi < \beta + \gamma = \bigcup_{\delta<\gamma}(\beta + \delta)$ allora $\xi \leq \beta + \delta$ per qualche $\delta < \gamma$ e quindi

$$\xi + 1 \leq (\beta + \delta) + 1 = \beta + (\delta + 1) < \beta + \gamma,$$

dove l'ultima disuguaglianza vale in quanto γ è limite, e dunque $\delta + 1 < \gamma$, ed anche per la proposizione precedente aggiungendo β a sinistra. Infine dunque si ha

$$(\alpha + \beta) + \gamma = \bigcup_{\delta<\gamma}(\alpha + (\beta + \delta)) = \bigcup_{\beta+\delta<\beta+\gamma}(\alpha + (\beta + \delta)) = \alpha + (\beta + \gamma),$$

dove la seconda uguaglianza si ha perché $\delta < \gamma$ se e solo se $\beta + \delta < \beta + \gamma$ e poi l'ultima uguaglianza si ha perché $\beta + \gamma$ è un ordinale limite. □

Come ultimo fatto riguardo alla somma di ordinale vogliamo vedere che esiste anche un'operazione di sottrazione di ordinali, ossia una inversa per l'operazione di somma:

Proposizione 7.7.3. *Se $\alpha \leq \beta$ allora esiste un unico γ tale che $\alpha + \gamma = \beta$.*

Dimostrazione. Affermiamo che esistono ordinali strettamente maggiori di β: infatti intanto si ha $\alpha + \beta \geq \beta$ e dunque $\alpha + (\beta + 1) = (\alpha + \beta) + 1 > \beta$. Dunque esiste $\delta = \min\{\xi \mid \alpha + \xi > \beta\}$. Affermiamo che δ è un successore: supponiamo per assurdo che δ sia un limite avremmo

$$\beta < \alpha + \delta = \bigcup_{\xi<\delta}(\alpha + \xi),$$

e quindi esisterebbe $\xi < \delta$ tale che $\beta < \alpha + \xi$, ed è assurdo per la minimalità di δ. Quindi sia γ tale che $\delta = \gamma + 1$. Allora

$$\alpha + \gamma \leq \beta < \alpha + (\gamma + 1) = \alpha + \gamma + 1,$$

da cui $\alpha + \gamma = \beta$. L'unicità segue dalla legge di cancellazione: se esistesse un γ' tale che $\alpha + \gamma' = \beta$ allora avremmo $\alpha + \gamma' = \alpha + \gamma$, da cui $\gamma' = \gamma$. □

Esempio 7.7.5. Attenzione che anche nel caso delle sottrazioni abbiamo dei fenomeni non usuali. Ad esempio consideriamo $\alpha = 7$ e $\beta = \omega$ con $7 < \omega$. L'ordinale differenza è $\omega - 7 = \omega$ in quanto $7 + \omega = \omega$.

7.8 Aritmetica degli ordinali: moltiplicazione e esponenziazione

Ancora una volta è il teorema di ricursione sugli ordinali che ci permette di definire la moltiplicazione in modo ricorsivo:

Definizione 7.8.1. Per ogni ordinale β:
(1) $\beta \cdot 0 = 0$;
(2) $\beta \cdot (\alpha + 1) = \beta \cdot \alpha + \beta$ per ogni ordinale α;
(3) $\beta \cdot \alpha = \bigcup_{\gamma<\alpha}(\beta \cdot \gamma)$ per ogni ordinale limite α.

Ormai forti dalla definizione di addizione andiamo subito a vedere degli esempi semplici di calcolo di prodotto di ordinali:

Esempio 7.8.1. Calcoliamo il prodotto $\beta \cdot 1$, che ci aspettiamo sia β:

$$\beta \cdot 1 = \beta \cdot (0 + 1) = \beta \cdot 0 + \beta = 0 + \beta = \beta,$$

come segue immediatamente dalle definizioni. Ma allora, volendo estendere dagli interi, ci potremmo chiedere se l'ordinale 1 possa essere l'elemento neutro del prodotto. Come fatto per la somma, vale anche che per ogni ordinale β si ha

$$1 \cdot \beta = \beta,$$

e ancora una volta si può mostrare questo fatto per induzione (il lettore lo dimostri!). Abbiamo dimostrato che 1 è l'*elemento neutro* della moltiplicazione tra ordinali.

Esempio 7.8.2. Vediamo i prodotti tra ordinali e ordinali finiti:

$$\beta \cdot 2 = \beta \cdot (1 + 1) = \beta \cdot 1 + \beta \cdot 1 = \beta + \beta.$$

Come si intuirà vale che per ogni $n < \omega$ si ha

$$\beta \cdot n = \underbrace{\beta + \beta + \ldots + \beta}_{n \text{ volte}},$$

la dimostrazione è una semplice induzione su n naturale.

Esempio 7.8.3. Con questo esempio faremo vedere che in generale neanche il prodotto è commutativo. Infatti si ha che $\omega \cdot 2 = \omega + \omega$ per l'esempio precedente, però si ha

$$2 \cdot \omega = \bigcup_{n<\omega}(2 \cdot n) = \omega,$$

il quale è diverso da $\omega + \omega$. Infatti $\omega + \omega$ è isomorfo all'ordinamento della somma di due copie di $\mathbb{N}$, mentre ω è una sola copia ed è isomorfo ad un segmento iniziale di $\omega + \omega$, dunque non possono essere isomorfi tra loro.

Non ci mettiamo a dare una dimostrazione formale di tutte le proprietà del prodotto perché sono esattamente analoghe a quelle della somma. Per i dettagli delle dimostrazioni di alcune di esse si veda la parte relativa negli esercizi. Ci limitiamo solo a dire che vale la *legge di cancellazione solo a sinistra*[5], che il prodotto è associativo e che vale la *proprietà distributiva solo a sinistra*. Ossia si ha:

$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma) \quad \text{e} \quad \alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma.$$

Come nel caso della somma si ha che la definizione dell'ordinale prodotto $\alpha \cdot \beta$ è coerente con la definizione di ordine antilessicografico che abbiamo denotato con $A_1 \odot A_2$.

Teorema 7.8.1. *Siano $(A_1, <_1)$ e $(A_2, <_2)$ due insiemi ben ordinati isomorfi agli ordinali α e β, e sia $A = A_1 \odot A_2$ l'ordine prodotto. Se $\prec$ denota l'ordine antilessicografico allora $(A_1 \odot A_2, \prec)$ è isomorfo a $\alpha \cdot \beta$. Se invece $\prec'$ denota l'ordine lessicografico allora $(A_1 \odot A_2, \prec')$ è isomorfo a $\beta \cdot \alpha$.*

Dimostrazione. Definiamo un isomorfismo tra $(A_1 \odot A_2, \prec)$ e $\alpha \cdot \beta$ come segue: per $\xi < \alpha$ e $\eta < \beta$ poniamo

$$f(\xi, \eta) = \alpha \cdot \eta + \xi.$$

L'immagine di f è l'insieme $\{\alpha \cdot \eta + \xi \mid \eta < \beta \text{ e } \xi < \alpha\} = \alpha \cdot \beta$ e f è un isomorfismo. Lasciamo i dettagli al lettore limitandoci a dire che si procede per induzione e che vanno utilizzate le proprietà enunciate prima del teorema. □

Infine vale un teorema di divisione tra ordinali, che permette di avere una sorta di inversa dell'operazione di moltiplicazione (come la sottrazione nel caso della somma), vediamo di che si tratta:

Proposizione 7.8.1. *Sia $\beta \geq 1$ un ordinale. Allora esistono unici γ e ρ tali che $\alpha = \beta \cdot \gamma + \rho$ con $\rho < \beta$.*

Dimostrazione. Intanto affermiamo che esistono ordinali che moltiplicati a sinistra per β superano α: infatti vale $\beta \cdot \alpha \geq \alpha$ e quindi $\beta \cdot (\alpha + 1) = \beta \cdot \alpha + \beta > \alpha$. Esiste dunque

$$\delta = \min\{\xi \mid \beta \cdot \xi > \alpha\}.$$

Sempre per minimalità di δ si può mostrare analogamente al caso della somma che δ è un successore, ossia $\delta = \gamma + 1$ per un certo γ. Si ha allora

$$\beta \cdot \gamma \leq \alpha < \beta \cdot (\gamma + 1).$$

[5] come nel caso della somma la legge di cancellazione segue da un fatto più generale: se α_1, α_2 e $\beta \neq 0$ sono ordinali allora $\beta \cdot \alpha_1 < \beta \cdot \alpha_2$ se e solo se $\alpha_1 < \alpha_2$.

Per il teorema sulla differenza di ordinali esiste ρ tale che $\alpha = \beta \cdot \gamma + \rho$; vale anche che $\rho < \beta$ in quanto sennò

$$\alpha = \beta \cdot \gamma + \rho \geq \beta \cdot \gamma + \beta = \beta \cdot (\gamma + 1) > \alpha,$$

e ciò è assurdo. Adesso ci rimane da dimostrare la parte sull'unicità: supponiamo che si possa scrivere $\alpha = \beta \cdot \gamma + \rho = \beta \cdot \gamma' + \rho'$. Se per assurdo $\gamma \neq \gamma'$, diciamo $\gamma < \gamma'$, allora avremmo

$$\alpha = \beta \cdot \gamma + \rho < \beta \cdot \gamma + \beta = \beta \cdot (\gamma + 1) \leq \beta \cdot \gamma' \leq \beta \cdot \gamma' + \rho' = \alpha,$$

assurdo. A questo punto l'uguaglianza dei resti si ha per l'unicità della differenza di ordinali (o per la legge di cancellazione). □

Per un esempio di divisione tra numeri ordinali si vada alla sezione corrispondente nella parte degli esercizi.
A questo punto possiamo definire l'esponenziazione tra ordinali sempre in modo ricorsivo, vediamo subito la definizione:

Definizione 7.8.2. Per ogni ordinale β:
(1) $\beta^0 = 1$;
(2) $\beta^{\alpha+1} = \beta^\alpha \cdot \beta$ per ogni ordinale α;
(3) $\beta^\alpha = \bigcup_{\gamma<\alpha} \beta^\gamma$ per ogni ordinale limite α.

Esempio 7.8.4. Osserviamo intanto che

$$\beta^1 = \beta^{0+1} = \beta^0 \cdot \beta = 1 \cdot \beta = \beta.$$

In modo analogo le potenze finite rispecchiamo quelle che già conosciamo in quanto ad esempio $\beta^2 = \beta^{1+1} = \beta^1 \cdot \beta = \beta \cdot \beta$, e in modo analogo per ogni $n < \omega$

$$\beta^n = \underbrace{\beta \cdot \beta \cdot \ldots \cdot \beta}_{n \text{ volte}}.$$

Il lettore provi a dimostrare l'uguaglianza per induzione su $n < \omega$.

Esempio 7.8.5. Per definizione abbiamo visto che

$$\beta^\omega = \bigcup_{n<\omega} \beta^n;$$

quindi in particolare $1^\omega = 1$, $2^\omega = \omega$ e vale (sempre per induzione) che $n^\omega = \omega$ per ogni $n \in \omega$ con $n > 1$. Infine

$$\omega^\omega = \bigcup_{n<\omega} \omega^n > \omega,$$

come segue dalla definizione di estremo superiore.

Adesso enunciamo alcune proprietà dell'esponenziazione tra ordinali, le cui dimostrazioni sono rimandate alle sezioni relative nella parte degli esercizi. Valgono due proprietà delle potenze, ossia

$$\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma \quad \text{e} \quad (\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}.$$

Non vale ad esempio la proprietà $(\alpha \cdot \beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma$. Vediamo il seguente esempio:

Esempio 7.8.6. Mostriamo che $(\omega \cdot 2)^2 \neq \omega^2 \cdot 2^2$. Da un lato abbiamo

$$(\omega \cdot 2)^2 = (\omega \cdot 2) \cdot (\omega \cdot 2) = \omega \cdot (2 \cdot \omega) \cdot 2 = (\omega \cdot \omega) \cdot 2 = \omega^2 \cdot 2,$$

mentre dall'altro $\omega^2 \cdot 2^2 = \omega^2 \cdot 4$, e se fossero uguali allora avremmo $2 = 4$ per la legge di cancellazione, e ciò è assurdo.

Teniamo inoltre a precisare che, a differenza dell'addizione e della moltiplicazione tra ordinali, nel caso dell'esponenziazione non caratterizzeremo l'ordinale α^β (se $\alpha \cong A_1$ e $\beta \cong A_2$) con un buon ordinamento di $A_1^{A_2}$. Vedremo, sempre nella parte degli esercizi, che la caratterizzazione dell'esponenziazione viene fatta mediante buon ordinamento di un certo sottoinsieme di $A_1^{A_2}$.

7.8.1 Operazioni tra ordinali e cardinalità

In questo brevissimo paragrafo, traendo spunto dall'ultima osservazione appena fatta, vogliamo sviluppare un discorso che poi riprenderemo in seguito e che riguarda le cardinalità degli ordinali ottenuti come addizione, prodotto o esponenziazione di altri.
Siano α e β due ordinali rispettivamente isomorfi ai due buoni ordini $(A_1, <_1)$ e $(A_2, <_2)$. Abbiamo mostrato che l'ordinale somma $\alpha + \beta$ è isomorfo all'ordine somma $(A_1 \oplus A_2, <)$, ottenuto ordinando due copie disgiunte di A_1 e A_2 secondo l'ordine che "mette A_2 subito dopo A_1".[6] Da questo segue in modo ovvio che

$$|\alpha + \beta| = |\alpha| + |\beta|.$$

Esempio 7.8.7. Da quanto appena detto segue per esempio che

$$|\omega + \omega| = |\omega| + |\omega| = \aleph_0 + \aleph_0 = \aleph_0 = |\omega|,$$

nonostante poi si abbia che $\omega + \omega \neq \omega$.

[6] ricordiamo che la costruzione che si fa è di ordinare gli insiemi disgiunti $A_1 \times \{0\}$ e $A_2 \times \{1\}$ secondo l'ordine antilessicografico, ossia si controlla prima la seconda componente e poi la prima. Talvolta per non appesantire troppo la notazione si utilizza la scrittura $A_1 \sqcup A_2$, che denota l'unione disgiunta.

L'ordine prodotto $(A_1 \odot A_2, \prec)$, con $\prec$ che denota l'ordine antilessicografico, è isomorfo all'ordinale $\alpha \cdot \beta$, come abbiamo mostrato. Visto che l'ordine prodotto non è altro che un ordinamento particolare del prodotto cartesiano dei due insiemi si avrà

$$|\alpha \cdot \beta| = |\alpha| \cdot |\beta|.$$

Un discorso analogo non si può invece fare per l'esponenziazione, in quanto abbiamo detto che α^β è isomorfo ad un certo sottoinsieme di $A_1^{A_2}$, ma non a tutto $A_1^{A_2}$. In generale varrà dunque che

$$|\alpha^\beta| \neq |\alpha|^{|\beta|}.$$

Esempio 7.8.8. Consideriamo ω^ω. Vale che $|\omega^\omega| = \aleph_0$: questo fatto non possiamo ancora mostrarlo formalmente in quanto non abbiamo ancora definito la somma di infiniti cardinali, però quella definizione sarà molto intuitiva, tant'é che noi adesso faremo il calcolo come l'intuizione ci suggerisce, rassicurando chi legge che poi in effetti sarà davvero così (anche se sarà necessario l'assioma della scelta). Si ha

$$|\omega^\omega| = \left|\bigcup_{n<\omega} \omega^n\right| = \sum_{n=0}^{\infty} |\omega^n| = 1 + \sum_{n=1}^{\infty} \aleph_0 = 1 + \aleph_0 \cdot \aleph_0 = \aleph_0.$$

Invece però $|\omega|^{|\omega|} \neq \aleph_0$. Infatti si ha che

$$|\omega|^{|\omega|} = \aleph_0^{\aleph_0},$$

e vogliamo mostrare che questo è uguale a $2^{\aleph_0} > \aleph_0$. Vale in modo ovvio $2^{\aleph_0} \leq \aleph_0^{\aleph_0}$; per l'altra disuguaglianza basta notare che

$$2^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = (2^{\aleph_0})^{\aleph_0} \geq \aleph_0^{\aleph_0},$$

e si conclude l'uguaglianza per il teorema di Cantor–Bernstein.

Come finale, un'osservazione d'insieme. Si possono usare le operazioni aritmetiche per generare ordinali sempre più grandi, come segue:

$0, 1, 2, \ldots, \omega, \omega{+}1, \ldots, \omega{\cdot}2, \omega{\cdot}2{+}1, \ldots, \omega{\cdot}3, \ldots, \omega{\cdot}\omega = \omega^2, \omega^2{+}1, \ldots, \omega^2{\cdot}2, \ldots,$

$\omega^3, \ldots, \omega^4, \ldots, \omega^\omega, \omega^\omega{+}1, \ldots, \omega^{\omega+1}, \ldots, \omega^{\omega^2}, \ldots, \omega^{\omega^3}, \ldots, \omega^{\omega^\omega}, \ldots, \omega^{\omega^{\omega^\omega}}, \ldots$

Il processo può essere facilmente proseguito definendo, seppur ancora informalmente, l'ordinale $\sup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \ldots\} = \varepsilon_0$. Quindi si può prendere

$$\varepsilon_0 + 1, \ldots, \varepsilon_0 + \omega, \ldots, \varepsilon_0^\omega, \ldots, \varepsilon_0^{\varepsilon_0} \ldots.$$

Adesso diamo una definizione formale di ε_0. Intanto si consideri la successione definita per ricorsione numerabile come segue:

$$\begin{cases} \alpha_0 = \omega \\ \alpha_{n+1} = \omega^{\alpha_n}. \end{cases}$$

Definizione 7.8.3. Definiamo

$$\varepsilon_0 = \bigcup_{n<\omega} \alpha_n = \omega^{\omega^{\omega^{\cdot^{\cdot}}}}.$$

Non abbiamo ancora gli strumenti necessari ma mostreremo che anche ε_0 è un ordinale ancora numerabile (!). La domanda se esistono ordinali non numerabili a questo punto è giustificata e daremo una risposta – che sarà affermativa – solo nel prossimo capitolo. Intanto però vediamo una proprietà di ε_0, che dovrebbe essere abbastanza intuitiva per come è stato definito:

Proposizione 7.8.2. *Vale* $\omega^{\varepsilon_0} = \varepsilon_0$.

Dimostrazione. Visto che ε_0 è un ordinale limite si ha

$$\omega^{\varepsilon_0} = \bigcup_{\gamma<\varepsilon_0} \omega^\gamma = \bigcup_{n<\omega} \omega^{\alpha_n} = \bigcup_{n<\omega} \alpha_{n+1} = \varepsilon_0,$$

ed abbiamo concluso. □

7.9 Forma normale

Usando l'esponenziazione si possono rappresentare i numeri ordinali in una forma simile a quella utilizzata per l'espansione decimale degli interi, che chiameremo *forma normale*, e che utilizza come "base" il numero ω.

Teorema 7.9.1. *Ogni* $\alpha > 0$ *ordinale può essere espresso unicamente come*

$$\alpha = \omega^{\beta_1} \cdot n_1 + \omega^{\beta_2} \cdot n_2 + \ldots + \omega^{\beta_k} \cdot n_k,$$

con $\beta_1 > \cdots > \beta_k$ *e* $n_1 > 0$, $n_2 > 0$, $\ldots$, $n_k > 0$ *sono finiti.*

Dimostrazione. Intanto occupiamoci dell'esistenza della forma normale, e procediamo per induzione su $\alpha > 0$. Supponiamo che $\alpha = 1$, la tesi è vera in modo banale; sia dunque $\alpha > 1$. Osserviamo che esistono γ tali che $\omega^\gamma > \alpha$, ad esempio

$$\omega^{\alpha+1} > \omega^\alpha \geq \alpha.$$

Sia $\beta = \min\{\xi \mid \omega^\xi > \alpha\}$: si noti che non può essere limite sennò $\alpha < \omega^\beta = \bigcup_{\gamma<\beta} \omega^\gamma$ e quindi esisterebbe $\gamma < \beta$ tale che $\alpha < \omega^\gamma$, assurdo per la minimalità di β. Dunque $\beta = \delta + 1$. Ora osserviamo che

$$\omega^\delta \leq \alpha < \omega^{\delta+1};$$

dunque possiamo dividere α per ω^δ e ottenere

$$\alpha = \omega^\delta \cdot m + \rho$$

con $\rho < \omega^\delta \leq \alpha$. In effetti $m < \omega$ (ossia è un naturale) sennò $\alpha \geq \omega^\delta \cdot m \geq \omega^\delta \cdot \omega = \omega^{\delta+1} > \alpha$. Se $\rho = 0$ abbiamo finito, altrimenti si applica l'ipotesi induttiva a ρ e dunque

$$\rho = \omega^{\beta_1} \cdot n_1 + \ldots + \omega^{\beta_k} \cdot n_k,$$

e dobbiamo mostrare che $\delta > \beta_1$. Se così non fosse

$$\omega^\delta \leq \omega^{\beta_1} \leq \rho.$$

Adesso dobbiamo mostrare l'unicità. Intanto osserviamo che se $\gamma > \beta$ allora $\omega^\beta \cdot n < \omega^\gamma$ per ogni $n < \omega$. Infatti ciò discende da

$$\omega^\beta \cdot n < \omega^\beta \cdot \omega = \omega^{\beta+1} \leq \omega^\gamma.$$

Da ciò discende immediatamente che se $\gamma > \beta_1$ e $\alpha = \omega^{\beta_1} \cdot n_1 + \ldots + \omega^{\beta_k} \cdot n_k$ è la forma normale allora $\omega^\gamma > \alpha$. A questo punto, per l'unicità della forma normale si procede per induzione su $\alpha \geq 1$. Se $\alpha = 1$ la forma $\omega^0 \cdot 1$ è chiaramente unica. Adesso supponiamo

$$\alpha = \omega^{\beta_1} \cdot n_1 + \ldots + \omega^{\beta_k} \cdot n_k = \omega^{\gamma_1} \cdot m_1 + \ldots + \omega^{\gamma_h} \cdot m_h.$$

Da tutta l'osservazione precedente si ha intanto che $\beta_1 = \gamma_1$ e si pone per comodità $\delta = \omega^{\beta_1} = \omega^{\gamma_1}$, $\sigma = \omega^{\beta_2} \cdot n_2 + \ldots + \omega^{\beta_k} \cdot n_k$ e $\rho = \omega^{\gamma_2} \cdot m_2 + \ldots + \omega^{\gamma_h} \cdot m_h$. Quindi si può scrivere

$$\alpha = \delta \cdot n_1 + \sigma = \delta \cdot m_1 + \rho,$$

e visto che $\sigma, \rho < \delta$ si ha, per il teorema di divisione, che $n_1 = m_1$ e che $\sigma = \rho$. A questo punto si conclude molto agevolmente.

