

ELEMENTI DI TEORIA DEGLI INSIEMI
Dispensa 1

Mauro Di Nasso

Ultimo aggiornamento: October 21, 2024

Introduzione

Scopo di questo corso è introdurre i primi elementi fondamentali della *teoria degli insiemi*. Questa disciplina riveste un ruolo del tutto speciale. Molti dei suoi aspetti possono essere presentati come si farebbe in un qualsiasi altro corso di matematica, ma la sua particolare importanza sta nel suo cruciale ruolo *fondazionale*. Infatti, al suo interno può essere formalizzata virtualmente tutta la matematica, in accordo col cosiddetto *programma riduzionista* il cui scopo è quello di ridurre ogni nozione matematica al concetto primitivo di insieme. La presentazione e la discussione di questo ruolo fondazionale servirà anche come introduzione ai concetti fondamentali della *logica matematica*.

Nelle prime lezioni del corso ci muoveremo all'interno della cosiddetta *teoria intuitiva* degli insiemi. Assumeremo come “intuitivamente validi” i principi di *estensionalità* e *comprensione*, che risultano coerenti con la consueta pratica matematica, e ne dedurremo alcuni primi risultati sulla cardinalità. Questa introduzione ci sarà utile per familiarizzare con alcuni concetti importanti, che verranno poi ripresi e sviluppati con maggiore rigore nel seguito. In questa prima parte saranno anche presentati alcuni *paradossi* che storicamente evidenziarono la contraddittorietà di questo modo di procedere. La crisi che ne seguì durante gli anni a cavallo del 1900, portò alla formulazione di *teorie assiomatiche degli insiemi*, il cui ambizioso scopo era quello di rifondare su basi rigorose l'intera matematica.

Dopo questa breve parte introduttiva, tutto il resto del corso sarà proprio dedicato allo sviluppo sistematico di una di quelle teorie, cioè la teoria ZFC di Zermelo-Fraenkel con scelta, che è quella attualmente più usata. Introduciamo anche la teoria delle classi GB di Gödel-Bernays, che risulterà più conveniente per trattare alcune parti del programma, in particolare la ricorsione transfinita. Attenendoci al metodo assiomatico, tutte le nozioni e i risultati presentati verranno giustificati rigorosamente a partire da una iniziale lista di principi, cioè gli assiomi, che saranno gli unici ad essere assunti come validi.

Nella parte finale del corso, introdurremo la nozione di *modello della teoria degli insiemi*, e saremo in grado di dare un significato preciso ad affermazioni del tipo: “il Teorema di Hahn-Banach *non è dimostrabile* senza l'assioma di scelta”, oppure “l'ipotesi del continuo è *indipendente* dai principi della matematica”.

CHAPTER 1

Il linguaggio degli insiemi

1. Simboli logici

In questo corso faremo un massiccio uso di “formule”, un po’ più di quanto sia consuetudine fare in altri settori della matematica. 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. Per il momento sarà sufficiente seguire l’uso comune, prestando però una particolare attenzione ai seguenti *simboli logici*, che useremo sistematicamente.

DEFINIZIONE 1.1. Per *simboli logici* intendiamo i seguenti simboli:

- *Connettivi*:
negazione: $\neg$ (“non”); congiunzione: $\wedge$ (“e”); disgiunzione: $\vee$ (“o”); implicazione: $\rightarrow$ (“se ... allora”); equivalenza: $\leftrightarrow$ (“se e solo se”).
- *Variabili*:
 $x, y, z, t, \dots, x_1, x_2, x_3 \dots$
- *Quantificatori*:
esistenziale $\exists$ (“esiste”); universale $\forall$ (“per ogni”).

Il significato di questi simboli può sembrare evidente, ma un loro uso corretto richiederà qualche cautela. Cominciamo con i connettivi.

DEFINIZIONE 1.2. Siano P e Q enunciati, cioè affermazioni cui si possa attribuire uno ed uno solo dei valori di verità *vero* o *falso*. Allora:

- $\neg P$ è vera quando P è falsa, ed è falsa quando P è vera;
- $P \wedge Q$ è vera quando sia P che Q sono vere, ed è falsa altrimenti;
- $P \vee Q$ è falsa quando sia P che Q sono false, ed è vera altrimenti;
- $P \rightarrow Q$ è falsa quando l’*ipotesi* (o *premessa*) P è vera e la *tesi* (o *consequenza*) Q è falsa, ed è vera negli altri casi;
- $P \leftrightarrow Q$ è vera quando P e Q hanno lo stesso valore di verità (entrambe vere o entrambe false), ed è falsa altrimenti.

Allo scopo di visualizzare queste definizioni, è consuetudine usare le cosiddette *tavole di verità*. In queste, viene indicato il valore di verità “V” (vero) o “F” (falso) degli enunciati ottenuti usando i vari connettivi, a partire dai possibili valori di verità degli enunciati P e Q di partenza.

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \rightarrow Q$	$P \leftrightarrow Q$
V	V	F	V	V	V	V
V	F	F	F	V	F	F
F	V	V	F	V	V	F
F	F	V	F	F	V	V

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 $P \rightarrow Q$ anche quando P è falsa e Q è vera. Tuttavia le definizioni date sono in pieno accordo con la pratica, come avremo modo di vedere con diversi esempi. Ad esempio, in matematica un enunciato $P \rightarrow Q$ viene considerato vero “d’ufficio” nel caso in cui P sia falso.²

Utilizzando ripetutamente i vari connettivi, si possono formare nuovi *enunciati composti* a partire da enunciati assegnati, che chiamiamo *enunciati atomici*. A partire dai valori di verità degli enunciati atomici, si attribuisce un valore di verità a tutti gli enunciati composti. Quando due enunciati composti $\mathcal{A}$ e $\mathcal{B}$ hanno la stessa tavola di verità, diremo che sono *logicamente equivalenti*, e scriveremo $\mathcal{A} \equiv \mathcal{B}$. In questo caso attribuiremo ad $\mathcal{A}$ e $\mathcal{B}$ lo stesso significato e quindi – a seconda della convenienza – potremo sostituire uno all’altro in ogni ragionamento. Nel prossimo esercizio sono raccolte le equivalenze logiche più usate nella pratica.

ESERCIZIO 1.3. Verificare che le seguenti coppie di enunciati composti (a partire dagli enunciati atomici P e Q) hanno la stessa tavola di verità:

- (1) Doppia negazione: $\neg(\neg P) \equiv P$.
- (2) Leggi di De Morgan:
 - $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$.
 - $\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$.
- (3) Negazione dell’implicazione: $\neg(P \rightarrow Q) \equiv P \wedge (\neg Q)$.
- (4) Contronominale: $P \rightarrow Q \equiv \neg Q \rightarrow \neg P$.
- (5) Doppia implicazione: $P \leftrightarrow Q \equiv ((P \rightarrow Q) \wedge (Q \rightarrow P))$.
- (6) Negazione della doppia implicazione: $\neg(P \leftrightarrow Q) \equiv (P \wedge \neg Q) \vee (\neg P \wedge Q)$.

Quasi sempre negli enunciati matematici si fa uso di *quantificazioni* su variabili; precisamente si usano *quantificatori esistenziali* $\exists x$ (“esiste x ”) e *quantificatori universali* $\forall x$ (“per ogni x ”). Il loro significato verrà assunto come evidente. Di particolare importanza è il comportamento rispetto alla negazione, che ricordiamo qua sotto.

Scriviamo “ $P(x)$ ” per indicare che “l’oggetto x soddisfa la proprietà P ”, e scriviamo $Q(x, y)$ per indicare che “la coppia (x, y) soddisfa la proprietà Q ”. Allora:

- “ $\neg(\forall x P(x))$ ” è logicamente equivalente a “ $\exists x \neg P(x)$ ”;
- “ $\neg(\exists x P(x))$ ” è logicamente equivalente a “ $\forall x \neg P(x)$ ”.
- “ $\neg(\forall x \forall y Q(x, y))$ ” è logicamente equivalente a “ $\exists x \exists y \neg Q(x, y)$ ”.
- “ $\neg(\exists x \exists y Q(x, y))$ ” è logicamente equivalente a “ $\forall x \forall y \neg Q(x, y)$ ”.
- “ $\neg(\forall x \exists y Q(x, y))$ ” è logicamente equivalente a “ $\exists x \forall y \neg Q(x, y)$ ”.
- “ $\neg(\exists x \forall y Q(x, y))$ ” è logicamente equivalente a “ $\forall x \exists y \neg Q(x, y)$ ”.

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 $\vee$), e “*aut*” per la disgiunzione esclusiva, dove $P \text{ aut } Q$ è falsa quando P e Q sono entrambe vere.

² L’enunciato “*Se B è uno spazio di Banach non separabile di dimensione finita, allora B è compatto*” è vero, per il semplice fatto che *non* esistono spazi di Banach non separabili di dimensione finita.

Per memorizzare le equivalenze di sopra può essere utile pensare che in ogni enunciato il connettivo della negazione $\neg$ può “passare attraverso” i quantificatori scambiando $\exists$ con $\forall$ e viceversa, mantenendo l’equivalenza logica. In modo informale, possiamo scrivere:

$$\neg \exists \equiv \forall \neg \quad \text{e} \quad \neg \forall \equiv \exists \neg$$

ESEMPIO 1.4. Sia $f : \mathbb{R} \rightarrow \mathbb{R}$ una funzione reale. La proprietà “ f è continua su $\mathbb{R}$ ” è espressa dalla seguente formula:

$$\forall x_0 \forall \varepsilon > 0 \exists \delta > 0 \forall x (|x - x_0| < \delta \rightarrow |f(x) - f(x_0)| < \varepsilon).$$

La proprietà “ f non è continua su $\mathbb{R}$ ” è la negazione della precedente. Facendo “passare la negazione attraverso i quantificatori”, otteniamo la seguente formula equivalente:

$$\exists x_0 \exists \varepsilon > 0 \forall \delta > 0 \exists x \neg (|x - x_0| < \delta \rightarrow |f(x) - f(x_0)| < \varepsilon),$$

che è a sua volta è equivalente alla formula:

$$\exists x_0 \exists \varepsilon > 0 \forall \delta > 0 \exists x (|x - x_0| < \delta \wedge |f(x) - f(x_0)| \geq \varepsilon).$$

2. I tre principi della teoria intuitiva degli insiemi

Dopo questo breve preambolo sui simboli logici, passiamo ad occuparci finalmente degli insiemi, sui quali è incentrato tutto questo corso. 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 a che costituiscono un insieme A si dicono i suoi *elementi*. In questo caso si scrive “ $a \in A$ ”, che si legge: “ a appartiene ad A ” oppure “ A contiene a ”.

Per lo sviluppo di questa prima parte intuitiva di teoria degli insiemi, ci atterremo ai seguenti tre principi informali, ognuno dei quali sarà ripresentato in forma precisa e rigorosa più avanti nel corso.

Principio del Linguaggio. Ogni proprietà che consideriamo deve essere esprimibile nel *linguaggio della teoria degli insiemi*, cioè deve poter essere scritta come formula nella quale compaiono soltanto i simboli logici, il simbolo di uguaglianza “=”, e il simbolo di appartenenza “ $\in$ ”.³

In altre parole, in base a questo principio possiamo identificare le *proprietà insiemistiche* con opportune *formule*.

NOTAZIONE 2.1. Scriviamo “ $A \neq B$ ” per intendere la formula “ $\neg(A = B)$ ”, e scriviamo “ $A \notin B$ ” per intendere “ $\neg(A \in B)$ ”.

L’intuizione che un insieme è completamente determinato dai suoi elementi è racchiusa nel seguente principio.

Principio di Estensionalità. Due insiemi sono uguali se e solo se hanno gli stessi elementi, cioè:

$$\forall A \forall B [\forall x (x \in A \leftrightarrow x \in B) \leftrightarrow A = B].$$

³ Naturalmente, resta inteso che nella scrittura delle formule possiamo anche usare parentesi.

Osserviamo che – grazie a questo principio – potremmo anche fare a meno del simbolo di uguaglianza. Infatti, potremmo sostituire ogni formula “ $A = B$ ” con la formula equivalente “ $\forall x (x \in A \leftrightarrow x \in B)$ ”.

Una fondamentale intuizione nella pratica matematica riguarda la possibilità di formare un insieme a partire da ogni assegnata proprietà. Precisamente, nella pratica sembra evidente che l'*estensione* di una proprietà, cioè la collezione di tutti gli oggetti che la soddisfano, formi un insieme. A questo corrisponde il terzo principio della teoria intuitiva degli insiemi, che è il seguente.

Principio di Comprensione (o di Astrazione). Se P è una proprietà “ammissibile”, allora esiste la sua estensione:

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

Cosa intendiamo per “ammissibile” sarà chiarito più avanti nel corso. Per adesso non dobbiamo preoccuparci, tutte le proprietà che si considerano nella comune pratica matematica, e in particolare tutte quelle che incontreremo in queste prime lezioni, saranno “ammissibili”. Ad esempio, le proprietà di essere un numero naturale, intero, razionale, reale, complesso, sono tutte “ammissibili”;⁴ di conseguenza, applicando il principio di comprensione, potremo formare i corrispondenti insiemi dei numeri naturali $\mathbb{N}$, dei numeri interi $\mathbb{Z}$, dei numeri razionali $\mathbb{Q}$, dei numeri reali $\mathbb{R}$, e dei numeri complessi $\mathbb{C}$.

Osserviamo che l'insieme X nell'enunciato del principio di comprensione è necessariamente unico, in conseguenza del principio di *estensionalità*. Per denotarlo, si scrive:

$$X = \{x \mid P(x)\}.$$

Quando $X = \{x \mid P(x)\}$ è l'estensione della proprietà P , adottiamo le seguenti ovvie notazioni:

- “ $x \in X$ ” denota $P(x)$;
- “ $y = X$ ” denota “ $\forall x (P(x) \leftrightarrow x \in y)$ ”.
- “ $X \in z$ ” significa “ $\exists y (y = X \wedge y \in z)$ ”, dove “ $y = X$ ” denota la formula di sopra.

Attenzione! Anche se nei consueti corsi di matematica tutte le proprietà che si usano per formare insiemi sono “ammissibili”, è comunque bene sapere che non tutte le proprietà lo sono. L'esempio più famoso, che ha avuto una cruciale importanza nella storia dei fondamenti della matematica, è dato dal celebre *paradosso di Russell*. Consideriamo la proprietà P di *non* essere elemento di se stesso. Notiamo subito che P soddisfa il principio del *linguaggio*, perché $P(x)$ si scrive “ $x \notin x$ ”. Ad esempio, l'insieme $\mathbb{N}$ dei numeri naturali soddisfa P perchè $\mathbb{N}$ *non* è un numero naturale e quindi $\mathbb{N} \notin \mathbb{N}$. Nella lettera originale in cui formulò il suo paradosso, Bertrand Russell menzionò l'insieme delle *non-teiere* come esempio di insieme che non soddisfa P , visto che l'insieme delle non-teiere certamente è una non-teiera! Vediamo ora che l'estensione della proprietà P non può essere un insieme. Infatti, supponiamo per assurdo che esista l'insieme $R = \{x \mid x \notin x\}$. Si hanno due casi. Se $R \in R$, allora R stesso è uno di quegli insiemi che non appartengono a se stessi, e quindi $R \notin R$. Se invece $R \notin R$, allora non è vero che R non appartiene a se

⁴ Anche se può sembrare strano, vedremo più avanti che anche queste proprietà soddisfano il principio del linguaggio, cioè sono esprimibili da formule che contengono soltanto simboli logici e i simboli di uguaglianza e di appartenenza.

stesso, e quindi $R \in R$. In entrambi i casi otteniamo un assurdo; dobbiamo così concludere che R non può essere un insieme, e “ $x \notin x$ ” non può essere una proprietà “ammissibile”. Più avanti vedremo che neppure la banale proprietà “ $x = x$ ” è “ammissibile”, perchè ammettere l’esistenza della sua *estensione*, cioè dell’insieme universale di tutti gli insiemi $V = \{x \mid x = x\}$, porta a contraddizioni.⁵

3. Alcune notazioni fondamentali

Nel caso di alcune proprietà particolarmente importanti, fisseremo una volta per tutte delle particolari scritture per denotare i corrispondenti insiemi che si ottengono per estensione. È bene chiarire che si tratta di scritture *metalinguistiche*, cioè scritture contenenti simboli esterni al linguaggio. Il primo semplice esempio è il seguente.

NOTAZIONE 3.1. Con la scrittura “ $\emptyset$ ” denotiamo l’insieme $\{x \mid x \neq x\}$.

Visto che “ $x \neq x$ ” è chiaramente una proprietà che non è verificata da alcun x , l’insieme “ $\emptyset$ ” si chiama *insieme vuoto*. Notiamo che, in conseguenza del principio di *estensionalità*, $\emptyset$ è l’unico insieme senza elementi.

Più formalmente, ciò che faremo è usare “ $\emptyset$ ” come utile abbreviazione metalinguistica (cioè fuori dal linguaggio formale). Precisamente, conveniamo che:

NOTAZIONE 3.2.

- Con la scrittura “ $A = \emptyset$ ” denotiamo la proprietà: “ $\forall t (t \in A \leftrightarrow t \neq t)$ ”.
- Con la scrittura “ $A \in \emptyset$ ” denotiamo la proprietà: “ $A \neq A$ ”.
- Con la scrittura “ $\emptyset \in A$ ” denotiamo la proprietà: “ $\exists t (t = \emptyset) \wedge t \in A$ ”, fove “ $t = \emptyset$ ” è a sua volta l’abbreviazione di una formula, come indicato sopra.

ESERCIZIO 3.3. Verificare che la proprietà denotata dalla scrittura “ $A \neq \emptyset$ ” equivale alla proprietà “ $\exists t (t \in A)$ ”.

Un’altra notazione comunemente usata è la seguente:

NOTAZIONE 3.4. Siano fissati $a_1, \dots, a_n$. Scrivendo “ $\{a_1, \dots, a_n\}$ ” denotiamo l’insieme $\{x \mid (x = a_1) \vee \dots \vee (x = a_n)\}$ i cui elementi sono tutti e soli gli a_i .

Dunque:

- “ $t \in \{a_1, \dots, a_n\}$ ” è una notazione per “ $t = a_1 \vee \dots \vee t = a_n$ ”.
- “ $t = \{a_1, \dots, a_n\}$ ” sta per “ $\forall x (x \in t \leftrightarrow (x = a_1 \vee \dots \vee x = a_n))$ ”.
- “ $\{a_1, \dots, a_n\} \in t$ ” sta per “ $\exists x (x \in t \wedge x = \{a_1, \dots, a_n\})$ ”, dove la scrittura “ $x = \{a_1, \dots, a_n\}$ ” è a sua volta l’abbreviazione di una formula, come indicato sopra.

In generale, se denotiamo con $A_{a_1, \dots, a_n} = \{x \mid \varphi(x, a_1, \dots, a_n)\}$ dove φ è una formula del linguaggio della teoria degli insiemi, allora conveniamo che

- “ $t \in A_{a_1, \dots, a_n}$ ” è una notazione per “ $\varphi(t, a_1, \dots, a_n)$ ”.
- “ $t = A_{a_1, \dots, a_n}$ ” sta per “ $\forall x (x \in t \leftrightarrow \varphi(x, a_1, \dots, a_n))$ ”.
- “ $A_{a_1, \dots, a_n} \in t$ ” sta per “ $\exists x (x \in t \wedge \varphi(x, a_1, \dots, a_n))$ ”.

⁵ Si osservi che se V fosse un insieme, si avrebbe $V \in V$ e quindi $V \notin V$.

Introduciamo ora altre notazioni molto familiari, corrispondenti a proprietà “ammissibili” che si riferiscono ad insiemi assegnati A, B .

NOTAZIONE 3.5. Siano A e B insiemi assegnati. Allora

- La scrittura “ $A \cup B$ ” denota l’insieme $\{x \mid (x \in A) \vee (x \in B)\}$, che viene chiamato l’*unione* di A e B ;
- La scrittura “ $A \cap B$ ” denota l’insieme $\{x \mid (x \in A) \wedge (x \in B)\}$, chiamato l’*intersezione* di A e B ;
- La scrittura “ $A \setminus B$ ” denota l’insieme $\{x \mid (x \in A) \wedge (x \notin B)\}$, chiamato la *differenza insiemistica* di A e B , o il *complemento relativo* di B in A .
- La scrittura “ $A \triangle B$ ” denota l’insieme $(A \setminus B) \cup (B \setminus A)$, chiamato la *differenza simmetrica* di A e B .

Dunque, l’unione è il corrispettivo insiemistico della disgiunzione inclusiva “ $\vee$ ”, e l’intersezione corrisponde alla congiunzione “ $\wedge$ ”.⁶

ESERCIZIO 3.6. Verificare le seguenti uguaglianze:

- (1) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$.
- (2) $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$.
- (3) $X \triangle (Y \triangle Z) = (X \triangle Y) \triangle Z$.

Seguendo il principio del *linguaggio*, anche le proprietà insiemistiche più semplici dovranno essere espresse da formule.