Capitolo 8

Ordinabilità e aleph

Nei capitoli precedenti abbiamo iniziato l'indagine riguardo alla cardinalità degli insiemi infiniti. Benché abbiamo già provato alcuni risultati che coinvolgono il concetto di $|X|$, la cardinalità di un insieme X, non abbiamo ancora definito formalmente $|X|$ in sé. Quando abbiamo dato le prime nozioni sull'aritmetica cardinale avevamo fatto l'assunzione che tali cardinali esistessero e che ad ogni insieme si possa associare uno e un solo cardinale, adesso è arrivato il momento di dimostrarlo: in questo capitolo considereremo la questione di trovare "rappresentanti" per le cardinalità. Abbiamo generalizzato i numeri naturali e abbiamo mostrato che i risultanti numeri ordinali hanno molte proprietà simili a quelle dei numeri naturali, in particolare le prove per induzione e le definizioni per ricursione sono sempre possibili. Tuttavia gli ordinali non rappresentano le cardinalità, ma rappresentano invece i tipi d'ordine. E proprio perché un insieme infinito può essere ordinato in diversi modi, ci saranno diversi numeri ordinali della stessa cardinalità, ad esempio

$$|\omega| = |\omega + 1| = |\omega + \omega| = |\omega \cdot \omega| = \aleph_0.$$

Per scegliere uno degli ordinali come rappresentante di cardinalità di un insieme infinito e ben ordinabile, prenderemo semplicemente il più piccolo ordinale della data cardinalità.

8.1 Lemma di Zorn e teorema di Zermelo

Abbiamo accennato alla fine dell'introduzione precedente che prenderemo un rappresentante per la cardinalità per gli insiemi ben ordinabili. Abbiamo già accennato che la possibilità di bene ordinare ogni insieme è data dal teorema di Zermelo, per il quale è necessario l'assioma della scelta. Abbiamo già anche detto che l'assioma della scelta *equivale* al teorema di Zermelo, ma per ora abbiamo mostrato

solo che se vale il teorema di Zermelo allora vale l'assioma della scelta. In questo paragrafo mostreremo l'altra implicazione, passando però anche attraverso il lemma di Zorn. Il nostro programma è il seguente:

$$\text{assioma di scelta} \Longrightarrow \text{lemma di Zorn} \Longrightarrow \text{teorema di Zermelo},$$

e avendo già mostrato che "teorema di Zermelo $\Longrightarrow$ assioma di scelta" si ha che tutti e tre i teoremi scritti sopra sono equivalenti.
Il lemma di Zorn è un risultato sugli ordini parziali equivalente all'assioma della scelta (sulla base degli altri assiomi della teoria degli insiemi). Esso trova molte applicazioni in matematica (esistenza di basi di spezi vettoriali di dimensione infinita, esistenza di ideali massimali in anelli, ecc...). Per il lemma ci servono delle definizioni:

Definizione 8.1.1. Sia $(A, <)$ un ordine parziale e sia $B \subseteq A$. Diremo che B è una *catena* se per ogni $a, b \in B$ si ha $a < b$ o $b < a$.[1]

Definizione 8.1.2. Un elemento $a \in A$ viene detto un *maggiorante* della catenza $B \subseteq A$ se per ogni $b \in B$ si ha $b \leq a$.

Ricordiamo che un elemento $a \in A$ è *massimale* se non esistono $b \in A$ tali che $b > a$. 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 la definizione di massimale con quella di massimo: di elementi massimi ce ne può essere al più uno e se esiste un massimo esso è anche massimale. Se $(A, <)$ è un ordine totale il concetto di massimo e di massimale coincidono.

Definizione 8.1.3. Dato un ordine parziale $(A, <)$ diciamo che $B \subseteq A$ è una *catena bene ordinata* se B è una catena che è anche un buon ordine (rispetto all'ordine indotto). Diciamo inoltre che B è una catena bene ordinata *non prolungabile* se non esiste alcun $a \in A$ che maggiora strettamente tutti gli elementi di B (ovvero B non ha maggioranti, o se ne ha uno esso appartiene a B ed è il massimo di B).

Teorema 8.1.1 (lemma di Zorn)**.** *Sia $(A, <)$ un ordine parziale in cui ogni catena ha un maggiorante. Allora esiste un elemento massimale in A.*

Dimostrazione. L'idea è di definire una catena bene ordinata $B \subseteq A$ più lunga possibile e di prendere come elemento massimale un maggiorante di tale catena. Per la dimostrazione ci serve il seguente lemma:

Lemma 8.1.1. *Sia $(A, <)$ un ordine parziale. Allora esiste una catena bene ordinata D di $(A, <)$ non prolungabile.*

[1] ossia se è un ordine totale rispetto all'ordine indotto da $<$ su B.

Dimostrazione. In base all'assioma della scelta, esiste una funzione f che associa ad ogni sottoinsieme proprio X di A un elemento $f(X) \in X$. Dato un sottoinsieme B di A e $b \in B$ si definisce B^b l'insieme degli elementi di A che sono maggiori di ogni elemento minore di b, ossia

$$B^b = \{a \in A \mid (\forall c \in B)(c < b)(a > c)\}.$$

Diremo poi che B è una f–catena se B è una catena bene ordinata con l'ulteriore proprietà che per ogni $b \in B$ si ha che $b = f(B^b)$.
Dimostriamo ora che se B e C sono due f–catene, allora una delle due è un segmento iniziale dell'altra. A tal fine consideriamo l'unione D di tutti segmenti iniziali comuni di B e C:

$$D = \bigcup_{\substack{S \subseteq_i B \\ S \subseteq_i C}} S.$$

Tale D è evidentemente il più grande segmento iniziale comune a B e C. Ci basta dimostrare che $D = B$ oppure $D = C$. Se così non fosse, D sarebbe propriamente incluso sia in B che in C. Possiamo allora considerare

$$a = \min(B - D) \quad \text{e} \quad b = \min(C - D).$$

Siccome B e C sono f–catene, allora $a = f(B^a)$ e $b = f(C^b)$. Ma evidentenemente $B_a = D = C_b$, e quindi $B^a = C^b$ perché il primo è l'insieme dei maggioranti di B_a e il secondo è l'insieme dei maggioranti di $C_b = B_a$. Ma allora segue che $a = f(B^a) = f(C^b) = b$, e ciò è assurdo perché allora $a \in D$, essendo $B_a \cup \{a\} = C_b \cup \{b\}$ un segmento iniziale comune alle due catene B e C.
Sia $X \subseteq A$ l'unione di tutte le f–catene. Per il teorema sulle unioni di buoni ordini di cui uno è segmento iniziale dell'altro sappiamo che X è ancora una catena ben ordinata, di cui ogni f–catena è segmento iniziale. Inoltre X è pure una f–catena in quanto per ogni $d \in X$ esiste una f–catena B con $d \in B$ e otteniamo $d = f(B^d) = f(X^d)$ (essendo $X^d = B^d$).
Per finire, dobbiamo mostrare che X non è prolungabile, ossia che non esiste alcun $a \in A$ che maggiora strettamente tutti gli elementi di X. Se così non fosse, l'insieme M di tali a sarebbe non vuoto. Ma allora $X \cup \{f(M)\}$ è ancora una f–catena, contraddicendo il fatto che X è l'unione di tutte le f–catene e $f(M) \notin X$. □

Torniamo ora alla dimostrazione del lemma di Zorn. Sia X una catena bene ordinata non prolungabile in $(A, <)$, che esiste per il lemma appena mostrato. Per le ipotesi del lemma di Zorn X ha un maggiorante x, che evidentemente deve appartenere ad X perché altrimenti potremmo prolungare X con tale elemento. Inoltre tale $x \in X$ deve essere un elemento massimale di A: se così non fosse esisterebbe $a > x$, ma $X \cup \{a\}$ sarebbe un prolungamento di X, assurdo. □

Teorema 8.1.2 (teorema di Zermelo)**.** *Ogni insieme X è ben ordinabile.*

Dimostrazione. Vogliamo dimostrare l'esistenza di un buon ordinamento su X. Sia P l'insieme di tutte le coppie della forma $(A, <)$ dove A è un sottoinsieme di X e $<$ 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 $\prec$:

$$(A, <) \preceq (A', <') \iff A \subseteq_i A' \text{ e } <=<'|_A.$$

In base al teorema sui limiti di buoni ordini ogni catena in $(P, \preceq)$ ha un maggiorante, e quindi per il lemma di Zorn esiste un elemento massimale $(M, <)$ in P. Per finire dimostriamo che $M = X$. Nel caso contrario sia $a \in X - M$, e definiamo un buon ordinamento $<'$ su $M \cup \{a\}$ mantenendo su M il precedente ordinamento $<$ e stabilendo che a è maggiore rispetto a $<'$ di ogni elemento di M, ossia

$$<'=< \cup \{(m, a) \mid m \in M\}.$$

Evidentemente $(M, <)$ è un segmento iniziale di $(M \cup \{a\}, <')$, contraddicendo la massimalità di $(M, <)$ in P. □

Con ciò abbiamo mostrato l'equivalenza logica tra assioma della scelta, lemma di Zorn e teorema di Zermelo. Il teorema di Zermelo appena mostrato ha anche un interessantissimo corollario, ossia la tricotomia dei cardinali. In effetti le cardinalità di due insiemi sono sempre confrontabili:

Corollario 8.1.1. *Siano X e Y due insiemi. Allora o $|X| = |Y|$ o $|X| < |Y|$ o $|X| > |Y|$.*

Dimostrazione. Bene ordiniamo sia X che Y. La tesi segue considerando che i due buoni ordini ottenuti o sono isomorfi, o uno è isomorfo ad un segmento iniziale proprio dell'altro. □

8.2 Ordinali iniziali e numeri di Hartogs

Adesso vedremo come scegliere un rappresentante canonico per ogni insieme che sarà la sua cardinalità, e nell'introduzione al capitolo abbiamo detto che ciò può essere fatto per ogni insieme ben ordinabile. Alla luce del precedente paragrafo se si accetta l'assioma della scelta l'esistenza della cardinalità è assicurata per ogni insieme (giacché ogni insieme è ben ordinabile), mentre se non si accetta l'assioma dovremmo specificare sempre "per ogni insieme ben ordinabile". Visto che noi accetteremo l'assioma della scelta affermeremo che ogni insieme ha un unico cardinale ad esso associato.

Definizione 8.2.1. Un ordinale α si dice *iniziale* se non è equipotente ad alcun $\beta < \alpha$.

Esempio 8.2.1. Ogni ordinale finito è un ordinale iniziale, ω è un ordinale iniziale, in quanto non è equipotente a nessun numero naturale. Invece $\omega+1$ non è iniziale, in quanto $|\omega| = |\omega + 1|$. Similmente nessuno tra

$$\omega + 2,\ \omega + 3,\ \omega + \omega,\ \omega \cdot \omega,\ \omega^{\omega},\ \ldots$$

è un ordinale iniziale.

Teorema 8.2.1. *Ogni insieme X è equipotente ad uno e un solo ordinale iniziale.*

Dimostrazione. Bene ordiniamo X grazie al teorema di Zermelo. Come sappiamo, X è isomorfo ad un certo ordinale α; basta considerare α_0 il minimo ordinale della stessa cardinalità di α (esiste per il principio del minimo). Allora α_0 è un ordinale iniziale per minimalità: infatti se $|\alpha_0| = |\beta|$ per qualche $\beta < \alpha$ avremmo $|X| = |\beta|$, e ciò è assurdo.
Se $\alpha_0 \neq \alpha_1$ sono due ordinali iniziali, questi non possono essere equipotenti in quanto sennò avremmo $|\alpha_0| = |\alpha_1|$ e, per esempio, $\alpha_1 < \alpha_0$, e ciò contraddice il fatto che α_0 sia iniziale. Questo prova l'unicità. □

Definizione 8.2.2. Se X è un insieme chiameremo *cardinalità* di X (o numero cardinale di X), e lo denoteremo con $|X|$, l'unico ordinale iniziale cui X è equipotente.

Osservazione 8.2.1. Notiamo che secondo la definizione precedente $|X| = n$ per ogni X finito di n elementi e $|X| = \omega$ per ogni insieme X numerabile.

Secondo il teorema precedente le cardinalità degli insiemi sono precisamente gli ordinali iniziali. Una domanda che a questo punto sorge spontanea è la seguente: esistono insiemi ben ordinati non numerabili? Abbiamo visto grazie al teorema di Zermelo che possiamo bene ordinare ogni insieme, ma ciò richiede l'assioma della scelta. Adesso mostreremo l'esistenza di tali insiemi indipendentemente dall'assioma della scelta, ed anzi dimostreremo che ne possiamo creare di arbitrariamente grandi. Introduciamo la *funzione classe di Hartogs*. Sia A un insieme qualunque, e definiamo

$$\mathbb{H}(A) = \{\alpha \text{ ordinale} \mid |\alpha| \leq |A|\}.^{2}$$

Intanto, tale collezione di ordinali è un insieme? L'intuizione, grazie al principio di limitazione delle grandezza, ci suggerisce che $\mathbb{H}(A)$ sia in effetti un insieme. Ora però dimostriamolo formalmente:

[2] abbiamo parlato di funzione classe perché, nonostante come vedremo fra un attimo $\mathbb{H}(A)$ sia un insieme per ogni A, il dominio di $\mathbb{H}$ è una classe propria perché è la classe di tutti gli insiemi.

Proposizione 8.2.1. *La classe $\mathbb{H}(A)$ è un insieme.*

Dimostrazione. Definiamo la classe

$$\Gamma = \{(X, \leq_X) \mid X \subseteq A \text{ e } \leq_X \text{ è un buon ordine su } X\}.$$

Visto che $\Gamma \subseteq \mathcal{P}(A) \times \mathcal{P}(A \times A)$, per l'assioma di separazione Γ è in realtà un insieme. Ad ogni elemento $(X, \leq_X) \in \Gamma$ corrisponde uno ed un solo ordinale ad esso isomorfo. Dunque per l'assioma di rimpiazzamento sarà un insieme anche

$$\hat{\Gamma} = \{\gamma \text{ ordinale} \mid \gamma \cong (X, \leq_X) \text{ con } X \in \Gamma\}.$$

A questo punto basta dimostrare che $\hat{\Gamma} = \mathbb{H}(A)$, e lo faremo mostrando la doppia inclusione. Supponiamo che $\gamma \in \mathbb{H}(A)$, allora esiste $f : \gamma \to A$ iniettiva; preso $X = \operatorname{imm} f$ e ordinato questo insieme per eredità da γ si ha $(X, \leq_X) \cong \gamma$. Viceversa supponiamo che $\gamma \in \hat{\Gamma}$, allora esiste $\psi : \gamma \to (X, \leq_X)$ isomorfismo di ordini; allora ψ è una bigezione e si ha $|\gamma| = |X| \leq |A|$, da cui $\gamma \in \mathbb{H}(A)$. □

Lemma 8.2.1. *Valgono le seguenti proprietà della funzione di Hartogs:*
(1) $\mathbb{H}(A)$ è un ordinale;
(2) $|\mathbb{H}(A)| \not\leq |A|$;
(3) $\mathbb{H}(A)$ è un cardinale, cioè un ordinale iniziale.

Dimostrazione. (1) Intanto $\mathbb{H}(A)$ è un insieme di ordinali, pertanto esso è un ordinale se e solo se è transitivo. Supponiamo $\beta \in \gamma \in \mathbb{H}(A)$, allora esiste una funzione iniettiva $f : \gamma \to A$; poi $\beta \in \gamma$ significa che $\beta \subseteq \gamma$ e $f|_\beta : \beta \to A$ è iniettiva. Dunque $\beta \in \mathbb{H}(A)$.
(2) Se per assurdo esistesse $f : \mathbb{H}(A) \to A$, avremmo $\mathbb{H}(A) \in \mathbb{H}(A)$ e ciò è assurdo.
(3) Sia $\gamma < \mathbb{H}(A)$, cioè $\gamma \in \mathbb{H}(A)$. Se fosse $|\gamma| = |\mathbb{H}(A)|$ allora $|\mathbb{H}(A)| \leq |A|$ per definizione di $\mathbb{H}(A)$, ma abbiamo appena visto che ciò non è possibile. □

Si faccia attenzione a questo fatto importante. La proprietà (2) del precedente lemma ci dice che non può esistere una funzione iniettiva da $\mathbb{H}(A)$ ad A, e ciò lo scriviamo con $|\mathbb{H}(A)| \not\leq |A|$. Ciò però *non* significa che $|\mathbb{H}(A)| > |A|$ per ogni insieme A: infatti abbiamo visto che la relazione di tricotomia tra cardinali si ha solo se si assume l'assioma della scelta.
Però c'è un caso particolare in cui ciò è vero, che peraltro è quello che a noi interessa, che è il caso in cui l'insieme A in questione sia un ordinale. Se infatti α è un ordinale allora, visto che $\alpha \not\leq \mathbb{H}(\alpha)$, deve essere necessariamente

$$|\mathbb{H}(\alpha)| = \mathbb{H}(\alpha) > |\alpha|,$$

in quanto invece sugli ordinali la tricotomia è valida, e lo è senza assumere l'assioma della scelta. Adesso mostriamo che in realtà $\mathbb{H}(\alpha)$, tra tutti i cardinali più grandi di $|\alpha|$, è quello più piccolo[3].

[3] osserviamo che cardinali più grandi di $|\alpha|$ ce ne sono, basta prendere $2^{|\alpha|} = |\mathcal{P}(\alpha)|$.

Proposizione 8.2.2. *Sia α un ordinale; $\mathbb{H}(\alpha)$ è il minimo cardinale tale che $\mathbb{H}(\alpha) > |\alpha|$.*

Dimostrazione. Intanto vale $\mathbb{H}(\alpha) > |\alpha|$ per quanto osservato subito prima della proposizione. Supponiamo per assurdo che la tesi sia falsa, allora esisterà $\beta < \mathbb{H}(\alpha)$ tale che $|\beta| > |\alpha|$. Ma $\beta < \mathbb{H}(\alpha)$, tra ordinali significa $\beta \in \mathbb{H}(\alpha)$, e il fatto che $|\beta| > |\alpha|$ è assurdo per come è stata definita $\mathbb{H}(\alpha)$. □

Da un qualunque ordinale iniziale, dunque, sappiamo trovare un ordinale iniziale *strettamente* più grande, e di cardinalità la più piccola tra tutte quelle più grandi. Per rispondere alla domanda posta all'inizio del paragrafo osserviamo che dunque $\mathbb{H}(\omega) > \omega$, e poniamo per definizione $\mathbb{H}(\omega) = \omega_1$: questo sarà il più piccolo ordinale (ordinale iniziale, quindi cardinale) non numerabile. In questo modo si possono generare numeri ordinali sempre più grandi per ricursione. Definiamo infatti:

$$\begin{cases} \omega_0 = \omega \\ \omega_{\alpha+1} = \mathbb{H}(\omega_\alpha) \ \text{ per ogni } \alpha \\ \omega_\alpha = \bigcup_{\beta<\alpha} \omega_\beta \ \text{ per ogni } \alpha \text{ ordinale limite.} \end{cases}$$

Per quanto già abbiamo avuto modo di dire varrà chiaramente che $|\omega_{\alpha+1}| > |\omega_\alpha|$ per ogni α ordinale, e dunque $|\omega_\alpha| < |\omega_\beta|$ se $\alpha < \beta$.
In realtà la successione che abbiamo generato è una successione composta interamente da cardinali infiniti, e di più, ogni cardinale infinito è della forma ω_α per qualche α. Mostriamo questi due fatti:

Teorema 8.2.2. *ω_α è un ordinale iniziale infinito per ogni α ordinale.*

Dimostrazione. Procediamo per induzione su α. Se $\alpha = 0$ o α è un successore la tesi è banale: nel primo caso perché $\omega_0 = \omega$, nel secondo perché la funzione di Hartogs ha come immagine un cardinale, ed è infinito perché strettamente più grande del precedente.
L'unico caso non banale è il caso in cui α sia un limite. Il fatto che ω_α sia un ordinale infinito è del tutto ovvio perché è un estremo superiore di ordinali e dunque è un ordinale, e avrà cardinalità più grande di ogni ω_β con $\beta < \alpha$. Dobbiamo dunque mostrare che l'estremo superiore di ordinali iniziali è ancora un ordinale iniziale. Supponiamo che $\bigcup_{\beta<\alpha} \omega_\beta$ non sia iniziale, allora esiste un ordinale iniziale $\gamma < \omega_\alpha$ tale che $|\gamma| = |\omega_\alpha|$. Ma se $\gamma < \omega_\alpha$ allora per definizione di estremo superiore esisterà un $\beta < \alpha$ tale che $\gamma < \omega_\beta$. Ma allora

$$|\omega_\alpha| = |\gamma| \leq |\omega_\beta| \leq |\omega_\alpha|,$$

da cui $|\gamma| = |\omega_\beta|$. Ciò è assurdo in quanto ω_β è iniziale e quindi non può essere isomorfo ad un ordinale più piccolo. □

Teorema 8.2.3. *Se Ω è un ordinale iniziale infinito allora $\Omega = \omega_\alpha$ per qualche α ordinale.*

Dimostrazione. Intanto, una semplice induzione su α mostra che $\alpha \leq \omega_\alpha$ per ogni α (il lettore provi i dettagli). Quindi, per ogni ordinale iniziale infinito Ω esiste un ordinale α tale che $\Omega < \omega_\alpha$ (basta prendere $\alpha = \Omega + 1$). Quindi per il punto (1) è sufficiente provare il seguente fatto: per ogni ordinale iniziale infinito $\Omega < \omega_\alpha$ esiste qualche $\gamma < \alpha$ tale che $\Omega = \omega_\gamma$; mostriamolo per induzione su α. L'asserto è banalmente vero se $\alpha = 0$. Supponiamo $\alpha = \beta + 1$ allora

$$\Omega < \omega_\alpha = \mathbb{H}(\omega_\beta)$$

implica che $|\Omega| \leq |\omega_\beta|$: allora avremo che $\Omega = \omega_\beta$ e quindi basta porre $\gamma = \beta$, o altrimenti abbiamo $\Omega < \omega_\beta$, che permette di concludere grazie all'ipotesi induttiva. Se α è un ordinale limite allora

$$\Omega < \omega_\alpha = \bigcup_{\beta<\alpha} \omega_\beta$$

e ciò garantisce l'esistenza di un $\beta < \alpha$ tale che $\Omega < \omega_\beta$. Ancora l'ipotesi induttiva ci permette di concludere. □

Visto che sappiamo già che ogni ω_α è un ordinale iniziale infinito la conclusione della sezione è la seguente: ogni insieme (o ogni insieme bene ordinabile se non si assume la scelta) è equipotente ad un unico ordinale iniziale, e gli ordinali iniziali infiniti formano una sequenza ω_α, ove α varia su tutti gli ordinali. Gli ω_α sono tutti e soli gli ordinali iniziali infiniti. In altre parole l'applicazione che manda α in ω_α è una corrispondenza biunivoca (!) tra la classe degli ordinali e la classe dei cardinali infiniti. È di norma chiamare tali ω_α con il nome di *aleph*, e poniamo

$$\aleph_\alpha = \omega_\alpha.$$

Adesso un'ultima osservazione riguardo alle operazioni. A questo punto abbiamo definito delle operazioni sia sui numeri cardinali che sui numeri ordinali: queste concidono fintanto che gli ordinali coinvolti sono i numeri naturali, invece possono differire quando si ha a che fare con ordinali infiniti. Per esempio $\omega_0 + \omega_0 = \omega_0$ se il $+$ sta per l'addizione cardinale, mentre $\omega_0 + \omega_0 \neq \omega_0$ se il $+$ sta per l'addizione ordinale. Inoltre l'addizione fra cardinali è commutativa, mentre non lo è quella tra ordinali. Per evitare confusione utilizzeremo il simbolismo con gli ω quando vorremo parlare di ordinali, mentre utilizzeremo il simbolismo con gli aleph quando vorremo parlare di cardinali. Quindi per esempio

$$\omega_0 + \omega_0 = \bigcup_{n<\omega_0} (\omega_0 + n) > \omega_0 \quad \text{e} \quad 2^{\omega_0} = \omega_0,$$

mentre invece

$$\aleph_0 + \aleph_0 = \aleph_0 \quad \text{e} \quad 2^{\aleph_0} > \aleph_0.$$

8.3 Addizione e moltiplicazione di aleph

Ricordiamo rapidamente le definizione delle operazioni tra numeri cardinali. Siano κ e λ due cardinali con $\kappa = |X|$ e $\lambda = |Y|$. Abbiamo definito la somma $\kappa + \lambda$ come la cardinalità di $X \cup Y$ se questi erano disgiunti[4], possiamo scrivere:

$$\kappa + \lambda = |X \sqcup Y|.$$

Inoltre abbiamo definito il prodotto grazie al prodotto cartesiano di X e Y, infatti per definizione

$$\kappa \cdot \lambda = |X \times Y|.$$

Abbiamo anche già mostrato che le precedenti definizioni sono indipendenti dalla scelta del rappresentante di equipotenza per i due cardinali. Abbiamo anche dimostrato molte proprietà di queste operazioni:

$$\kappa + \lambda = \lambda + \kappa, \qquad \kappa \cdot \lambda = \lambda \cdot \kappa,$$

$$\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu, \qquad \kappa \cdot (\lambda \cdot \mu) = (\kappa \cdot \lambda) \cdot \mu,$$

$$\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu.$$

Se κ e λ sono cardinali finiti allora non dobbiamo dire niente, in quanto le operazioni di somma e prodotto coincidono con le ordinarie operazioni artimetiche. Quindi quello che tratteremo in questo paragrafo è il caso dei cardinali infiniti, ossia degli aleph: le operazioni infatti differiscono in moso sostanziale da quelle sugli interi, tant'è che ad esempio non conferiscono alcuna struttra di anello. Ci siamo già resi conto di questo fatto perché abbiamo già mostrato che

$$\aleph_0 + n = \aleph_0$$

per ogni n numero naturale. Ma di più, abbiamo anche mostrato che

$$\aleph_0 + \aleph_0 = \aleph_0,$$

in quanto unire due insiemi numerabili produce ancora un insieme numerabile. Inoltre, per quanto riguarda il prodotto, sappiamo ad esempio che

$$\aleph_0 \cdot \aleph_0 = \aleph_0,$$

in quanto il prodotto cartesiano di due insiemi numerabili è numerabile. Adesso proveremo un teorema generale che ci consentirà di determinare completamente il risultato di addizione e moltiplicazione tra aleph.