DEFINIZIONE 3.7. Siano A e B insiemi. Diciamo che A è *sottoinsieme* di B (o che A è *incluso* in B) se vale la proprietà: “ $\forall x (x \in A \rightarrow x \in B)$ ”. In questo caso scriviamo “ $A \subseteq B$ ”.

Dunque per noi “ $A \subseteq B$ ” è una scrittura *metalinguistica*, cioè non appartenente al linguaggio, che però verrà usata come comoda abbreviazione per indicare la formula di sopra.

Usando la notazione di sottoinsieme, il principio di *estensionalità* può essere riscritto così:

$$\forall A \forall B [(A \subseteq B) \wedge (B \subseteq A)] \leftrightarrow A = B.$$

In effetti, nella pratica, per dimostrare che due insiemi A e B sono uguali si verificano separatamente le due inclusioni $A \subseteq B$ e $B \subseteq A$.

Se $X = \{x \mid P(x)\}$ è l’insieme *estensione* di una proprietà P , e Y è un insieme, allora:

- “ $Y \subseteq X$ ” significa “ $\forall x (x \in Y \rightarrow P(x))$ ”.
- “ $X \subseteq Y$ ” significa “ $\forall x (P(x) \rightarrow x \in Y)$ ”.

Per ogni insieme A , vale banalmente l’inclusione “ $\emptyset \subseteq A$ ”. Infatti, la corrispondente formula “ $\forall x (x \in \emptyset \rightarrow x \in A)$ ”, cioè “ $\forall x (x \neq x \rightarrow x \in A)$ ”, è banalmente vera perché per ogni x si ha un’implicazione dove la premessa è falsa.

NOTAZIONE 3.8. La scrittura “ $\mathcal{P}(A)$ ” denota l’insieme $\{X \mid X \subseteq A\}$, che è chiamato l’*insieme potenza* o l’*insieme delle parti* di A .

⁶ Non è un caso che i simboli $\cup$ e $\vee$, e simboli $\cap$ e $\wedge$, siano molto simili.

Elenchiamo qui di seguito altre comode abbreviazioni che si usano molto nella pratica.

NOTAZIONE 3.9.

- Scrivendo “ $\{x \in A \mid P(x)\}$ ” intendiamo $\{x \mid x \in A \wedge P(x)\}$;
- Scrivendo “ $\forall x \in A P(x)$ ” intendiamo “ $\forall x (x \in A \rightarrow P(x))$ ”;
- Scrivendo “ $\exists x \in A P(x)$ ” intendiamo “ $\exists x (x \in A \wedge P(x))$ ”.
- Scrivendo “ $\exists!x P(x)$ ”, che si legge: “esiste ed unico x tale che $P(x)$ ”, intendiamo “ $\exists x (P(x) \wedge \forall y (P(y) \rightarrow y = x))$ ”.

4. Coppie ordinate

Una conseguenza del principio di *estensionalità* è l'impossibilità dell'esistenza di *atomi*, cioè di oggetti matematici che non siano insiemi. Osserviamo infatti che ognuno di questi atomi – in quanto privo di elementi – dovrebbe coincidere con l'*insieme vuoto*. Non c'è dubbio che questo contrasta con la pratica matematica. Ad esempio, i numeri e le coppie ordinate sono usualmente pensati come atomi e non come insiemi: è ben raro trovare un matematico che pensi al numero “pi greco” π come ad un insieme!

In questo corso svilupperemo una *teoria pura degli insiemi*, cioè assumeremo che tutti gli oggetti con cui avremo a che fare siano insiemi, compresi i numeri e le coppie ordinate. In particolare, gli elementi di insiemi saranno a loro volta insiemi, e quindi il nostro campo d'azione sarà ristretto alle *famiglie di insiemi*, per usare un termine dell'ordinario linguaggio matematico. Come vedremo, limitarsi agli *insiemi puri* è però una restrizione più apparente che reale. Uno degli scopi fondazionali della teoria degli insiemi è infatti proprio quello di mostrare come virtualmente *tutti* gli oggetti matematici, numeri compresi, possono essere “codificati” (cioè definiti) come particolari insiemi. Il primo esempio fondamentale che vedremo è quello di coppia ordinata.

Il concetto di coppia ordinata consiste nell'assegnare in modo “ordinato” due elementi (non necessariamente distinti), detti *componenti* o *coordinate*. Si usa la notazione (a, b) per indicare che a è la prima componente, e b la seconda.

La nozione di coppia ordinata potrebbe essere considerata come una nuova nozione primitiva, intuitivamente evidente, da aggiungere alla nozione primitiva di insieme. Ma il nostro scopo qui è quello di ricondurre ogni nozione matematica alla nozione di insieme. Con la prossima definizione, vedremo infatti che anche le coppie ordinate possono essere “codificate” da opportuni insiemi.

DEFINIZIONE 4.1. Chiamiamo *coppia ordinata* di prima componente a e seconda componente b , il seguente insieme, detto *coppia di Kuratowski*:

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

ESERCIZIO 4.2. Scrivere per esteso due formule $\varphi(X, a, b)$ e $\psi(X)$ della teoria degli insiemi che corrispondono rispettivamente alle proprietà: “ X è la coppia ordinata (a, b) ” e “ X è una coppia ordinata”.

A prima vista, quella di sopra può sembrare una definizione piuttosto bizzarra, ma ciò che importa è che essa raggiunga lo scopo, realizzando tutte le proprietà richieste. Abbiamo infatti:

PROPOSIZIONE 4.3.

- (1) Se (a, b) è una coppia ordinata, allora la prima componente a è quell'unico elemento tale che $a \in x$ per ogni $x \in (a, b)$.
- (2) Se $(a, b) = (a', b')$ allora $a = a'$.
- (3) Se $(a, b) = (a', b')$ allora $b = b'$.
- (4) $(a, b) = (a', b')$ se e solo se $a = a'$ e $b = b'$.

PROOF. (1). Se $(a, b) = \{\{a\}, \{a, b\}\}$ è una coppia ordinata, allora l'intersezione dei suoi elementi $\bigcap_{x \in (a, b)} x = \{a\} \cap \{a, b\} = \{a\}$ ha come unico elemento la prima componente a .

(2). Se $(a, b) = (a', b')$ allora, per la (1), $\{a\} = \bigcap_{x \in (a, b)} x = \bigcap_{y \in (a', b')} y = \{a'\}$, e quindi $a = a'$.

(3). Supponiamo che $(a, b) = (a', b')$. Se $a = b$, allora $\{\{a\}, \{a, b'\}\} = (a, b') = (a, b) = \{\{a\}, \{a, a\}\} = \{\{a\}\} \Rightarrow \{a, b'\} = \{a\} \Rightarrow b' = a$, e quindi le seconde componenti $b = b'$ sono uguali perché entrambe uguali ad a . Assumiamo ora che $a \neq b$. Visto che $\{a, b\} \in (a, b) = (a, b')$, deve essere $\{a, b\} = \{a\}$ o $\{a, b\} = \{a, b'\}$. Il primo caso è impossibile perché si avrebbe $b \in \{a\}$ e quindi $b = a$, contro l'ipotesi. Allora abbiamo che $\{a, b\} = \{a, b'\} \Rightarrow b \in \{a, b'\} \Rightarrow b = b'$, visto che $b \neq a$.

(4). Basta mettere insieme le proprietà (2) e (3) di sopra. $\square$

A partire dalla nozione di coppia ordinata, si definiscono poi le triple ordinate ponendo $(a, b, c) = ((a, b), c)$, le quadruple ordinate $(a, b, c, d) = ((a, b, c), d)$, e così via.

ESERCIZIO 4.4. Consideriamo le seguenti definizioni alternative di coppia ordinata:⁷

- (1) $(a, b)_1 := \{\{a, \emptyset\}, \{b, \{\emptyset\}\}\}$ (Hausdorff 1914);
- (2) $(a, b)_2 := \{\{\{a\}, \emptyset\}, \{\{b\}\}\}$ (Wiener 1914);
- (3) $(a, b)_3 := \{\{a\}, \{b, \emptyset\}\}$ (Quine).
- (4) $(a, b)_4 := \{a, \{b\}\}$.

Dimostrare che le prime tre soddisfano la proprietà caratterizzante delle coppie ordinate, cioè per $i = 1, 2, 3$:

- $(a, b)_i = (a', b')_i \Leftrightarrow a = a' \wedge b = b'$ per ogni a, a', b, b' .

Dimostrare che invece $(a, b)_4$ non soddisfa la proprietà caratterizzante delle coppie ordinate.

ESERCIZIO 4.5. Consideriamo la seguente definizione alternativa di coppia ordinata:

- $(a, b)_* = \{a, \{a, b\}\}$.

⁷ Vedi: A. Oberschelp, On pairs and tuples, *Z. Math. Logik Grundlag. Math.* 37 (1991), 55–56. Vedi anche Mendelson, Introduction to Mathematical Logic, p. 236 (Exercise 4.8)

Assumendo che non esistano cicli di appartenenza $x \in y \in x$, dimostrare che $(a, b)_*$ soddisfa la proprietà caratterizzante delle coppie ordinate.

Dimostrare che invece, assumendo l'esistenza di opportuni cicli di appartenenza, $(a, b)_*$ non soddisfa la proprietà caratterizzante delle coppie ordinate.

DEFINIZIONE 4.6. Il *prodotto cartesiano* di A con B , denotato $A \times B$, è l'insieme di tutte le coppie ordinate la cui prima componente appartiene ad A e la cui seconda componente appartiene a B . In formule:

$$A \times B = \{x \mid \exists a \in A \exists b \in B \ x = (a, b)\}$$

Strettamente parlando, questa operazione di prodotto cartesiano non è associativa, perché in generale $(A \times B) \times C \neq A \times (B \times C)$. Coerentemente con la nostra definizione di tripla ordinata $(a, b, c) = ((a, b), c)$, conveniamo che $A \times B \times C = (A \times B) \times C$, e analogamente per prodotti cartesiani di quattro insiemi, ecc.

5. Relazioni di equivalenza e d'ordine

A partire dalle coppie ordinate, possiamo definire il concetto di relazione.

DEFINIZIONE 5.1. Una *relazione binaria* R è un insieme di coppie ordinate.

- L'insieme $\text{dom}(R) = \{a \mid \exists b \ (a, b) \in R\}$ si dice *dominio* di R ;
- L'insieme $\text{imm}(R) = \{b \mid \exists a \ (a, b) \in R\}$ si dice *immagine* di R .

Si dice che R è una *relazione su* A quando $\text{dom}(R), \text{imm}(R) \subseteq A$.

Spesso si scrive aRb per intendere che la coppia ordinata (a, b) “soddisfa” la relazione R , cioè $(a, b) \in R$. Ad esempio, con la nostra definizione, la consueta relazione $<$ sui numeri naturali $\mathbb{N}$ è identificata con l'insieme di tutte quelle coppie ordinate (n, m) di numeri naturali dove n è minore di m .

Ricordiamo qui di seguito un altro paio di fondamentali definizioni.

DEFINIZIONE 5.2. Una *relazione di equivalenza* su un insieme A è una relazione R su A che gode delle proprietà seguenti:

- *Riflessiva*: Per ogni $a \in A$, aRa ;
- *Simmetrica*: Per ogni $a, b \in A$, $aRb \rightarrow bRa$;
- *Transitiva*: Per ogni $a, b, c \in A$, $(aRb \wedge bRc) \rightarrow aRc$.

Notiamo che la proprietà riflessiva garantisce che $A = \text{dom}(R) = \text{imm}(R)$.

DEFINIZIONE 5.3. Sia A un insieme, e sia $\approx$ una relazione di equivalenza su A . La *classe di equivalenza* di un elemento $a \in A$ rispetto a $\approx$ è l'insieme:

$$[a] = \{a' \mid a' \approx a\}.$$

L'*insieme quoziente* di A rispetto a $\approx$ è l'insieme di tutte le classi di equivalenza:

$$A/\approx = \{x \mid \exists a \in A \ x = [a]\}.$$

Notiamo che la scrittura “ $x = [a]$ ” è in realtà una abbreviazione che sta ad indicare la seguente formula nel linguaggio degli insiemi: “ $\forall a' (a' \in x \leftrightarrow a' \approx a)$ ”.

La nozione di ordine è uno dei temi centrali della matematica. Ricordiamo qui le definizioni.

DEFINIZIONE 5.4. Un *insieme parzialmente ordinato* è una coppia $(A, \leq)$ dove il *dominio* A è un insieme, e l'*ordine parziale* $\leq$ è una relazione su A che gode delle proprietà seguenti:

- *Riflessiva*: Per ogni $a \in A$, $a \leq a$;
- *Anti-simmetrica*: Per ogni $a, b \in A$, $(a \leq b \wedge b \leq a) \rightarrow a = b$;
- *Transitiva*: Per ogni $a, b, c \in A$, $(a \leq b \wedge b \leq c) \rightarrow a \leq c$.

DEFINIZIONE 5.5. Una relazione $<$ su A è un *ordine parziale stretto* se gode delle proprietà seguenti:

- *Irriflessiva*: Per ogni $a \in A$, $a \not< a$;
- *Asimmetrica*: Per ogni $a, b \in A$, $a < b \rightarrow b \not< a$;
- *Transitiva*: Per ogni $a, b, c \in A$, $(a < b \wedge b < c) \rightarrow a < c$.

Osserviamo che la lista con le tre proprietà di sopra è ridondante. Infatti, come si può facilmente verificare, la proprietà irreflessiva segue dalla proprietà asimmetrica, e la proprietà asimmetrica segue dalla congiunzione della proprietà transitiva con la proprietà asimmetrica. Abbiamo comunque lasciato le tre proprietà per maggiore chiarezza.

Le nozioni di ordine parziale e di ordine parziale stretto sono sostanzialmente equivalenti, nel senso specificato dall'esercizio qua sotto. Di conseguenza, useremo indifferentemente i simboli $<$ o $\leq$ a seconda della convenienza.

ESERCIZIO 5.6. Sia $\leq$ un ordine parziale su A , e definiamo

$$a < b \Leftrightarrow a \leq b \wedge a \neq b.$$

Allora $<$ è un ordine parziale *stretto* su A . Viceversa, se $<$ è un ordine parziale *stretto* su A e definiamo

$$a \leq b \Leftrightarrow a < b \vee a = b,$$

allora $\leq$ è un ordine parziale su A .

Con abuso di notazione, quando la cosa non crea confusione, spesso si identifica un insieme parzialmente ordinato $(A, <)$ con il suo dominio A .

DEFINIZIONE 5.7. Un insieme parzialmente ordinato $(A, <)$ si dice *totalmente ordinato* (o, più semplicemente, *ordinato*) se vale la:

- *Tricotomia*: Per ogni $a, b, c \in A$, vale una delle seguenti tre possibilità:

$$(1) a < b; \quad (2) a = b; \quad (3) b < a$$

In modo equivalente, avremmo potuto richiedere la validità di *una ed una sola* delle tre possibilità di sopra. Vale infatti il seguente risultato:

ESERCIZIO 5.8. Una relazione $<$ è una relazione d'ordine totale stretto su A se e solo se valgono le due proprietà:

- (1) *Transitiva*: Per ogni $a, b, c \in A$, $(a < b \wedge b < c) \Rightarrow a < c$;
- (2) *Tricotomia forte*: Per ogni $a, b, c \in A$, vale *una ed una sola* delle seguenti tre possibilità: $a < b$, $a = b$, $b < a$.

DEFINIZIONE 5.9. Un insieme totalmente ordinato $(A, <)$ si dice *buon ordine* se ogni sottoinsieme non vuoto $X \subseteq A$ ha elemento minimo.

Un esempio fondamentale di buon ordine è dato dai numeri naturali $(\mathbb{N}, <)$.

È immediato vedere che non tutti gli ordini totali sono buoni ordini. Ad esempio, l'insieme dei numeri reali $(\mathbb{R}, <)$ non è un buon ordine perché esistono sottoinsiemi non vuoti senza minimo (basta considerare gli intervalli aperti $(a, +\infty)$ per ogni $a \in \mathbb{R}$).

6. Funzioni

Un altro dei fondamentali concetti primitivi della matematica è quello di funzione. Si può pensare ad una funzione f come ad una “legge” che ad ogni elemento a di un insieme fissato, chiamato dominio di f , associa in modo unico un elemento $f(a)$, chiamato l'immagine di a . Questa è però solo una descrizione informale, che dobbiamo rendere precisa. Grazie alla nozione di coppia ordinata, siamo in grado di definire in modo rigoroso il concetto di funzione come un insieme di tipo speciale.

DEFINIZIONE 6.1. Una *funzione* f è una relazione *univoca*, cioè una relazione con la proprietà che per ogni elemento $a \in \text{dom}(f)$, esiste un unico b tale che $(a, b) \in f$. Si usa la notazione $f(a) = b$, o anche $f : a \mapsto b$, per intendere che $(a, b) \in f$. In questo caso si dice che b è l'*immagine* di a mediante f , oppure che b è il *valore* assunto da f in a .

Attenzione! Con la nostra definizione, non ha senso parlare di “grafico” di una funzione. Infatti, per noi una funzione f è il suo grafico, nel senso che coincide con l'insieme delle coppie ordinate della forma $(x, f(x))$.

La *funzione identità* id_A su un insieme A è la funzione avente come dominio A e tale che $\text{id}_A(a) = a$ per ogni $a \in A$. Quando una funzione assume un solo valore b , essa si dice *funzione costante* di valore b , e si denota c_b .

NOTAZIONE 6.2.

- Con la scrittura “ $f : A \rightarrow B$ ” si intende che f è una funzione il cui dominio è l'insieme A , e la cui immagine è un sottoinsieme di B . Quando $\text{imm}(f) = B$, si dice che $f : A \rightarrow B$ è *suriettiva*.⁸

ESERCIZIO 6.3. Scrivere esplicitamente nel linguaggio degli insiemi la proprietà “ $f : A \rightarrow B$ ”.

DEFINIZIONE 6.4. Dato un prodotto cartesiano $A \times B$, le *proiezioni canoniche* $\pi_1 : A \times B \rightarrow A$ e $\pi_2 : A \times B \rightarrow B$ sono le funzioni definite ponendo $\pi_1(a, b) = a$ e $\pi_2(a, b) = b$ per ogni $(a, b) \in A \times B$.

Viste le proprietà della Proposizione 4.3, le proiezioni canoniche sono effettivamente relazioni univoche.

Ricordiamo ora alcune fondamentali definizioni.

DEFINIZIONE 6.5. Una funzione f è *iniettiva* quando elementi diversi del dominio hanno immagini diverse. In formula:

$$\forall a, a' \in A \ (a \neq a' \rightarrow f(a) \neq f(a')).$$

⁸ Nella nostra definizione insiemistica invece il codominio non è specificato, e quindi la nozione di suriettività non ha senso di per sé.

Ricordiamo che ogni implicazione $P \rightarrow Q$ è logicamente equivalente alla sua *contronominale* $\neg Q \rightarrow \neg P$. Dunque possiamo riformulare l'iniettività in questo modo equivalente, più comodo da usare nella pratica:

$$\forall a, a' \in A (f(a) = f(a') \rightarrow a = a').$$

DEFINIZIONE 6.6. Una funzione $f : A \rightarrow B$ si dice *biunivoca* o *bigezione* se è sia iniettiva che suriettiva.

DEFINIZIONE 6.7. Sia $f : A \rightarrow B$, e siano $X \subseteq A$ e $Y \subseteq B$.

- L'*immagine* di X mediante f è l'insieme di tutte le immagini di elementi di X :

$$f[X] := \{y \mid \exists x \in X f(x) = y\}.$$

- La *controimmagine* di Y mediante f è l'insieme degli elementi la cui immagine appartiene ad Y :

$$f^{-1}[Y] := \{x \in A \mid f(x) \in Y\}.$$

NOTAZIONE 6.8. Con abuso di notazione, quando non ci sono rischi di fraintendimento, è consuetudine scrivere $f(X)$ per intendere l'insieme immagine $f[X]$. Analogamente, si scrive $f^{-1}(Y)$ per intendere l'insieme controimmagine $f^{-1}[Y]$.

ESERCIZIO 6.9. Sia $f : A \rightarrow B$ una funzione. Verificare che le seguenti proprietà valgono per ogni $X, X' \subseteq A$ e per ogni $Y, Y' \subseteq B$:

- (1) $X \subseteq f^{-1}(f(X))$.
- (2) $Y = f(f^{-1}(Y))$.
- (3) $f(X \cap X') \subseteq f(X) \cap f(X')$.
- (4) $f(X \cup X') = f(X) \cup f(X')$.
- (5) $f^{-1}(Y \cup Y') = f^{-1}(Y) \cup f^{-1}(Y')$.
- (6) $f^{-1}(Y \cap Y') = f^{-1}(Y) \cap f^{-1}(Y')$.

ESERCIZIO 6.10. Sia $f : A \rightarrow B$ una funzione. Dimostrare che valgono le seguenti equivalenze:

- (1) f è iniettiva se e solo se $X = f^{-1}(f(X))$ per ogni $X \subseteq A$.
- (2) f è suriettiva se e solo se $Y = f(f^{-1}(Y))$ per ogni $Y \subseteq B$.
- (3) f è iniettiva se e solo se $f(X \cap X') = f(X) \cap f(X')$ per ogni $X, X' \subseteq A$.
- (4) f è iniettiva se e solo se $f(X \setminus X') = f(X) \setminus f(X')$ per ogni $X, X' \subseteq A$.

NOTAZIONE 6.11.

- Data una funzione $f : A \rightarrow B$, denotiamo con $\hat{f} : \mathcal{P}(A) \rightarrow \mathcal{P}(B)$ la funzione dove $\hat{f}(X) = f[X]$ è l'immagine dell'insieme X mediante f .

ESERCIZIO 6.12.

- (1) $f : A \rightarrow B$ è iniettiva se e solo se $\hat{f} : \mathcal{P}(A) \rightarrow \mathcal{P}(B)$ è iniettiva.
- (2) $f : A \rightarrow B$ è suriettiva se e solo se $\hat{f} : \mathcal{P}(A) \rightarrow \mathcal{P}(B)$ è suriettiva.

SOLUZIONE. (1). Se f non è iniettiva, allora esistono $x \neq y$ in A tali che $f(x) = f(y)$. Ma allora $\{x\} \neq \{y\}$ sono sottoinsiemi diversi di A con $\widehat{f}(\{x\}) = \{f(x)\} = \{f(y)\} = \widehat{f}(\{y\})$, e $\widehat{f}$ non è iniettiva. Viceversa supponiamo che $\widehat{f}(X) = \widehat{f}(Y)$ dove $X \neq Y$ sono sottoinsiemi diversi di A . Prendiamo un elemento x che “testimonia” il fatto che $X \neq Y$, ad esempio prendiamo $x \in X \setminus Y$ (altrimenti, prendiamo $x \in Y \setminus X$ e la dimostrazione non cambia). Allora $f(x) \in \widehat{f}(X) = \widehat{f}(Y)$, dunque esiste $y \in Y$ con $f(x) = f(y)$. Ma per ipotesi $x \notin Y$, dunque $x \neq y$ e perciò f non è iniettiva.

(2). f non suriettiva significa che $\text{imm}(f) \subset B$ è un sottoinsieme proprio di B . Adesso, per ogni $X \subseteq A$, $\widehat{f}(X) \subseteq \text{imm}(f) \subset B$, dunque $\widehat{f}(X) \neq B$ e $\widehat{f}$ non è suriettiva. Viceversa, supponiamo che f sia suriettiva. Per ogni $Y \subseteq B$, sia $X_Y = f^{-1}[Y] = \{x \in A \mid f(x) \in Y\}$. Allora è facile verificare che $\widehat{f}(X_Y) = Y$, e questo dimostra la suriettività di $\widehat{f}$. $\square$

NOTAZIONE 6.13. Per denotare l'insieme $\{f \mid f : A \rightarrow B\}$, si usa la scrittura “ $\text{Fun}(A, B)$ ”, o anche “ B^A ”.

Vediamo un paio di esercizi su insiemi di funzioni e ordini.

ESERCIZIO 6.14. Sia $(A, <)$ un insieme ordinato e I un insieme che contiene almeno due elementi. Verificare che il seguente *ordine puntuale* sull'insieme di funzioni $\text{Fun}(I, A)$ è un ordine parziale, ed è un ordine totale se solo se A consiste di un solo punto.

$$f \leq g \iff f(i) \leq g(i) \text{ per ogni } i \in I.$$

In casi particolari, è possibile definire ordini totali su insiemi di funzioni. Un importante esempio è il seguente:

ESERCIZIO 6.15. Verificare che l'ordine della *minima differenza* su $\text{Fun}(\mathbb{N}, \mathbb{N})$:

$$f < g \iff f(k) < g(k) \text{ dove } k = \min\{n \mid f(n) \neq g(n)\}$$

è un ordine totale.

Un'importante classe di funzioni è la seguente:

DEFINIZIONE 6.16. Dato un insieme X , la *funzione caratteristica* di un suo sottoinsieme $A \subseteq X$ è la funzione $\chi_A : X \rightarrow \{0, 1\}$ tale che

$$\chi_A(x) = \begin{cases} 1 & \text{se } x \in A \\ 0 & \text{se } x \notin A \end{cases}$$

Notiamo che ogni funzione $\chi : X \rightarrow \{0, 1\}$ è la funzione caratteristica di uno ed un solo sottoinsieme $A \subseteq X$. Infatti, $\chi = \chi_A$ dove $A = \{x \in X \mid \chi(x) = 1\}$.

NOTAZIONE 6.17. In teoria degli insiemi, si denota con $2 = \{0, 1\}$. In particolare, scrivendo 2^X si intende denotare l'insieme di tutte le funzioni $\chi : X \rightarrow \{0, 1\}$, cioè l'insieme delle *funzioni caratteristiche* su X .

DEFINIZIONE 6.18. La *restrizione* di una funzione f ad un sottoinsieme $X \subseteq \text{dom}(f)$ del suo dominio, è la funzione $f|_X$ avente come dominio X e tale che $f|_X(x) = f(x)$ per ogni $x \in X$.

DEFINIZIONE 6.19. Siano f e g due funzioni con $\text{imm}(f) \subseteq \text{dom}(g)$. La *composizione* $g \circ f$ è definita ponendo:

$$g \circ f = \{(x, y) \mid \exists z \, f(x) = z \wedge g(z) = y\}.$$

Dunque la composizione $g \circ f$ è quella funzione avente come dominio $\text{dom}(f)$ e tale che $g \circ f : x \mapsto g(f(x))$ per ogni x .

ESERCIZIO 6.20. Verificare le seguenti proprietà:

- (1) Siano f e g funzioni con $\text{imm}(f) \subseteq \text{dom}(g)$. Allora per ogni X si ha che $(g \circ f)^{-1}(X) = f^{-1}(g^{-1}(X))$.
- (2) Sia $f : A \rightarrow B$. Allora f è iniettiva se e solo se ammette un'*inversa sinistra*, cioè esiste $g : B \rightarrow A$ tale che $g \circ f = \text{id}_A$.⁹
- (3) $f : A \rightarrow B$ è biunivoca se e solo se è invertibile, cioè esiste $g : B \rightarrow A$ tale che $g \circ f = \text{id}_A$ e $f \circ g = \text{id}_B$.

DEFINIZIONE 6.21. Una *successione* è una funzione il cui dominio è l'insieme dei numeri naturali $\mathbb{N}$. Si parla di *I-successione* o *I-sequenza* per indicare una funzione f avente come dominio l'insieme I .

NOTAZIONE 6.22. Per indicare una *I-sequenza* f , si usa spesso la scrittura $(f(i))_{i \in I}$ oppure $(f(i) \mid i \in I)$.

Attenzione! Non confondere la scrittura $(f(i) \mid i \in I)$ con $\{f(i) \mid i \in I\}$. Infatti con la prima si denota la funzione f , mentre con la seconda si denota l'insieme immagine $\text{imm}(f)$. Si tratta di oggetti diversi (ad esempio, funzioni diverse possono avere la stessa immagine), ed è quindi importante tenere distinte le notazioni.

7. Unioni, intersezioni e prodotti infiniti

NOTAZIONE 7.1. Se $\mathcal{F}$ è una famiglia non vuota di insiemi, si denota:¹⁰

- $\bigcup \mathcal{F} = \bigcup_{F \in \mathcal{F}} F = \{x \mid \exists F \in \mathcal{F} \, x \in F\}$.
- $\bigcap \mathcal{F} = \bigcap_{F \in \mathcal{F}} F = \{x \mid \forall F \in \mathcal{F} \, x \in F\}$.

Se $\langle F_i \mid i \in I \rangle$ è una sequenza non vuota di insiemi (cioè $I \neq \emptyset$), analogamente a sopra si denota:

- $\bigcup_{i \in I} F_i = \{x \mid \exists i \in I \, x \in F_i\}$.
- $\bigcap_{i \in I} F_i = \{x \mid \forall i \in I \, x \in F_i\}$.

Come è immediato verificare a partire dalle definizioni, se $\mathcal{F} = \{F_i \mid i \in I\}$ è l'immagine della sequenza $\langle F_i \mid i \in I \rangle$, allora $\bigcup_{i \in I} F_i = \bigcup_{F \in \mathcal{F}} F$ e $\bigcap_{i \in I} F_i = \bigcap_{F \in \mathcal{F}} F$.

ESERCIZIO 7.2. Sia $\langle F_i \mid i \in I \rangle$ è una sequenza non vuota di insiemi. Allora

- (1) $X \cap (\bigcup_{i \in I} F_i) = \bigcup_{i \in I} (X \cap F_i)$.
- (2) $X \cup (\bigcap_{i \in I} F_i) = \bigcap_{i \in I} (X \cup F_i)$.

⁹ Un'analoga caratterizzazione vale per le funzioni suriettive, ma la vedremo più avanti quando introdurremo l'assioma di scelta (cf. Proposizione 8.1).

¹⁰ Come abbiamo già osservato, visto che stiamo sviluppando una teoria *pura* degli insiemi, per noi tutti gli insiemi sono in realtà famiglie di insiemi. Manteniamo comunque il termine ridondante "famiglia" per seguire l'uso comune.

$$(3) \quad X \setminus \left(\bigcup_{i \in I} F_i \right) = \bigcap_{i \in I} (X \setminus F_i).$$

$$(4) \quad X \setminus \left(\bigcap_{i \in I} F_i \right) = \bigcup_{i \in I} (X \setminus F_i).$$

Le nozioni di sottoinsieme e di unione si usano anche per insiemi parzialmente ordinati.

DEFINIZIONE 7.3. Diciamo che l'insieme parzialmente ordinato $(A, <_A)$ è *restrizione* dell'insieme parzialmente ordinato $(B, <_B)$ se $A \subseteq B$, ed inoltre l'ordine su A è quello indotto da B , cioè $a <_A a' \Leftrightarrow a <_B a'$ per ogni $a, a' \in A$.

Chiaramente una restrizione di un insieme totalmente ordinato è totalmente ordinato.

DEFINIZIONE 7.4. Una famiglia di insiemi parzialmente ordinati $\mathcal{F}$ si dice *catena* se per ogni $(A, <_A), (B, <_B) \in \mathcal{F}$ si ha che $(A, <_A)$ è restrizione di $(B, <_B)$ o viceversa. Chiamiamo *unione* di una catena $\mathcal{F}$ di insiemi parzialmente ordinati, l'insieme parzialmente ordinato $(X, <)$ dove

- Il dominio $X = \bigcup \{A \mid (A, <_A) \in \mathcal{F}\}$ è l'unione di tutti i domini.
- La relazione $< = \bigcup \{<_A \mid (A, <_A) \in \mathcal{F}\}$ è l'unione di tutte le relazioni degli elementi di $\mathcal{F}$, cioè $x < y \Leftrightarrow x <_A y$ per ogni $(A, <_A) \in \mathcal{F}$ tale che $x, y \in A$.

È facile verificare che la relazione di sopra è effettivamente una relazione d'ordine parziale. Inoltre:

PROPOSIZIONE 7.5. L'unione di una catena di insiemi totalmente ordinati è un insieme totalmente ordinato.

DIM. Sia $\mathcal{F}$ la famiglia assegnata, e sia $(X, <)$ l'insieme parzialmente ordinato ottenuto come unione. Dati $a, b \in X$, prendiamo $(A, <_A), (B, <_B) \in \mathcal{F}$ tali che $a \in A$ e $b \in B$. Per la compatibilità, possiamo supporre ad esempio che $(A, <_A)$ sia un sottoinsieme di $(B, <_B)$. Allora a, b sono confrontabili in $(B, <_B)$, e quindi nell'unione $(X, <)$. $\square$

Ricordiamo che il prodotto cartesiano di due insiemi $A_1 \times A_2$ era stato definito come l'insieme di tutte le coppie ordinate (a, b) dove $a \in A_1$ e $b \in A_2$. Inoltre, avevamo definito $A_1 \times A_2 \times A_3 = (A_1 \times A_2) \times A_3$ come l'insieme di tutte le triple ordinate $(a, b, c) = ((a, b), c)$ dove $a \in A_1$, $b \in A_2$ e $c \in A_3$; e così via per tutti i prodotti cartesiani $A_1 \times \dots \times A_n$ di un numero finito di insiemi.¹¹ Per definire un prodotto di infiniti insiemi è necessario procedere in modo diverso. Precisamente:

DEFINIZIONE 7.6. Sia $(A_i)_{i \in I}$ una sequenza di insiemi. Il corrispondente *prodotto* è definito ponendo:

$$\prod_{i \in I} A_i = \{f \mid f \text{ è una } I\text{-sequenza} \wedge \forall i \in I f(i) \in A_i\}.$$

In questo caso, ogni elemento $f \in \prod_{i \in I} A_i$ si chiama *I-upla*, e per ogni $i \in I$, l'elemento $f(i) \in A_i$ si dice *i-esima coordinata* della *I-upla* f .

¹¹ La formalizzazione di questo procedimento richiede il principio di induzione, che sarà discusso in seguito.

Attenzione! La definizione di sopra non verrà applicata quando I è finito, perché in quel caso si otterrebbe una nozione diversa (anche se simile) a quella già introdotta di *prodotto cartesiano*. Ad esempio, $\prod_{i \in \{1,2\}} A_i \neq A_1 \times A_2$ perché gli elementi del primo insieme sono funzioni f della forma $f = \{(1, a), (2, b)\}$ dove $a \in A_1$ e $b \in A_2$, mentre gli elementi del secondo insieme sono coppie ordinate (a, b) dove $a \in A_1$ e $b \in A_2$.

8. Assioma di scelta

Può sembrare a prima vista un fatto evidente che quando in una sequenza $(A_i)_{i \in I}$ nessun insieme A_i è vuoto, anche il prodotto $\prod_{i \in I} A_i$ non è vuoto. In effetti, in alcuni casi particolari questa proprietà si può verificare direttamente. Ad esempio, se $I = \{1, \dots, n\}$ è finito, questo segue dalla definizione di insieme non vuoto; ricordiamo infatti che $A_i \neq \emptyset$ significa che esiste un elemento $a_i \in A_i$, e quindi si può formare la I -upla $(a_i)_{i=1, \dots, n} \in \prod_{i=1}^n A_i$.¹² Un altro caso è quando tutti gli insiemi $A_i = B$ sono uguali tra loro: per trovare un elemento del prodotto basta prendere un elemento $b \in B$, e considerare la I -upla costante $c_b = (b)_{i \in I}$ con tutte le coordinate uguali a b ; chiaramente $c_b \in \prod_{i \in I} B$.

Un esempio più interessante sono i prodotti infiniti $\prod_{i \in I} A_i$ dove gli $A_i \subseteq \mathbb{N}$ sono insiemi non vuoti qualunque di numeri naturali; in questo caso basta definire $f(i) = \min A_i$ ed abbiamo che la I -upla $(f(i))_{i \in I} \in \prod_{i \in I} A_i$. Tuttavia – per quanto sorprendente possa sembrare – nel caso generale di sequenze infinite di insiemi non vuoti $(A_i)_{i \in I}$, non c'è modo di dimostrare che $\prod_{i \in I} A_i \neq \emptyset$ a partire dai nostri tre principi. Allo scopo, è necessario assumere un apposito assioma.¹³

Assioma di Scelta. *Se $(A_i)_{i \in I}$ è una sequenza di insiemi non vuoti, allora $\prod_{i \in I} A_i \neq \emptyset$.*

Informalmente, un elemento $f \in \prod_{i \in I} A_i$ è una funzione che “sceglie” un elemento $f(i)$ da ciascun $A_i \neq \emptyset$. Nonostante che la sua validità sembri intuitivamente evidente, l'assioma di scelta ha alcune conseguenze molto bizzarre e controintuitive, e per questo è stato oggetto di lunghe discussioni e forti critiche a cavallo del 1900 e oltre. Oggigiorno, l'assioma di scelta è usato comunemente nella pratica matematica, e riveste un ruolo essenziale in numerose applicazioni.

Vediamone subito alcune utili formulazioni equivalenti (ne vedremo anche altre più avanti nel corso).

TEOREMA 8.1. *Le seguenti proprietà sono equivalenti.*¹⁴

- (1) *Assioma di scelta.*
- (2) *Ogni famiglia $\mathcal{F}$ di insiemi non vuoti ha una “funzione di scelta”, cioè esiste una funzione f tale che $f(F) \in F$ per ogni $F \in \mathcal{F}$ non vuoto.*

¹² L'esistenza di tale I -upla finita segue dal fatto che possiamo scrivere una formula che la descrive, in cui si elencano gli elementi ad uno ad uno. Ovviamente questo non è invece possibile nel caso in cui I sia infinito (ricordiamo che una formula è una stringa *finita* di simboli).

¹³ Questa affermazione può essere resa precisa. Infatti se **ZF** è la teoria degli insiemi di Zermelo-Fraenkel (che introdurremo più avanti), allora si può dimostrare che **ZF** non dimostra l'assioma di scelta.

¹⁴ Ciò che in realtà intendiamo qui è che l'equivalenza delle proprietà elencate è dimostrabile a partire dai soli tre principi informali della teoria degli insiemi che stiamo assumendo. Vedremo più avanti che possiamo rendere rigorose queste equivalenze, mostrando come esse siano dimostrabili all'interno della teoria di Zermelo-Fraenkel **ZF**.

- (3) Ogni insieme A ha una “funzione di scelta” $f : \mathcal{P}(A) \setminus \{\emptyset\} \rightarrow A$ tale che $f(B) \in B$ per ogni B .
- (4) Ogni famiglia non vuota $\mathcal{F}$ di insiemi non vuoti a due a due disgiunti ha un “insieme di scelta”, cioè un insieme X tale che $X \cap F = \{x_F\}$ contiene un unico elemento x_F per ogni $F \in \mathcal{F}$.¹⁵
- (5) Ogni funzione suriettiva $f : A \rightarrow B$ ammette un’inversa destra, cioè esiste $g : B \rightarrow A$ tale che $f \circ g = id_B$. (Tale g è necessariamente iniettiva.)

DIM. L’equivalenza (1) $\Leftrightarrow$ (2) è immediata. Infatti, se f è una funzione di scelta per la famiglia $\mathcal{F} = \{A_i \mid i \in I\}$, allora la I -upla $(f(A_i))_{i \in I} \in \prod_{i \in I} A_i$. Viceversa, data una famiglia di insiemi non vuoti $\mathcal{F}$, ogni $f \in \prod_{F \in \mathcal{F}} F$ è una funzione di scelta per $\mathcal{F}$.

(2) $\Rightarrow$ (3) è banale.

(3) $\Rightarrow$ (4). Sia $A = \bigcup_{F \in \mathcal{F}} F$; notiamo che $\mathcal{F} \subseteq \mathcal{P}(A)$. Se $f : \mathcal{P}(A) \setminus \{\emptyset\} \rightarrow A$ è una funzione di scelta per A , visto che gli insiemi in $\mathcal{F}$ sono a due a due disgiunti, segue subito che $X = \{f(F) \mid F \in \mathcal{F}\}$ è un insieme di scelta per $\mathcal{F}$.

(4) $\Rightarrow$ (5). Consideriamo la famiglia di insiemi disgiunti $\mathcal{F} = \{\Lambda_b \mid b \in B\}$, dove $\Lambda_b = f^{-1}(\{b\}) = \{a \in A \mid f(a) = b\}$ è la controimmagine di b . Visto che f è suriettiva, ogni $\Lambda_b \neq \emptyset$. Esiste allora un insieme di scelta X per $\mathcal{F}$. Se definiamo $g : B \rightarrow A$ ponendo $g(b)$ come l’unico elemento di $X \cap \Lambda_b$, allora chiaramente $f(g(b)) = b$, come volevamo.

(5) $\Rightarrow$ (1). Per ogni $i \in I$ e per ogni $a \in A_i$, poniamo $f(a, i) = A_i$. Otteniamo così una funzione suriettiva $f : \bigcup_{i \in I} (A_i \times \{i\}) \rightarrow \mathcal{F}$, dove $\mathcal{F} = \{A_i \mid i \in I\}$. Sia adesso $g : \mathcal{F} \rightarrow \bigcup_{i \in I} (A_i \times \{i\})$ una inversa destra di f . Questo significa che se $g(A_i) = (b_i, j_i)$ dove $b_i \in A_{j_i}$, allora $A_i = f(g(A_i)) = A_{j_i}$, e quindi $b_i \in A_i$. Concludiamo che $(b_i)_{i \in I} \in \prod_{i \in I} A_i \neq \emptyset$. $\square$

ESERCIZIO 8.2. Dimostrare che l’assioma di scelta AC è equivalente alla seguente proprietà: Per ogni sequenza di insiemi $(F_{i,j} \mid (i,j) \in I \times J)$, vale l’uguaglianza:¹⁶

$$\bigcap_{i \in I} \bigcup_{j \in J} F_{i,j} = \bigcup_{f \in J^I} \bigcap_{i \in I} F_{i,f(i)}.$$

Per chiarezza, nel seguito marcheremo con la sigla (AC) ogni risultato la cui dimostrazione richiede necessariamente un’applicazione dell’assioma di scelta.¹⁷

¹⁵ La richiesta che gli insiemi di $\mathcal{F}$ siano a due a due disgiunti è necessaria. Ad esempio se $\mathcal{F} = \{\{0\}, \{1\}, \{0, 1\}\}$, un insieme di scelta per $\mathcal{F}$ dovrebbe contenere necessariamente 0 e 1 e quindi non potrebbe intersecare $\{0, 1\}$ in un solo elemento.