[4] sennò c'è sempre il solito artifizio di prendere $X \times \{0\}$ e $Y \times \{1\}$, che hanno il pregio di avere le stesse cardinalità degli insiemi di partenza ma di essere disgiunti.

Teorema 8.3.1. *Per ogni α ordinale si ha $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$.*

Dimostrazione. Proveremo il teorema per induzione transfinita. Per ogni α costruiremo un certo buon ordinamento $\prec$ sull'insieme $\omega_\alpha \times \omega_\alpha$ e, usando l'ipotesi induttiva $\aleph_\beta \cdot \aleph_\beta \leq \aleph_\beta$ per ogni $\beta < \alpha$, mostreremo che il tipo d'ordine di $(\omega_\alpha \times \omega_\alpha, \prec)$ è al massimo ω_α. Da ciò seguirà $\aleph_\alpha \cdot \aleph_\alpha \leq \aleph_\alpha$. Essendo ovvia l'altra disuguaglianza avremo la tesi. Definiamo intanto l'ordinamento uniformemente rispetto ad α, cioè definiremo $\prec$ sulle coppie di ordinali e mostreremo che $\prec$ bene ordina $\omega_\alpha \times \omega_\alpha$ per ogni α.

$$(\alpha_1, \alpha_2) \prec (\beta_1, \beta_2) \iff \begin{cases} \max\{\alpha_1, \alpha_2\} < \max\{\beta_1, \beta_2\}, \text{ oppure} \\ \max\{\alpha_1, \alpha_2\} = \max\{\beta_1, \beta_2\} \text{ e } \alpha_1 < \beta_1, \text{ oppure} \\ \max\{\alpha_1, \alpha_2\} = \max\{\beta_1, \beta_2\}, \ \alpha_1 = \beta_1 \text{ e } \alpha_2 < \beta_2 \end{cases}.$$

Lasciamo al lettore il compito di dimostrare che $\prec$ è un ordine stretto totale: dovrà dimostrare che $\prec$ è asimmetrico, transitivo e totale, e tutte queste seguono facilmente dalla definizione. Noi mostreremo che $\prec$ è un buon ordinamento. Sia dunque X un sottoinsieme non vuoto di coppie di ordinali e sia

$$\delta = \min\{\max\{\alpha, \beta\} \mid (\alpha, \beta) \in X\},$$

che esiste in quanto X è non vuoto e dunque neanche l'insieme di cui stiamo prendendo il minimo. Poi poniamo

$$Y = \{(\alpha, \beta) \in X \mid \max\{\alpha, \beta\} = \delta\}.$$

Tale insieme $Y \subseteq X$ è non vuoto, e per ogni $(\alpha, \beta) \in Y$ abbiamo $\max\{\alpha, \beta\} = \delta$ per definizione. Inoltre, sempre per costruzione, $\delta < \max\{\alpha', \beta'\}$ per ogni $(\alpha', \beta') \in X - Y$ e dunque $(\alpha, \beta) \prec (\alpha', \beta')$ quando $(\alpha, \beta) \in Y$ e $(\alpha', \beta') \in X - Y$. Dunque il minimo elemento di Y, se esiste, sarà anche il minimo elemento di X. Siano

$$\alpha_0 = \min\{\alpha \mid \exists \beta \text{ tale che } (\alpha, \beta) \in Y\} \quad \text{e} \quad Z = \{(\alpha, \beta) \in Y \mid \alpha = \alpha_0\}.$$

L'insieme $Z \subseteq Y$ è non vuoto e abbiamo $(\alpha, \beta) \prec (\alpha', \beta')$ quando $(\alpha, \beta) \in Z$ e $(\alpha', \beta') \in Y - Z$, dunque cerchiamo un minimo per Z. Sia

$$\beta_0 = \min\{\beta \mid (\alpha_0, \beta) \in Z\}.$$

A questo punto (α_0, β_0) è il minimo di Z, ossia il minimo di Y, ossia il minimo di X. Dunque $\prec$ è un buon ordinamento.
Adesso mostreremo per induzione transfinita su α che vale $|\omega_\alpha \times \omega_\alpha| \leq \aleph_\alpha$, ossia $\aleph_\alpha \cdot \aleph_\alpha \leq \aleph_\alpha$. Sappiamo che $\aleph_0 \cdot \aleph_0 = \aleph_0$, e quindi la nostra tesi è vera nel caso base. Sia adesso $\alpha > 0$ e assumiamo che $\aleph_\beta \cdot \aleph_\beta \leq \aleph_\beta$ per ogni $\beta < \alpha$. Se per assurdo avessimo $\aleph_\alpha \cdot \aleph_\alpha > \aleph_\alpha$ allora esisterebbe $(\alpha_1, \alpha_2) \in \omega_\alpha \times \omega_\alpha$ tale che, detto

$$X = \{(\xi_1, \xi_2) \in \omega_\alpha \times \omega_\alpha \mid (\xi_1, \xi_2) \prec (\alpha_1, \alpha_2)\}$$

avremmo $|X| \geq \aleph_\alpha$. Quindi è sufficiente provare che $|X| < \aleph_\alpha$. Sia $\beta = \max\{\alpha_1, \alpha_2\}+1$, allora $\beta \in \omega_\alpha$ e per ogni $(\xi_1, \xi_2) \in \omega_\alpha \times \omega_\alpha$ abbiamo $\max\{\xi_1, \xi_2\} \leq \max\{\alpha_1, \alpha_2\} < \beta$, così $\xi_1 \in \beta$ e $\xi_2 \in \beta$. In altre parole $X \subseteq \beta \times \beta$. Sia adesso $\gamma < \alpha$ take che $|\beta| \leq \aleph_\gamma$. Allora

$$|X| \leq |\beta \times \beta| = |\beta| \cdot |\beta| \leq \aleph_\gamma \cdot \aleph_\gamma,$$

e per ipotesi induttiva $\aleph_\gamma \cdot \aleph_\gamma \leq \aleph_\gamma$. Quindi $|X| \leq \aleph_\gamma$ e dunque $|X| < \aleph_\alpha$ è provato. Abbiamo raggiunto l'assurdo. La tesi si ottiene dall'osservazione fatta ad inizio dimostrazione. □

Corollario 8.3.1. *Per ogni α e β ordinali tali che $\alpha \leq \beta$ si ha*

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

Inoltre per ogni n numero naturale $n \cdot \aleph_\alpha = \aleph_\alpha$.

Dimostrazione. Abbiamo sempre $\aleph_\beta = 1 \cdot \aleph_\beta \leq \aleph_\alpha \cdot \aleph_\beta$, ed inoltre per il teorema precedente ci dice che se $\alpha \leq \beta$ allora

$$\aleph_\alpha \cdot \aleph_\beta \leq \aleph_\beta \cdot \aleph_\beta \leq \aleph_\beta.$$

Si conclude dunque per il teorema di Cantor–Bernstein. L'altra uguaglianza si prova in modo del tutto analogo. □

Corollario 8.3.2. *Per ogni α e β ordinali tali che $\alpha \leq \beta$ si ha*

$$\aleph_\alpha + \aleph_\beta = \aleph_\beta.$$

Inoltre per ogni n numero naturale $n + \aleph_\alpha = \aleph_\alpha$.

Dimostrazione. Vale sempre $\aleph_\beta = 0 + \aleph_\beta \leq \aleph_\alpha + \aleph_\beta$, ed inoltre per il teorema precedente ci dice che se $\alpha \leq \beta$ allora

$$\aleph_\alpha + \aleph_\beta \leq \aleph_\beta + \aleph_\beta = 2 \cdot \aleph_\beta \leq \aleph_\beta \cdot \aleph_\beta = \aleph_\beta.$$

Si conclude ancora per il teorema di Cantor–Bernstein. L'altra uguaglianza si prova in modo del tutto analogo. □

In parole povere, quando si ha a che fare con cardinali infiniti, nel caso della somma e del prodotto "vince" sempre il cardinale più grande. Volendo riscrivere la tesi dei corollari, per ogni κ e λ infiniti si ha

$$\kappa + \lambda = \kappa \cdot \lambda = \max\{\kappa, \lambda\}.$$

8.3.1 Un'osservazione sull'assioma della scelta

Vogliamo adesso far osservare una correlazione tra quanto visto nel precedente paragrafo e l'assioma della scelta. Il teorema che abbiamo mostrato che afferma $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$ per ogni α ordinale può essere anche riformulato in un altro modo.
Se non si accetta l'assioma di scelta diremo: per ogni insieme infinito A *ben ordinabile* si ha che

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

Infatti bene ordiniamo A con un certo $<$ e dopodiché abbiamo un unico ordinale α cui $(A, <)$ è isomorfo; ma allora esiste un unico cardinale κ equipotente ad α e quindi esiste un unico γ ordinale tale che $\kappa = \aleph_\gamma$. A questo punto basta applicare il teorema 8.3.1.
Se si accetta l'assioma di scelta (AC) possiamo arrivare alla stessa conclusione precedente però *per ogni* insieme infinito A. Infatti ogni tale insieme è ben ordinabile. In effetti tale proprietà non è solo conseguenza dell'assioma di scelta, bensì è una sua formulazione equivalente:

Teorema 8.3.2. *Vale l'assioma di scelta AC se e solo se per ogni insieme infinito A si ha $|A \times A| = |A|$.*

Dimostrazione. ($\Longrightarrow$) È quanto abbiamo detto prima del teorema.
($\Longleftarrow$) Facciamo vedere che ogni insieme infinito A è ben ordinabile (ossia il teorema di Zermelo), che tanto è equivalente all'assioma della scelta. La classe $A \cup \mathbb{H}(A)$ è un insieme, in quanto lo sono A e $\mathbb{H}(A)$ e quindi lo è la loro unione; per ipotesi

$$|(A \cup \mathbb{H}(A)) \times (A \cup \mathbb{H}(A))| = |A \cup \mathbb{H}(A)|.$$

Senza perdere di generalità possiamo supporre $\mathbb{H}(A) \cap A = \emptyset$ (al massimo si fa il solito $\mathbb{H}(A) \times \{0\}$ e $A \times \{1\}$). Dall'ipotesi, per restrizione, segue che esiste una funzione iniettiva

$$f : \mathbb{H}(A) \times A \to \mathbb{H}(A) \cup A.$$

Adesso per ogni $a \in A$ consideriamo l'applicazione

$$\begin{array}{rccc} f_a : & \mathbb{H}(A) & \longrightarrow & \mathbb{H}(A) \cup A \\ & \beta & \longmapsto & f(\beta, a) \end{array},$$

che è iniettiva perché può essere vista come restrizione di f. Visto che $|\mathbb{H}(A)| \not\leq |A|$ abbiamo che $\operatorname{imm} f_a \not\subseteq A$, dunque esiste

$$\beta_a = \min\{\beta \in \mathbb{H}(A) \mid \beta \in \operatorname{imm} f_a\} = \min(\operatorname{imm} f_a \cap \mathbb{H}(A)).$$

Adesso possiamo considerare l'applicazione $\varphi : A \to \mathbb{H}(A)$ che associa ad ogni $a \in A$ associa β_a: questa è chiaramente iniettiva e dunque si può bene ordinare A per eredità da $\operatorname{imm} \varphi \subseteq \mathbb{H}(A)$ (che è ben ordinato perché sottoinsieme di un ben ordinato). □

Capitolo 9

Aritmetica cardinale e cofinalità

9.1 Somme e prodotti infiniti

Nei capitoli precedenti abbiamo introdotto le operazioni tra numeri cardinali; ha senso però generalizzare tali operazioni e considerare somme e prodotti di quantità infinite di cardinali. Per esempio, vorremmo che

$$\underbrace{1+1+\cdots}_{\aleph_0 \text{ volte}} = \aleph_0,$$

o più in generale che

$$\underbrace{\kappa+\kappa+\cdots}_{\lambda \text{ volte}} = \kappa \cdot \lambda.$$

La somma di due cardinali κ_1 e κ_2 era definita come cardinalità di $A_1 \cup A_2$, dove A_1 e A_2 sono due insiemi qualsiasi disgiunti e di cardinalità rispettivamente κ_1 e κ_2. È proprio questo il modo di generalizzare la somma:

Definizione 9.1.1. Sia $\langle A_i \mid i \in I \rangle$ una sequenza di insiemi a due a due disgiunti, e sia $|A_i| = \kappa_i$ per ogni $i \in I$. Definiamo la *somma* della sequenza $\langle \kappa_i \mid i \in I \rangle$ come

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

La definizione della somma utilizza particolari insiemi A_i (con $i \in I$). Nel caso finito, che si ha quando $I = \{1, 2\}$, abbiamo visto che la somma di due cardinali non dipende da quali insiemi di quelle cardinalità di prendano. In effetti, nel caso generale in cui I è un arbitrario insieme di indici, è necessario l'assioma della scelta per poter dimostrare la buona definizione. Senza l'assioma della scelta non possiamo escludere la seguente (paradossale) possibilità: potrebbero esistere due sequenze

$$\langle A_n \mid n \in \mathbb{N} \rangle \quad \text{e} \quad \langle A'_n \mid n \in \mathbb{N} \rangle$$

di insiemi a due a due disgiunti e ciascuno di essi con due elementi ma tali che $\bigcup_{n=0}^{\infty} A_n$ e $\bigcup_{n=0}^{\infty} A'_n$ hanno diverse cardinalità (!).
Per questo motivo, e anche per altri che fra poco saranno chiari, d'ora innanzi faremo uso dell'assioma della scelta AC anche se non lo diremo esplicitamente.

Lemma 9.1.1. *Siano $\langle A_i \mid i \in I\rangle$ e $\langle A'_i \mid i \in I\rangle$ due famiglie di insiemi disgiunti a due a due e tali che $|A_i| = |A'_i|$ per ogni $i \in I$. Allora*

$$\left|\bigcup_{i\in I} A_i\right| = \left|\bigcup_{i\in I} A'_i\right|.$$

Dimostrazione. Per ogni $i \in I$ possiamo *scegliere* una mappa biunivoca f_i da A_i a A'_i. In questo modo $\bigcup_{i\in I} f_i$ è una mappa biunivoca da $\bigcup_{i\in I} A_i$ a $\bigcup_{i\in I} A'_i$. □

Il lemma precedente è quanto basta per affermare la buona definizione della somma di cardinali.

Osservazione 9.1.1. Come al solito, potevamo anche dare la definizione senza dire che gli insiemi A_i dovevano essere disgiunti. In tal caso bastava prendere la sequenza $\langle A_i \times \{i\} \mid i \in I\rangle$, e questa è fatta da insiemi disgiunti ma della stessa cardinalità.

Visto che l'unione ha delle buone proprietà quali l'associatività, queste saranno anche ereditate dalla somma di cardinali: lasciamo da provare per esercizio la *proprietà associativa*. Inoltre vale anche la proprietà

$$\kappa_i \leq \lambda_i \quad \forall i \in I \Longrightarrow \sum_{i\in I} \kappa_i \leq \sum_{i\in I} \lambda_i,$$

anch'essa da provare per esercizio (basta trovare una corrispondenza iniettiva dall'unione degli insiemi di cardinalità κ_i a quella degli insiemi di cardinalità λ_i). Osserviamo che se invece $\kappa_i < \lambda_i$ per ogni $i \in I$ non è detto che la relazione di minore stretto valga anche tra le rispettive somme. Basta prendere ad esempio la sequenza $\langle \kappa_n \mid n \in \mathbb{N}\rangle$ con $\kappa_n = 1$ per ogni $n \in N$ e la famiglia $\langle \lambda_n \mid n \in \mathbb{N}\rangle$ tale che $\lambda_n = 2 > \kappa_n$ per ogni $n \in \mathbb{N}$; infatti per essa si ha

$$\sum_{n\in\mathbb{N}} \kappa_n = \aleph_0 = \sum_{n\in\mathbb{N}} \lambda_n.$$

Sapere che risultato dà una somma di cardinali non è molto difficile. Già abbiamo visto che nel caso di due cardinali infiniti avevamo che "vinceva" il più grande, a dire che $\aleph_\alpha \cdot \aleph_\beta = \aleph_\beta$ se $\beta > \alpha$. Un risultato simile permette anche di conoscere la somma di cardinali:

Teorema 9.1.1. *Sia λ un cardinale infinito e siano κ_α con $\alpha < \lambda$ cardinali non nulli. Detto $\kappa = \bigcup_{\alpha<\lambda} \kappa_\alpha$ allora*

$$\sum_{\alpha<\lambda} \kappa_\alpha = \lambda \cdot \bigcup_{\alpha<\lambda} \kappa_\alpha = \lambda \cdot \kappa.$$

Dimostrazione. Visto che $\kappa_\alpha \leq \kappa$ per ogni $\alpha < \lambda$ avremo ovviamente che

$$\sum_{\alpha<\lambda} \kappa_\alpha \leq \sum_{\alpha<\lambda} \kappa = \lambda \cdot \kappa.$$

Dall'altro lato osserviamo che $\lambda = \sum_{\alpha<\lambda} 1 \leq \sum_{\alpha<\lambda} \kappa_\alpha$. Inoltre abbiamo anche $\kappa \leq \sum_{\alpha<\lambda} \kappa_\alpha$: infatti la somma è un maggiorante di ogni κ_α e κ è proprio il minimo di essi. Adesso abbiamo che sia κ che λ sono entrambi minori o uguali della somma, e dunque

$$\kappa \cdot \lambda \leq \sum_{\alpha<\lambda} \kappa_\alpha.$$

La tesi si ha grazie al teorema di Cantor–Bernstein. □

Adesso veniamo al prodotto di cardinali. Ricordiamo che anche il prodotto era già stato definito fra due cardinali come cardinalità del prodotto cartesiano; ossia se $\kappa_1 = |A_1|$ e $\kappa_2 = |A_2|$ allora si definisce $\kappa_1 \cdot \kappa_2 = |A_1 \times A_2|$. Abbiamo dato già in capitoli precedenti la nozione di prodotto cartesiano di una sequenza di insiemi come

$$\prod_{i\in I} A_i = \left\{ f : I \to \bigcup_{i\in I} A_i \mid (\forall i \in I)(f(i) \in A_i) \right\}.$$

Questa definizione mediante le funzioni in realtà è comoda per il prodotto generico, però non è la stessa data come insieme di coppie ordinate per il prodotto $A_1 \times A_2$: in effetti le due nozioni non coincidono, però possiamo trovare una bigezione tra $\prod_{i\in\{1,2\}} A_i$ e $A_1 \times A_2$. Forti di questa premessa generalizziamo il prodotto:

Definizione 9.1.2. Sia $\langle A_i \mid i \in I\rangle$ una sequenza di insiemi e sia $|A_i| = \kappa_i$ per ogni $i \in I$. Definiamo il *prodotto* della sequenza $\langle \kappa_i \mid i \in I\rangle$ come

$$\prod_{i\in I} \kappa_i = \left| \prod_{i\in I} A_i \right|.$$

C'è un'ambiguità di notazione nellla formula appenza scritta: nel membro di destra intendiamo il prodotto cartesiano arbitrario degli insiemi A_i, mentre a destra abbiamo il prodotto come operazione tra cardinali che stiamo definendo. In seguito tanto sarà chiaro dal contesto quale delle due stiamo usando.
Detto ciò bisogna osservare che anche nel caso del prodotto abbiamo dato una buona definizione. Sempre grazie all'assioma della scelta vale il seguente:

Lemma 9.1.2. *Siano $\langle A_i \mid i \in I\rangle$ e $\langle A'_i \mid i \in I\rangle$ due famiglie di insiemi tali che $|A_i| = |A'_i|$ per ogni $i \in I$. Allora*

$$\left|\prod_{i\in I} A_i\right| = \left|\prod_{i\in I} A'_i\right|.$$

Dimostrazione. Per ogni $i \in I$ possiamo *scegliere* una mappa biunivoca f_i da A_i a A'_i. Definiamo la funzione f su $\prod_{i\in I} A_i$ come segue: se $x = \langle x_i \mid i \in I\rangle \in \prod_{i\in I} A_i$ diciamo

$$f(x) = \langle f_i(x_i) \mid i \in I\rangle \in \prod_{i\in I} A'_i.$$

Non è difficile vedere che f è una mappa biunivoca. □

Anche il prodotto infinito gode di molte proprietà di gode l'usuale prodotto tra numeri naturali, ma anche tra due cardinali (le abbiamo già viste nel rispettivo capitolo). Ad esempio, se almeno uno tra i κ_i è nullo allora $\prod_{i\in I} \kappa_i = 0$; inoltre vale nuovamente una *legge associativa*. Inoltre vale ancora che se $\kappa_i \leq \lambda_i$ per ogni $i \in I$ allora

$$\prod_{i\in I} \kappa_i \leq \prod_{i\in I} \lambda_i.$$

Se tutti i fattori κ_i sono uguali ad un certo κ allora abbiamo l'intuitiva proprietà che

$$\prod_{i\in\lambda} \kappa_i = \underbrace{\kappa \cdot \kappa \cdot \cdots}_{\lambda \text{ volte}} = \kappa^\lambda.$$

Inoltre si generalizzano anche delle proprietà delle potenze analoghe a quelle nel caso finito, che sono le seguenti:

$$\left(\prod_{i\in I} \kappa_i\right)^\lambda = \prod_{i\in I} \kappa_i^\lambda \qquad \text{e} \qquad \prod_{i\in I} \kappa^{\lambda_i} = \kappa^{\sum_{i\in I}\lambda_i}.$$

Il lettore dovrebbe, per esercizio, dimostrare tutte queste proprietà: basterà solo applicare le definizioni dei termini che compaiono nelle uguaglianze.
I prodotti infiniti sono più difficili da valutare che delle somme infinite. In certi casi, ad esempio quando dobbiamo calcolare $\prod_{\alpha<\lambda} \kappa_\alpha$, con sequenza crescenti di κ_α il calcolo può essere fatto esplicitamente e si possono provare alcune semplici regole. Vediamo un esempio:

Esempio 9.1.1. Si vuol calcolare $\prod_{0<n<\omega} n = \prod_{n=1}^{\infty} n = 1 \cdot 2 \cdot 3 \cdot \cdots$. Valgono le seguenti due catene di disuguaglianze:

$$\prod_{n=1}^{\infty} n \leq \prod_{n=1}^{\infty} \aleph_0 = \aleph_0^{\aleph_0} = 2^{\aleph_0} \qquad \text{e} \qquad 2^{\aleph_0} = \prod_{n=1}^{\infty} 2 \leq \prod_{n=2}^{\infty} n = \prod_{n=1}^{\infty} n.$$

Dal teorema di Cantor–Bernstein si ha allora che il prodotto richiesto è $2^{\aleph_0}$.

Adesso però mostreremo un teorema molto importante in teoria delle cardinalità: esso non ci dice come calcolare il prodotto di cardinali, ma ci fornisce una disuguaglianza *stretta* tra cardinalità, cosa molto utile in quanto le disuguaglianza strette sono molto difficili da ottenere generalmente.

Teorema 9.1.2 (di König)**.** *Se κ_i e λ_i (con $i \in I$) sono cardinali e se $\kappa_i < \lambda_i$ per ogni $i \in I$ allora*

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

Dimostrazione. In questa dimostrazione, visto che i λ_i sono cardinali ma sono anche insiemi, denoteremo con $\bigotimes$ il prodotto cartesiano, mentre con la produttoria $\prod$ il prodotto tra ordinali. Sia $j \in I$ fissato e si consideri il seguente diagramma:

$$\begin{array}{ccc} \kappa_j & \xrightarrow{\quad f_j \quad} & \lambda_j \\ \Big\downarrow{\scriptstyle I_j} & & \Big\uparrow{\scriptstyle p_j} \\ \bigcup_{i \in I}(\kappa_i \times \{i\}) & \xrightarrow{\quad f \quad} & \bigotimes_{i \in I} \lambda_i \end{array},$$

che ci apprestiamo a spiegare. L'applicazione I_j è una sorta di inclusione nell'unione dei prodotti cartesiani, infatti è l'applicazione che manda $x \in \kappa_j$ in (x, j); l'applicazione p_j invece altro non è che la proiezione sulla j–esima componente. Data un'applicazione

$$f : \bigcup_{i \in I}(\kappa_i \times \{i\}) \longrightarrow \bigotimes_{i \in I} \lambda_i$$

vogliamo mostrare che non può essere surgettiva; da ciò seguirà la tesi. Data tale f avremo un'applicazione f_j che fa commutare il diagramma, ossia $f_j = p_j \circ f \circ I_j$. Intanto, visto che per ipotesi $\kappa_j < \lambda_j$ per ogni $j \in I$ avremo che f_j non può essere surgettiva per ogni $j \in I$. Ma allora per ogni $j \in I$ esisterà un $b_j \in \lambda_j$ tale che $b_j \notin \operatorname{imm} f_j$. Adesso, preso

$$(b_j \mid j \in I) \in \bigotimes_{i \in I} \lambda_i$$

non può appartenere all'immagine di f. Infatti se $(b_j \mid j \in I) = f(x, i) = (f \circ I_i)(x)$ e applichiamo p_i ad entrambi i membri si ha

$$b_i = (p_i \circ f \circ I_i)(x) = f_i(x),$$

e ciò è assurdo perché b_i non stava nell'immagine di f_i. □

Osservazione 9.1.2. Osserviamo che il teorema di König è una generalizzazione del teorema di Cantor: in effetti tale risultato segue in modo facile dalla disuguaglianza appena mostrata. Se κ è un cardinale, infatti, allora

$$\kappa = \sum_{i \in \kappa} 1 < \prod_{i \in \kappa} 2 = 2^{\kappa}.$$

9.1.1 L'ipotesi del continuo

Adesso vogliamo spiegare perché il problema dell'esponenziazione sia così difficile da risolvere (se non impossibile se si pretende di dare una risposta completa). Dal teorema di Cantor sappiamo che vale la disuguaglianza $2^{\aleph_0} > \aleph_0$, in quanto l'insieme dei numeri reali è più che numerabile. Visto che abbiamo introdotto la sequenza degli aleph, possiamo dunque dire che, essendo un cardinale non numerabile, dovrà essere che $2^{\aleph_0} \geq \aleph_1$. Il fatto è che non conosciamo se vale l'uguaglianza o se vale la maggiorazione stretta, o se comunque vale l'uguaglianza con qualche $\aleph_\beta$. In effetti l'ipotesi che

$$2^{\aleph_0} = \aleph_1$$

va sotto il nome di *ipotesi del continuo* e fu avanzata da Georg Cantor, che tentò invano di dimostrarla per diversi anni. Nel 1940 Kurt Gödel fece un passo in avanti, dimostrando che l'ipotesi del continuo non può essere dimostrata falsa usando il sistema di assiomi di Zermelo–Fraenkel (ZF), neppure con l'aggiunta dell'assioma della scelta (AC). D'altra parte, nel 1963 Paul Cohen dimostrò (con nuove tecniche in logica note come tecniche di *forcing*) che l'ipotesi del continuo non può essere neppure dimostrata vera a partire da quegli assiomi. Il risultato complessivo è che l'ipotesi del continuo è indipendente dal sistema di assiomi di Zermelo–Fraenkel e dall'assioma della scelta. Occorre precisare però che entrambi questi risultati partono dall'assunto che gli assiomi di Zermelo–Fraenkel non siano tra loro contraddittori, cosa che si suppone generalmente essere vera. Qualcosa su $2^{\aleph_0}$ si può dire però:

Teorema 9.1.3. *Vale che* $2^{\aleph_0} \neq \aleph_\omega$.

Dimostrazione. Supponiamo per assurdo che $2^{\aleph_0} = \aleph_\omega$. Per ogni $n < \omega$ vale dunque $\aleph_n < 2^{\aleph_0}$, e allora per il teorema di König

$$2^{\aleph_0} = \aleph_\omega = \sum_{n \in \omega} \aleph_n < \prod_{n < \omega} 2^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0},$$

e ciò è assurdo. □

Si possono mostrare anche risultati simili a questo, come vedremo nel prossimo paragrafo; non è comunque noto se valga qualche disuguaglianza tra $2^{\aleph_0}$ e $\aleph_\omega$.

Esiste poi anche una versione generalizzata dell'ipotesi del continuo. Analogamente a quanto detto sopra, l'ipotesi generalizzata del continuo assume che

$$2^{\aleph_\alpha} = \aleph_{\alpha+1}$$

per ogni α ordinale. Per questa ipotesi più generale valgono comunque le stesse considerazioni fatte sopra.

9.2 Cofinalità

Prima di iniziare diamo alcune definizioni di terminologia sui cardinali: diremo che un cardinale infinito $\aleph_\alpha$ è un *successore* se α è un successore; se invece α è un limite allora diremo che $\aleph_\alpha$ è un cardinale *limite*. Se κ è un cardinale infinito $\aleph_\beta$ allora talvolte indicheremo il cardinale successore $\aleph_{\beta+1}$ con κ^+.
Iniziamo ora con una definizione, che è quella che aprirà le porte ad una serie di fondamentali risultati per quanto riguarda l'esponenziazione di cardinali, su cui sappiamo dire ben poco.

Definizione 9.2.1. Siano α e β ordinali. Un'applicazione $f : \alpha \to \beta$ si dice *cofinale* se per ogni $\gamma \in \beta$ esiste una $\delta \in \alpha$ tale che $f(\delta) \geq \gamma$ (diremo talvolta che l'applicazione è *illimitata*).

Esempio 9.2.1. Esiste un'applicazione cofinale da ω in $2^{\aleph_0}$: basta considerare l'immersione canonica e questa sicuramente ha la proprietà richiesta.

Definizione 9.2.2. Sia α un ordinale. La *cofinalità* di α, indicata con $\mathrm{cf}(\alpha)$, è il minimo ordinale β tale che esiste una mappa cofinale da β a α.

Si osservi che, essendo l'identità su α un'applicazione cofinale, abbiamo subito che $\mathrm{cf}(\alpha) \leq \alpha$. Notiamo inoltre che se α è un ordinale successore allora $\mathrm{cf}(\alpha) = 1$: infatti se $\alpha = \beta + 1$ basta prendere l'applicazione $\{0\} \to \alpha$ che manda 0 in β e questa è cofinale.

Esempio 9.2.2. Si ha $\mathrm{cf}(2^{\aleph_0}) = \omega$. Nell'esempio precedente abbiamo mostrato che esiste un'applicazione cofinale da ω in $2^{\aleph_0}$, che è l'immersione canonica. In effetti nessun ordinale più piccolo di ω (che sarebbe finito) può andare in $2^{\aleph_0}$ in modo cofinale, dunque ω è il minimo di essi.

Esempio 9.2.3. Si ha $\mathrm{cf}(\aleph_1) = \mathrm{cf}(\omega_1) = \omega_1$. Certamente vale il minore o uguale come per ogni altro ordinale, adesso mostriamo che non può valere il minore stretto. Preso qualunque $\alpha < \omega_1$, ossia numerabile, ogni funzione $f : \alpha \to \aleph_1$ è limitata. Infatti

$$\sup_{\beta<\alpha} f(\beta) = \bigcup_{\beta<\alpha} f(\beta)$$

è numerabile perché unione numerabile di insiemi numerabili.

Esempio 9.2.4. Si ha $\mathrm{cf}(\aleph_\omega) = \omega$. Questa volta si deve prendere la mappa $f : \omega \to \aleph_\omega$ tale che $n \mapsto \aleph_n$ e osservare che è cofinale. In effetti, ragionando come nell'esempio precedente si mostra che la cofinalità di $\aleph_\omega$ non può essere $< \omega$.

Proposizione 9.2.1. *Per ogni ordinale limite α si ha che* $\mathrm{cf}(\alpha)$ *è un cardinale (infinito).*

Dimostrazione. Sappiamo che esiste un'applicazione $f : \mathrm{cf}(\alpha) \to \alpha$ cofinale. Se per assurdo avessimo che $\mathrm{cf}(\alpha)$ non fosse un ordinale iniziale avremmo un $\beta < \mathrm{cf}(\alpha)$ e tale che esiste $g : \beta \to \mathrm{cf}(\alpha)$ applicazione biunivoca. Ma allora $f \circ g : \beta \to \alpha$ sarebbe un'applicazione cofinale, contro la minimalità di $\mathrm{cf}(\alpha)$. □

Osservazione 9.2.1. Potevamo anche omettere che α fosse un'ordinale limite, però allora avremmo dovuto dire che $\mathrm{cf}(\alpha)$ è un cardinale. Infatti se α è un successore sappiamo che la sua cofinalità è 1, quindi è un caso banale. Molti testi, infatti, definiscono la cofinalità solo per ordinali limite.

Lemma 9.2.1. *Sia α un ordinale. Esiste una mappa cofinale $f : \mathrm{cf}(\alpha) \to \alpha$ che è anche strettamente crescente.*

Dimostrazione. Sia $g : \mathrm{cf}(\alpha) \to \alpha$ una mappa cofinale, che esiste per definizione di cofinalità. Vogliamo dimostrare che esiste anche $f : \mathrm{cf}(\alpha) \to \alpha$ cofinale e crescente. Possiamo considerare α ordinale limite, altrimenti come al solito siamo nel caso banale $\mathrm{cf}(\alpha) = 1$. Definiamo una funzione per ricorsione transfinita su ogni $\beta < \mathrm{cf}(\alpha)$:

$$\begin{cases} f(0) = g(0) + 1 \\ f(\beta + 1) = \max\{f(\beta),\, g(\beta + 1)\} + 1 \\ f(\beta) = \max\{\sup_{\gamma<\beta} f(\gamma),\, g(\gamma)\} + 1 \quad \text{se } \beta \text{ è limite.} \end{cases}$$

Ora che abbiamo definito f dobbiamo dimostrare che $\mathrm{imm}\, f \subseteq \alpha$, e lo faremo per induzione transfinita su β, mostrando che $f(\beta) < \alpha$. Intanto $f(0) = g(0) + 1 < \alpha$ in quanto α è limite e $g(0) < \alpha$; poi $f(\beta + 1) < \alpha$ in quanto $f(\beta)$ lo è per ipotesi induttiva e $g(\beta+1)$ lo è per ipotesi. Se β è limite allora $\sup_{\gamma<\beta} f(\gamma) < \alpha$ altrimenti $f : \beta \to \alpha$ sarebbe cofinale, assurdo perché $\mathrm{cf}(\alpha) > \beta$. □

Vediamo adesso un'importante definizione:

Definizione 9.2.3. Un cardinale κ si dice *regolare* se $\mathrm{cf}(\kappa) = \kappa$. In caso contrario si dice *singolare*.

Vogliamo imparare meglio a vedere quali cardinali sono regolari. Abbiamo visto che se α è un limite allora $\mathrm{cf}(\alpha)$ è un cardinale infinito; ebbene i prossimi due risultati mostreranno che è anche un cardinale regolare.

Lemma 9.2.2. *Sia α un ordinale limite e sia $f : \alpha \to \beta$ un'applicazione cofinale crescente. Allora* $\mathrm{cf}(\alpha) = \mathrm{cf}(\beta)$.

Dimostrazione. Consideriamo un'applicazione $g : \mathrm{cf}(\alpha) \to \alpha$ cofinale e crescente, che esiste per il lemma precedente. L'applicazione $f \circ g : \mathrm{cf}(\alpha) \to \beta$ è cofinale e crescente e dunque per definizione di cofinalità si ha $\mathrm{cf}(\beta) \leq \mathrm{cf}(\alpha)$.
Mostriamo ora che esiste una $\psi : \mathrm{cf}(\beta) \to \alpha$ cofinale. Intanto si ha $g : \mathrm{cf}(\beta) \to \beta$ cofinale e sia $\xi \in \mathrm{cf}(\beta)$. Considerato $g(\xi)$ avremo, essendo f cofinale, che esiste

$$\zeta_\xi = \min\{\zeta \in \alpha \mid f(\zeta) > g(\xi)\}.$$

Adesso definiamo ψ come l'applicazione che manda ξ in ζ_ξ. Dobbiamo mostrare che ψ è cofinale. Consideriamo $\xi_0 \in \alpha$ e $f(\xi_0) \in \beta$; esiste dunque $\bar{\xi} \in \mathrm{cf}(\beta)$ tale che $g(\bar{\xi}) > f(\xi_0)$. Ma allora

$$\psi(\bar{\xi}) = \zeta_{\bar{\xi}} = \min\{\zeta \in \alpha \mid f(\zeta) > g(\bar{\xi})\} > \xi_0,$$

visto che $f(\xi_0) < g(\bar{\xi})$ e f è crescente. □

Corollario 9.2.1. *Per ogni α ordinale limite, si ha* $\mathrm{cf}(\aleph_\alpha) = \mathrm{cf}(\alpha)$.

Dimostrazione. Visto che α è limite basta considerare l'applicazione $\alpha \to \aleph_\alpha$ che manda $\beta \in \alpha$ in $\aleph_\beta$: questa è cofinale crescente e quindi grazie al lemma 9.2.1 possiamo concludere. □

Corollario 9.2.2. *Per ogni α limite* $\mathrm{cf}(\mathrm{cf}(\alpha)) = \mathrm{cf}(\alpha)$.

Dimostrazione. Ovvia. □

Proprio il corollario precedente mostra che per ogni α limite vale che $\mathrm{cf}(\alpha)$ è un cardinale regolare, tant'è che la sua cofinalità coincide con lui stesso.

Proposizione 9.2.2. *Ogni cardinale successore è regolare.*

Dimostrazione. Sia κ^+ un cardinale successore. Sia $\alpha < \kappa^+$ e sia per assurdo $f : \alpha \to \kappa^+$ un'applicazione cofinale, allora $\kappa^+ = \bigcup_{\beta<\alpha} f(\beta)$. Ma allora

$$\kappa^+ = \left|\bigcup_{\beta<\alpha} f(\beta)\right| \leq \sum_{\beta<\alpha} |f(\beta)| = \max\left\{\alpha, \sup_{\beta<\alpha} |f(\beta)|\right\} \leq \kappa,$$

e ciò è assurdo. □

Osservazione 9.2.2. Possiamo anche scrivere il risultato precedente dicendo che ogni $\aleph_{\alpha+1}$ è un cardinale regolare. Varrà dunque

$$\mathrm{cf}\,(\aleph_\alpha) = \begin{cases} \aleph_\alpha & \text{se } \alpha = \beta + 1 \\ \mathrm{cf}\,(\alpha) & \text{se } \alpha \text{ è limite} \end{cases}.$$

Adesso, prima di occuparci nel prossimo paragrafo di esponenziali, vogliamo osservare un fatto molto singolare. Prendiamo il cardinale $\aleph_\omega$: questo è singolare in quanto

$$\mathrm{cf}\,(\aleph_\omega) = \omega < \aleph_\omega.$$

Allo stesso modo anche i cardinali $\aleph_{\omega+\omega}$, $\aleph_{\omega\cdot\omega}$ e $\aleph_{\omega_1}$ sono singolari. Questi cardinali limite non numerabili sono tutti singolari, ed anzi ne possiamo trovare sempre di più grandi:

Lemma 9.2.3. *Esistono cardinali singolari arbitrariamente grandi.*

Dimostrazione. Sia $\aleph_\alpha$ un cardinale. Si consideri adesso $\aleph_{\alpha+\omega}$: l'applicazione $\omega \to \aleph_{\alpha+\omega}$ che manda $n \mapsto \aleph_{\alpha+n}$ è cofinale e dunque

$$\mathrm{cf}\,(\aleph_{\alpha+\omega}) < \omega \leq \alpha + \omega \leq \aleph_{\alpha+\omega}.$$

Ciò mostra che $\aleph_{\alpha+\omega}$ è un cardinale singolare, ed è più grande di $\aleph_\alpha$. □

Una domanda che adesso è naturale porsi è se esistono cardinali limiti regolari; supponiamo che $\aleph_\alpha$ sia un tale cardinale, allora $\aleph_\alpha = \mathrm{cf}\,(\aleph_\alpha) = \mathrm{cf}\,(\alpha) \leq \alpha$. Visto che inoltre vale sempre $\alpha \leq \aleph_\alpha$ avremo dunque che

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

Quindi se un cardinale $\aleph_\alpha$ è limite e regolare avremo che $\aleph_\alpha = \alpha$; tuttavia la condizione non è sufficiente perché possiamo costruire un cardinale non regolare tale che soddisfi la condizione precedente. In realtà ne possiamo costruire di arbitrariamente grandi:

Lemma 9.2.4. *Esistono cardinali singolari con $\aleph_\alpha = \alpha$ arbitrariamente grandi.*

Dimostrazione. Sia $\aleph_\gamma$ un cardinale. Definiamo ricorsivamente

$$\begin{cases} \alpha_0 = \omega_\gamma \\ \alpha_{n+1} = \omega_{\alpha_n} \quad \text{per } n < \omega \end{cases}.$$

Sia adesso $\alpha = \bigcup_{n<\omega} \alpha_n$: abbiamo che α è il primo ordinale a soddisfare $\aleph_\alpha = \alpha$, infatti

$$\aleph_\alpha = \omega_\alpha = \bigcup_{n<\omega} \omega_{\alpha_n} = \bigcup_{n<\omega} \alpha_{n+1} = \alpha.$$

Ma α non è un cardinale regolare, in quanto è facile vedere che $\mathrm{cf}\,(\alpha) = \omega < \alpha$. □

Il lemma suggerisce che un $\aleph_\alpha$ che soddisfa

$$\aleph_\alpha = \alpha$$

deve essere molto grande. In ogni caso la condizione precedente, a dispetto di quanto si pensi, è più debole di quanto si crede visto che ne possiamo costruire quanti vogliamo.

Definizione 9.2.4. Un cardinale non numerabile $\aleph_\alpha$ è detto *inaccessibile* se è un cardinale limite ed è anche regolare.

In effetti è impossibile provare l'esistenza di tali cardinali usando solo gli assiomi della teoria di Zermelo–Fraenkel anche con l'assioma di scelta.

9.3 Esponenziazione di cardinali

Come già abbiamo avuto modo di dire, mentre l'addizione e la moltiplicazione di cardinali sono operazioni semplici (visto che il risultato è sempre il più grande tra i due cardinali), la valutazione dell'esponenziazione tra cardinali è piuttosto complicata. Non daremo qui tutte le regole note – anche perché in effetti il problema è ancora aperto – ma proveremo solo le proprietà di base. Inizieremo da risultati piuttosto semplici, per poi arrivare invece a dimostrare la formula di Hausdorff.

Lemma 9.3.1. *Si ha* $\operatorname{cf}(2^{\aleph_\alpha}) > \aleph_\alpha$.