¹⁶ Ricordiamo che J^I denota l’insieme di tutte le funzioni $f : I \rightarrow J$.

¹⁷ Diciamo “necessariamente” per intendere che quei risultati *non* possono essere dimostrati senza l’assioma di scelta. (Con gli strumenti della logica matematica è possibile dimostrare la *non dimostrabilità* di un enunciato a partire da una data lista di assiomi.)

CHAPTER 2

Cardinalità numerabile e cardinalità del continuo

Adesso che tutta la terminologia di base è stata introdotta, possiamo finalmente cominciare ad entrare nel vivo della teoria degli insiemi.

Come anticipato nell'*Introduzione*, in questa prima fase procederemo in modo semi-formale, così come si farebbe in una qualunque altra disciplina matematica, rimandando a più avanti le questioni legate ai fondamenti logici della teoria. Più precisamente, ci baseremo sui tre principi insiemistici formulati nel primo capitolo, ma assumeremo anche come conosciute le nozioni fondamentali che si usano nella pratica, e i relativi risultati di base. In particolare, assumeremo come note le nozioni di numero *naturale*, *intero*, *razionale*, *reale*.

Ricordiamo la seguente fondamentale definizione.

DEFINIZIONE 0.1. Un insieme A si dice *finito* se è equipotente ad un segmento iniziale $\{1, \dots, n\}$ dei numeri naturali. A si dice *infinito* in caso contrario.

Nel seguito useremo direttamente le proprietà fondamentali dei numeri naturali, interi, razionali, reali, e degli insiemi finiti ed infiniti, tra cui le seguenti:

- Un sottoinsieme di un insieme finito è finito, e il soprainsieme di un insieme infinito è infinito.
- L'unione di un numero finito di insiemi finiti è un insieme finito.
- Il principio del *buon ordinamento* dei numeri naturali, cioè la proprietà che ogni insieme non vuoto $A \subseteq \mathbb{N}$ ha minimo;
- Il principio di *induzione* sui numeri naturali¹;
- Il procedimento di *ricorsione* (o di “induzione”, come si dice usualmente con termine improprio) per definire successioni;
- La proprietà di *completezza* dei numeri reali;
- La proprietà di *densità* dei numeri razionali nei numeri reali: “Se $r < s$ sono due numeri reali, allora esiste $q \in \mathbb{Q}$ tale che $r < q < s$ ”.

È bene chiarire che tutte queste nozioni, proprietà e principi saranno reintrodotti e dimostrati in modo formale più avanti. Inoltre, tutte le dimostrazioni date in questo capitolo, saranno formalizzabili all'interno della teoria assiomatica che presenteremo, e quindi saranno da considerarsi del tutto rigorose.

¹ Vedremo in seguito che il principio di induzione e la proprietà del buon ordinamento sono in realtà proprietà equivalenti.

1. Equipotenza

La cruciale nozione di equipotenza è stata introdotta da Cantor nella seconda metà del XIX per catturare l'idea di “grandezza” o “cardinalità” di un insieme infinito. Per un insieme finito A , la cardinalità è data da quell'unico numero naturale n per cui si ha una bigezione $f : \{1, \dots, n\} \rightarrow A$; tale numero n rappresenta la “quantità” degli elementi di A . Partendo dalla considerazione che due insiemi finiti hanno lo stesso numero di elementi se e solo se esiste una bigezione tra di loro, Cantor propose la seguente definizione generale:

DEFINIZIONE 1.1. Due insiemi A e B sono *equipotenti* o hanno la stessa *cardinalità* se esiste una funzione biunivoca $f : A \rightarrow B$. In questo caso scriviamo $|A| = |B|$.

Un primo esempio importante è il seguente:

PROPOSIZIONE 1.2. *L'insieme delle funzioni caratteristiche su un insieme X è equipotente all'insieme delle parti, cioè $|2^X| = |\mathcal{P}(X)|$.*

DIM. Sia $\Psi : \mathcal{P}(X) \rightarrow 2^X$ la funzione che associa ad ogni sottoinsieme $A \subseteq X$ la corrispondente funzione caratteristica χ_A . Come abbiamo già osservato nel capitolo precedente, ogni funzione $\chi : X \rightarrow \{0, 1\}$ è la funzione caratteristica di uno ed un solo sottoinsieme $A_\chi \subseteq X$, precisamente $A_\chi = \{x \in X \mid \chi(x) = 1\}$, e quindi Ψ è biunivoca. $\square$

Le seguenti proprietà dell'equipotenza sono la controparte insiemistica delle uguaglianze algebriche $a^b \cdot a^c = a^{b+c}$ e $(a^b)^c = a^{bc}$, dove l'unione disgiunta corrisponde alla somma, il prodotto cartesiano corrisponde al prodotto, e l'esponentiale corrisponde all'insieme delle funzioni.

La nostra notazione $|A| = |B|$ è giustificata dal fatto che l'equipotenza gode delle tre proprietà di relazione di equivalenza.

PROPOSIZIONE 1.3.

- (1) *Proprietà riflessiva:* $|A| = |A|$;
- (2) *Proprietà simmetrica:* Se $|A| = |B|$ allora $|B| = |A|$;
- (3) *Proprietà transitiva:* Se $|A| = |B|$ e $|B| = |C|$ allora $|A| = |C|$.

DIM. (1) La funzione identità $\text{id}_A : A \rightarrow A$ è banalmente una bigezione. (2) Se $f : A \rightarrow B$ è una bigezione, allora anche la sua inversa $f^{-1} : B \rightarrow A$ è una bigezione. (3) Se $f : A \rightarrow B$ e $g : B \rightarrow C$ sono bigezioni, allora anche la composizione $g \circ f : A \rightarrow C$ è una bigezione. $\square$

Attenzione! Non possiamo propriamente parlare dell'equipotenza come di una relazione di equivalenza perché si tratterebbe di una relazione avente come dominio la collezione di tutti gli insiemi. Come vedremo fra poco (vedi Corollario 1.8), assumere che esista l'insieme di tutti gli insiemi porta a contraddizioni.

Attenzione! Abbiamo scritto $|A| = |B|$ per intendere che A e B sono equipotenti, ma la scrittura $|A|$ da sola *non* ha (per il momento) alcun significato.²

² L'intuizione ci suggerirebbe di attribuirgliene uno come classe di equivalenza, definendo $|A| = \{B \mid |A| = |B|\}$. Anche in questo caso però, assumere che una tale collezione sia un insieme condurrebbe a contraddizioni perché la sua unione sarebbe l'insieme di tutti gli insiemi.

È bene anticipare che, quando avremo sviluppato una teoria assiomatica degli insiemi, i problemi evidenziati sopra saranno superati. Avremo infatti un modo rigoroso per definire degli speciali oggetti, detti *cardinali*, che saranno i rappresentanti canonici delle “classi” di equipotenza. Precisamente, per ogni insieme A esisterà ed unico un cardinale κ tale che $|A| = |\kappa|$. A quel punto scriveremo direttamente $|A| = \kappa$, e diremo che κ è la *cardinalità* dell'insieme A .³

La relazione di equipotenza è coerente con le operazioni insiemistiche di unione disgiunta, prodotto cartesiano, insieme delle funzioni, e insieme potenza.

ESERCIZIO 1.4. Supponiamo che $|A| = |A'|$ e $|B| = |B'|$. Allora

- (1) $|A \cup B| = |A' \cup B'|$ se $A \cap B = A' \cap B' = \emptyset$;
- (2) $|A \times B| = |A' \times B'|$;
- (3) $|\text{Fun}(A, B)| = |\text{Fun}(A', B')|$;
- (4) $|\mathcal{P}(A)| = |\mathcal{P}(A')|$.

ESERCIZIO 1.5.

- (1) $|A^B \times A^C| = |A^{B \cup C}|$ quando $A \cap B = \emptyset$.
- (2) $|(A^B)^C| = |A^{(B \times C)}|$.

Ciò che rende significativa la teoria delle cardinalità è il fatto che non tutti gli insiemi infiniti sono tra loro equipotenti. Cantor dimostrò infatti che per ogni insieme assegnato, ne esiste uno di cardinalità diversa.

Come primo esempio, consideriamo i numeri naturali $\mathbb{N}$, e l'insieme $2^{\mathbb{N}}$ delle funzioni caratteristiche su $\mathbb{N}$.

TEOREMA 1.6. *Non esistono funzioni suriettive $\Psi : \mathbb{N} \rightarrow 2^{\mathbb{N}}$, dunque $|\mathbb{N}| \neq |2^{\mathbb{N}}|$.*

DIM. Supponiamo data una funzione $\Psi : \mathbb{N} \rightarrow 2^{\mathbb{N}}$ qualunque. Vogliamo dimostrare che Ψ non è suriettiva. Per ogni $n \in \mathbb{N}$, denotiamo con $(a_{n,k} \mid k \in \mathbb{N})$ la successione $\Psi(n)$.

a ₁₁	a ₁₂	a ₁₃	a ₁₄	a ₁₅	a ₁₆	a ₁₇	...
a ₂₁	a ₂₂	a ₂₃	a ₂₄	a ₂₅	a ₂₆	a ₂₇	...
a ₃₁	a ₃₂	a ₃₃	a ₃₄	a ₃₅	a ₃₆	a ₃₇	...
a ₄₁	a ₄₂	a ₄₃	a ₄₄	a ₄₅	a ₄₆	a ₄₇	...
a ₅₁	a ₅₂	a ₅₃	a ₅₄	a ₅₅	a ₅₆	a ₅₇	...
a ₆₁	a ₆₂	a ₆₃	a ₆₄	a ₆₅	a ₆₆	a ₆₇	...
a ₇₁	a ₇₂	a ₇₃	a ₇₄	a ₇₅	a ₇₆	a ₇₇	...
a _{n1}	a _{n2}	a _{n3}	a _{n4}	a _{n5}	a _{n6}	a _{n7}	...

Per ogni n , sia $b_n = 0$ se $a_{n,n} = 1$; e sia $b_n = 1$ se invece $a_{n,n} = 0$. Allora la successione $(b_k \mid k \in \mathbb{N})$ non appartiene all'immagine di Ψ . Infatti, per ogni n , $\Psi(n) = (a_{n,k} \mid k \in \mathbb{N}) \neq (b_k \mid k \in \mathbb{N})$, visto che per la definizione data, l' n -esimo elemento $a_{n,n} \neq b_n$. $\square$

³ Anche a questo riguardo è interessante il ruolo fondamentale rivestito dall'*assioma di scelta*. Infatti si può dimostrare che senza assioma di scelta, non esiste alcun modo “definibile” per individuare un unico rappresentante in ogni classe di equipotenza (Teorema di Pincus del 1974).

Il metodo usato nella dimostrazione di sopra è noto come “argomento diagonale”. La successione $(b_k \mid k \in \mathbb{N})$ è stata infatti definita a partire dagli elementi $a_{n,n}$ i cui indici stanno sulla diagonale di $\mathbb{N} \times \mathbb{N}$. Usando lo stesso procedimento diagonale, più in generale si dimostra che nessun insieme è equipotente al corrispondente insieme delle parti.⁴

TEOREMA 1.7 (Cantor). *Per ogni insieme A , non esistono funzioni suriettive $f : A \rightarrow \mathcal{P}(A)$. Dunque $|A| \neq |\mathcal{P}(A)|$.*

DIM. Data una funzione $f : A \rightarrow \mathcal{P}(A)$, dimostriamo che il seguente insieme non appartiene all'immagine di f :

$$B = \{a \in A \mid a \notin f(a)\}.$$

Supponiamo per assurdo che esista un elemento $\alpha \in A$ con $f(\alpha) = B$. Si hanno due possibilità. Se $\alpha \in B$ allora, per definizione di B , avremmo che $\alpha \notin f(\alpha) = B$, contro l'ipotesi. Se invece $\alpha \notin B$, di nuovo per la definizione di B , avremmo che $\alpha \in f(\alpha) = B$, contro l'ipotesi. Entrambi i casi ci portano ad una conseguenza assurda, e concludiamo che f non può essere suriettiva. $\square$

Osserviamo che la dimostrazione dei Teoremi 1.6 e 1.7 sono essenzialmente le stesse. Infatti, identifichiamo ogni sottoinsieme $A \subseteq \mathbb{N}$ con la corrispondente funzione caratteristica $\chi_A \in 2^{\mathbb{N}}$. Prendendo $\Psi(n) = \chi_{f(n)}$, l'insieme B definito nella dimostrazione del teorema di sopra, ha come funzione caratteristica χ_B precisamente la successione $b = (b_k \mid k \in \mathbb{N})$, come definita con l'argomento diagonale nella dimostrazione del Teorema 1.6.

COROLLARIO 1.8. Non può esistere l'insieme universale $V = \{x \mid x = x\}$ che contiene tutti gli insiemi.

DIM. Se V fosse un insieme, allora avremmo che $V = \mathcal{P}(V)$. Infatti, $\mathcal{P}(V) \subseteq V$, perché banalmente ogni elemento di $\mathcal{P}(V)$ è un insieme. Per vedere l'altra inclusione ricordiamo che – in conseguenza del principio di estensionalità – non esistono atomi, e quindi per noi gli elementi di un insieme sono essi stessi insiemi (ogni insieme è un insieme di insiemi). Allora $A \in V \Rightarrow A \subseteq V$, e quindi $V \subseteq \mathcal{P}(V)$, come volevamo. Finalmente otteniamo un assurdo perché se $V = \mathcal{P}(V)$, allora banalmente la funzione identità $\iota : V \rightarrow \mathcal{P}(V)$ sarebbe suriettiva, contro il teorema di Cantor. $\square$

Notiamo che, ripercorrendo la dimostrazione del Teorema di Cantor nel caso della funzione identità $\iota : V \rightarrow \mathcal{P}(V)$, la collezione $\{x \in V \mid x \notin \iota(x)\} = \{x \mid x \notin x\}$ è la collezione paradossale di Russell.

Abbiamo così trovato, dopo la proprietà di Russell “ $x \notin x$ ”, un secondo esempio di proprietà *non* ammissibile, cioè “ $x = x$ ”, cui non possiamo applicare il principio di comprensione.

⁴ Ricordiamo che per ogni X , l'insieme delle parti $\mathcal{P}(X)$ è equipotente all'insieme delle funzioni caratteristiche 2^X (vedi Proposizione 1.2).

2. Ordine tra cardinalità

Oltre alla nozione di uguaglianza tra grandezze data dall'equipotenza, c'è anche una naturale nozione di confrontabilità.

DEFINIZIONE 2.1. Diciamo che l'insieme A ha *cardinalità minore o uguale* a quella di B , e scriviamo $|A| \leq |B|$, se vale una delle due seguenti proprietà equivalenti:

- (1) Esiste una funzione iniettiva $f : A \rightarrow B$;
- (2) Esiste un sottoinsieme $A' \subseteq B$ tale che $|A| = |A'|$.

Useremo la disuguaglianza stretta $|A| < |B|$ se $|A| \leq |B|$ ma $|A| \neq |B|$.

Che le due condizioni di sopra siano equivalenti, segue dalla ovvia osservazione che una funzione $f : A \rightarrow B$ è iniettiva se e solo se $f : A \rightarrow \text{imm}(f)$ è biunivoca. Notiamo inoltre che la definizione data è coerente con l'equipotenza; vale infatti la seguente proprietà:

PROPOSIZIONE 2.2. Se $|A| = |A'|$ e $|B| = |B'|$, allora $|A| \leq |B| \Leftrightarrow |A'| \leq |B'|$.

DIM. Siano $f : A \rightarrow A'$ e $g : B \rightarrow B'$ biezioni. Se $|A| \leq |B|$, prendiamo $h : A \rightarrow B$ iniettiva. Allora anche $g \circ h \circ f^{-1} : A' \rightarrow B'$ è iniettiva, perché composizione di funzioni iniettive. Analogamente per l'altra implicazione.

$$\begin{array}{ccc}
 A & \xrightarrow{h} & B \\
 \uparrow f^{-1} & & \uparrow g \\
 A' & \xrightarrow{g \circ h \circ f^{-1}} & B'
 \end{array}$$

□

Il prossimo teorema è di importanza centrale nella teoria delle cardinalità, ed è utilissimo nella pratica per dimostrare l'equipotenza fra insiemi. La sua dimostrazione non è facile, ed è rimandata a quando tratteremo la teoria assiomatica degli insiemi.

TEOREMA 2.3 (Cantor-Bernstein).

Se esistono funzioni iniettive $f : A \rightarrow B$ e $g : B \rightarrow A$, allora esiste una funzione biunivoca $h : A \rightarrow B$. In formula: $|A| \leq |B|$ e $|B| \leq |A| \Rightarrow |A| = |B|$.

Il minore o uguale tra cardinalità gode delle tre proprietà di ordine parziale, e questo giustifica la scrittura $|A| \leq |B|$.

PROPOSIZIONE 2.4.

- (1) *Proprietà riflessiva:* $|A| \leq |A|$;
- (2) *Proprietà anti-simmetrica:* Se $|A| \leq |B|$ e $|B| \leq |A|$, allora $|A| = |B|$;
- (3) *Proprietà transitiva:* Se $|A| \leq |B|$ e $|B| \leq |C|$, allora $|A| \leq |C|$.

PROOF. (1) è banale. (2) è il teorema di Cantor-Bernstein. (3). Basta notare che se $f : A \rightarrow B$ e $g : B \rightarrow C$ sono iniettive, allora anche la composizione $g \circ f : A \rightarrow C$ è iniettiva. □

In modo del tutto simile all'equipotenza, anche la relazione di minore o uguale tra cardinalità è coerente con le operazioni insiemistiche di unione disgiunta, prodotto cartesiano, insieme delle funzioni, e insieme potenza.

ESERCIZIO 2.5. Supponiamo che $|A| \leq |A'|$ e $|B| \leq |B'|$. Allora

- (1) $|A \cup B| \leq |A' \cup B'|$ se $A \cap B = A' \cap B' = \emptyset$;
- (2) $|A \times B| \leq |A' \times B'|$;
- (3) $|\text{Fun}(A, B)| \leq |\text{Fun}(A', B')|$;
- (4) $|\mathcal{P}(A)| \leq |\mathcal{P}(A')|$.

Dati due insiemi A e B , nella pratica è spesso più facile trovare una funzione suriettiva $g : B \rightarrow A$ piuttosto che una funzione iniettiva $f : A \rightarrow B$. Le due proprietà sono equivalenti, ma per dimostrare una delle due implicazioni è necessario l'uso dell'assioma di scelta.

PROPOSIZIONE 2.6.

- (1) Se $|A| \leq |B|$, allora esiste una funzione suriettiva $g : B \rightarrow A$.
- (2) (AC). Se esiste $g : B \rightarrow A$ suriettiva, allora $|A| \leq |B|$.

DIM. (1). Prendiamo $f : A \rightarrow B$ iniettiva. Per ogni $b \in \text{imm}(f)$, sia $g(b) \in A$ quell'unico elemento tale che $f(g(b)) = b$ (l'unicità segue dall'ipotesi di f iniettiva). Fissiamo poi un qualunque elemento $a_0 \in A$ e poniamo $g(b) = a_0$ se $b \notin \text{imm}f$. Resta così definita una funzione suriettiva $g : B \rightarrow A$.

(2). Data una funzione $g : B \rightarrow A$ suriettiva, usando l'assioma di scelta possiamo prendere una sua inversa destra f , cioè una funzione $f : A \rightarrow B$ tale che $g \circ f = \text{id}_A$ (cf. Proposizione ??). Una tale f è necessariamente iniettiva, e quindi $|A| \leq |B|$. $\square$

ESERCIZIO 2.7. Dimostrare che sono proprietà equivalenti:

- (1) Assioma di scelta.
- (2) Per ogni relazione binaria, $|\text{dom}(R)| \leq |R|$.
- (3) Per ogni relazione binaria, $|\text{imm}(R)| \leq |R|$.

Come curiosità, e come indicazione dell'importanza dell'assioma di scelta nella teoria delle cardinalità, anticipiamo qui due importanti risultati che dimostreremo più avanti. Si tratta di due formulazioni equivalenti dell'assioma di scelta che andranno ad aggiungersi a quelle già viste nella Proposizione ??.

TEOREMA. Ognuna delle due seguenti proprietà è equivalente all'assioma di scelta:

- (1) (Confrontabilità) Per ogni A e B , si ha che $|A| \leq |B|$ o $|B| \leq |A|$.
- (2) Per ogni A infinito, $|A \times A| = |A|$.

3. Cardinalità numerabile

Iniziamo finalmente lo studio delle cardinalità, iniziando con il caso numerabile. Seguendo l'uso comune in matematica, *non* includeremo il numero 0 tra i numeri naturali, cioè

$$\mathbb{N} = \{1, 2, 3, \dots, n, n+1, \dots\}.$$

Useremo la notazione $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ per denotare l'insieme degli interi non negativi.

DEFINIZIONE 3.1. Un insieme A ha *cardinalità numerabile* se $|A| = |\mathbb{N}|$. In questo caso scriviamo $|A| = \aleph_0$, che si legge: “ A ha cardinalità aleph-zero”.