Dimostrazione. Sia $\nu = \operatorname{cf}(2^{\aleph_\alpha})$ e per assurdo supponiamo $\nu \leq \aleph_\alpha$. Per definizione di cofinalità esiste $f : \nu \to 2^{\aleph_\alpha}$ cofinale e crescente, e allora $2^{\aleph_\alpha} = \bigcup_{\eta\in\nu} f(\eta)$. Dunque

$$2^{\aleph_\alpha} = \left|\bigcup_{\eta\in\nu} f(\eta)\right| \leq \sum_{\eta\in\nu} |f(\eta)| < \prod_{\eta\in\nu} 2^{\aleph_\alpha} = (2^{\aleph_\alpha})^\nu = 2^{\aleph_\alpha\cdot\nu} = 2^{\aleph_\alpha},$$

e abbiamo raggiunto l'assurdo. □

Lemma 9.3.2. *Si ha* $\aleph_\alpha^{\operatorname{cf}(\aleph_\alpha)} > \aleph_\alpha$.

Dimostrazione. Esiste un'applicazione $f : \operatorname{cf}(\aleph_\alpha) \to \aleph_\alpha$ cofinale e crescente, e dunque ancora grazie al teorema di König si ha

$$\aleph_\alpha = \left|\bigcup_{\beta\in\operatorname{cf}(\aleph_\alpha)} f(\beta)\right| = \sum_{\beta\in\operatorname{cf}(\aleph_\alpha)} |f(\beta)| < \prod_{\beta\in\operatorname{cf}(\aleph_\alpha)} \aleph_\alpha = \aleph_\alpha^{\operatorname{cf}(\aleph_\alpha)},$$

e abbiamo concluso. □

Lemma 9.3.3. *Se $\alpha \leq \beta$ si ha $\aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta}$.*

Dimostrazione. Certamente vale $2^{\aleph_\beta} \leq \aleph_\alpha^{\aleph_\beta}$. Per l'altra basta osservare

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

e si conclude per il teorema di Cantor–Bernstein. □

Teorema 9.3.1 (formula di Hausdorff)**.** *Per ogni α e β si ha*

$$\aleph_{\alpha+1}^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} \cdot \aleph_{\alpha+1}.$$

Dimostrazione. Distinguiamo due casi, e supponiamo intanto che $\beta \geq \alpha+1$. Allora per quanto visto nel precedente lemma

$$\aleph_{\alpha+1}^{\aleph_\beta} = 2^{\aleph_\beta} \quad \text{e} \quad \aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta}.$$

Visto che inoltre $\aleph_{\alpha+1} \leq \aleph_\beta \leq 2^{\aleph_\beta}$ possiamo concludere che il prodotto a secondo membro della formula da dimostrare fa $2^{\aleph_\beta}$, uguale al primo membro.
Adesso veniamo al caso in cui $\beta < \alpha + 1$, ossia $\beta \leq \alpha$. Visto che valgono naturalmente

$$\aleph_\alpha^{\aleph_\beta} \leq \aleph_{\alpha+1}^{\aleph_\beta} \quad \text{e} \quad \aleph_{\alpha+1} \leq \aleph_{\alpha+1}^{\aleph_\beta},$$

dobbiamo mostrare solo che $\aleph_{\alpha+1}^{\aleph_\beta} \leq \aleph_\alpha^{\aleph_\beta} \cdot \aleph_{\alpha+1}$. Sappiamo che

$$\aleph_{\alpha+1}^{\aleph_\beta} = |\{f \mid f : \aleph_\beta \to \aleph_{\alpha+1}\}| = |Fun(\aleph_\beta, \aleph_{\alpha+1})|\,;$$

inoltre $\operatorname{cf}(\aleph_{\alpha+1}) = \aleph_{\alpha+1}$ e quindi, essendo $\aleph_\beta < \aleph_{\alpha+1}$, si ha che ogni $f : \aleph_\beta \to \aleph_{\alpha+1}$ deve essere limitata. Questo significa che esiste $\gamma < \aleph_{\alpha+1}$ tale che $\operatorname{imm} f \subseteq \gamma$. Dunque

$$Fun(\aleph_\beta, \aleph_{\alpha+1}) = \bigcup_{\gamma < \aleph_{\alpha+1}} Fun(\aleph_\beta, \gamma), \quad \text{ossia} \quad \aleph_{\alpha+1}^{\aleph_\beta} = \bigcup_{\gamma < \aleph_{\alpha+1}} \gamma^{\aleph_\beta}.$$

Dunque si ha

$$\aleph_{\alpha+1}^{\aleph_\beta} = \left| \bigcup_{\gamma < \aleph_{\alpha+1}} \gamma^{\aleph_\beta} \right| \leq \sum_{\gamma < \aleph_{\alpha+1}} \left| \gamma^{\aleph_\beta} \right| \leq \sum_{\gamma < \aleph_{\alpha+1}} \aleph_\alpha^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} \cdot \aleph_{\alpha+1},$$

e quindi abbiamo concluso. □

Capitolo 10

L'assioma di fondazione e gli insiemi ben fondati

La nozione di buon ordinamento è uno dei concetti chiave della teoria degli insiemi. Abbiamo introdotto i numeri naturali e abbiamo visto come la relazione di appartenenza sia un buon ordinamento su di essi e abbiamo altresì visto come ciò, sostanzialmente, equivalga al principio di induzione. Poi abbiamo studiato i buoni ordini in tutta generalità e abbiamo visto gli sviluppi a cui hanno portato. È ovvio dunque chiedersi se tale concetto permette ulteriori altrettanto utili generalizzazioni. Per molte ragioni il concetto di ordinamento in sé non è molto importante, ciò che ha dato la svolta ai nostri ragionamenti è il concetto di buon ordine, ossia richiedere che ogni insieme non vuoto abbia un minimo elemento. È da questo che prenderanno le mosse gli sviluppi che daremo in questo capitolo.

10.1 Relazioni ben fondate

Alla luce dell'introduzione appena vista appare naturale dare una definizione di fondatezza, di bontà, di minimalità per le relazioni. Alcuni testi adottano una definizione analoga a quella data per gli insiemi ben ordinati, ossia con l'utilizzo di un minimo elemento, noi però preferiamo adottare una definizione che si richiama alle catene discendenti infinite:

Definizione 10.1.1. Sia R una relazione. Diremo che R è *ben fondata* se non esiste una sequenza di insiemi $\langle X_n \mid n \in \mathbb{N}\rangle$ tale che $X_{n+1}\, R\, X_n$ per ogni $n \in \mathbb{N}$.

Definizione 10.1.2. Un insieme X si dice *ben fondato* se non esiste una sequenza di insiemi $\langle X_0 = X,\, X_n \mid n \in \mathbb{N}_0\rangle$ tale che $X_{n+1} \in X_n$ per ogni $n \in \mathbb{N}$.

Richiamiamo adesso l'assioma di fondazione: questo asseriva per per ogni insieme X non vuoto esiste un $Y \in X$ tale che $X \cap Y = \emptyset$. Ciò equivale all'esistenza di

un insieme $\in$–minimale in X, ossia di un elemento di X che non contiene altri elementi di X. La formulazione è

$$(\forall X \neq \emptyset)(\exists Y)(Y \in X \wedge X \cap Y = \emptyset).$$

Dall'assioma di fondazione seguiva anche che non esiste alcun insieme X non vuoto tale che sia elemento di se stesso, ossia tale che $X \in X$.
È importante precisare sin da subito il fatto seguente: se X è un insieme ben fondato allora X verifica l'assioma di fondazione come mostreremo subito nella prossima proposizione (freccia $\Longleftarrow$). *Non* vale però che se X soddisfa l'assioma di fondazione allora X è ben fondato: infatti basta prendere $X = \{X, \emptyset\}$. Questo insieme soddisfa l'assioma di fondazione perché $X \cap \emptyset = \emptyset$ ma non è ben fondato perché vale $X \ni X \ni X \ni \cdots$. Si equivalgono invece l'assioma di fondazione e il fatto che *tutti* gli insiemi sono ben fondati. Vediamo ora la dimostrazione:

Proposizione 10.1.1. *L'assioma di fondazione equivale a richiedere che la relazione $\in$ di appartenenza sia ben fondata.*

Dimostrazione. ($\Longrightarrow$) Supponiamo per assurdo che esista una catena discendente infinita di appartenenze, ossia supponiamo che esista $\langle X_n \mid n \in \mathbb{N}\rangle$ con $X_{n+1} \in X_n$ per ogni $n \in \mathbb{N}$. Consideriamo l'insieme

$$X = \{X_n \mid n \in \mathbb{N}\},$$

allora vogliamo mostrare che per questo insieme, che è non vuoto per costruzione, non vale l'assioma di fondazione. Preso un $Y \in X$ abbiamo che $Y = X_k$ per qualche $k \in \mathbb{N}$; ma allora

$$X \cap Y = X \cap X_k$$

e questo insieme ha come elemento X_{k+1}, e dunque è non vuoto.
($\Longleftarrow$) Supponiamo adesso che per assurdo non valga l'assioma di fondazione, allora riusciremo a costruire una catena discendente infinita di appartenenze, che mostrera che $\in$ non è ben fondata. Sia dunque X un insieme non vuoto che non soddisfa l'assioma di fondazione, allora

$$(\forall Y)(Y \in X \to X \cap Y \neq \emptyset).$$

Prendiamo dunque $X_0 \in X$ (che esiste perché X è non vuoto), varrà dunque $X_0 \cap X \neq \emptyset$; ma allora possiamo prendere $X_1 \in X_0 \cap X$ e ricorsivamente (si mostra per induzione) per ogni $n \in \mathbb{N}$ esiste $X_{n+1} \in X_n \cap X$, con $X_0 \in X$ scelto all'inizio. Ma allora la sequenza $\langle X_n \mid n \in \mathbb{N}\rangle$ è una catena discendente infinita di appartenenze, fatto che contraddice la buona fondatezza di $\in$. $\square$

10.2 Gerarchia di von Neumann

È tempo di riconsiderare il nostro modo intuitivo di concepire gli insiemi. Richiamiamo l'originale descrizione di Cantor: un insieme è una collezione dentro un universo di oggetti definiti e distinti della nostra intuizione o del nostro pensiero. Sembra ragionevole interpretare questo fatto nel senso dell'esistenza di tali oggetti nella nostra mente prima ancora che essi vengano collezionati in un insieme. Adesso accettiamo questa posizione e richiamiamo che gli insiemi sono gli unici oggetti a cui siamo interessati. Supponiamo di voler costruire un insieme "per la prima volta", ciò significa che non ci sono già degli oggetti disponibili (insiemi) nella nostra mente, e quindi l'unica collezione che possiamo formare è l'insieme vuoto $\emptyset$. Ma ora abbiamo qualcosa! $\emptyset$ è un oggetto definito della nostra mente, e quindi possiamo collezionare l'insieme $\{\emptyset\}$. A questo punto ci sono due oggetti nella nostra mente, $\emptyset$ e $\{\emptyset\}$ e quindi possiamo collezionare vari insiemi di questi: $\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\}\}$ e $\{\emptyset, \{\emptyset\}\}$. A questo punto possiamo descrivere questo processo formalmente e mostreremo che da questo si possono ottenere tutti gli insiemi ben fondati.

Definizione 10.2.1. La gerarchia di von Neumann è definita risorsivamente come segue:

$$\begin{cases} V_0 = \emptyset \\ V_{\alpha+1} = \mathcal{P}(V_\alpha) \\ V_\alpha = \bigcup_{\beta<\alpha} V_\beta \quad \text{se } \alpha \text{ è limite} \end{cases}.$$

Intanto dobbiamo vedere qualche proprietà di questi insiemi di von Neumann, per poi vedere che relazione hanno con l'assioma di fondazione. Vale dunque

Lemma 10.2.1. *Per ogni α ordinale, se $x \in V_\alpha$ e $y \in x$ allora $y \in V_\beta$ per qualche $\beta < \alpha$.*

Dimostrazione. Si procede per induzione transfinita su α. Se $\alpha = 0$ l'affermazione è vera a vuoto; se α è un ordinale limite allora si ha che

$$x \in V_\alpha = \bigcup_{\beta<\alpha} V_\beta \Longrightarrow \exists \beta < \alpha \text{ tale che } x \in V_\beta.$$

Ma allora per ipotesi induttiva $y \in V_\gamma$ con $\gamma < \beta$, e inoltre $\gamma < \beta < \alpha$. Supponiamo adesso che α sia un ordinale successore, ossia $\alpha = \gamma + 1$: abbiamo allora

$$x \in V_\alpha = V_{\gamma+1} = \mathcal{P}(V_\gamma) \Longrightarrow x \subseteq V_\gamma,$$

e dunque $y \in V_\gamma$. □

Il lemma appena enunciato è solo un lemma tecnico che ci serve per dimostrare i due risultati importanti riguardo agli insiemi di von Neumann, che sono i prossimi.

Proposizione 10.2.1. *Se $\beta < \alpha$ allora $V_\alpha \subseteq V_\beta$.*

Dimostrazione. Usiamo ancora l'induzione transfinita su α. Solo il caso successore è non banale, quindi lo svolgiamo: mostriamo che $V_\alpha \subseteq V_{\alpha+1}$. Dal lemma 10.2.1 sappiamo che se $x \in V_\alpha$ allora $x \subseteq \bigcup_{\beta<\alpha} V_\beta$. Per ipotesi induttiva $\bigcup_{\beta<\alpha} V_\beta \subseteq V_\alpha$. Ma allora $x \subseteq V_\alpha$ e quindi $x \in \mathcal{P}(V_\alpha) = V_{\alpha+1}$. Segue dunque che $V_\beta \subseteq V_\alpha \subseteq V_{\alpha+1}$ per ogni $\beta \leq \alpha$. □

Proposizione 10.2.2. *Per ogni α ordinale abbiamo che V_α è transitivo.*

Dimostrazione. Ancora una volta si procede per induzione transfinita su α. Il caso $\alpha = 0$ è banale; per il caso limite non occorrono neanche i risultati precedenti. Supponiamo $y \in x \in V_\lambda$ con λ ordinale limite, allora

$$x \in V_\lambda = \bigcup_{\gamma<\lambda} V_\gamma \Longrightarrow \exists \gamma < \lambda \text{ tale che } x \in V_\gamma.$$

Ma per ipotesi induttiva $y \in x \in V_\gamma$ implica $y \in V_\gamma$ e dunque $y \in \bigcup_{\gamma<\lambda} V_\gamma = V_\lambda$. Adesso dobbiamo mostrare il caso successore, e quindi supponiamo $\alpha = \beta + 1$ e $y \in x \in V_\alpha$. Visto che $x \in V_\alpha = \mathcal{P}(V_\beta)$ si ha che $x \subseteq V_\beta$ e dunque $y \in V_\beta$. Ma visto che per la proposizione precedente si ha $V_\beta \subseteq V_\alpha$ segue che $y \in V_\alpha$. □

Osservazione 10.2.1. Per mostrare la proposizione può essere utile osservare il seguente fatto. Definiamo per ricorsione transfinita la sequenza di insiemi

$$V'_\alpha = \bigcup_{\beta<\alpha} \mathcal{P}(V'_\beta).$$

Non è difficile mostrare che $V'_\alpha = V_\alpha$ per ogni α. Il caso $\alpha = 0$ è banale; per il caso successore basta osservare che

$$V'_{\alpha+1} = \bigcup_{\beta\leq\alpha} \mathcal{P}(V'_\beta) = \mathcal{P}(V'_\alpha) = \mathcal{P}(V_\alpha) = V_{\alpha+1},$$

dove nel secondo (terzo) passaggio abbiamo usato il fatto che i V'_α sono una famiglia crescente (rispettivamente l'ipotesi induttiva). Il caso limite si ha altrettanto facilmente in quanto

$$V'_\lambda = \bigcup_{\beta<\lambda} \mathcal{P}(V'_\beta) = \bigcup_{\beta<\lambda} V'_{\beta+1} = \bigcup_{\beta<\lambda} V_{\beta+1} = V_\lambda,$$

dove nel penultimo passaggio abbiamo usato quanto dimostrato nel caso successore. Qual è il vantaggio di questa nuova definizione? Il vantaggio sta nel fatto che, per costruzione, la famiglia V'_α è una famiglia crescente e quindi, coincidendo con la famiglia dei V_α abbiamo già che questa è crescente.

Adesso vogliamo vedere come sono messi gli ordinali rispetto alla gerarchia di von Neumann; valgono i seguenti risultati:

Lemma 10.2.2. *Per ogni α ordinale, $\alpha \subseteq V_\alpha$ ma $\alpha \notin V_\alpha$.*

Dimostrazione. Procediamo per induzione transfinita su α e mostreremo parallelamente le due proprietà. Se $\alpha = 0$ vale certamente $0 = \emptyset \subseteq V_0 = \emptyset$ ma $0 \notin V_0$. Supponiamo adesso che $\alpha = \beta + 1$ sia un successore; per ipotesi induttiva abbiamo che $\beta \subseteq V_\beta$, e quindi $\beta \in \mathcal{P}(V_\beta) = V_{\beta+1}$. Ora abbiamo che $\beta \subseteq V_\beta \subseteq V_{\beta+1}$ e $\beta \in V_{\beta+1}$ e dunque

$$\beta + 1 = \beta \cup \{\beta\} \subseteq V_{\beta+1}.$$

Poniamo per assurdo che sia $\beta + 1 \in V_{\beta+1} = \mathcal{P}(V_\beta)$; allora $\beta + 1 \subseteq V_\beta$, da cui $\beta \in V_\beta$, che contraddice l'ipotesi induttiva.
Infine prendiamo $\alpha = \lambda$ ordinale limite; per ipotesi induttiva $\beta \subseteq V_\beta$ per ogni $\beta < \lambda$. Da questo segue che

$$\lambda = \bigcup_{\beta<\lambda} \beta \subseteq \bigcup_{\beta<\lambda} V_\beta = V_\lambda.$$

Supponiamo per assurdo che $\lambda \in V_\lambda$, allora esiste $\beta < \lambda$ tale che $\lambda \in V_\beta$ per definizione di V_λ; a questo punto abbiamo $\beta \in \lambda \in V_\beta$ implica $\beta \in V_\beta$, contro l'ipotesi induttiva. □

Osservazione 10.2.2. Dal teorema precedente abbiamo che $\alpha \subseteq V_\alpha$, da cui $\alpha \in V_{\alpha+1}$. Inoltre, per la transitività dei V_α abbiamo che $V_\alpha \cap \mathrm{Ord} = \alpha$.

Definizione 10.2.2. Definiamo il *rango* di un insieme X come

$$\rho(X) = \min\{\alpha \text{ ordinale} \mid X \in V_{\alpha+1}\} = \min\{\alpha \text{ ordinale} \mid X \subseteq V_\alpha\}.$$

Proposizione 10.2.3. *Se esiste α ordinale tale che $X \in V_\alpha$ allora X soddisfa l'assioma di fondazione.*

Dimostrazione. Sia X fissato con $X \in V_\alpha$ per qualche α ordinale. Consideriamo adesso $\beta = \min\{\rho(Y) \mid Y \in X\}$, e sia $\bar{Y} \in X$ quello per cui $\rho(\bar{Y}) = \beta$. Per transitività abbiamo che se $Z \in \bar{Y}$ allora $\rho(Z) < \rho(\bar{Y})$ e dunque per ogni $Y \in X$ si ha $\rho(Y) > \rho(\bar{Y}) > \rho(Z)$, da cui segue che $Z \neq Y$ per ogni $Y \in X$. Dunque $\bar{Y} \cap X = \emptyset$. □

Teorema 10.2.1. *L'assioma di fondazione equivale a chiedere*

$$\mathbb{V} = \bigcup_{\alpha\in\mathrm{Ord}} V_\alpha,$$

Ossia, $X \in \bigcup_{\alpha\in\mathrm{Ord}} V_\alpha$ se e solo se X è ben fondato.

Dimostrazione. ($\Longleftarrow$) Per assurdo sia B un insieme tale che per ogni α ordinale $B \notin V_\alpha$. Notiamo che esiste b tale che per ogni α si ha $b \notin V_\alpha$. Infatti se non esistesse allora

$$\text{per ogni } b \in B \text{ esiste } \alpha_b = \min\{\alpha \mid b \in V_\alpha\},$$

e per rimpiazzamento $\{\alpha_b \mid b \in B\}$ sarebbe un insieme, e quindi potremmo prendere $\gamma = \sup_{b\in B} \alpha_b$. Ma allora per ogni $b \in B$ si ha $b \in V_{\alpha_b} \subseteq V_\gamma$. Quindi $B \subseteq V_\gamma$ e dunque $B \in V_{\gamma+1}$.
($\Longrightarrow$) Utilizziamo la nozione di rango; se per assurdo avessimo $X \in X_1 \in X_2 \in \cdots$ allora segue $\rho(x) > \rho(x_1) > \rho(x_2) > \cdots$. Ma questa è una catena discendente infinita di ordinali, assurdo. $\square$

Appendice A

L'insieme dei numeri reali

Abbiamo definito i numeri naturali e il loro ordinamento e abbiamo indicato come possono essere definite le operazioni aritmetiche sui numeri naturali. Il prossimo passo logico nello sviluppo della fondazione della matematica è quello di definire gli interi e i razionali. Dopodiché sarà la volta di definire i numeri reali e così avremo concluso la costruzione degli insiemi numerici. Abbiamo deciso di porre questa sezione in appendice per non appesantire troppo lo svolgimento degli argomenti nel loro ordine naturale, che ha come fulcro la trattazione dei cardinali e degli ordinali.

A.1 Gli interi e i razionali

L'idea guida per costruire questi insiemi è quella di costruire delle operazioni parziali sui numeri naturali (la sottrazione nel caso degli interi, e la divisione nel caso dei razionali) e di portarle ad essere operazioni vere e proprie; cioè chiuderemo l'insieme dei numeri naturali per sottrazione e per divisione, ottenendo così due nuovi insiemi, che saranno poi gli interi e i razionali. Visto che queste costruzioni più propriamente fanno parte dell'algebra astratta, ci limiteremo a esporre le idee principali, e non daremo molte dimostrazioni. Tali dimostrazioni possono essere facilmente trovate sui libri di algebra astratta, o, meglio ancora, il lettore potrebbe svolgerle come esercizio.
Per tutte le coppie di numeri naturali (n, m) in cui $n \geq m$ abbiamo definito la *differenza* dei due numeri, denotata con $n - m$: la differenza è quell'unico k naturale per il quale $m + k = n$. Se $n < m$ nessun tale k in effetti esiste, e la differenza non è definita. Se $n - m$ deve essere definito anche in questo caso, deve essere un nuovo oggetto; per ora lo rappresenteremo semplicemente con la coppia ordinata (n, m). Tuttavia, intuitive proprietà dei numeri interi familiari al lettore, suggeriscono che differenti coppie ordinate possano rappresentare lo stesso intero,

ad esempio le coppie $(2,5)$ e $(6,9)$. In generale, due coppie (n_1, m_1) e (n_2, m_2) rappresentano lo stesso intero se e solo se $n_1 - m_1 = n_2 - m_2$. A questo punto, ma ciò che stiamo per dire prende senso solo intuitivamente, la precedente relazione può essere riscritta nella forma

$$n_1 + m_2 = n_2 + m_1,$$

scrittura che coinvolge solo l'addizione. Tutto questo discorso motiva la seguente definizione:

Definizione A.1.1. Su $\mathbb{N} \times \mathbb{N}$ si definisce $(a,b) \sim (c,d)$ se e solo se $a + d = b + c$. L'insieme quoziente $\mathbb{N} \times \mathbb{N}/\sim$ prende il nome di *insieme degli interi*, e viene denotato con $\mathbb{Z}$.

Poi si può definire su $\mathbb{Z}$ una relazione $<$ come segue:

$$[(a,b)] < [(c,d)] \iff a + d < b + c;$$

si ricordi il significato intuitivo di (a,b), che rappresenta la differenza $a - b$. Si può dimostrare che $<$ è ben definito, nel senso che non dipende dalla scelta dei rappresentanti, e che è un ordine totale su $\mathbb{Z}$.
Si osservi che se abbiamo (a,b) con $a \geq b$ allora $(a,b) \sim (a-b, 0)$, dove $a - b$ in questo caso è la differenza ed è ben definita. Inoltre se abbiamo (a,b) con $a < b$ si ha $(a,b) \sim (0, b-a)$. Così appare chiaro che ogni intero contiene una coppia della forma $(n,0)$ con $n \in \mathbb{N}$ o $(0,n)$ con $n \in \mathbb{N} - \{0\}$.

Definizione A.1.2. Gli interi del tipo $[(n,0)]$ con $n \in \mathbb{N}$ sono gli *interi positivi*; quelli del tipo $[(0,n)]$ con $n \in \mathbb{N} - \{0\}$ sono detti *interi negativi*.

La mappa $F : \mathbb{N} \to \mathbb{Z}$ che manda n in $[(n,0)]$ è una mappa iniettiva e preserva l'ordine: questo significa che $\mathbb{Z}$ contiene una copia isomorfa di $\mathbb{N}$. È dunque consuetudine indicare gli interi $[(n,0)]$ con il corrispondente naturale n, mentre gli interi $[(0,n)]$ vengono indicati con $-n$.
Il resto della teoria a questo punto segue. Uno può provare che $\mathbb{Z}$ è illimitato, che ogni insieme non vuoto limitato dall'alto (dal basso) ammette un massimo (minimo) elemento. Poi si possono definire addizione e moltiplicazione nel modo seguente:

$$[(a,b)] + [(c,d)] = [(a+c, b+d)] \quad \text{e} \quad [(a,b)] \cdot [(c,d)] = [(ac+bd, ad+bc)],$$

e vedere che queste operazioni soddisfano le leggi usuali dell'algebra, e che nel caso in cui i due interi siano numeri naturali, tali due operazioni coincidono con quelle definite sui naturali.

Definizione A.1.3. Diremo che un intero a è *divisibile* per l'intero b se esiste un unico intero x tale che $a = b \cdot x$. Tale unico x è chiamato *quoziente* di a e b.

Ora, $0 \cdot x = 0$ è vera per ogni x intero, quindi concludiamo che non esiste il quoziente di zero per se stesso (viene meno l'unicità); analogamente osserviamo che alcun intero $a \neq 0$ è divisibile per zero. Quello che dunque possiamo sperare se vogliamo estendere la divisione è che per ogni a e per ogni $b \neq 0$ esiste il quoziente.

Definizione A.1.4. Su $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ definiamo $(a, b) \sim (c, d)$ se e solo se $a \cdot d = b \cdot c$. L'insieme quoziente $(\mathbb{Z} \times (\mathbb{Z} - \{0\}))/\sim$ è detto *insieme dei razionali* ed è denotato con $\mathbb{Q}$.

D'ora innanzi indicheremo le coppie $(a, b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$ con $\frac{a}{b}$, e dunque gli elementi di $\mathbb{Q}$ saranno delle classi $\left[\frac{a}{b}\right]$; poi indicheremo queste classi semplicemente con $\frac{a}{b}$, intendendo così tutte le frazioni equivalenti a $\frac{a}{b}$. Come prima, c'è una mappa naturale $G : \mathbb{Z} \to \mathbb{Q}$, quella che manda a in $\left[\frac{a}{1}\right]$, e proprio per questo di seguito identificheremo i razionali $\frac{a}{1}$ con il corrispondenti interi a.
Si possono anche definire due operazioni:

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{a \cdot d + b \cdot c}{b \cdot d}\right] \quad \text{e} \quad \left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] = \left[\frac{a \cdot c}{b \cdot d}\right].$$

Alcune proprietà sono le seguenti: (1) addizione e moltiplicazione sono ben definite; (2) per gli interi le nuove definizioni estendono quelle vecchie per gli interi, ossia

$$G(a + b) = G(a) \cdot G(b) \quad \text{e} \quad G(a \cdot b) = G(a) \cdot G(b),$$

a dire che G è un omomorfismo di gruppi; (3) l'addizione e la moltiplicazione tra razionali soddisfano le usuali regole che il lettore già conosce. Infine osserviamo che è possibile definire una relazione $<$ su $\mathbb{Q}$ nel modo seguente: se $b > 0$ e $d > 0$ allora

$$\left[\frac{a}{b}\right] < \left[\frac{c}{d}\right] \iff a \cdot d < b \cdot c.$$

Teorema A.1.1. *L'insieme $(\mathbb{Q}, <)$ è un insieme totalmente ordinato, infinito e denso.*

Dimostrazione. La semplice prova è lasciata per esercizio. Osserviamo solo che per densità si intende che per ogni $r \neq s$ esiste un razionale tra essi compreo strettamente (basta prendere la media aritmetica). □

A.2 Numeri reali

È importante far presente subito che, dal punto di vista fondazionale, la riduzione dei numeri reali ai numeri razionali è un processo essenzialmente più "complicato" rispetto alle altre riduzioni viste sin qui. Infatti, le costruzioni coinvolte per le definizioni dei numeri interi e razionali richiedevano soltanto l'uso di prodotti cartesiani e di loro quozienti rispetto ad opportune relazioni di equivalenza. Invece, come vedremo, la costruzione dei reali richiede un uso essenziale dell'assioma delle parti, che tra l'altro determinerà il salto di cardinalità dal numerabile al continuo non numerabile.
La prima parte della costruzione si basa esclusivamente sulle proprietà di $\mathbb{Q}$ come insieme ordinato, senza alcun riferimento alla sua struttura algebrica di campo.

Definizione A.2.1. Un sottoinsieme $X \subseteq \mathbb{Q}$ si dice *taglio di Dedekind* se:
(1) X è non banale, cioè $X \neq \emptyset$ e $X \neq \mathbb{Q}$;
(2) X è un segmento iniziale;
(3) X non ha massimo.

Notiamo che, in base alla condizione (2), $x \notin X$ se e solo se x è un maggiorante di X. Il segmento iniziale X_q generato da un razionale $q \in \mathbb{Q}$, è un taglio di Dedekind:

$$X_q = \{q' \in \mathbb{Q} \mid q' < q\}.$$

Ma ci sono anche tagli di Dedekind che non sono di quella forma. Un tipico esempio è dato dal seguente taglio, che sarà identificato con il numero reale $\sqrt{2}$: $X = \{q \in \mathbb{Q} \mid q \leq 0 \vee q^2 < 2\}$.

Definizione A.2.2. L'insieme $\{X \subseteq \mathbb{Q} \mid X$ è taglio di Dedekind$\}$ è detto *insieme dei numeri reali*, ed è denotato con $\mathbb{R}$.

Osserviamo che l'esistenza dell'insieme $\mathbb{R}$ è garantita dall'assioma delle parti e dall'assioma di separazione. La relazione d'inclusione tra gli elementi di $\mathbb{R}$ è una relazione d'ordine totale e *completa*. Precisamente:

Teorema A.2.1. *Valgono i seguenti fatti:*
(1) *per $X, Y \in \mathbb{R}$ poniamo $X \leq Y$ quando $X \subseteq Y$. Allora $(\mathbb{R}, \leq)$ è un insieme totalmente ordinato;*
(2) *per ogni $q, q' \in \mathbb{Q}$ si ha $q \leq q'$ se e solo se $X_q \leq X_{q'}$; dunque per identificazione, $(\mathbb{Q}, \leq)$ è un sottoinsieme totalmente ordinato di $(\mathbb{R}, \leq)$;*
(3) *$\mathbb{Q}$ è denso in $\mathbb{R}$;*
(4) *$(\mathbb{R}, \leq)$ è completo, cioè ogni sottoinsieme non vuoto $A \subseteq \mathbb{R}$ che sia superiormente limitato, ammette estremo superiore:*

$$\sup A = \min\{x \in \mathbb{R} \mid x > a \text{ per ogni } a \in A\}.$$

Dimostrazione. (1) La dimostrazione di questa parte è lasciata per esercizio.
(2) Siano $q < q'$ due numeri razionali. Banalmente $X_q \subseteq X_{q'}$. Quindi dobbiamo solo vedere che i due tagli sono diversi, e questo segue subito dalla densità che mostreremo al prossimo punto. Preso r con $q < r < q'$ avremo $r \in X_{q'}$ ma $r \notin X_q$. Il viceversa segue direttamente da quanto appena dimostrato, in quanto $q \geq q'$ allora $X_{q'} \supseteq X_q$.
(3) Siano $X < Y$, dobbiamo trovare $q \in Y - X$. Osserviamo che non si può escludere che $X = X_q$. Per definizione di taglio di Dedekind, Y non ha massimo, dunque esiste $q' \in Y$ con $q < q'$. Così $q \in X_{q'} - X$ e dunque $X < X_{q'}$. Inoltre da $q' \in Y$ segue subito che $X_{q'} < Y$.
(4) Sia $A \subseteq \mathbb{R}$ un insieme di tagli di Dedekind come nelle ipotesi. Consideriamo l'unione $Y = \bigcup A = \bigcup_{X \in A} X$ di tutti i suoi elementi. Vogliamo dimostrare che $Y \in \mathbb{R}$, cioè che Y stesso è un taglio di Dedekind. Da questo seguirà subito la tesi perché banalmente $X \subseteq Y$ per ogni $X \in A$, dunque Y è un maggiorante. Inoltre Y è il più piccolo dei maggioranti perché se $Y' \supseteq X$ per ogni $X \in A$, allora chiaramente $Y' \supseteq \bigcup_{X \in A} X = Y$. Il lettore mostri per esercizio che Y è un taglio di Dedekind. □

La nostra costruzione di $(\mathbb{R}, \leq)$ ha avuto come punto di partenza l'insieme ordinato $(\mathbb{Q}, \leq)$ dei numeri razionali. Più in generale, dato un qualunque insieme denso $(P, <)$ senza massimo né minimo, possiamo considere l'insieme e $\tilde{P}$ dei suoi tagli di Dedekind. Con gli stessi argomenti visti sopra, si dimostra che $(\tilde{P}, <)$ è un insieme ordinato completo che ha (una copia di) P come sottoinsieme denso. Questo procedimento di completamento è unico a meno di isomorfismi.

Appendice A

Esercizi risolti

Presenteremo nei paragrafi seguenti una grande quantità di esercizi risolti. Alcuni saranno piuttosto applicativi, altri invece avranno carattere più teorico e generalmente saranno ordinati per difficoltà crescente all'interno del relativo paragrafo. Invitiamo lo studente che volesse mettersi alla prova a risolverli per proprio conto e a guardarne dopo la soluzione, anche perché può così trovare nuove vie risolutive degli esercizi stessi, che sicuramente sono possibili.

A.1 Teoria degli insiemi generale

Esercizio A.1.1. Dimostrare che vale l'implicazione $(\mathcal{P}(x) \in \mathcal{P}(y)) \to (x \in y)$. Stabilire poi se ciascuna delle quattro proprietà vale o no:

$$\text{(a) } \bigcup \mathcal{P}(X) = X; \qquad \text{(b) } X = \mathcal{P}\left(\mathcal{P}\left(\bigcup X\right)\right); \qquad \text{(c) } X \in \mathcal{P}\left(\mathcal{P}\left(\bigcup X\right)\right);$$
$$\text{(d) } \mathcal{P}\left(\bigcup X\right) = \{\mathcal{P}(x) \mid x \in X\}.$$

Soluzione. Dimostrare l'implicazione è molto semplice, infatti vale

$$\mathcal{P}(x) \in \mathcal{P}(y) \to \mathcal{P}(x) \subseteq y,$$

e dunque, visto che $x \in \mathcal{P}(x)$ avremo $x \in y$.
(a) La proprietà è vera e la dimostrazione è la seguente:

$$x \in \bigcup \mathcal{P}(X) \leftrightarrow (\exists y)(y \in \mathcal{P}(X) \wedge x \in y) \leftrightarrow (\exists y)(y \subseteq X \wedge x \in y) \leftrightarrow x \in X.$$

(b) La proprietà è falsa: si consideri $X = 1 = \{\emptyset\}$. Vale che

$$\bigcup X = \emptyset \Longrightarrow \mathcal{P}\left(\bigcup X\right) = \{\emptyset\} \Longrightarrow \mathcal{P}\left(\mathcal{P}\left(\bigcup X\right)\right) = \{\emptyset, \{\emptyset\}\} = 2,$$

che è diverso da $1 = X$.

(c) La terza proprietà è vera e ha la seguente dimostrazione: sia $x \in X$, allora ogni $y \in x$ appartiene a $\bigcup X$, ossia $x \subseteq \bigcup X$. Dunque tutti gli elementi di $x \in X$ sono elementi di $\mathcal{P}\left(\bigcup X\right)$, cioè $X \subseteq \mathcal{P}\left(\bigcup X\right)$, ossia la tesi.
(d) Controesempi a questa proprietà si trovano facilmente considerando singoletti del tipo $X = \{x\}$, con $x \neq \emptyset$. Infatti

$$\{\mathcal{P}(x) \mid x \in X\} = \{\mathcal{P}(x)\},$$

mentre $\mathcal{P}\left(\bigcup X\right) = \mathcal{P}(x)$ contiene almeno due elementi, cioè $\emptyset$ e x.

A.2 Cardinalità

Esercizio A.2.1. Calcolare la cardinalità dei seguenti insiemi:
(1) $F_1 = \{f : \mathbb{N} \to \mathbb{N} \mid f \text{ crescente}\}$;
(2) $F_2 = \{f : \mathbb{N} \to \mathbb{N} \mid \forall n,\ f(n) \neq n\}$;
(3) $F_3 = \{f : \mathbb{N} \to \mathbb{N} \mid f \text{ è bigezione}\}$
Soluzione. (1) Essendo $F_1 \subseteq \mathbb{N}^{\mathbb{N}}$ varrà certamente $|F_1| \leq \aleph_0^{\aleph_0} = 2^{\aleph_0}$. Mostriamo che in realtà vale l'uguaglianza. Costruiamo la seguente applicazione

$$\begin{array}{ccc} \mathbb{N}^{\mathbb{N}} & \longrightarrow & F_1 \\ f & \longmapsto & \tilde{f} \end{array}, \quad \text{con } \tilde{f}(n) = \sum_{i=0}^{n} (f(i) + 1).$$

Intanto osserviamo che $\tilde{f} \in F_1$: infatti $\tilde{f}(n+1) - \tilde{f}(n) = f(n+1) + 1 > 0$. Inoltre l'applicazione costruita è iniettiva, ossia se $f \neq g$ allora $\tilde{f} \neq \tilde{g}$. Se $f \neq g$ esiste certamente

$$n_0 = \min\{n \in \mathbb{N} \mid f(n) \neq g(n)\}.$$

Ma allora si ha che

$$\tilde{f}(n_0) = f(n_0) + \sum_{i=0}^{n_0-1} (f(i) + 1) = f(n_0) + \sum_{i=0}^{n_0-1} (g(i) + 1),$$

e questa espressione è diversa da $g(n_0) + \sum_{i=0}^{n_0-1}(g(i)+1)$, ossia da $\tilde{g}(n_0)$. Essendo la corrispondenza iniettiva si ha l'altra disuguaglianza e quindi si può concludere che $|F_1| = 2^{\aleph_0}$ per il teorema di Cantor–Bernstein.
(2) Nuovamente $|F_2| \leq 2^{\aleph_0}$ per inclusione. Grazie alla stessa corripondenza del punto precedente si conclude nuovamente l'uguaglianza.
(3) Ancora, $|F_3| \leq 2^{\aleph_0}$. Stavolta costruiremo un'applicazione iniettiva da $\mathcal{P}(\mathbb{N})$ in F_3, e un modo è il seguente:

$$\begin{array}{ccc} \mathcal{P}(\mathbb{N}) & \longrightarrow & F_3 \\ A & \longmapsto & \sigma_A \end{array}, \quad \text{con } \sigma_A(n) = \begin{cases} n + \chi_A & \text{se } n \text{ è pari} \\ n + \chi_{A^C} & \text{se } n \text{ è dispari} \end{cases}.$$

L'applicazione costruita, essendo iniettiva, permette di concludere.

Esercizio A.2.2. Calcolare la cardinalità di $S = \{s : \mathbb{N} \to \mathbb{R} \mid s \text{ è convergente}\}$.
Soluzione. Sempre per inclusione in $\mathbb{R}^{\mathbb{N}}$ vale che $|S| \leq 2^{\aleph_0}$. Per l'altra disuguaglianza si considera l'applicazione che ad ogni $r \in \mathbb{R}$ associa la successione f_r tale che

$$f_r(n) = r + \frac{1}{n+1}.$$

Intanto per ogni $r \in R$ si ha che f_r è una successione convergente; inoltre se $r \neq s$ allora $f_r \neq f_s$, in quanto $f_r(0) = r \neq s = f_s(0)$. Dunque $|S| = 2^{\aleph_0}$.

Esercizio A.2.3. Calcolare la cardinalità dell'insieme delle applicazioni lineari da $\mathbb{R}^n$ in $\mathbb{R}^k$ con $n, k > 0$ interi.
Soluzione. La risposta è molto semplice. È noto dall'algebra lineare che si hanno i seguenti isomorfismi di spazi vettoriali:

$$\mathscr{L}(\mathbb{R}^n, \mathbb{R}^k) \cong \mathscr{M}_{nk}(\mathbb{R}) \cong \mathbb{R}^{nk}.$$

Ma allora sappiamo che ogni $\mathbb{R}^N$ con $N > 0$ ha la cardinalità del continuo.

Esercizio A.2.4. Calcolare la cardinalità di $F = \{A \subseteq \mathbb{R} \mid A \text{ è finito}\}$.
Soluzione. Visto che ogni singoletto $\{x\}$ con $x \in \mathbb{R}$ appartiene a F, segue che $|F| \geq 2^{\aleph_0}$. Adesso mostreremo che vale l'altra disuguaglianza; supponiamo ogni $A \in F$ ordinato con $A = \{r_0 < \cdots < r_n\}$ e costruiamo

$$\begin{array}{ccc} F & \longrightarrow & \mathbb{R}^{\mathbb{N}} \\ A & \longmapsto & f_A \end{array}, \quad \text{con } f_A(i) = \begin{cases} r_i & \text{se } i \in \{0, \ldots, n\} \\ 0 & \text{se } i > n \end{cases}.$$

Se $f_A = f_B$ per qualche $A, B \in F$ allora $A = B$. Infatti $\operatorname{imm} f_A = A \cup \{0\}$ e $\operatorname{imm} f_B = B \cup \{0\}$ e tali due immagini sono uguali.

Esercizio A.2.5. Calcolare la cardinalità di $A = \bigcup_{\gamma<\omega_1} A_\gamma$, dove $\{A_\gamma \mid \gamma < \omega_1\}$ è una famiglia di aperti non vuoti di $\mathbb{R}$.
Soluzione. Visto che $A \subseteq \mathbb{R}$ segue che $|A| \leq 2^{\aleph_0}$. Per mostrare l'altra uguaglianza facciamo ricorso alle regole di calcolo per cardinali:

$$|A| \leq \sum_{\gamma<\omega_1} |A_\gamma| \leq \sum_{\gamma<\omega_1} 2^{\aleph_0} = 2^{\aleph_0} \cdot \aleph_1 = 2^{\aleph_0},$$

e abbiamo concluso.

Esercizio A.2.6. Calcolare la cardinalità di $A = \bigcup_{\alpha<\omega_1} \mathbb{N}^\alpha$, ossia l'insieme di tutte le sequenza di numeri naturali di lunghezza un ordinale numerabile α.
Soluzione. Nuovamente usiamo le regole di calcolo per cardinali:

$$|A| = \sum_{\alpha<\omega_1} |\mathbb{N}^\alpha| = \sum_{\alpha<\omega_1} \aleph_0^{|\alpha|} = \aleph_1 \cdot \aleph_0^{\aleph_1} = \aleph_0 \cdot 2^{\aleph_1} = 2^{\aleph_1}.$$

Esercizio A.2.7. Calcolare la cardinalità di $X = \{f : A \to \mathbb{R} \mid A \text{ è finito}\}$.
Soluzione. Certamente per ogni insieme finito A c'è l'applicazione di inclusione come elemento di X, e dunque questa sorta di inclusione comporta che $|X| \geq |Fin(\mathbb{R})| = 2^{\aleph_0}$, come abbiamo mostrato in un esercizio precedente. A questo punto

$$|X| = \left| \bigcup_{A \in Fin(\mathbb{R})} \mathbb{R}^A \right| \leq \sum_{A \in Fin(\mathbb{R})} |\mathbb{R}^A| = |Fin(\mathbb{R})| \cdot 2^{\aleph_0} = 2^{\aleph_0}.$$

Dunque in definitiva X ha la cardinalità del continuo.

Esercizio A.2.8. Calcolare la cardinalità di $X = \{A \subseteq \mathbb{R} \mid |A| = |\mathbb{R} - A| = |\mathbb{R}|\}$, ossia l'insieme di tutti i sottoinsiemi dei numeri reali che hanno la potenza del continuo e tali che anche il loro complementare ce l'abbia.
Soluzione. Denotiamo con $FN(\mathbb{R})$ l'insieme dei sottoinsiemi di $\mathbb{R}$ che sono finiti o numerabili, ossia $FN(\mathbb{R}) = Fin(\mathbb{R}) \cup Num(\mathbb{R})$; denotiamo poi con $CFN(\mathbb{R})$ l'insieme dei sottoinsiemi di $\mathbb{R}$ il cui complementare è finito o numerabile. Si ha allora

$$X = \mathcal{P}(\mathbb{R}) - FN(\mathbb{R}) - CFN(\mathbb{R}).$$

Già sappiamo che $|Fin(\mathbb{R})| = 2^{\aleph_0}$; adesso occupiamoci di $Num(\mathbb{R})$, e affermiamo che anche questo insieme ha la potenza del continuo. Sia $A \subseteq \mathbb{R}$ numerabile, allora esiste $f_A : \mathbb{N} \to A$ biunivoca. L'applicazione

$$\begin{array}{ccc} Num(\mathbb{R}) & \longrightarrow & Fun\left(\aleph_0, 2^{\aleph_0}\right) \\ A & \longmapsto & f_A \end{array}$$

è iniettiva e dunque $|Num(\mathbb{R})| \leq \left|Fun\left(\aleph_0, 2^{\aleph_0}\right)\right| = \left(2^{\aleph_0}\right)^{\aleph_0} = 2^{\aleph_0}$. Considerata poi l'applicazione iniettiva che a $r \in \mathbb{R}$ associa $\{r + n \mid n \in \mathbb{N}\} \in Num(\mathbb{R})$ si ha anche l'altra disuguaglianza. Dunque concludiamo che $FN(\mathbb{R})$ ha la potenza del continuo.
A questo punto trattare $CFN(\mathbb{R})$ è molto semplice. La corrispondenza $CFN(\mathbb{R}) \to FN(\mathbb{R})$ che associa ad ogni $A \in CFN(\mathbb{R})$ il proprio complementare è biunivoca, e pertanto $|CFN(\mathbb{R})| = |FN(\mathbb{R})| = 2^{\aleph_0}$. Da tutto ciò segue che

$$|X| = |\mathcal{P}(\mathbb{R})| = 2^{2^{\aleph_0}},$$

in quanto gli altri due sottoinsiemi non hanno la cardinalità di $\mathcal{P}(\mathbb{R})$.