Un’*enumerazione* di A è una funzione biunivoca $(a_n \mid n \in \mathbb{N})$ da $\mathbb{N}$ in A .⁵

Scriveremo $\aleph_0 \leq |A|$ e $|A| \leq \aleph_0$ per intendere rispettivamente $|\mathbb{N}| \leq |A|$ e $|A| \leq |\mathbb{N}|$.⁶

Per gli insiemi numerabili, la proprietà (2) della Proposizione ?? si può dimostrare senza fare uso dell’assioma di scelta.

ESERCIZIO 3.2. Senza assumere l’assioma di scelta, dimostrare che se B è numerabile, allora $|A| \leq |B|$ se e solo se esiste una funzione suriettiva $g : B \rightarrow A$.

PROPOSIZIONE 3.3. Se $A \subseteq \mathbb{N}$ è un sottoinsieme infinito, allora $|A| = \aleph_0$.

DIM. Procedendo per ricorsione, definiamo la successione:

$$a_1 = \min A; \quad a_{n+1} = \min (A \setminus \{a_1, \dots, a_n\}).$$

Visto che A è infinito, per ogni n abbiamo che $A \neq \{a_1, \dots, a_n\}$, quindi la differenza insiemistica $A \setminus \{a_1, \dots, a_n\}$ non è vuota, e la definizione è ben posta. Chiaramente, la successione $(a_n \mid n \in \mathbb{N})$ è crescente, e quindi iniettiva e illimitata. Inoltre la sua immagine $\{a_n \mid n \in \mathbb{N}\} = A$. Infatti, è immediato verificare per induzione che per ogni k , si ha $\{a_1, \dots, a_k\} = A \cap [1, a_k]$, e quindi

$$\{a_n \mid n \in \mathbb{N}\} = \bigcup_{k \in \mathbb{N}} \{a_1, \dots, a_k\} = \bigcup_{k \in \mathbb{N}} (A \cap [1, a_k]) = A.$$

Resta così dimostrato che la sequenza $(a_n \mid n \in \mathbb{N})$ è la bigezione cercata. $\square$

COROLLARIO 3.4. Se A è un insieme infinito e $|A| \leq \aleph_0$ allora $|A| = \aleph_0$.

DIM. Per ipotesi esiste una funzione iniettiva $f : A \rightarrow \mathbb{N}$. Dunque $|A| = |\text{imm}(f)|$ dove $\text{imm}(f)$ è un sottoinsieme infinito di $\mathbb{N}$. Allora, applicando la proposizione precedente, si ottiene che $|A| = |\text{imm}(f)| = \aleph_0$. $\square$

In conseguenza dei risultati di sopra, otteniamo una dimostrazione del Teorema di Cantor-Bernstein nel caso particolare in cui uno dei due insiemi è numerabile.

COROLLARIO 3.5. Sia B un insieme numerabile. Se $|A| \leq |B|$ e $|B| \leq |A|$ allora $|A| = |B|$.

DIM. Visto che $|A| \leq |B| = \aleph_0$, la tesi segue dal corollario precedente una volta mostrato che A è infinito. Supponiamo per assurdo che A sia finito; allora esisterebbe $n \in \mathbb{N}$ ed una bigezione $f : A \rightarrow \{1, \dots, n\}$. Dall’ipotesi $|\mathbb{N}| = |B| \leq |A|$ sappiamo che esiste una funzione iniettiva $g : \mathbb{N} \rightarrow A$. Ma allora la composizione $f \circ g : \mathbb{N} \rightarrow \{1, \dots, n\}$ sarebbe iniettiva.⁷ $\square$

⁵ Per alcuni autori, una enumerazione di A è una funzione *suriettiva* da $\mathbb{N}$ su A . Noi invece chiediamo anche l’iniettività, in modo da non avere ripetizioni.

⁶ Per il momento, per noi $\aleph_0$ è solo un simbolo. Quando svilupperemo la teoria in modo assiomatico, $\aleph_0$ sarà uno speciale insieme che viene preso come rappresentante canonico di tutti gli insiemi numerabili.

⁷ Qui diamo per nota la seguente proprietà, intuitivamente evidente: “Per ogni $n \in \mathbb{N}$ non esistono funzioni iniettive $\varphi : \mathbb{N} \rightarrow \{1, \dots, n\}$ ”. Tale proprietà sarà dimostrata formalmente più avanti, a partire dagli assiomi della teoria di Zermelo-Fraenkel (vedi Proposizione ??).

Come è suggerito dal sottoindice “zero”, $\aleph_0$ rappresenta la più piccola delle cardinalità infinite. Vale infatti il

TEOREMA 3.6. (AC) *Se A è un insieme infinito allora esiste un sottoinsieme numerabile $A' \subseteq A$, e quindi $\aleph_0 \leq |A|$.*

DIM. Per l'assioma di scelta, possiamo prendere una funzione f tale che $f(B) \in B$ per ogni sottoinsieme non vuoto $B \subseteq A$. Adesso procediamo in modo del tutto simile a sopra, e definiamo per ricorsione la successione:

$$a_1 = f(A); \quad a_{n+1} = f(A \setminus \{a_1, \dots, a_n\}).$$

Visto che A è infinito, $A \setminus \{a_1, \dots, a_n\} \neq \emptyset$ per ogni n , e dunque il passo induttivo a_{n+1} è ben definito. È immediato verificare che gli elementi a_n sono tutti distinti, e la successione $(a_n \mid n \in \mathbb{N})$ è la funzione iniettiva cercata. $\square$

C'è una differenza importante tra la dimostrazione della Proposizione 3.3 e di quest'ultimo teorema. Mentre nella Proposizione 3.3 ogni elemento a_n è definito in modo univoco come il minimo di un certo insieme di numeri naturali, nella dimostrazione del Teorema 3.6 i termini a_n sono stati “scelti” dentro certi insiemi non vuoti. Per definire la successione $(a_n \mid n \in \mathbb{N})$ è stato quindi necessario usare una funzione di scelta su A , per la cui esistenza occorre l'assioma di scelta.

Nel caso numerabile, le proprietà (2) e (3) dell'Esercizio 2.7 non richiedono l'assioma di scelta.

ESERCIZIO 3.7. Senza usare l'assioma di scelta, dimostrare che se R è una relazione binaria numerabile, allora $|\text{dom}(R)| \leq |R|$ e $|\text{imm}(R)| \leq |R|$.

Mostriamo ora che togliere o aggiungere un numero finito di elementi da un insieme infinito, non ne cambia la cardinalità.

PROPOSIZIONE 3.8. *Sia A un insieme numerabile e sia B un insieme finito. Allora $|A \setminus B| = |A \cup B| = |A|$.*

DIM. Consideriamo l'insieme $B' = B \setminus A$. Chiaramente $B' = \{b'_1, \dots, b'_k\} \subseteq B$ è finito, B' è disgiunto da A , e $A \cup B' = A \cup B$. Fissata una bigezione $f : \mathbb{N} \rightarrow A$, definiamo la funzione $g : \mathbb{N} \rightarrow A \cup B$ ponendo:

$$g(n) = \begin{cases} b'_n & \text{se } n \leq k \\ f(n - k) & \text{se } n > k. \end{cases}$$

(Se $B' = \emptyset$, poniamo $g = f$.) Si può verificare direttamente che g è una bigezione, e quindi $|A \cup B| = |A|$.

L'altra equipotenza $|A \setminus B| = |A|$ si dimostra in modo analogo. Notiamo che $A \setminus B$ è infinito, altrimenti $A = (A \setminus B) \cup B$ sarebbe l'unione di due insiemi finiti, e quindi sarebbe finito, contro l'ipotesi. Inoltre $|A \setminus B| \leq |A| = \aleph_0$ e quindi, per il Corollario 3.4, esiste una bigezione $\varphi : \mathbb{N} \rightarrow A \setminus B$. Consideriamo l'insieme finito $B'' = B \cap A = \{b''_1, \dots, b''_m\}$. Chiaramente B'' è disgiunto da $A \setminus B$ e $A = (A \setminus B) \cup B$. La seguente funzione $\psi : A \setminus B \rightarrow A$ è una bigezione:

$$\psi(n) = \begin{cases} b''_n & \text{se } n \leq m \\ \varphi(n - m) & \text{se } n > m. \end{cases}$$

(Se $B'' = \emptyset$ poniamo $\psi = \varphi$.) $\square$

Con l'assioma di scelta, la proprietà di sopra si estende a tutti gli insiemi infiniti.

PROPOSIZIONE 3.9. (AC) Sia A un insieme infinito e B un insieme finito. Allora $|A \setminus B| = |A \cup B| = |A|$.

DIM. Sia $B' = A \cap B$. Chiaramente B' è finito in quanto sottoinsieme di B ; inoltre $A \setminus B'$ è infinito, altrimenti $A = (A \setminus B') \cup B'$ sarebbe finito perché unione di due insiemi finiti. Per il Teorema 3.6, possiamo prendere un insieme numerabile $A' \subseteq A \setminus B'$. Per la Proposizione precedente, $|A'| = |A' \cup B'| = |A' \cup B|$. Sia ora $C = (A \setminus A') \setminus B' = A \setminus (A' \cup B')$. Visto che $A \setminus B = A \setminus B' = A' \cup C$, $A = (A' \cup B') \cup C$, e $A \cup B = (A' \cup B) \cup C$, e che si tratta di unioni disgiunte, possiamo concludere che $|A \setminus B| = |A| = |A \cup B|$, come volevamo. $\square$

ESERCIZIO 3.10. (AC) Sia X un insieme infinito. Se la differenza simmetrica $X \triangle Y$ è finita, allora $|X| = |Y| = |X \cap Y| = |X \cup Y|$.⁸ (Se l'insieme X è numerabile, la proprietà si dimostra senza usare l'assioma di scelta).

4. Esempi fondamentali di insiemi numerabili

Immaginiamoci un albergo con infinite camere, numerate con i numeri naturali.⁹ Supponiamo che tutte le stanze dell'albergo siano occupate, e che arrivi un nuovo cliente. Per quanto a prima vista possa sembrare impossibile, c'è un modo per risistemare gli ospiti in modo da alloggiare anche il nuovo arrivato; infatti, tutto quello che ci occorre è una bigezione $f : \mathbb{N} \rightarrow \mathbb{N} \setminus \{1\}$. Ad esempio, se chiediamo ad ogni ospite di spostarsi nella camera successiva, cioè se consideriamo la bigezione $f : \mathbb{N} \rightarrow \mathbb{N} \setminus \{1\}$ dove $f : n \mapsto n + 1$, allora si libera la camera 1 dove possiamo sistemare il nuovo cliente. Un simile procedimento si può adottare anche nel caso in cui arrivi un numero finito di nuovi ospiti, perché esistono bigezioni $f : \mathbb{N} \rightarrow \mathbb{N} \setminus \{1, \dots, k\}$ per ogni k (ad esempio, $f : n \mapsto n + k$).

Consideriamo ora la situazione in cui si presentino infiniti nuovi clienti, uno per ogni numero naturale. Ci chiediamo se sia possibile anche in questo caso risistemare i vecchi clienti nelle camere in modo da liberare posti per tutti i nuovi arrivati. La risposta è positiva; ad esempio basta far spostare ogni ospite nella camera il cui numero è il doppio di quella che ha; in questo modo rimangono libere tutte e sole le camere con numero dispari. A questo punto, il nuovo cliente corrispondente al numero n sarà alloggiato nella camera con l' n -esimo numero dispari, cioè nella camera $2n - 1$.

Notiamo che la strategia adottata sopra si basa sull'esistenza di una bigezione tra l'unione di due copie dei numeri naturali, corrispondenti ai vecchi ospiti e ai nuovi clienti, e l'insieme dei numeri naturali, cioè le stanze dell'albergo. Più in generale, vale il seguente risultato.

PROPOSIZIONE 4.1. Se A e B sono numerabili, anche $A \cup B$ è numerabile.

⁸ Ricordiamo la *differenza simmetrica*: $X \triangle Y = (X \setminus Y) \cup (Y \setminus X)$.

⁹ Questo tipo di albergo immaginario è spesso chiamato "albergo di Hilbert", perché fu proprio Hilbert ad introdurlo per illustrare i paradossi dell'equipotenza tra insiemi infiniti.

DIM. Per ipotesi esistono due bigezioni $f : A \rightarrow \mathbb{N}$ e $g : B \rightarrow \mathbb{N}$. Allora si ottiene una funzione iniettiva $h : A \cup B \rightarrow \mathbb{N}$ ponendo:¹⁰

$$h(x) = \begin{cases} 2 \cdot f(x) & \text{se } x \in A \\ 2 \cdot g(x) - 1 & \text{se } x \in B \setminus A \end{cases}$$

Visto che f e g sono funzioni iniettive, dalla definizione segue subito che anche h è una funzione iniettiva. Notiamo inoltre che l'immagine di h è infinita perché include tutti i numeri pari. Se A e B sono disgiunti, l'immagine di h ricopre anche tutti i numeri dispari, e quindi la funzione h è biunivoca. Nel caso generale, abbiamo che $A \cup B$ è equipotente all'immagine di h , che è un sottoinsieme infinito di $\mathbb{N}$. Applicando la Proposizione 3.6, concludiamo che $|A \cup B| = \aleph_0$. $\square$

Come immediata conseguenza, otteniamo che anche l'insieme degli interi è numerabile.

COROLLARIO 4.2. $|\mathbb{Z}| = \aleph_0$.

DIM. Basta osservare che $\mathbb{Z} = \mathbb{Z}_{\leq 0} \cup \mathbb{N}$, dove $\mathbb{Z}_{\leq 0} = \{-n \mid n \in \mathbb{N}\} \cup \{0\}$ è chiaramente numerabile. $\square$

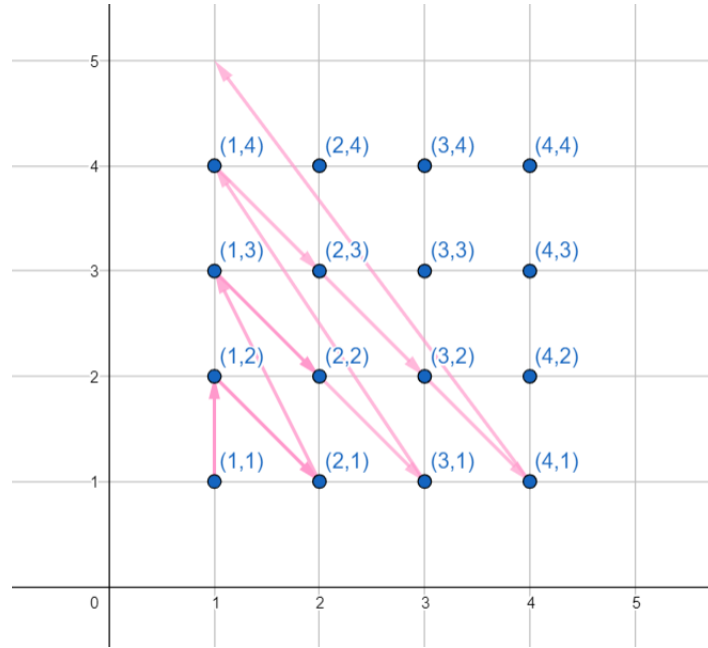
Sviluppando la storiella dell'albergo, supponiamo ora di avere infiniti piani, uno per ogni numero naturale, in ciascuno dei quali ci siano infinite camere, una per ogni numero naturale. Se abbiamo due piani occupati, possiamo risistemare tutti gli ospiti dei due piani nelle camere di un solo piano; basta infatti ragionare come nell'esempio precedente, dove i vecchi ospiti siano quelli di un piano, e i nuovi arrivati quelli dell'altro. Supponiamo ora che tutte le camere di tutti i piani siano occupate. Ci chiediamo se sia possibile sistemare tutti i clienti in un unico piano. Anche in questo caso, per quanto appaia paradossale, la cosa è possibile, perché esistono bigezioni tra il prodotto cartesiano $\mathbb{N} \times \mathbb{N}$ ed $\mathbb{N}$ (possiamo pensare alla coppia ordinata (n, m) come alla camera n posta al piano m).

PROPOSIZIONE 4.3. $|\mathbb{N} \times \mathbb{N}| = \aleph_0$.

Vista la particolare importanza di questo risultato, ne diamo due dimostrazioni diverse.

DIM. 1. L'idea intuitiva di questa dimostrazione è data dalla possibilità di "enumerare" tutte le coppie ordinate $(n, m) \in \mathbb{N} \times \mathbb{N}$ procedendo nel modo diagonale rappresentato in figura:

¹⁰ Notiamo che h è anche suriettiva se e solo se A e B sono disgiunti.



Prendiamo un generica coppia (n, m) , e cerchiamo di stabilire quale posizione occupa nella enumerazione indicata in figura. Si comincia contando la coppia $(1, 1)$; poi si contano le 2 coppie $(1, 2)$ e $(2, 1)$ la cui somma delle coordinate è 3; poi si contano le 3 coppie $(1, 3)$, $(2, 2)$ e $(3, 1)$ la cui somma delle coordinate è 4; poi si contano le 4 coppie $(1, 4)$, $(2, 3)$, $(3, 2)$ e $(4, 1)$ la cui somma delle coordinate è 5; e così via, fino ad arrivare a contare le $m+n-2$ coppie la cui somma delle componenti è $m+n-1$. Restano infine da contare n coppie dove la somma delle componenti è $n+m$, e cioè $(1, m+n)$, $(2, m+n-1)$, $\dots$, (n, m) . Dunque, per arrivare fino alla coppia (n, m) , in tutto abbiamo contato $1 + 2 + 3 + \dots + (n+m-2) + n$ coppie. Il numero della posizione che la coppia (n, m) occupa nella nostra enumerazione è allora il seguente:¹¹

$$f(n, m) = 1 + 2 + 3 + \dots + (n+m-2) + n = \frac{(n+m-2)(n+m-1)}{2} + n.$$

Che la funzione $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ così definita sia biunivoca, è evidente dalla sua definizione. $\square$

Una dimostrazione alternativa si ottiene sfruttando una fondamentale proprietà algebrica dei numeri naturali, e cioè l'esistenza ed unicità della fattorizzazione in numeri primi.

DIM. 2. Ricordiamo che ogni naturale $k \in \mathbb{N}$ si scrive in modo unico nella forma $k = 2^\alpha(2\beta + 1)$ per opportuni interi $\alpha, \beta \geq 0$. Si ha quindi una bigezione

¹¹ Ricordiamo che la somma dei primi k interi positivi è data da:

$$1 + 2 + \dots + k = \frac{k(k+1)}{2}.$$

$f : \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \mathbb{N}$ dove $f(n, m) = 2^n(2m + 1)$.¹² Verifichiamo questo fatto in dettaglio. Per ogni $a \in \mathbb{N}$, sia $g(a) = \alpha$ dove α è il più grande esponente $\alpha \in \mathbb{N} \cup \{0\}$ tale che 2^α divide a (dunque $\alpha = 0$ se e solo se a è dispari). Sia inoltre $h(a) = \frac{1}{2} \cdot \left(\frac{a}{2^{g(a)}} + 1\right)$. Si può verificare direttamente che la funzione $\Psi : \mathbb{N} \rightarrow \mathbb{N}_0 \times \mathbb{N}_0$ dove $\Psi(a) = (g(a), h(a))$ è la funzione inversa di f , che è dunque una bigezione. Infine, visto che $|\mathbb{N}_0| = |\mathbb{N}|$, possiamo concludere che $|\mathbb{N}| = |\mathbb{N}_0 \times \mathbb{N}_0| = |\mathbb{N} \times \mathbb{N}|$. $\square$

Come immediato corollario, ricaviamo anche che tutti i prodotti cartesiani finiti $A_1 \times \dots \times A_k$ di insiemi A_i numerabili, sono numerabili.

Nonostante l'intuizione possa suggerire che ampliando l'insieme ordinato *discreto* dei naturali all'insieme ordinato *denso* dei razionali si ottenga un insieme più "grande", la cardinalità rimane numerabile.

PROPOSIZIONE 4.4. *L'insieme dei numeri razionali $\mathbb{Q}$ è numerabile.*

DIM. Ogni numero razionale $q \in \mathbb{Q}$ si può scrivere in modo unico nella *forma canonica* "ridotta ai minimi termini" $q = \frac{n}{m}$ dove $n \in \mathbb{Z}$ è un intero, $m \in \mathbb{N}$ è un naturale, e il massimo comune divisore $\text{MCD}(n, m) = 1$. La forma canonica determina così una funzione iniettiva $\Psi : \mathbb{Q} \rightarrow \mathbb{Z} \times \mathbb{N}$, e perciò $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N}| = |\mathbb{N} \times \mathbb{N}| = \aleph_0$. Visto che $\mathbb{Q}$ è un insieme infinito e $|\mathbb{Q}| \leq \aleph_0$, segue necessariamente che $|\mathbb{Q}| = \aleph_0$ (cf. Corollario 3.4). $\square$

Più esplicitamente, un possibile modo di enumerare i numeri razionali è il seguente. Iniziamo con il numero 0; poi, per ogni $k \in \mathbb{N}$, elenchiamo tutte le frazioni $\pm \frac{n}{m}$ dove $n, m \in \mathbb{N}$ sono tali che $n + m = k + 1$ (sono esattamente $2k$ frazioni), cancellando poi quelle che non sono ridotte ai minimi termini, in modo da evitare ripetizioni. Dunque $q_1 = 0$; poi per $k = 1$ abbiamo $q_2 = -\frac{1}{1}$, $q_3 = \frac{1}{1}$; per $k = 2$ abbiamo $q_4 = -\frac{2}{1}$, $q_5 = -\frac{1}{2}$, $q_6 = \frac{2}{1}$, $q_7 = \frac{1}{2}$; per $k = 3$ abbiamo $q_8 = -\frac{3}{1}$, $q_9 = -\frac{1}{3}$, $q_{10} = \frac{3}{1}$, $q_{11} = \frac{1}{3}$ (dove abbiamo ommesso le frazioni $-\frac{2}{2}$ e $\frac{2}{2}$ perché non ridotte ai minimi termini); e così via.

ESERCIZIO 4.5. Dimostrare che ogni famiglia di intervalli di numeri reali a due a due disgiunti ha cardinalità al più numerabile.

La numerabilità di $\mathbb{Q}$ permette di dimostrarne la seguente caratterizzazione come insieme ordinato denso.

TEOREMA 4.6 (Cantor). *Sia $(X, <)$ un insieme totalmente ordinato denso senza massimo né minimo. Se $|X| = \aleph_0$ allora $(X, <)$ è isomorfo a $(\mathbb{Q}, <)$.*

DIM. Fissiamo un'enumerazione $(x_n \mid n \in \mathbb{N})$ degli elementi di X , ed un'enumerazione $(q_n \mid n \in \mathbb{N})$ degli elementi di $\mathbb{Q}$. Notiamo che tali enumerazioni non necessariamente rispettano l'ordine, cioè non possiamo aspettarci che $x_n < x_m$ (o $q_n < q_m$) quando $n < m$.

Per definire un isomorfismo di ordini $\psi : X \rightarrow \mathbb{Q}$, poniamo intanto $\psi(x_1) = q_1$. Se $x_2 < x_1$, definiamo $\psi(x_2) = q_k$ dove k è il più piccolo indice tale che $q_k < q_1$; e se $x_2 > x_1$, definiamo $\psi(x_2) = q_k$ dove k è il più piccolo indice tale che $q_k > q_1$. Prendiamo ora q_2 . Se $q_2 = \psi(x_2)$, non facciamo niente. Altrimenti, se $q_2 < q_1, q_k$ poniamo $\psi(x_h) = q_2$ dove h è il più piccolo indice tale che $x_h < x_1, x_2$, e se $q_2 > q_1, q_k$, definiamo $\psi(x_h) = q_2$ dove h è il più piccolo indice tale che $x_h > x_1$.

¹² Ricordiamo che $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ denota l'insieme degli interi non negativi.

Infine se q_2 è compreso tra q_1 e q_k (cioè se $q_1 < q_2 < q_k$ oppure $q_k < q_2 < q_1$), allora poniamo $\psi(x_h) = q_2$, dove h è il più piccolo indice tale che x_h è compreso tra x_1 e x_2 . L'idea è proseguire in questo modo.

Per formalizzare e rendere rigorosa la costruzione accennata sopra, procediamo per ricorsione su $n \in \mathbb{N}$, definendo isomorfismi d'ordine parziali $\psi_n : X_n \rightarrow Q_n$ tra sottoinsiemi finiti $X_n \subset X$ e $Q_n \subset \mathbb{Q}$ in modo che:

- ψ_{n+1} è un'estensione di ψ_n ;
- $x_1, \dots, x_n \in X_n$ e $q_1, \dots, q_n \in Q_n$.

Per la base $n = 1$, poniamo $X_1 = \{x_1\}$, $Q_1 = \{q_1\}$, e $\psi_1 : x_1 \mapsto q_1$. Definiamo ora ψ_{n+1} a partire da ψ_n . Lo faremo in due passi, con un procedimento che viene spesso chiamato *back and forth* ("avanti e indietro"). Precisamente, definiremo prima un'estensione intermedia $\vartheta_n : X'_n \rightarrow Q'_n$ di ψ_n dove $x_{n+1} \in X'_n$; e poi l'estensione $\psi_{n+1} : X_{n+1} \rightarrow Q_{n+1}$ di ϑ_n dove $q_{n+1} \in Q_{n+1}$. In questo modo avremo che $x_1, \dots, x_n, x_{n+1} \in X_{n+1}$ e $q_1, \dots, q_n, q_{n+1} \in Q_{n+1}$, come voluto.

Poniamo intanto $\vartheta_n(x) = \psi_n(x)$ per ogni $x \in X_n$, in modo che ϑ_n risulti un'estensione di ψ_n . Se $x_{n+1} \in X_n$ non facciamo niente, perché abbiamo già definito $\vartheta_n(x_{n+1}) = \psi_n(x_{n+1})$. Se $x_{n+1} < \min X_n$, definiamo $\vartheta_n(x_{n+1}) = q_k$ dove $k = \min\{n \mid q_n < \min Q_n\}$; e analogamente, se $x_{n+1} > \max X_n$, definiamo $\vartheta_n(x_{n+1}) = q_k$ dove $k = \min\{n \mid q_n > \max Q_n\}$. Infine, se $y < x_{n+1} < y'$ dove $y < y'$ sono due elementi consecutivi di X_n , definiamo $\vartheta_n(x_{n+1}) = q_k$ dove $k = \min\{n \mid \psi_n(y) < q_n < \psi_n(y')\}$. In questo modo, abbiamo esteso ψ_n ad un isomorfismo d'ordine parziale $\vartheta_n : X'_n \rightarrow Q'_n$ dove $X'_n = X_n \cup \{x_{n+1}\}$ e $Q'_n = Q_n \cup \{\vartheta_n(x_{n+1})\}$.

Per definire l'estensione ψ_{n+1} di ϑ_n procediamo in modo simile a sopra. Poniamo intanto $\psi_{n+1}(x) = \vartheta_n(x)$ per ogni $x \in X'_n$, in modo che ψ_{n+1} risulti un'estensione di ϑ_n , e quindi di ψ_n . Se $q_{n+1} \in Q'_n$ non facciamo niente, perché esiste già un elemento $x \in X'_n$ tale che $\psi_{n+1}(x) = \vartheta_n(x) = q_{n+1}$. Se $q_{n+1} < \min Q'_n$, allora poniamo $\psi_{n+1}(x_k) = q_{n+1}$ dove $k = \min\{n \mid x_n < \min X'_n\}$; e analogamente se $q_{n+1} > \max Q'_n$, poniamo $\psi_{n+1}(x_k) = q_{n+1}$ dove $k = \min\{n \mid x_n > \max X'_n\}$. Se invece $r < q_{n+1} < r'$ dove $r < r'$ sono due elementi consecutivi di Q'_{n+1} , prendiamo gli elementi consecutivi $y < y'$ in X'_n tali che $r = \vartheta_n(y)$ e $r' = \vartheta_n(y')$; poi prendiamo $k = \min\{n \mid y < x_n < y'\}$, e definiamo $\psi_{n+1}(x_k) = q_{n+1}$. In questo modo, abbiamo esteso ϑ_n , e quindi ψ_n , ad un isomorfismo d'ordine $\psi_{n+1} : X_{n+1} \rightarrow Q_{n+1}$ dove $X_{n+1} = X_n \cup \{x_{n+1}, \psi_{n+1}^{-1}(q_{n+1})\}$ e $Q_{n+1} = Q_n \cup \{\vartheta_n(x_{n+1}), q_{n+1}\}$. È immediato verificare dalle definizioni che l'unione $\psi = \bigcup_n \psi_n$ è un isomorfismo d'ordine tra $X = \bigcup_n X_n$ e $\mathbb{Q} = \bigcup_n Q_n$.

Come osservazione finale, notiamo come l'ipotesi che i due insiemi ordinati $\mathbb{Q}$ ed X siano densi senza massimo né minimo sia necessaria affinché tutte le definizioni date risultino ben poste. $\square$

Col prossimo risultato mostriamo che un'unione al più numerabile di insiemi al più numerabili è al più numerabile.

TEOREMA 4.7. (AC)

Sia $(A_i \mid i \in I)$ una sequenza di insiemi dove $|I| \leq \aleph_0$ e $|A_i| \leq \aleph_0$ per ogni $i \in I$. Allora anche l'unione $|\bigcup_{i \in I} A_i| \leq \aleph_0$.

DIM. Per ogni $i \in I$, l'insieme $\mathcal{F}_i = \{\psi \mid \psi : \mathbb{N} \rightarrow A_i \text{ suriettiva}\}$ è non vuoto e quindi, grazie all'assioma di scelta, esiste una I -sequenza $(\psi_i \mid i \in I) \in \prod_{i \in I} \mathcal{F}_i$.

Fissiamo inoltre una funzione suriettiva $\varphi : \mathbb{N} \rightarrow I$. Definiamo infine la funzione $F : \mathbb{N} \times \mathbb{N} \rightarrow \bigcup_{i \in I} A_i$ ponendo $F(n, m) = \psi_{\varphi(n)}(m)$. Se $a \in \bigcup_{i \in I} A_i$, allora $a \in A_j$ per un opportuno j , e possiamo prendere $n \in \mathbb{N}$ tale che $\varphi(n) = j$, e $m \in \mathbb{N}$ tale che $\psi_j(m) = a$. Si verifica facilmente che $F(n, m) = a$. Questo dimostra la suriettività di F , e dunque $|\bigcup_{i \in I} A_i| \leq |\mathbb{N} \times \mathbb{N}| = \aleph_0$. $\square$

Attenzione. Nel caso in cui possa essere definita esplicitamente una sequenza $(\psi_i \mid i \in I)$ di funzioni suriettive $\psi_i : \mathbb{N} \rightarrow A_i$, allora il risultato precedente si dimostra senza usare l'assioma di scelta.

ESERCIZIO 4.8. (AC) Sia $(A_i \mid i \in I)$ una sequenza di insiemi dove $|I| \leq \aleph_0$ e $|A_i| \leq \aleph_0$ per ogni $i \in I$.

- (1) Se esiste un insieme A_j infinito allora l'unione $|\bigcup_{i \in I} A_i| = \aleph_0$.
- (2) Se gli insiemi $A_i \neq \emptyset$ sono a due a due disgiunti e I è infinito allora l'unione $|\bigcup_{i \in I} A_i| = \aleph_0$.

NOTAZIONE 4.9. Dato un insieme non vuoto X , denotiamo con:

- $\text{Fin}(X) = \{A \subseteq X \mid A \text{ finito}\}$ l'insieme dei *sottoinsiemi finiti* di X .
- $\text{FSeq}(X) = \bigcup_{n \in \mathbb{N}} \text{Fun}(\{1, \dots, n\}, X) = \{\sigma \mid \exists n \in \mathbb{N} \ \sigma : \{1, \dots, n\} \rightarrow X\}$ l'insieme delle *sequenze finite* di elementi di X .

Si usa spesso la scrittura $(a_i \mid i = 1, \dots, n)$, o anche direttamente $(a_1, a_2, \dots, a_n)$, per denotare la sequenza finita σ dove $\sigma(i) = a_i$ per $i = 1, 2, \dots, n$.¹³

Per convenzione, si impone che anche la *sequenza vuota* $(\cdot)$, cioè l'insieme vuoto, appartenga a $\text{FSeq}(X)$.

ESERCIZIO 4.10. Supponiamo che $|X| = |Y|$. Allora $|\text{Fin}(X)| = |\text{Fin}(Y)|$ e $|\text{FSeq}(X)| = |\text{FSeq}(Y)|$. Lo stesso risultato vale se rimpiazziamo la relazione di equipotenza con la relazione di minore o uguale tra cardinalità.

Denotiamo con $\text{FSeq}^\uparrow(\mathbb{N}) = \{\sigma \in \text{FSeq}(\mathbb{N}) \mid i < j \Rightarrow \sigma(i) < \sigma(j)\}$ l'insieme delle *sequenze finite crescenti* di numeri naturali.

PROPOSIZIONE 4.11. $|\text{FSeq}^\uparrow(\mathbb{N})| = |\text{FSeq}(\mathbb{N})| = |\text{Fin}(\mathbb{N})| = \aleph_0$.

DIM. La funzione iniettiva $f : \mathbb{N} \rightarrow \text{Fin}(\mathbb{N})$ dove $f(n) = \{n\}$ è chiaramente iniettiva, dunque $\aleph_0 \leq |\text{Fin}(\mathbb{N})|$. Dato $A \in \text{Fin}(\mathbb{N})$, disponiamo i suoi elementi in ordine crescente $A = \{a_1 < a_2 < \dots < a_n\}$, e definiamo $g(A) = (a_1, a_2, \dots, a_n) \in \text{FSeq}(\mathbb{N})^\uparrow$. La funzione g è iniettiva, e quindi $|\text{Fin}(\mathbb{N})| \leq |\text{FSeq}^\uparrow(\mathbb{N})|$. Dall'inclusione $\text{FSeq}^\uparrow(\mathbb{N}) \subseteq \text{FSeq}(\mathbb{N})$ segue poi banalmente che $|\text{FSeq}^\uparrow(\mathbb{N})| \leq |\text{FSeq}(\mathbb{N})|$. Per concludere, resta allora da dimostrare che $|\text{FSeq}(\mathbb{N})| \leq \aleph_0$.

A questo scopo, consideriamo $(p_n \mid n \in \mathbb{N})$, la successione crescente dei numeri primi: $p_1 = 2, p_2 = 3, p_3 = 5, \text{ etc.}$ Per ogni sequenza finita $(a_1, a_2, \dots, a_n)$ di numeri naturali, poniamo:

$$\vartheta(a_1, a_2, \dots, a_n) = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}.$$

¹³ Attenzione, questa notazione può essere ambigua. Ad esempio (a_1, a_2) può denotare la sequenza σ con dominio $\{1, 2\}$ e dove $\sigma(1) = a_1$ e $\sigma(2) = a_2$, ma può anche denotare la coppia ordinata di Kuratowski $\{\{a_1\}, \{a_1, a_2\}\}$. Quale dei due possibili significati intenderemo sarà sempre chiaro dal contesto.

Nel caso della sequenza vuota, poniamo $\vartheta(\cdot) = 1$. L'unicità della scomposizione in fattori primi garantisce l'iniettività di ϑ , e dunque $|\text{FSeq}(\mathbb{N})| \leq |\mathbb{N}|$, come volevamo.

Una dimostrazione alternativa della disuguaglianza $|\text{FSeq}(\mathbb{N})| \leq \aleph_0$ è la seguente. Se ad ogni sequenza finita (non vuota) $\langle a_1, \dots, a_k \rangle$ facciamo corrispondere la k -upla ordinata $(a_1, \dots, a_k) \in \mathbb{N}^k$, si ottiene una bigezione tra $\text{FSeq}(\mathbb{N})$ (senza la sequenza vuota) e $\bigcup_{k \in \mathbb{N}} \mathbb{N}^k$. Basta allora notare che quest'ultimo insieme è numerabile perché unione numerabile di insiemi numerabili. $\square$

Vedremo più avanti che, usando l'assioma di scelta, si può dimostrare che $|\text{FSeq}(X)| = |\text{Fin}(X)| = |X|$ per ogni insieme infinito X .

ESERCIZIO 4.12. Sia X un insieme tale che $\aleph_0 \leq |X| = |X \times X|$. Senza mai utilizzare l'*assioma di scelta*, dimostrare che $|\text{FSeq}(X)| = |X|$.

PROPOSIZIONE 4.13. L'insieme $\mathbb{Z}[X]$ dei polinomi a coefficienti interi è numerabile.

DIM. Ad ogni polinomio $P(X) = a_0 + a_1X + \dots + a_nX^n$ a coefficienti interi, si può associare la sequenza finita $(a_0, a_1, \dots, a_n)$. Questa corrispondenza determina una funzione iniettiva $f : \mathbb{Z}[X] \rightarrow \text{FSeq}(\mathbb{Z})$, dunque $|\mathbb{Z}[X]| \leq |\text{FSeq}(\mathbb{Z})| = |\text{FSeq}(\mathbb{N})| = \aleph_0$. Banalmente $\mathbb{Z}[X]$ è infinito, e quindi $|\mathbb{Z}[X]| = \aleph_0$. $\square$

Il prossimo risultato è un famoso teorema dimostrato da Cantor. Fu una delle prime importanti applicazioni della sua teoria delle cardinalità.

TEOREMA 4.14. *L'insieme dei numeri reali algebrici è numerabile.*¹⁴

DIM. È un risultato noto dell'algebra che ogni polinomio non nullo $P(X) \in \mathbb{Z}[X]$ di grado n ha al più n radici reali; dunque $\text{Root}(P(X)) = \{r \in \mathbb{R} \mid P(r) = 0\}$ è finito. Notiamo che l'insieme $\mathcal{A}$ dei numeri reali algebrici si ottiene come la seguente unione

$$\mathcal{A} = \bigcup_{P(X) \in \mathbb{Z}[X] \setminus \{0\}} \text{Root}(P(X)).$$

Visto che $|\mathbb{Z}[X] \setminus \{0\}| = |\mathbb{Z}[X]| = \aleph_0$, l'insieme $\mathcal{A}$ è al più numerabile perché è unione numerabile di insiemi finiti. Inoltre $\mathcal{A}$ è infinito perché banalmente $\mathbb{Z} \subseteq \mathcal{A}$, e dunque otteniamo la tesi.

Infine osserviamo che l'assioma di scelta non è necessario in questo caso, perché è possibile definire in modo canonico una funzione suriettiva $f_{P(X)} : \mathbb{N} \rightarrow \text{Root}(P(X))$ per ogni $P(X) \in \mathbb{Z}[X]$ che ammette radici reali.¹⁵

$\square$

Come vedremo nel prossimo paragrafo, i numeri reali *non* sono numerabili, e dunque, come conseguenza diretta del teorema di sopra, si ottiene l'esistenza di una infinità più che numerabile di numeri trascendenti.

¹⁴ Ricordiamo che un numero $r \in \mathbb{R}$ si dice *algebrico* se esiste un polinomio non nullo a coefficienti interi $P(X) \in \mathbb{Z}[X]$ tale che $P(r) = 0$, e si dice *trascendente* se non è algebrico.

¹⁵ Basta ordinare esplicitamente gli elementi di $\text{Root}(P(X)) = \{r_1 < \dots < r_n\}$ e poi porre $f_{P(X)}(k) = r_k$ per $k \leq n$ e $f_{P(X)}(k) = r_1$ per $k > n$.

5. Cardinalità del continuo

Il fatto che i numeri reali non sono numerabili può essere dimostrato direttamente a partire da proprietà di ordine.

TEOREMA 5.1. $|\mathbb{R}| \neq \aleph_0$.

DIM. Supponiamo per assurdo che i numeri reali siano numerabili. Visto che l'insieme ordinato $(\mathbb{R}, <)$ è denso senza massimo né minimo, allora per il teorema di Cantor si avrebbe che $(\mathbb{R}, <) \cong (\mathbb{Q}, <)$. Questo assurdo perché il primo è un ordine *completo*, mentre i razionali non lo sono.¹⁶ $\square$

Un modo alternativo, più preciso, di dimostrare che i numeri reali non sono numerabili, è mostrare che sono equipotenti alle parti dei numeri naturali.

TEOREMA 5.2. $|\mathbb{R}| = |2^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})|$.

DIM. Per ogni successione $(a_n \mid n \in \mathbb{N}) \in 2^{\mathbb{N}}$ a valori in $\{0, 1\}$, poniamo

$$\varphi((a_n \mid n \in \mathbb{N})) = \sum_{n=1}^{\infty} \frac{a_n}{10^n}.$$

Visto che la successione $S_N = \sum_{n=1}^N a_n/10^n$ è crescente e limitata, per la *completezza* di $\mathbb{R}$ esiste il limite $\lim_{N \rightarrow \infty} S_N = \sum_{n=1}^{\infty} a_n/10^n$, e dunque la nostra definizione è ben posta.¹⁷

Dimostriamo ora che la funzione $\varphi : 2^{\mathbb{N}} \rightarrow \mathbb{R}$ così definita è iniettiva, e dunque $|2^{\mathbb{N}}| \leq |\mathbb{R}|$. Se $(a_n \mid n \in \mathbb{N}) \neq (b_n \mid n \in \mathbb{N})$, prendiamo $k = \min\{n \mid a_n \neq b_n\}$, e denotiamo con $r = \sum_{n < k} a_n/10^n = \sum_{n < k} b_n/10^n$; se $k = 1$, conveniamo che $r = 0$. Supponiamo che $a_k = 1$ e $b_k = 0$ (se invece $a_k = 0$ e $b_k = 1$ la dimostrazione è del tutto analoga). Valgono le disuguaglianze

$$\begin{aligned} \varphi((a_n \mid n \in \mathbb{N})) - r &= \sum_{n=k}^{\infty} \frac{a_n}{10^n} \geq \frac{1}{10^k} > \\ &> \sum_{n=k+1}^{\infty} \frac{1}{10^n} \geq \sum_{n=k+1}^{\infty} \frac{b_n}{10^n} = \varphi((b_n \mid n \in \mathbb{N})) - r. \end{aligned}$$

Sia ora $\psi : \mathbb{R} \rightarrow \mathcal{P}(\mathbb{Q})$ la funzione definita ponendo $\psi(r) = \{q \in \mathbb{Q} \mid q < r\}$. Dalla *densità* di $\mathbb{Q}$ in $\mathbb{R}$ segue che ψ è iniettiva. Infatti se $r < r'$, prendendo un numero razionale q con $r < q < r'$, si ha che $q \in \psi(r')$ ma $q \notin \psi(r)$, e quindi $\psi(r) \neq \psi(r')$. Concludiamo che $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})| = |\mathcal{P}(\mathbb{N})| = |2^{\mathbb{N}}| \leq |\mathbb{R}|$, e la tesi si ottiene applicando il Teorema di Cantor-Bernstein. $\square$

Notiamo che $|\mathbb{N}| < |2^{\mathbb{N}}|$, visto che il teorema di Cantor garantisce $|\mathbb{N}| \neq |2^{\mathbb{N}}|$. Dunque, nel senso preciso dato dalla nozione di cardinalità, possiamo affermare che i numeri reali sono “più numerosi” dei numeri naturali.