Esercizio A.2.9. Dimostrare che per ogni κ cardinale infinito vale $|Fin(\kappa)| = \kappa$.
Soluzione. Sia $A = \{\alpha_1 < \cdots < \alpha_n\} \subseteq \kappa$ un sottoinsieme finito. Allora possiamo considerare la mappa iniettiva

$$\begin{array}{ccc} Fin(\kappa) & \longrightarrow & \bigcup_{n<\omega} \kappa^n \\ A & \longmapsto & (\alpha_1, \ldots, \alpha_n) \end{array}.$$

Intanto osserviamo che

$$\left|\bigcup_{n<\omega} \kappa^n\right| = \sum_{n<\omega} |\kappa^n| = \aleph_0 \cdot \kappa = \kappa,$$

da cui $|Fin(\kappa)| \leq \kappa$. Poi esiste l'applicazione iniettiva che associa ad ogni $\lambda \in \kappa$ il sottoinsieme finito $\{\lambda\} \in Fin(\kappa)$, e questa fornisce l'altra disuguaglianza.

Esercizio A.2.10. Siano $\kappa \geq \nu$ cardinali infiniti, e sia $S(\kappa)_\nu = \{A \subseteq \kappa \mid |A| = \nu\}$ l'insieme di tutte le parti di κ aventi cardinalità ν. Dimostrare che

$$|S(\kappa)_\nu| = \kappa^\nu.$$

Soluzione. Sia $A \subseteq \kappa$ di cardinalità ν e fissiamo una bigezione $f_A : \nu \to A$. La corrispondenza $S(\kappa)_\nu \to Fun(\nu, \kappa)$ che associa ad ogni A la bigezione f_A è certamente iniettiva. Dunque

$$|S(\kappa)_\nu| \leq |Fun(\nu, \kappa)| = \kappa^\nu.$$

Ora si osservi che $|\nu \times \kappa| = \nu \cdot \kappa = \kappa$, e dunque $|S(\kappa)_\nu| = |S(\nu \times \kappa)_\nu|$. Ora però, ogni funzione $f : \nu \to \kappa$ è un sottoinsieme del prodotto cartesiano $\nu \times \kappa$ e inoltre $|f| = \nu$.[1] Ma allora si ha che $Fun(\nu, \kappa) \subseteq S(\nu \times \kappa)_\nu$, e da ciò si ottiene l'altra disuguaglianza.

Esercizio A.2.11. Calcolare la cardinalità di $X_i = \{A \subseteq \omega_{17} \mid |A| = \aleph_i\}$, per ogni $i \in \{0, \ldots, 17\}$.
Soluzione. Questa è una semplice applicazione dell'esercizio precedente. Grazie alla formula di Hausdorff si ha

$$|X_i| = \aleph_{17}^{\aleph_i} = \aleph_{17} \cdot \aleph_{16}^{\aleph_i} = \aleph_{17} \cdot \aleph_0^{\aleph_i} = \aleph_{17} \cdot 2^{\aleph_i} = \begin{cases} 2^{\aleph_i} & \text{se } i \in \{17, 16\} \\ \aleph_{17} \cdot 2^{\aleph_i} & \text{se } i \leq 15 \end{cases}.$$

Osserviamo che nel caso $i \leq 15$ non possiamo dire di più di quanto abbiamo scritto perché non sappiamo "quanto sia grande" $2^{\aleph_i}$. Se assumiamo la validità dell'ipotesi generalizzata del continuo si ha in quei casi

$$\aleph_{17} \cdot 2^{\aleph_i} = \aleph_{17} \cdot \aleph_{i+1} = \aleph_{17}.$$

Assumendola anche per gli altri due casi scritti, avremo che $|X_{16}| = 2^{\aleph_{16}} = \aleph_{17}$ ancora, mentre $|X_{17}| = 2^{\aleph_{17}} = \aleph_{18}$.

[1] e questo perché $x \mapsto (x, f(x))$ è una bigezione tra ν e f.

Esercizio A.2.12. Sia $X = \{f : \omega_{17} \to \omega_{17} \mid f \text{ strettamente crescente e continua}\}$, dove la continuità è la continuità ai limiti.[2] Calcolare la cardinalità di X assumendo l'ipotesi generalizzata del continuo.
Soluzione. Intanto $X \subseteq Fun(\omega_{17}, \omega_{17})$, e dunque $|X| \leq |Fun(\omega_{17}, \omega_{17})| = \aleph_{17}^{\aleph_{17}} = 2^{\aleph_{17}} = \aleph_{18}$. Adesso consideriamo un $A \subseteq \omega_{17}$ e la funzione $g_A : \omega_{17} \to \omega_{17}$ definita come

$$\begin{cases} g_A(0) = 0 \\ g_A(\alpha + 1) = g_A(\alpha) + 1 + \chi_{A^C}(\alpha) \\ g_A(\lambda) = \sup_{\beta<\lambda} g_A(\beta) \text{ se } \lambda \text{ è limite.} \end{cases}$$

Segue subito dalla definizione che g_A è strettamente crescente e continua ai limiti. Se $A \neq B$ vogliamo mostrare che $g_A \neq g_B$. Sia

$$\gamma = \min((A - B) \cup (B - A))$$

il più piccolo elemento che ci dice che i due insiemi sono diversi; è immediato verificare per induzione che per ogni $\delta \leq \gamma$ si ha $g_A(\delta) = g_B(\delta)$, ma invece $g_A(\gamma + 1) \neq g_B(\gamma + 1)$. Ne segue che la corrispondenza $\mathcal{P}(\omega_{17}) \to X$, che associa ad A la funzione g_A, è una corrispondenza iniettiva, e dunque

$$|\mathcal{P}(\omega_{17})| = 2^{\aleph_{17}} = \aleph_{18} \leq |X|,$$

e abbiamo concluso. Notiamo che se non avessimo assunto l'ipotesi generalizzata del continuo avremmo potuto dire che $|X| = 2^{\aleph_{17}}$.

A.2.1 I boreliani di $\mathbb{R}^N$

Dato un insieme X, una σ–algebra di parti di X è un sottoinsieme di $\mathcal{P}(X)$ che ha X come elemento ed è chiuso per complementare e per unione numerabile di suoi elementi. Considerato un certo $B \subseteq X$ esiste sempre la cosidetta σ–algebra generata da B, ossia la più piccola σ–algebra che contiene B: infatti questa può essere ottenuta per intersezione di tutte le σ–algebre che contengono B (tra cui sicuramente c'è $\mathcal{P}(X)$).
Adesso consideriamo $X = \mathbb{R}^N$ e come base per la σ–algebra l'insieme degli aperti di $\mathbb{R}^N$, che denoteremo con $\mathcal{A}(\mathbb{R}^N)$:

Definizione A.2.1. La σ–algebra generata dagli aperti prende il nome di *insieme dei boreliani* di $\mathbb{R}^N$, e la indicheremo con $\mathcal{B}(\mathbb{R}^N)$.

Intanto, qual è la cardinalità dell'insieme degli aperti? Abbiamo mostrato nella parte di teoria che gli aperti di $\mathbb{R}$ sono $2^{\aleph_0}$. Ora non è difficile mostrare questo fatto anche più in generale:

[2] data f definita su un ordinale α, si dice *continua* se per ogni $\lambda < \alpha$ ordinale limite si ha $f(\lambda) = \bigcup_{\gamma<\lambda} f(\gamma)$.

Proposizione A.2.1. *Per ogni $N \geq 1$ l'insieme degli aperti di $\mathbb{R}^N$ ha la potenza del continuo.*

Dimostrazione. Vale certamente che gli aperti sono più di $2^{\aleph_0}$, in quanto tutte le palle aperte di centro l'origine e raggio reale sono aperte. Adesso mostriamo che vale anche l'altra disuguaglianza. Costruiamo l'applicazione

$$\begin{array}{ccc} \mathcal{A}(\mathbb{R}^N) & \longrightarrow & \mathcal{P}\left(\bigotimes_{i=1}^{N} \mathbb{Q} \times \mathbb{Q}^+\right) \\ A & \longmapsto & \{(q_1, \ldots, q_N, r) \mid B((q_1, \ldots, q_N), r) \subseteq A\} \end{array} .$$

Tale applicazione si dimostra essere iniettiva, e quindi abbiamo concluso. □

Adesso lavoreremo con i boreliani di $\mathbb{R}$. Intanto è noto dal corso di analisi che i boreliani non esuriscono tutte le parti di $\mathbb{R}$ perché ci sono insiemi non misurabili (come l'insieme di Vitali) che non sono boreliani; infatti i boreliani sono inclusi negli insiemi misurabili e quindi l'esistenza di insiemi non misurabili (per la quale serve l'assioma di scelta) prova che $\mathcal{B}(\mathbb{R}) \subset \mathcal{P}(\mathbb{R})$.
Adesso però mostreremo che $\mathcal{B}(\mathbb{R}) \subset \mathcal{M}(\mathbb{R})$, ma non costruendo un misurabile non boreliano, bensì ragionando per questioni di cardinalità. Intanto vediamo quanti sono i misurabili: visto che la misura di Lebesgue è completa, ogni sottoinsieme di un insieme di misura nulla è misurabile e ha misura nulla. Dato che l'insieme di Cantor C ha misura nulla avremo che l'insieme dei misurabili $\mathcal{M}(\mathbb{R})$ contiene tutti i sottoinsiemi dell'insieme di Cantor, ossia $\mathcal{P}(\mathbb{R}) \supseteq \mathcal{M}(\mathbb{R}) \supseteq \mathcal{P}(C)$. Ma visto che l'insieme di Cantor ha cardinalità $2^{\aleph_0}$ si ha

$$|\mathcal{M}(\mathbb{R})| = 2^{2^{\aleph_0}}.$$

Adesso invece mostreremo che i boreliani di $\mathbb{R}$ sono solo $2^{\aleph_0}$. Invece di costruire la σ–algebra dei boreliani dall'alto (come intersezione) adesso daremo una versione più costruittiva e che parte proprio dalla classedegli aperti. Partendo da questa effettueremo operazioni di chiusura rispetto al complementare e alle unioni numerabili e vedremo che dopo un certo "numero di passi" arriveremo ad ottenere proprio $\mathcal{B}(\mathbb{R})$. Diamo la seguente definizione ricorsiva sugli ordinali, poi vedremo fin dove dovremo spingerci:

$$\begin{cases} \mathcal{B}_0 = \mathcal{A}(\mathbb{R}) \\ \mathcal{B}_{\alpha+1} = \mathcal{B}_\alpha \cup \{B^C \mid B \in \mathcal{B}_\alpha\} \cup \left\{\bigcup_{n=1}^{\infty} B_n \mid B_n \in \mathcal{B}_\alpha\right\} \cup \left\{\bigcap_{n=1}^{\infty} B_n \mid B_n \in \mathcal{B}_\alpha\right\} \\ \mathcal{B}_\lambda = \bigcup_{\alpha<\lambda} \mathcal{B}_\alpha \text{ se } \lambda \text{ è limite} \end{cases} .$$

Intanto affermiamo che $\mathcal{B}_\omega$ non è certamente $\mathcal{B}(\mathbb{R})$ in quanto è chiuso per unioni finite, ma non per unioni numerabili. Sia B_0 un aperto, B_1 un chiuso e poi sia $B_k \in \mathcal{B}_k - \bigcup_{i=0}^{k-1} \mathcal{B}_i$ per ogni $k \geq 2$; vale allora che $\bigcup_{k=0}^{\infty} B_k$ non sta in $\mathcal{B}_\omega$.

Questo controesempio ci fa venire in mente che i boreliani, per essere così "grandi" da contenere le unioni di sequenze numerabili (di lunghezza ω), si ottengano ad un passo in cui l'indice α è un ordinale di cofinalità maggiore di $\aleph_0$. Il primo che incontriamo è prorpio $\mathcal{B}_{\omega_1}$, e in effetti è quello corretto.

Teorema A.2.1. *Vale* $\mathcal{B}(\mathbb{R}) = \mathcal{B}_{\omega_1}$.

Dimostrazione. È immediato verificare per induzione transfinita che $\mathcal{B}_\alpha \subseteq \mathcal{B}(\mathbb{R})$ per ogni $\alpha < \omega_1$. Dunque $\mathcal{B}_{\omega_1} = \bigcup_{\alpha<\omega_1} \mathcal{B}_\alpha \subseteq \mathcal{B}(\mathbb{R})$.
Adesso, come è standard in questo tipo di dimostrazioni, per mostrare che $\mathcal{B}(\mathbb{R}) \subseteq \mathcal{B}_{\omega_1}$ ci basta dimostrare che $\mathcal{B}_{\omega_1}$ è una σ–algebra che contiene gli aperti; la tesi segue poi per minimalità dei boreliani. Certamente contiene gli aperti, in quanto $\mathcal{B}_0 \subseteq \mathcal{B}_{\omega_1}$ e in particolare contiene anche $\mathbb{R}$; se poi $B \in \mathcal{B}_{\omega_1}$ allora esiste un $\alpha < \omega_1$ tale che $B \in \mathcal{B}_\alpha$, ma allora $B^C \in \mathcal{B}_{\alpha+1}$. Sia adesso $\{B_n \mid n \in \mathbb{N}\} \subseteq \mathcal{B}_{\omega_1}$ una famiglia numerabile, e per ogni $n \in \mathbb{N}$ sia

$$\alpha_n = \min\{\alpha < \omega_1 \mid B_n \in \mathcal{B}_\alpha\}.$$

Consideriamo $\alpha = \sup_{n<\omega} \alpha_n$; visto che ω_1 non è numerabile deve essere certamente $\gamma \in \omega_1$.[3] Dunque la famiglia è contenuta in $\mathcal{B}_\gamma$, e allora la sua unione e la sua intersezione sono contenute in $\mathcal{B}_{\gamma+1}$. □

A questo punto ci resta in sospeso solo la questione della cardinalità di $\mathcal{B}_{\omega_1}$, questione che risolviamo subito:

Teorema A.2.2. *Vale* $|\mathcal{B}_{\omega_1}| = 2^{\aleph_0}$.

Dimostrazione. Intanto

$$|\mathcal{B}_{\omega_1}| = \sum_{\alpha<\omega_1} |\mathcal{B}_\alpha|.$$

Adesso vogliamo mostrare che per ogni $\alpha < \omega_1$ si ha $|\mathcal{B}_\alpha| = 2^{\aleph_0}$. Sappiamo da quanto visto nella parte di teoria che $|\mathcal{B}_0| = 2^{\aleph_0}$; supponiamo adesso che $|\mathcal{B}_\alpha| = 2^{\aleph_0}$ e consideriamo

$$\begin{aligned} |\mathcal{B}_{\alpha+1}| \;\leq\; & |\mathcal{B}_\alpha| + \left|\{B^C \mid B \in \mathcal{B}_\alpha\}\right| + \left|\left\{\bigcup_{n=1}^{\infty} B_n \mid B_n \in \mathcal{B}_\alpha\right\}\right| + \\ & + \left|\left\{\bigcap_{n=1}^{\infty} B_n \mid B_n \in \mathcal{B}_\alpha\right\}\right| \leq 2^{\aleph_0} \cdot 4 = 2^{\aleph_0}. \end{aligned}$$

Per l'insieme $\mathcal{B}_\alpha$ abbiamo l'ipotesi induttiva e quello dei suoi complementari ha chiaramente la stessa cardinalità. Per maggiorare la cardinalità dell'insieme delle

[3] potevamo anche ragionare con la cofinalità come segue. La corrispondenza $f : \omega \to \omega_1$ che manda $n \mapsto \alpha_n$ è necessariamente limitata, perché sennò $\mathrm{cf}(\omega_1) \leq \aleph_0$. Dunque esiste un $\gamma < \omega_1$ tale che $\gamma \geq \alpha_n$ per ogni $n \in \mathbb{N}$.

unioni basta pensare che queste siano tutte distinte: questo modo se ne vengono ad avere tante quante le sequenze di insiemi uniti, ossia tante quante $\mathcal{B}_\alpha^{\mathbb{N}}$, ossia $2^{\aleph_0}$. Per le intersezioni il ragionamento è analogo. Adesso ci manca il passo limite, ma questo è facile. Sia $\lambda < \omega_1$ un ordinale limite, allora

$$|\mathcal{B}_\lambda| \leq \sum_{\alpha<\lambda} |\mathcal{B}_\alpha| = \sum_{\alpha<\lambda} 2^{\aleph_0} = \aleph_0 \cdot 2^{\aleph_0} = 2^{\aleph_0}.$$

Per l'altra disuguaglianza basta osservare che ogni $\mathcal{B}_\lambda$ contiene gli aperti. A questo punto non ci resta altro che proseguire il calcolo iniziale

$$|\mathcal{B}_{\omega_1}| = \sum_{\alpha<\omega_1} |\mathcal{B}_\alpha| = \aleph_1 \cdot 2^{\aleph_0} = 2^{\aleph_0},$$

e abbiamo finito. □

A.3 Buoni ordini e numeri ordinali

Esercizio A.3.1. Calcolare $5 + \omega$.
Soluzione. Intanto ω è un ordinale limite, quindi per definizione

$$5 + \omega = \bigcup_{n<\omega} (5 + n) = \omega.$$

Esercizio A.3.2 (associatività del prodotto)**.** Dimostrare che per ogni α, β e γ numeri ordinali vale

$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma).$$

Soluzione. Si procede, così come per la somma, per induzione su γ. Se $\gamma = 0$ la tesi è banale; supponiamo dunque $\gamma = \delta + 1$, allora

$$\begin{aligned} (\alpha \cdot \beta) \cdot \gamma &= (\alpha \cdot \beta) \cdot (\delta + 1) = \alpha \cdot (\beta \cdot \delta) + \alpha \cdot \beta = \\ &= \alpha \cdot (\beta \cdot \delta + \beta) = \alpha \cdot (\beta \cdot (\delta + 1)) = \alpha \cdot (\beta \cdot \gamma). \end{aligned}$$

Il caso in cui γ sia un limite si prova esattamente come nel caso dell'addizione: si dimostra che $\beta \cdot \gamma$ è un limite e poi si scrive

$$(\alpha \cdot \beta) \cdot \gamma = \bigcup_{\delta<\gamma} (\alpha \cdot \beta) \cdot \delta = \bigcup_{\delta<\gamma} \alpha \cdot (\beta \cdot \delta) = \bigcup_{\beta\cdot\delta<\beta\cdot\gamma} \alpha \cdot (\beta \cdot \delta) = \alpha \cdot (\beta \cdot \gamma),$$

e ciò basta per concludere.

Come scritto nella relativa sezione nella parte di teoria vogliamo desso caratterizzare da un punto di vista di buoni ordini, l'ordinale esponenziale. A dispetto di quanto si possa credere inizialmente, questo non corrisponde ad un buon ordinamento dell'insieme A^B delle funzioni da B ad A. Intanto denotiamo con $Fun_0(B, A)$ l'insieme delle funzioni da B ad A a supporto finito, ossia l'insieme $\{f : B \to A \mid \{b \in B \mid f(b) \neq 0\}$ è finito$\}$.

Proposizione A.3.1. *Sia* $(Fun_0(B, A), <)$ *l'insieme ben ordinato con l'ordine*

$$f < g \iff f \neq g \text{ e } f(\tilde{b}) < g(\tilde{b}) \text{ dove } \tilde{b} = \max\{b \in B \mid f(b) \neq g(b)\}.$$

Se $(A, <_A) \cong \alpha$ *e* $(B, <_B) \cong \beta$ *allora* $(Fun_0(B, A), <) \cong \alpha^\beta$.