DEFINIZIONE 5.3. Un insieme A ha la *cardinalità del continuo* se $|A| = |\mathbb{R}|$. In questo caso si usa la notazione $|A| = \mathfrak{c}$.

¹⁶ Ad esempio, l'insieme $A = \{q \in \mathbb{Q} \mid q^2 < 2\}$ è limitato superiormente ma non ha estremo superiore.

¹⁷ Si osservi che $\varphi(\sigma)$ è il numero reale la cui scrittura decimale è $0, \sigma(1)\sigma(2)\sigma(3)\sigma(4)\dots$

Visto il teorema precedente, si scrive che $\mathfrak{c} = 2^{\aleph_0}$.

ESERCIZIO 5.4. Per ogni coppia di numeri reali $a < b$, definire esplicitamente due bigezioni $\varphi_{a,b} : [a, b] \rightarrow \mathbb{R}$ e $\psi_{a,b} : [a, b] \rightarrow (a, b)$, senza usare il Teorema di Cantor-Bernstein.

ESERCIZIO 5.5. Dimostrare che per ogni coppia di numeri reali $a < b$, i seguenti intervalli hanno tutti la cardinalità $\mathfrak{c}$ del continuo:

$$(-\infty, b), (-\infty, b], (a, b), [a, b), (a, b], [a, b], (b, +\infty), [b, +\infty).$$

È naturale chiedersi se esistano cardinalità intermedie comprese tra $\aleph_0$ e $\mathfrak{c}$. L'ipotesi che questo non accada è nota come

- **Ipotesi del continuo.** Se $A \subseteq \mathbb{R}$ è un sottoinsieme infinito di reali, allora $|A| = |\mathbb{N}|$ oppure $|A| = |\mathbb{R}|$.

L'ipotesi del continuo è probabilmente l'esempio più famoso di proprietà *indecidibile*, cioè di una proprietà che non può essere nè dimostrata nè confutata a partire dai principi matematici comunemente accettati.¹⁸

Analogamente a quanto già visto per l'insieme $\mathbb{N}$ dei numeri naturali, il prodotto cartesiano $\mathbb{R} \times \mathbb{R}$ è equipotente ad $\mathbb{R}$.

PROPOSIZIONE 5.6. $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$.

Diamo due diverse dimostrazioni di questo risultato, entrambe molto brevi.

DIM. 1. Siano D l'insieme dei numeri naturali dispari e P l'insieme dei numeri naturali pari. Visto che $|D| = |P| = |\mathbb{N}|$, dal Teorema 5.2 segue che $|\mathbb{R}| = |2^{\mathbb{N}}| = |2^D| = |2^P|$, da cui $|\mathbb{R} \times \mathbb{R}| = |2^D \times 2^P| = |2^{D \cup P}| = |2^{\mathbb{N}}| = |\mathbb{R}|$. $\square$

DIM. 2. La funzione $f : \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$ dove $f : r \mapsto (r, 0)$ è iniettiva, e quindi $|\mathbb{R}| \leq |\mathbb{R} \times \mathbb{R}|$. Osserviamo inoltre che la funzione $g : \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N} \times \mathbb{N})$ dove $g : (A, B) \mapsto A \times B$ è iniettiva, e quindi si ottiene l'altra disuguaglianza $|\mathbb{R} \times \mathbb{R}| = |\mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N})| \leq |\mathcal{P}(\mathbb{N} \times \mathbb{N})| = |\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$. La tesi segue applicando il Teorema di Cantor-Bernstein. $\square$

ESERCIZIO 5.7. (AC)

Sia $(A_i \mid i \in I)$ una sequenza di insiemi dove $|I| \leq \mathfrak{c}$ e $|A_i| \leq \mathfrak{c}$ per ogni $i \in I$. Allora anche l'unione $|\bigcup_{i \in I} A_i| \leq \mathfrak{c}$.

ESERCIZIO 5.8. (AC) Sia $(A_i \mid i \in I)$ una sequenza di insiemi dove $|I| \leq \mathfrak{c}$ e $|A_i| \leq \mathfrak{c}$ per ogni $i \in I$.

- (1) Se esiste $j \in I$ con $|A_j| = \mathfrak{c}$ allora l'unione $|\bigcup_{i \in I} A_i| = \mathfrak{c}$.
- (2) Se gli insiemi $A_i \neq \emptyset$ sono a due a due disgiunti e $|I| = \mathfrak{c}$ allora l'unione $|\bigcup_{i \in I} A_i| = \mathfrak{c}$.

¹⁸ A breve, cominceremo a dare un senso preciso alle espressioni usate qua sopra. Ad esempio, per “principi matematici comunemente accettati”, intenderemo le proprietà formalizzate dagli assiomi della teoria degli insiemi ZFC di Zermelo-Fraenkel con scelta. Anche i concetti di “dimostrabilità” e “confutabilità” possono essere resi precisi. E tali concetti sono in effetti quelli fondamentali di cui si occupa la logica matematica.

Elenchiamo nei prossimi esercizi alcuni tra i più importanti insiemi aventi la cardinalità del continuo.

ESERCIZIO 5.9. Dimostrare che i seguenti insiemi hanno tutti la cardinalità del continuo:

- (1) Le parti finite dei reali $\text{Fin}(\mathbb{R})$.
- (2) Le sequenze finite di reali $\text{FSeq}(\mathbb{R})$.
- (3) Le sequenze finite crescenti di reali $\text{FSeq}^\uparrow(\mathbb{R})$.
- (4) Le successioni di numeri naturali $\mathbb{N}^\mathbb{N} = \text{Fun}(\mathbb{N}, \mathbb{N})$.
- (5) Le successioni crescenti di numeri naturali.
- (6) L'insieme $[\mathbb{N}]^{\aleph_0} = \{A \subseteq \mathbb{N} \mid |A| = \aleph_0\}$ dei sottoinsiemi infiniti di $\mathbb{N}$.
- (7) Le bigezioni dei numeri naturali $\mathfrak{S}(\mathbb{N}) = \{f \in \mathbb{N}^\mathbb{N} \mid f \text{ bigezione}\}$.
- (8) Le successioni di numeri reali $\mathbb{R}^\mathbb{N} = \text{Fun}(\mathbb{N}, \mathbb{R})$.
- (9) Le successioni crescenti di numeri reali.
- (10) (AC) Le parti numerabili dei reali $[\mathbb{R}]^{\aleph_0} = \{A \subseteq \mathbb{R} \mid |A| = \aleph_0\}$.
- (11) (AC) Le parti al più numerabili dei reali $[\mathbb{R}]^{\leq \aleph_0} = \{A \subseteq \mathbb{R} \mid |A| \leq \aleph_0\}$.

ESERCIZIO 5.10. Sia $\mathcal{C}^0(\mathbb{R})$ l'insieme di tutte le funzioni continue $f : \mathbb{R} \rightarrow \mathbb{R}$. Allora $|\mathcal{C}^0(\mathbb{R})| = \mathfrak{c}$.

ESERCIZIO 5.11. Sia $\mathcal{O}(\mathbb{R}^k)$ l'insieme di tutti i sottoinsiemi aperti di $\mathbb{R}^k$.¹⁹ Allora $|\mathcal{O}(\mathbb{R}^k)| = \mathfrak{c}$.

SOLUZIONE. Per semplicità, consideriamo solo il caso $k = 2$ del piano euclideo $\mathbb{R} \times \mathbb{R}$ (il caso generale è del tutto simile). Una base di aperti della topologia è costituito dalle palle

$$B((q_1, q_2), r) = \{(x_1, x_2) \in \mathbb{R} \times \mathbb{R} \mid d((x_1, x_2), (q_1, q_2)) < r\}$$

dove il centro (q_1, q_2) ha coordinate razionali, e il raggio $r > 0$ è razionale. Consideriamo ora la funzione $\Psi : \mathcal{O}(\mathbb{R} \times \mathbb{R}) \rightarrow \mathcal{P}(\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}^+)$ dove per ogni aperto A di $\mathbb{R} \times \mathbb{R}$,

$$\Psi(A) = \{(q_1, q_2, r) \in \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}^+ \mid B((q_1, q_2), r) \subseteq A\}.$$

Per dimostrare che Ψ è iniettiva, fissiamo due aperti distinti $A \neq A'$. Prendiamo un punto (x_1, x_2) che ne testimonia la differenza, ad esempio $(x_1, x_2) \in A$ ma $(x_1, x_2) \notin A'$. Per la proprietà di insieme aperto, esiste una palla $B((q_1, q_2), r)$ con centro (q_1, q_2) di coordinate razionali e raggio $r > 0$ razionale, tale che $(x_1, x_2) \in B((q_1, q_2), r) \subseteq A$. In particolare $B((q_1, q_2), r) \not\subseteq A'$, dunque $(q_1, q_2, r) \in \Psi(A)$ ma $(q_1, q_2, r) \notin \Psi(A')$, e perciò $\Psi(A) \neq \Psi(A')$. Concludiamo che

$$|\mathcal{O}(\mathbb{R} \times \mathbb{R})| \leq |\mathcal{P}(\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}^+)| = |\mathcal{P}(\mathbb{N} \times \mathbb{N} \times \mathbb{N})| = |\mathcal{P}(\mathbb{N})| = \mathfrak{c}.$$

L'altra disuguaglianza $\mathfrak{c} \leq |\mathcal{O}(\mathbb{R} \times \mathbb{R})|$ è immediata. $\square$

Togliendo un sottoinsieme numerabile da un insieme che ha la cardinalità del continuo, ciò che rimane ha ancora la cardinalità del continuo. Assumendo l'assioma di scelta, lo stesso risultato vale anche se togliamo un qualunque insieme purché di cardinalità minore del continuo.

PROPOSIZIONE 5.12.

¹⁹ La $\mathcal{O}$ sta per "open".

- (1) Sia $A \subset B$ dove $|A| \leq \aleph_0$ e $|B| = \mathfrak{c}$. Allora $|B \setminus A| = \mathfrak{c}$.
 (2) (AC) Sia $A \subset B$ dove $|A| < \mathfrak{c}$ e $|B| = \mathfrak{c}$. Allora $|B \setminus A| = \mathfrak{c}$.

Osserviamo che, assumendo l'*ipotesi del continuo*, il contenuto delle due proprietà di sopra è identico; altrimenti, assumendo che l'*ipotesi del continuo* non valga, la proprietà (2) è chiaramente più generale (ma la sua dimostrazione richiede l'assioma di scelta).

DIM. Per comodità, supponiamo prima che $B = \mathbb{R} \times \mathbb{R}$. In questo caso $A \subset B$ è una relazione binaria (un insieme di coppie ordinate); consideriamo allora il dominio $A' = \text{dom}(A) = \{x \in \mathbb{R} \mid \exists y \in \mathbb{R} (x, y) \in A\}$. Abbiamo già visto, senza uso dell'assioma di scelta, che se $|A| \leq \aleph_0$, allora anche $|A'| \leq \aleph_0$ (vedi Esercizio 3.7). Se invece $|A| < \mathfrak{c}$, questa volta usando l'assioma di scelta, possiamo concludere che $|A'| \leq |A| < \mathfrak{c}$. In entrambi i casi, segue necessariamente che $A' \neq \mathbb{R}$, e quindi possiamo prendere un elemento $a \in \mathbb{R} \setminus A'$. Notiamo che $\{a\} \times \mathbb{R} \subseteq (\mathbb{R} \times \mathbb{R}) \setminus A$, dunque $|(\mathbb{R} \times \mathbb{R}) \setminus A| \geq \mathfrak{c}$.

Supponiamo ora che B sia un qualunque insieme avente la cardinalità del continuo. Fissiamo una bigezione $\Psi : B \rightarrow \mathbb{R} \times \mathbb{R}$. Visto che $|\Psi(A)| = |A|$, possiamo applicare quanto già dimostrato sopra al sottoinsieme $\Psi(A) \subset \mathbb{R} \times \mathbb{R}$ al posto di A . Otteniamo così $\mathfrak{c} = |(\mathbb{R} \times \mathbb{R}) \setminus \Psi(A)| = |\Psi(B \setminus A)| = |B \setminus A|$. $\square$

Come immediato corollario, si ottengono i seguenti risultati, che non richiedono l'assioma di scelta.

PROPOSIZIONE 5.13.

- (1) L'insieme dei numeri irrazionali ha la cardinalità del continuo.
 (2) L'insieme dei numeri trascendenti ha la cardinalità del continuo.

DIM. Basta notare che gli irrazionali sono la differenza $\mathbb{R} \setminus \mathbb{Q}$, che i numeri trascendenti sono la differenza $\mathbb{R} \setminus \mathcal{A}$ dove $\mathcal{A}$ è l'insieme dei numeri algebrici, e ricordare che $|\mathbb{Q}| = |\mathcal{A}| = \aleph_0$. $\square$

ESERCIZIO 5.14. (AC) Sia $A \subset B$ dove $|A| < |B|$. Se $|B \times B| = |B|$, allora $|B \setminus A| = |B|$.²⁰

Facciamo ora un ulteriore passo in avanti con le cardinalità, e denotiamo

$$\bullet \quad 2^{\mathfrak{c}} = |2^{\mathbb{R}}| = |\mathcal{P}(\mathbb{R})|.$$

Chiaramente $2^{\mathfrak{c}} > \mathfrak{c}$ per il Teorema di Cantor.

A partire dall'equipotenza $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, si può dimostrare che $|\mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N})| = |\mathcal{P}(\mathbb{N})|$, e quindi che $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$; in modo analogo, a partire dall'equipotenza $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$, si può dimostrare che $|\mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R})| = |\mathcal{P}(\mathbb{R})|$.

ESERCIZIO 5.15. Senza usare l'assioma di scelta, dimostrare che $|\mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R})| = 2^{\mathfrak{c}}$.

ESERCIZIO 5.16. Senza usare l'assioma di scelta, dimostrare che $|\mathbb{N}^{\mathbb{R}}| = |\mathbb{R}^{\mathbb{R}}| = |\mathcal{P}(\mathbb{R})^{\mathbb{R}}| = 2^{\mathfrak{c}}$.

²⁰ Vedremo più avanti che l'ipotesi $|B \times B| = |B|$ non è necessaria. Infatti dimostreremo che $|B \times B| = |B|$ per ogni insieme infinito (di più, dimostreremo che tale proprietà è equivalente all'*assioma di scelta*).

ESERCIZIO 5.17. Senza usare l'assioma di scelta, dimostrare che se $A \subseteq B$ dove $|A| \leq \mathfrak{c}$ e $|B| = 2^{\mathfrak{c}}$, allora $|B \setminus A| = 2^{\mathfrak{c}}$.

Chiudiamo menzionando un'altra proprietà *indecidibile*. Provare a dimostrarla può essere istruttivo, basta non illudersi di riuscirci!

- Se $|\mathcal{P}(A)| = |\mathcal{P}(B)|$ allora $|A| = |B|$.

La teoria di Zermelo-Fraenkel

A partire da questo capitolo, cambieremo la nostra impostazione che, come hanno mostrato la collezione di Russell $R = \{x \mid x \notin x\}$ e la collezione universale $V = \{x \mid x = x\}$, si è rivelata contraddittoria. Procederemo in modo più attento e rigoroso seguendo il moderno metodo *assiomatico*, ed introdurremo, a partire dagli assiomi dati, tutti i fondamentali oggetti e principi della matematica, tra cui i numeri naturali e l'induzione. Precisamente, presenteremo e svilupperemo la teoria degli insiemi ZFC di Zermelo-Fraenkel, che è ad oggi quella più largamente adottata come fondamento della matematica.¹ Tutte le varie nozioni insiemistiche – anche le più elementari – saranno definite in dettaglio, a partire da quelle già viste informalmente nelle lezioni precedenti. Come è caratteristica del metodo assiomatico, le uniche proprietà che potremo assumere saranno quelle espresse dagli assiomi ZFC. È onesto ammettere però che, nel definire la teoria, verranno implicitamente assunti alcuni principi fondamentali, che costituiscono la nostra “metateoria”. Ad esempio, nella definizione di formula, il concetto di “stringa finita” e una qualche nozione intuitiva di numero naturale e di induzione, sono dati come noti.

1. Formule del linguaggio degli insiemi

Come abbiamo già anticipato nel primo capitolo, tutte le proprietà che considereremo, e in particolare gli assiomi, saranno espressi mediante formule nel linguaggio della teoria degli insiemi. Ricordiamo qua sotto quella nozione e – per maggiore precisione – specifichiamo anche con esattezza cosa debba intendersi per “formula”.

DEFINIZIONE 1.1. Chiamiamo *simboli logici* i seguenti simboli:

- *Connettivi*:
negazione: $\neg$ (“non”); congiunzione: $\wedge$ (“e”); disgiunzione: $\vee$ (“o”); implicazione: $\rightarrow$ (“se ... allora”); equivalenza: $\leftrightarrow$ (“se e solo se”).
- *Variabili*:
 $x, y, z, t, \dots, x_1, x_2, x_3 \dots$
- *Quantificatori*:
esistenziale $\exists$ (“esiste”); universale $\forall$ (“per ogni”).

DEFINIZIONE 1.2. Le *formule del linguaggio della teoria degli insiemi*, in breve le *formule*, sono particolari sequenze finite di simboli nelle quali possono comparire, oltre ai simboli logici e alle parentesi “(” e “)”, soltanto il simbolo di uguaglianza “=”, e il simbolo di appartenenza “ $\in$ ”. Precisamente:

- Se x e y sono variabili, $x = y$ e $x \in y$ sono formule. Le variabili x e y si dicono *variabili libere* in quelle formule ;
- Se φ è una formula, anche $\neg(\varphi)$ è una formula che ha le stesse variabili libere di φ ;

¹ Più avanti nel corso, sarà talvolta conveniente adottare una teoria assiomatica più ampia, cioè la teoria NGB di von Neumann-Gödel-Bernays. In tale teoria, oltre agli insiemi, esiste un’altro tipo di oggetti, chiamati *classi proprie*, che si possono pensare come collezioni di insiemi “troppo grandi” per poter essere esse stesse insiemi.

- Se φ e ψ sono formule, allora anche $(\varphi \vee \psi)$, $(\varphi \wedge \psi)$, $(\varphi \rightarrow \psi)$, $(\varphi \leftrightarrow \psi)$ sono formule, le cui variabili libere sono quelle di φ più quelle di ψ ;
- Se x è una variabile libera della formula φ , allora anche $\forall x(\varphi)$ e $\exists x(\varphi)$ sono formule, le cui variabili libere sono quelle di φ *tranne* x . In questo caso x si dice variabile *legata* ;
- Ogni formula si ottiene applicando un numero finito di volte le procedure indicate sopra.

Si dice *enunciato* una formula senza variabili libere, cioè una formula dove tutte le variabili sono legate.

Vediamo subito qualche esempio.

- (1) $\exists x$ e $\forall x$ *non* sono formule.
- (2) $\exists x(x \in y)$ è una formula dove la variabile x è legata, e la variabile y è libera.
- (3) $\forall x \exists y(x \in y)$ è un enunciato perché le sue due variabili x e y sono entrambe legate.

In algebra, quando scriviamo equazioni del tipo $E(x, y)$: “ $x^2 = y^2 - 1$ ”, pensiamo alle variabili libere x e y come a numeri non meglio precisati. Soltanto dopo aver specificato a quali numeri corrispondano x e y , avrà senso chiedersi se quell’equazione è valida o no.² Tuttavia, se leghiamo le variabili con quantificatori, allora si ottengono proprietà che sono o vere o false (in ogni specificato contesto). Ad esempio, nel contesto dei numeri reali, $\forall x \forall y E(x, y)$ e $\exists x \forall y E(x, y)$ sono proprietà false, mentre $\forall x \exists y E(x, y)$ e $\exists x \exists y E(x, y)$ sono vere.³

In modo del tutto analogo, le formule della teoria degli insiemi che contengono variabili libere non sono di per sé né vere né false, perché le variabili libere sono insiemi “generici”, non precisati. Ma se ogni variabile è legata da un quantificatore, cioè se abbiamo un *enunciato*, allora viene espressa una proprietà dal significato definito, cui possiamo attribuire un valore di verità: vero o falso. Ad esempio, la formula (2) di sopra ha un significato ambiguo, che dipende da quale insieme assegniamo alla variabile libera y (se ad y assegniamo l’insieme vuoto otteniamo una proprietà falsa, altrimenti otteniamo una proprietà vera). Al contrario, la formula (3), che è un enunciato, esprime una proprietà matematica precisa relativa alle coppie di insiemi x e y considerati nella loro totalità. Risulta quindi chiaro perché tutti gli assiomi che daremo, e tutti i teoremi che dimostreremo, saranno formulati mediante enunciati.