Dimostrazione. Procediamo per induzione transfinita su β. Se $\beta = 0$ allora l'insieme $(Fun_0(B, A), <)$ ha come unico elemento la funzione vuota e infatti per definizione che $\alpha^0 = 1$.
Supponiamo che $\beta = \gamma + 1$, per definizione vale

$$\alpha^{\gamma+1} = \alpha^\gamma \cdot \alpha.$$

Per ipotesi induttiva $B \cong B' \oplus 1$, dove $B' = \{b \in B \mid b < \max B\} \cong \gamma$ e $1 = \max B$. Se mostriamo che, con i rispettivi ordini, $Fun_0(B, A) \cong Fun_0(B', A) \odot A$ allora abbiamo finito. La corrispondenza

$$\psi : f \longmapsto \left(f|_{B'}, f(\bar{b})\right),$$

dove $\bar{b} = \max B$, è una corrispondenza biunivoca. Osserviamo che

$$f < g \iff (f \neq g) \wedge \left(f(\bar{b}) < g(\bar{b}) \vee \left(f(\bar{b}) = g(\bar{b}) \wedge f|_{B'} < g|_{B'}\right)\right);$$

ossia chiedere $f < g$ è equivalente a ordinare la coppia $\psi(f)$ nell'ordine antilessicografico nel prodotto $Fun_0(B', A) \odot A$. Cioè ψ è un isomorfismo.
Se $\beta = \lambda$ è un limite allora

$$\alpha^\lambda = \bigcup_{\gamma<\lambda} \alpha^\gamma.$$

Esiste $\psi : \lambda \to (B, <)$ isomorfismo e dunque, per le proprietà dei segmenti iniziali, per ogni $\gamma < \lambda$ abbiamo $\gamma = \lambda_\gamma \cong \left(B_{\psi(\gamma)}, <\right)$. Ciò significa che per ogni $\gamma < \lambda$ esiste φ_γ isomorfismo tra α^γ e $Fun_0(B_{\psi(\gamma)}, A)$. Per poter portare questi isomorfismi nell'insieme $Fun_0(B, A)$ utilizziamo l'inclusione canonica $i_\gamma : Fun_0(B_{\psi(\gamma)}, A) \to Fun_0(B, A)$, e poniamo dunque

$$\varphi = \bigcup_{\gamma<\lambda} (i_\gamma \circ \varphi_\gamma).$$

Questo è un isomorfismo tra α^λ e $Fun_0(B, A)$, e le ultime semplici verifiche sono lasciate per esercizio. □

Corollario A.3.1. *Se α e β sono ordinali numerabili allora α^β è numerabile.*

Dimostrazione. Se $\alpha \cong (A, <_1)$ e $\beta \cong (B, <_2)$, sappiamo dalla proposizione che $|\alpha^\beta| = |Fun_0(B, A)|$. Se $f : B \to A$ è una funzione di questo insieme si può considerare

$$\tilde{f} = f|_{\{b \in B \ | \ f(b) \neq 0\}}.$$

La mappa $f \mapsto \tilde{f}$ è una bigezione tra $Fun_0(B, A)$ e

$$F = \bigcup_{B' \subseteq B \text{ finiti}} Fun_0(B', A - \{0\}).$$

A questo punto basta calcolare la cardinalità di quest'ultimo insieme: osserviamo intanto che queste funzioni sono almeno $\aleph_0$ (ci sono le funzioni costanti ad ogni elemento di A), poi

$$|F| \leq \sum_{B' \subseteq B \text{ finiti}} \left|Fun_0(B', A - \{0\})\right| \leq \sum_{B' \subseteq B \text{ finiti}} \aleph_0 = \aleph_0;$$

la seconda maggiorazione è dovuta al fatto che $Fun_0(B', A - \{0\}) \subseteq Fun(B', A)$, che sono numerabili per ogni $B' \subseteq B$ finito; l'uguale successivo invece si ha perché i sottoinsiemi finiti di B sono numerabili essendo B numerabile. $\square$

Esercizio A.3.3. Mettere in ordine i seguenti sei ordinali:

$$\text{(a) } \omega^\omega \cdot (\omega + \omega); \qquad \text{(b) } (\omega + \omega) \cdot \omega^\omega; \qquad \text{(c) } \omega^\omega \cdot \omega + \omega^\omega \cdot \omega;$$
$$\text{(d) } \omega \cdot \omega^\omega + \omega \cdot \omega^\omega; \qquad \text{(e) } \omega^\omega \cdot \omega + \omega \cdot \omega^\omega; \qquad \text{(f) } \omega \cdot \omega^\omega + \omega^\omega \cdot \omega.$$

Soluzione. Vediamo di calcolare più esplicitamente qualcuno di questi ordinali. Applicando la proprietà distributiva a destra si ottiene che l'ordinale (a) e l'ordinale (c) sono uguali e uguali a $\omega^{\omega+1} \cdot 2$. Calcoliamo adesso il (b):

$$(\omega + \omega) \cdot \omega^\omega = \omega \cdot 2 \cdot \omega^\omega = \omega^\omega,$$

in quanto $\omega^\omega \leq \omega \cdot 2 \cdot \omega^\omega \leq \omega^2 \cdot \omega^\omega = \omega^\omega$. Ora calcoliamo il (d):

$$\omega \cdot \omega^\omega + \omega \cdot \omega^\omega = \omega \cdot (\omega^\omega + \omega^\omega) = \omega \cdot \omega^\omega \cdot 2 = \omega^\omega \cdot 2,$$

da cui si vede subito che $(b) < (d)$. Per quanto riguarda (e) invece $\omega^\omega \cdot \omega + \omega \cdot \omega^\omega = \omega^\omega \cdot \omega + \omega^\omega = \omega^{\omega+1} + \omega^\omega$, e infine per (f) si ha $\omega \cdot \omega^\omega + \omega^\omega \cdot \omega = \omega^\omega + \omega^\omega \cdot \omega = \omega^\omega \cdot (1 + \omega) = \omega^{\omega+1}$. In definitiva

$$\text{(b)} < \text{(d)} < \text{(f)} < \text{(e)} < \text{(a)} = \text{(c)},$$

e l'esercizio è concluso.

Esercizio A.3.4. Dimostrare che per ogni $\alpha < \beta$ si ha $\omega^\alpha + \omega^\beta = \omega^\beta$.
Soluzione. Se $\alpha < \beta$ allora esiste ξ tale che $\alpha + \xi = \beta$. Dunque si ha

$$\omega^\alpha + \omega^\beta = \omega^\alpha + \omega^\alpha \cdot \omega^\xi = \omega^\alpha \cdot (1 + \omega^\xi) = \omega^\alpha \cdot \omega^\xi = \omega^\beta,$$

e la dimostrazione è conclusa.

Definizione A.3.1. Un ordinale α è *additivamente chiuso* se per ogni $\beta, \gamma < \alpha$ vale $\beta + \gamma < \alpha$.

Proposizione A.3.2. *α è additivamernte chiuso se e solo se esiste δ tale che $\alpha = \omega^\delta$.*

Dimostrazione. ($\Longleftarrow$) Siano $\beta, \gamma < \omega^\delta$ e poniamo

$$\xi_1 = \min\{\zeta \mid \beta < \omega^\zeta\} \quad \text{e} \quad \xi_2 = \min\{\zeta \mid \gamma < \omega^\zeta\};$$

tali minimi esistono perché β e γ sono elementi del rispettivo insieme di cui si fa il minimo. Con il solito ragionamento per assurdo che si fa in questo tipo di dimostrazioni (che contraddice la minimalità) vale che ξ_i è successore, e sia $\xi_i = \vartheta_i + 1$. Vale allora

$$\omega^{\vartheta_1} \leq \beta < \omega^{\vartheta_1 + 1} \quad \text{e} \quad \omega^{\vartheta_2} \leq \gamma < \omega^{\vartheta_2 + 1}.$$

Ma allora, visto che ω è un ordinale limite, avremo $\beta \leq \omega^{\vartheta_1} \cdot n$ per qualche $n < \omega$ ed anche $\gamma \leq \omega^{\vartheta_2} \cdot k$ per qualche $k < \omega$. Dunque, detto $\vartheta = \max\{\vartheta_1, \vartheta_2\}$ si ha

$$\beta + \gamma \leq \omega^{\vartheta_1} \cdot n + \omega^{\vartheta_2} \cdot k \leq \omega^\vartheta (n + k) < \omega^\vartheta \cdot \omega = \omega^{\vartheta + 1} \leq \omega^\delta.$$

($\Longrightarrow$) Procediamo per assurdo, mostrando che per ogni ordinale fissato δ, se $\omega^\delta < \alpha < \omega^{\delta+1}$ allora α non è additivamente chiuso. Visto che $\omega^{\delta+1} = \sup_{n<\omega} \omega^\delta \cdot n$ possiamo prendere $1 \leq n < \omega$ con $\omega^\delta \cdot n < \alpha \leq \omega^\delta \cdot (n + 1)$. Ma allora si ha

$$\omega^\delta \cdot n + \omega^\delta \cdot n = \omega^\delta \cdot (n + n) \geq \omega^\delta \cdot (n + 1) \geq \alpha,$$

e quindi α non è additivamente chiuso. □

Osservazione A.3.1. Vogliamo notare che un analoga definizione si potrebbe dare per un ordinale *moltiplicativamente chiuso*. Diremo che $\alpha > 2$ è moltiplicativamente chiuso se vale che $\beta, \gamma < \alpha$ implica $\beta \cdot \gamma < \alpha$.
In modo analogo a quanto fatto nel precedente esercizio si può dimostrare che α è moltiplicativamente chiuso se e solo se esiste δ tale che $\alpha = \omega^{\omega^\delta}$.

Esercizio A.3.5. Calcolare $(\omega^2 + \omega \cdot 3 + 2) : (\omega + 4)$.
Soluzione. Abbiamo ad esempio

$$(\omega + 4) \cdot 3 = (\omega + 4) + (\omega + 4) + (\omega + 4) = \omega + (4 + \omega) + (4 + \omega) + 4 = \omega \cdot 3 + 4,$$

e procedendo analogamente si può dimostrare (induzione) che $(\omega+4) \cdot k = \omega \cdot k+4$ per ogni $k < \omega$. Vediamo dunque

$$(\omega + 4) \cdot \omega = \bigcup_{n<\omega} (\omega + 4) \cdot n = \bigcup_{n<\omega} \omega \cdot n + 4,$$

e l'ultimo estremo superiore fa ω in quanto è compreso tra due estremi superiori che danno per risultato ω. Ma neanche $(\omega + 4) \cdot (\omega + 1)$ basta. Adesso

$$(\omega + 4)(\omega + 3) = (\omega + 4) \cdot \omega + (\omega + 4) \cdot 3 = \omega^2 + \omega \cdot 3 + 4,$$

e ci siamo: abbiamo superato $\omega^2 + \omega \cdot 3 + 2$. Se si fa il prodotto con $\omega + 2$ si vede che invece non lo superiamo. Dunque il quoziente è $\omega + 2$, mentre il resto è

$$(\omega^2 + \omega \cdot 3 + 2) - (\omega + 4)(\omega + 2) = \omega + 2.$$

Esercizio A.3.6. Trovare dei sottoinsiemi di $\mathbb{R}$ isomorfi (con l'ordine indotto) agli ordinali ω^2, ω^3 e ω^ω.
Soluzione. (1) Per trovare un sottoinsieme isomorfo a ω^2 basta pensare a ω punti verso ognuno dei quali converge una successione dal basso. Basterà prendere

$$A = \left\{ n - \frac{1}{m} \mid n, m \in \mathbb{N}_0 \right\}.$$

Se vogliamo esplicitare l'isomorfismo con ω^2 basta mandare l'elemento $n - \frac{1}{m}$ in $\omega \cdot (n - 1) + m - 1 \in \omega^2$. Per ω^3 e per ω^n con $n < \omega$ la costruzione è del tutto simile; avremo in gioco insiemi con tre parametri anziché due.
(2) Per il punto precedente abbiamo degli insiemi $A_i \subseteq [i, i+1)$ con la proprietà che $(A_i, <) \cong \omega^i$ per ogni $i < \omega$ non nullo. Quello che vogliamo mostrare formalmente è che $\bigcup_{i=1}^{\infty} A_i \subseteq [1, \infty)$ è isomorfo con l'ordine indotto a ω^ω.
Intanto abbiamo

$$\left(\bigcup_{i=1}^{\infty} A_i, < \right) \cong \left(\bigcup_{i=1}^{\infty} \bigoplus_{j=1}^{i} A_j, < \right),$$

che chiameremo $(A, <)$: questo è un buon ordine perché unione di buoni ordini uno segmento iniziale dell'altro. Ciascun $\bigoplus_{j=1}^{i} A_j$ è segmento iniziale di A e è isomorfo a $\sum_{j=1}^{i} \omega^j = \omega^i$ (si provi per induzione su i). Dunque questo mostra che il tipo d'ordine di $(A, <)$ è almeno ω^ω. Del resto però non può essere strettamente superiore perché sennò in $(A, <)$ ci sarebbe un segmento iniziale isomorfo a ω^ω, ma ciascun segmento iniziale ha tipo d'ordine contenuto in qualche ω^n.

Esercizio A.3.7. Determinare tutte le coppie di ordinali (α, β) con $\alpha, \beta < \omega^2$ tali che $\alpha + \beta = \beta + \alpha$.
Soluzione. Banalmente si ha che la somma commuta quando almeno uno dei due ordinali è nullo. Dunque nel seguito suppporremo sempre $\alpha, \beta \neq 0$. Considerando la divisione euclidea per ω possiamo scrivere

$$\alpha = \omega \cdot n + m \quad \text{e} \quad \beta = \omega \cdot k + h,$$

con n, m, k, h numeri naturali. Supponiamo prima che n e k siano entrambi diversi da zero. Usando la proprietà associativa

$$\alpha + \beta = \omega \cdot n + (m + \omega \cdot k) + h = \omega \cdot (n + k) + h.$$

Procedendo in modo analogo si ha $\beta + \alpha = \omega \cdot (k + n) + m$. Quindi, se n e k sono non nulli la somma commuta se e solo se $h = m$. Nel caso in cui invece $n = k = 0$ la somma commuta sempre essendo fatta tra numeri naturali; se $n \neq 0$ e $k = 0$ oppure se $n = 0$ e $k \neq 0$ la somma non commuta, basta scrivere chi sono le due somme.

Esercizio A.3.8. Dimostrare in dettaglio che gli ordinali ξ tali che $\omega^\omega \cdot \xi = \xi$ sono tutti e soli i multipli di ω^{ω^2}.
Soluzione. Dimostriamo dapprima che 0 è l'unico ordinale $\xi < \omega^{\omega^2}$ tale che $\omega^\omega \cdot \xi = \xi$. Osserviamo intanto che $\omega^{\omega^2} = \sup_{n<\omega} \omega^{\omega \cdot n}$ e dunque se prendiamo uno $0 < \xi < \omega^{\omega^2}$ avremo che $\omega^{\omega \cdot n} \leq \xi < \omega^{\omega \cdot (n+1)}$. Ma allora

$$\omega^\omega \cdot \xi \geq \omega^\omega \cdot \omega^{\omega \cdot n} = \omega^{\omega \cdot (n+1)} > \xi.$$

Adesso passiamo al caso generale con $\xi \geq \omega^{\omega^2}$ qualsiasi. Dividendolo per ω^{ω^2} si ottiene dunque $\xi = \omega^{\omega^2} \cdot \zeta + \rho$, con $\rho < \omega^{\omega^2}$. Abbiamo allora

$$\omega^\omega \cdot \xi = \omega^\omega \cdot \left(\omega^{\omega^2} \cdot \zeta + \rho\right) = \omega^{\omega^2} \cdot \zeta + \omega^{\omega^2} \cdot \rho.$$

Dunque abbiamo $\omega^\omega \cdot \xi = \xi$ se e solo se $\omega^{\omega^2} \cdot \zeta + \omega^{\omega^2} \cdot \rho = \omega^{\omega^2} \cdot \zeta + \rho$, e questa se e solo se $\rho = \omega^{\omega^2} \cdot \rho$. Ma allora, per quanto mostrato, si ha che $\rho = 0$.

Esercizio A.3.9. Per ogni α individuare tutti e soli gli ordinali ξ tali che $\omega^\alpha \cdot \xi = \xi$.
Soluzione. Analogamente al precedente esercizio si dimostra che 0 è l'unico ordinale minore di $\omega^{\alpha \cdot \omega}$ tale che $\omega^\alpha \cdot \xi = \xi$.
Per il resto dell'esercizio si procede esattamente in modo analogo al precedente, e si riesce a ricavare che tutti e soli gli ordinali ξ che soddisfano $\omega^\alpha \cdot \xi = \xi$ sono i multipli di $\omega^{\alpha \cdot \omega}$.

A.4 Cardinali

Esercizio A.4.1. Dimostrare che $\prod_{n<\omega} \aleph_n = \aleph_\omega^{\aleph_0}$.
Soluzione. Intanto, visto che $\aleph_n \leq \aleph_\omega$ per ogni $n < \omega$ avremo immediatamente che

$$\prod_{n<\omega} \aleph_n \leq \prod_{n<\omega} \aleph_\omega = \aleph_\omega^{\aleph_0}.$$

Adesso osserviamo che possiamo partizxionare ω in sottoinsiemi A_i con $i < \omega$, numerabili e disgiunti, prendendo ad esempio $A_i = \{p_i^k \mid k \in \mathbb{N}\}$ per ogni $i < \omega$, dove $\{p_i\}_{i=0}^\infty$ è la successione dei numeri primi. Avremo dunque

$$\prod_{n<\omega} \aleph_n \geq \prod_{i=0}^{\infty} \left(\prod_{n=1}^{\infty} \aleph_{p_i^n} \right) \geq \prod_{i=0}^{\infty} \aleph_\omega = \aleph_\omega^{\aleph_0},$$

e l'esercizio è concluso per il teorema di Cantor–Bernstein.

Esercizio A.4.2. Un cardinale non numerabile si dice *limite forte* se $\nu^\mu < \kappa$ per ogni $\nu, \mu < \kappa$.
(1) Dimostrare che se κ è un limite forte allora è un cardinale limite;
(2) dimostrare che κ è limite forte se e solo se $2^\nu < \kappa$ per ofni $\nu < \kappa$ cardinale;
(3) dimostrare che esistono limiti forti.
Soluzione. (1) Supponiamo per assurdo che $\kappa = \lambda^+$ sia un cardinale successore. Allora, visto che $2^\lambda > \lambda$, avremo $2^\lambda \geq \lambda^+ = \kappa$, ma $2, \lambda < \kappa$. Dunque κ non è limite forte.
(2) L'implicazione verso destra è banale. Per quella verso sinistra consideriamo $\mu, \nu < \kappa$; detto $\bar{\mu} = \max\{\mu, \nu\} < \kappa$ avremo che $\mu^\nu \leq \bar{\mu}^{\bar{\mu}} = 2^{\bar{\mu}} < \kappa$.
(3) Sia μ un cardinale infinito. Definiamo per ricorsione la successione di cardinali

$$\begin{cases} \kappa_0 = \mu \\ \kappa_{n+1} = 2^{\kappa_n} \end{cases}.$$

Sia poi $\kappa = \sup_{n<\omega} \kappa_n$; affermiamo che κ è un limite forte. Infatti se $\nu < \kappa$ allora $\nu < \kappa_n$ per qualche $n < \omega$, e dunque $2^\nu \leq 2^{\kappa_n} = \kappa_{n+1} < \kappa$.

Esercizio A.4.3. Dimostrare che :
(1) per ogni ordinale α si ha $\aleph_{\alpha+1}^{\aleph_\alpha} = 2^{\aleph_\alpha}$;
(2) assumendo l'ipotesi del continuo, $\aleph_n^{\aleph_0} = \aleph_n$ per ogni $n < \omega$ non nullo.
Soluzione. (1) Per ogni ordinale α abbiamo che

$$2^{\aleph_\alpha} \leq \aleph_{\alpha+1}^{\aleph_\alpha} \leq \left(2^{\aleph_\alpha}\right)^{\aleph_\alpha} = 2^{\aleph_\alpha}.$$

(2) Si procede per induzione su $n > 0$. Se $n = 1$ abbiamo banalmente $\aleph_1^{\aleph_0} = 2^{\aleph_0} = \aleph_1$. Se adesso $n > 1$ possiamo utilizzare la formula di Hausdorff

$$\aleph_{n+1}^{\aleph_0} = \aleph_{n+1} \cdot \aleph_n^{\aleph_0} = \aleph_{n+1} \cdot \aleph_n = \aleph_{n+1}.$$

A.4.1 La succesione *beth*

Adesso definirimo un'altra successione di cardinali come abbiamo fatto per gli aleph, e vedremo che la loro introduzione ha molti collegamenti con argomenti svolti. Definiamo la successione *beth* come segue per ricursione trasnfinita:

$$\begin{cases} \beth_0 = \aleph_0 \\ \beth_{\alpha+1} = 2^{\beth_\alpha} \\ \beth_\lambda = \sup_{\alpha<\lambda} \beth_\alpha \end{cases}.$$

Osserviamo che grazie al teorema di Cantor $\beth_{\alpha+1} = 2^{\beth_\alpha} > \beth_\alpha$. Inoltre vale che $\beth_1 = 2^{\aleph_0} \geq \aleph_1$ e procedendo per induzione transfinita si può mostrare che per ogni ordinale α si ha $\beth_\alpha \geq \aleph_\alpha$. Si può anche mostrare che l'ipotesi generalizzata del continuo equivale a chiedere $\beth_\alpha = \aleph_\alpha$ per ogni α ordinale.
Intanto ci potremmo chiedere se, come accade per la successione degli aleph, anche la successione appena definita ammetta dei punti fissi.

Lemma A.4.1. *La successione $\beth$ ammette punti fissi arbitrariamente grandi.*

Dimostrazione. Fissiamo ν cardinale, e mostriamo che esiste $\kappa > \nu$ tale che $\beth_\kappa = \kappa$. Tale cardinale sarà ottenuto con un procedimento al limite; definiamo

$$\begin{cases} \kappa_0 = \nu \\ \kappa_{n+1} = \beth_{\kappa_n} \end{cases}$$

e consideriamo $\kappa = \bigcup_{n<\omega} \kappa_n$. Affermiamo che questo è il cardinale cercato, infatti vale $\beth_\kappa = \bigcup_{n<\omega} \beth_{\kappa_n} = \bigcup_{n<\omega} \kappa_{n+1} = \kappa$, e abbiamo concluso. □

I cardinali della successione *beth* hanno una correlazione con gli insiemi di Von Neumann; più precisamente vale

Proposizione A.4.1. *Per ogni ordinale α, $|V_{\omega+\alpha}| = \beth_\alpha$.*

Dimostrazione. Supponiamo adesso che $\beta = 0$, e consideriamo i V_n con $n < \omega$. Vale $|V_0| = 0$ e $|V_n| = 2^{n-1}$ per $n \in \{1, \ldots, 4\}$, mentre per $n > 4$ si ha $|V_n| > 2^n$ (ma sono sempre insiemi finiti). Dunque

$$|V_\omega| = \left| \bigcup_{n<\omega} V_n \right| = \aleph_0.$$

Ciò dimostra la base dell'induzione, ossia che $|V_{\omega+0}| = \aleph_0 = \beth_0$. Per il passo successore si ha $|V_{\omega+\gamma+1}| = |\mathcal{P}(V_{\omega+\gamma})| = 2^{|V_{\omega+\gamma}|} = 2^{\beth_\gamma} = \beth_{\gamma+1}$. Infine il caso limite segue subito

$$|V_{\omega+\lambda}| = \left| \bigcup_{\gamma<\lambda} V_{\omega+\gamma} \right| = \left| \bigcup_{\gamma<\lambda} (V_{\omega+\gamma+1} - V_{\omega+\gamma}) \right| = \sum_{\gamma<\lambda} |V_{\omega+\gamma+1} - V_{\omega+\gamma}| = \beth_\lambda,$$

e abbiamo concluso. □

Infine vogliamo mostrare una proprietà che collega i numeri *beth* con i limiti forti; ricordiamo che un cardinale κ si dice limite forte se per ogni $\nu, \mu < \kappa$ si ha $\nu^\mu < \kappa$.

Proposizione A.4.2. *Un cardinale $\kappa > \aleph_0$ è un limite forte se e solo se $\kappa = \beth_\lambda$ con λ ordinale limite.*

Dimostrazione. ($\Longrightarrow$) Sia κ un cardinale; la funzione $\beth$ è illimitata nei cardinali, e dunque avremo che per qualche α varrà $\beth_\alpha \leq \kappa < \beth_{\alpha+1}$. Ma allora $\kappa = \beth_\alpha$ in quanto non può valere l'altra alternativa. Una volta dimostrato questo fatto mostriamo che κ non può essere un $\beth_{\beta+1}$. Se così non fosse avremmo

$$2^{\beth_\beta} \geq \beth_{\beta+1} = \kappa,$$

e dunque κ non sarebbe limite forte.
($\Longleftarrow$) Sia $\kappa = \beth_\lambda = \bigcup_{\alpha<\lambda} \beth_\alpha$. Se $\nu, \mu < \kappa$ allora $\nu, \mu < \beth_\alpha$ per qualche $\alpha < \lambda$. Ma allora

$$\nu^\mu \leq \beth_\alpha^{\beth_\alpha} = 2^{\beth_\alpha} = \beth_{\alpha+1} < \beth_\lambda = \kappa,$$

e la dimostrazione è conclusa. □