Per non appesantire la scrittura delle formule, spesso ometteremo alcune parentesi, se non sono strettamente necessarie ad una corretta comprensione.⁴ Inoltre, seguendo l’uso comune, scriveremo:

- “ $x \neq y$ ” per intendere “ $\neg(x = y)$ ” ;
- “ $x \notin y$ ” per intendere “ $\neg(x \in y)$ ” ;

Seguiremo inoltre le usuali notazioni per le cosiddette *quantificazioni ristrette*:

² Nel linguaggio della logica, questo procedimento si chiama “assegnamento delle variabili libere”.

³ È consuetudine in algebra scrivere equazioni come “ $x^2 = y^2 - 1$ ”, sottintendendo la loro quantificazione universale, cioè “ $\forall x \forall y (x^2 = y^2 - 1)$ ”. Per evitare ambiguità, noi specificheremo sempre tutti i quantificatori coinvolti nelle nostre formule.

⁴ Ad esempio, al punto (3) di sopra abbiamo scritto $\forall x \exists y(x \in y)$ anziché $\forall x (\exists y(x \in y))$, come avremmo dovuto fare per attenerci strettamente alla definizione di formula.

- “ $\forall x \in y \varphi$ ” per intendere “ $\forall x (x \in y \rightarrow \varphi)$ ”;
- “ $\exists x \in y \varphi$ ” per intendere “ $\exists x (x \in y \wedge \varphi)$ ”;

2. I primi assiomi

Iniziamo finalmente ad elencare gli assiomi della teoria ZFC di Zermelo-Fraenkel, la più comunemente usata in matematica.

La teoria ZFC è guidata dal criterio intuitivo noto come “limitazione della grandezza” (“*limitation of size*”). Partendo dall’osservazione che le collezioni coinvolte nei paradossi sono “grandi”, si è pensato di considerare come sicuro un assioma quando esso determina solo l’esistenza di insiemi aventi “grandezza limitata”, a partire da insiemi già dati.⁵

Il primo assioma è la diretta formalizzazione del principio intuitivo di estensionalità, che abbiamo già visto e commentato nel primo capitolo.

Assioma 1: Estensionalità.

$$\forall A \forall B ((\forall x (x \in A \leftrightarrow x \in B)) \leftrightarrow A = B).$$

Per non rendere banale la nostra teoria ed evitare che parli di niente, dobbiamo garantire l’esistenza di almeno un insieme. Può sembrare un po’ strano, ma anche per questo occorre un assioma. Non dobbiamo infatti dimenticare che, procedendo col metodo assiomatico, *niente* può essere assunto se non quello che segue logicamente dagli assiomi.

Assioma 2: Insieme vuoto.

$$\exists x “x = \emptyset”.$$

I prossimi due assiomi ci forniscono due basilari principi per estendere l’universo degli insiemi.

Assioma 3: Coppia.

$$\forall a \forall b \exists X “X = \{a, b\}”.$$

Dunque, per ogni coppia assegnata, è possibile formare l’insieme che contiene esattamente di quei due elementi. Per l’assioma di estensionalità, tale insieme coppia è necessariamente unica.

Notiamo che se $a = b$, la coppia $X = \{a, a\}$ è uguale a $\{a\}$, che si chiama *singoleto* di a .

Con un uso ripetuto dell’assioma della coppia, si ottiene l’esistenza delle coppie ordinate di Kuratowski.

PROPOSIZIONE 2.1. *Per ogni a, b esiste ed unico insieme $(a, b) = \{\{a\}, \{a, b\}\}$.*

⁵Al di là della plausibilità filosofica di una tale assunzione, resta comunque il fatto oggettivo che esso ha prodotto la teoria ZFC, dalla quale non sono state mai derivate contraddizioni, anche dopo l’enorme lavoro di deduzioni operato dai migliori matematici in oltre un secolo (la prima incompleta formulazione di Zermelo risale al 1908).

Il prossimo assioma garantisce l'esistenza dell'unione di famiglie di insiemi.⁶

Assioma 4: Unione.

$$\forall \mathcal{F} \exists X \text{ “} X = \bigcup_{F \in \mathcal{F}} F \text{”}.$$

Di nuovo per *estensionalità*, un tale insieme unione è necessariamente unico.

Come abbiamo già ricordato, nel linguaggio degli insiemi, è più comune scrivere $\bigcup \mathcal{F}$ anziché $\bigcup_{F \in \mathcal{F}} F$; in altre parole, con $\bigcup \mathcal{F}$ si denota l'insieme degli elementi di elementi di $\mathcal{F}$. In maniera simile, si scrive talvolta $\bigcap \mathcal{F}$ anziché $\bigcap_{F \in \mathcal{F}} F$.

Nelle formule di sopra abbiamo usato delle notazioni metalinguistiche che erano già state introdotte nel primo capitolo come convenienti abbreviazioni di formule. Precisamente:

- “ $x = \emptyset$ ” indica la formula

$$\forall y (y \notin x).$$

- “ $X = \{a, b\}$ ” indica la formula

$$\forall x ((x \in X) \leftrightarrow (x = a \vee x = b)).$$

- “ $X = \bigcup_{F \in \mathcal{F}} F$ ” denota la formula

$$\forall x ((x \in X) \leftrightarrow \exists F (F \in \mathcal{F} \wedge x \in F)).$$

Combinando gli assiomi della *coppia* e dell'*unione*, otteniamo l'esistenza dell'unione di due insiemi.

PROPOSIZIONE 2.2. *Per ogni A e B esiste l'insieme*

$$A \cup B = \{x \mid (x \in A) \vee (x \in B)\}.$$

DIM. Per l'assioma della coppia esiste $\{A, B\}$, e per l'assioma dell'unione esiste $\bigcup \{A, B\} = \{x \mid \exists X \in \{A, B\} x \in X\} = \{x \mid (x \in A) \vee (x \in B)\}$. $\square$

Notiamo che, dall'equivalenza logica $(x \in A \vee x \in B) \leftrightarrow (x \in B \vee x \in A)$, segue banalmente che $A \cup B = B \cup A$.

Con gli assiomi dati fin qui, non è ancora possibile dimostrare l'esistenza dell'insieme intersezione $A \cap B$ nè, più in generale, l'esistenza di sottoinsiemi di un dato insieme A . A questo rimedierà il prossimo assioma di *separazione*, che permetterà di formare l'insieme di tutti e soli gli elementi che godono di una fissata proprietà, ma solo a patto che tali elementi siano presi dentro un insieme già dato. La *separazione* è quindi una versione più debole del principio di *comprensione* (che era contraddittorio!), che fornisce l'esistenza di opportuni sottoinsiemi di insiemi già assegnati, in pieno accordo con il criterio della “limitazione della grandezza”.

Assioma 5: Separazione.

Sia $\varphi(x, x_1, \dots, x_n)$ una formula dove $x, x_1, \dots, x_n$ sono tutte e sole le variabili libere. Allora il seguente è un assioma:

$$\forall A_1 \dots \forall A_n \forall X \exists B \text{ “} B = \{x \in X \mid \varphi(x, A_1, \dots, A_n)\} \text{”}.$$

⁶ Parliamo qui di “famiglie di insiemi” per seguire l'uso comune. Come abbiamo già osservato nel primo capitolo, in realtà nella teoria assiomatica degli insiemi, ogni insieme è una famiglia di insiemi.

Seguendo l'uso comune, scriviamo " $B = \{x \in X \mid \varphi(x, A_1, \dots, A_n)\}$ " per denotare quell'insieme i cui elementi sono tutti e soli gli $x \in X$ che soddisfano la proprietà $\varphi(x, A_1, \dots, A_n)$ relativa ad insiemi assegnati $A_1, \dots, A_n$. Ci riferiremo a proprietà di questo genere come a *proprietà con parametri* $A_1, \dots, A_n$.

Attenzione! La *separazione* non è in realtà un singolo assioma, ma piuttosto di uno *schema di assiomi*, uno per ogni formula.

Prime immediate conseguenze della *separazione* sono le seguenti.

PROPOSIZIONE 2.3. *Per ogni A e B , esistono gli insiemi:*

- (1) $A \cap B = \{x \mid (x \in A) \wedge (x \in B)\};$
- (2) $A \setminus B = \{x \mid (x \in A) \wedge (x \notin B)\}.$

DIM. Basta usare l'assioma di *separazione* dove si considerano rispettivamente le formule $\varphi_1(x, B) := "x \in B"$ e $\varphi_2(x, B) := "x \notin B"$. Infatti $A \cap B = \{x \in A \mid x \in B\}$ e $A \setminus B = \{x \in A \mid x \notin B\}$. $\square$

ESERCIZIO 2.4. Per ogni A_1, A_2, A_3 , esistono gli insiemi:

- (1) $A_1 \cap A_2 \cap A_3 = \{x \mid (x \in A_1) \wedge (x \in A_2) \wedge (x \in A_3)\};$
- (2) $A_1 \cup A_2 \cup A_3 = \{x \mid (x \in A_1) \vee (x \in A_2) \vee (x \in A_3)\}.$

Attenzione! Possiamo anche dimostrare le proprietà di sopra per 4 insiemi, per 5 insiemi, e così via. In altre parole, per ogni n fissato, possiamo dimostrare che l'unione di n insiemi e l'intersezione di n insiemi sono insiemi. Tuttavia *non* possiamo per il momento formalizzare all'interno della teoria la quantificazione "per ogni n ", perché non abbiamo ancora definito formalmente cosa sono i numeri naturali.

ESERCIZIO 2.5. Per ogni famiglia non vuota di insiemi $\mathcal{F}$, esiste l'insieme

$$\bigcap \mathcal{F} = \{x \mid \forall F \in \mathcal{F} \ x \in F\}.$$

Per ogni fissato insieme A , l'assioma di *separazione* garantisce l'esistenza di tutti i suoi sottoinsiemi che possono essere "descritti" usando una formula. Non possiamo però ancora dimostrare l'esistenza di un insieme che contenga *tutti* i sottoinsiemi di A .

Assioma 6: Potenza.

$$\forall A \exists X \text{ "X = } \mathcal{P}(A)\text{"}.$$

Ricordiamo che " $X = \mathcal{P}(A)$ " indica la formula

$$\forall x \ ((x \in X) \leftrightarrow "(x \subseteq A)")$$

dove, a sua volta, " $x \subseteq A$ " è una abbreviazione di

$$\forall y \ ((y \in x) \rightarrow (y \in A)).$$

Attenzione! Per ogni insieme A , l'*assioma delle parti* garantisce l'esistenza di un insieme $\mathcal{P}(A)$ che contiene tutti e soli quegli insiemi a che soddisfano la proprietà " $a \subseteq A$ "; non sappiamo però quali collezioni di elementi di A esistono effettivamente come insiemi, cioè come oggetti della nostra teoria. In altre parole, anche quando sia possibile "descrivere" una collezione a di elementi di A , *non* siamo autorizzati a concludere che un tale a sia un insieme, a meno che ciò non sia dimostrabile a

partire dagli assiomi. Per questo, è del tutto sbagliato pensare che l'assioma di *separazione* sia una conseguenza dell'assioma delle *parti*.

Osserviamo che, mentre gli assiomi dell'*insieme vuoto*, della *coppia*, dell'*unione*, e lo schema di *separazione*, sono in linea col principio della limitazione della grandezza, l'assioma della *potenza* ha una posizione più critica, visto che postula l'esistenza di una collezione più "grande" dell'insieme di partenza (nel senso preciso della cardinalità, come abbiamo visto nel primo capitolo).

ESERCIZIO 2.6. Dimostrare che se $\mathcal{P}(A) \in \mathcal{P}(B)$ allora $A \in B$. Vale l'implicazione inversa?

ESERCIZIO 2.7. Dimostrare che le seguenti proprietà valgono per ogni X :

- (1) $X = \bigcup \mathcal{P}(X)$.
- (2) $X \in \mathcal{P}(\mathcal{P}(\bigcup X))$.
- (3) $\bigcup \bigcup \mathcal{P}(X) \in \mathcal{P}(\bigcup X)$.
- (4) Se $x \in X$ allora $\mathcal{P}(x) \in \mathcal{P}(\mathcal{P}(\bigcup X))$.

Abbiamo già visto che per ogni a, b , esiste la coppia ordinata (a, b) . Tuttavia, dati due insiemi A e B , questo non garantisce l'esistenza del prodotto cartesiano $A \times B$, cioè dell'insieme di tutte le coppie ordinate (a, b) dove $a \in A$ e $b \in B$. A questo scopo è fondamentale l'uso dell'assioma delle *parti*.

PROPOSIZIONE 2.8. Per ogni A e per ogni B , esiste il prodotto cartesiano

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

DIM. Siano $a \in A$ e $b \in B$. Sia $\{a\}$ che $\{a, b\}$ sono sottoinsiemi di $A \cup B$, e quindi sono elementi di $\mathcal{P}(A \cup B)$. Dunque la coppia ordinata $(a, b) = \{\{a\}, \{a, b\}\}$ è un sottoinsieme di $\mathcal{P}(A \cup B)$, e quindi $(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B))$. Si osservi che l'esistenza di quest'ultimo insieme è garantita dall'esistenza dell'unione $A \cup B$ (Proposizione 2.3), e da una doppia applicazione dell'assioma delle *parti*. L'esistenza del prodotto cartesiano segue allora dall'assioma di *separazione*, visto che

$$A \times B = \{x \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid \varphi(x, A, B)\},$$

dove $\varphi(x, A, B)$ è la formula: $\exists a \exists b ((a \in A) \wedge (b \in B) \wedge "x = (a, b)")$.⁷ □

Sono adesso pienamente giustificate le definizioni di *relazione binaria* e di *funzione* che avevamo dato nel primo capitolo.

ESERCIZIO 2.9.

- (1) Se R è una relazione binaria, allora esistono:
 - L'insieme *dominio* $\text{dom}(R) = \{a \mid \exists b (a, b) \in R\}$
 - L'insieme *immagine* $\text{imm}(R) = \{b \mid \exists a (a, b) \in R\}$.
- (2) Per ogni relazione di equivalenza $\approx$ su un insieme A , esiste l'*insieme quoziente*, $A/\approx = \{[a] \mid a \in A\}$ i cui elementi sono tutte e sole le classi di equivalenza $[a] = \{a' \in A \mid a' \approx a\}$.
- (3) Per ogni A e B , esiste l'insieme $B^A = \text{Fun}(A, B) = \{f \mid f : A \rightarrow B\}$.

⁷ Ricordiamo che " $x = (a, b)$ " è un'abbreviazione della formula:

$$\exists s \exists t (s = \{a\} \wedge t = \{a, b\} \wedge x = \{s, t\}),$$

dove, a loro volta, le scritture " $s = \{a\}$ ", " $t = \{a, b\}$ " e " $x = \{s, t\}$ " abbreviano altre formule.

(4) Per ogni sequenza di insiemi $(A_i \mid i \in I)$, esiste l'*insieme prodotto*

$$\prod_{i \in I} A_i = \{f \mid f \text{ è una } I\text{-sequenza} \wedge \forall i \in I f(i) \in A_i\}.$$

Usando gli assiomi visti fin qui, con gli stessi argomenti usati nella prima parte di teoria “intuitiva” degli insiemi, possiamo dimostrare in modo formale le seguenti proprietà:

PROPOSIZIONE 2.10.

- (1) *Non esistono insiemi R tali che $R = \{x \mid x \notin x\}$.*
- (2) *Non esistono insiemi V tali che $V = \{x \mid x = x\}$.*

ESERCIZIO 2.11. Usando gli assiomi visti fin qui, dimostrare che per ogni insieme $A \neq \emptyset$, non esiste l'insieme classe di equipotenza $[A] := \{B \mid |B| = |A|\}$.

Gli assiomi dati fin qui garantiscono l'esistenza dei prodotti $\prod_{i \in I} A_i$, ma *non* garantiscono che tali prodotti siano non vuoti quando tutti gli A_i sono non vuoti. Come abbiamo anticipato nel primo capitolo, nel caso di prodotti infiniti questa proprietà viene postulata in un apposito assioma, cioè l'assioma di scelta. Visto che, per il momento, non abbiamo ancora definito la nozione di “finito” e “infinito”, adottiamo la seguente formulazione che postula l'esistenza di una funzione di scelta f per ogni famiglia $\mathcal{F}$ di insiemi:

Assioma 7: Scelta.

$$\forall \mathcal{F} \exists f (f \text{ funzione} \wedge \forall F \in \mathcal{F} (F \neq \emptyset \rightarrow f(F) \in F)).$$

3. L'assioma dell'infinito

Osserviamo che i primi 7 assiomi che abbiamo presentato non permettono di dimostrare l'esistenza di insiemi infiniti; infatti, supponendo di vivere in un universo dove tutti gli insiemi sono finiti, tutte le proprietà postulate dagli assiomi introdotti fin qua sono verificate. Occorre quindi introdurre un nuovo assioma, perché in matematica l'esistenza di insiemi infiniti è di centrale importanza.

Vedremo in questo capitolo come si possono introdurre i numeri naturali, forse l'esempio più importanti in matematica di insieme infinito. Poiché stiamo lavorando nel quadro di una teoria *pura* degli insiemi, anch'essi saranno definiti come opportuni insiemi. L'*euristica*, cioè l'intuizione informale, che seguiremo per costruirli è la seguente. Definiamo $0 = \emptyset$ come l'insieme vuoto; poi $1 = \{0\}$ come l'insieme che contiene 0 come suo unico elemento; poi $2 = \{0, 1\}$ come l'insieme contenente i due elementi precedenti, cioè 0 e 1; poi $3 = \{0, 1, 2\}$; poi $4 = \{0, 1, 2, 3\}$, e così via. Dunque:

- $0 = \emptyset$
- $1 = \{\emptyset\} = \{0\}$
- $2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$
- $3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}$
- $4 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2, 3\}$
- ...

Infine raccogliamo tutti questi numeri in un insieme, che sarà l'insieme dei numeri naturali. Il problema è riuscire a formalizzare questo procedimento intuitivo in modo preciso e rigoroso all'interno della nostra teoria.

Notiamo che, a partire dagli assiomi introdotti fin qui, è in effetti possibile dimostrare l'esistenza di ciascuno degli insiemi finiti di sopra. L'esistenza di 0 è garantita dall'assioma dell'*insieme vuoto*. Applicando l'assioma della *coppia* si ottiene l'esistenza di $\{0, 0\} = \{0\} = 1$. Di nuovo per l'assioma della *coppia* si ottiene $2 = \{0, 1\} = 1 \cup \{1\}$. Per l'esistenza di $3 = \{0, 1, 2\} = 2 \cup \{2\}$ è necessario anche l'assioma dell'*unione*. Analogamente per $4 = \{0, 1, 2, 3\} = 3 \cup \{3\}$, e così via.

È importante tenere presente che questo procedimento dimostra l'esistenza dei singoli numeri $0, 1, 2, 3, 4, \dots$ uno alla volta, ma *non* dimostra l'esistenza di un insieme che li contenga tutti.

Può venire la tentazione di postulare un nuovo assioma che dica: “Esiste un insieme $\mathbb{N}$ tale che $1 \in \mathbb{N}$ e $2 \in \mathbb{N}$ e $3 \in \mathbb{N}$ e $4 \in \mathbb{N}$ *etc.*”. Notiamo però che una tale proprietà *non* è formalizzabile nel nostro linguaggio: infatti per noi una formula è comunque una espressione *finita*, e quindi non possiamo congiungere tutte le infinite proprietà “ $n \in \mathbb{N}$ ”.

Riusciremo ad aggirare queste difficoltà con la nozione di “insieme induttivo”, che permetterà di formalizzare all'interno della teoria degli insiemi la nostra intuizione dei numeri naturali e del processo induttivo. Nella costruzione informale vista sopra, una volta definito un numero n , si definiva il numero successivo aggiungendo n stesso come nuovo elemento, cioè si considerava l'unione $n \cup \{n\}$. Come abbiamo già osservato, questo tipo di costruzione è giustificato dagli assiomi della *coppia* e dell'*unione*.

NOTAZIONE 3.1. Per ogni x , denotiamo $\hat{x} = x \cup \{x\}$.

La prossima definizione è suggerita dal procedimento *euristico* che abbiamo usato sopra per “generare” i numeri naturali.

DEFINIZIONE 3.2. Un insieme X si dice *induttivo* se soddisfa le proprietà:

- (1) $\emptyset \in X$;
- (2) $\forall x (x \in X \rightarrow \hat{x} \in X)$.

Notiamo che la proprietà “ X è induttivo” è in effetti esprimibile da una formula. L'intuizione ci suggerisce che un insieme induttivo è necessariamente infinito, perché $0 \in X$ per definizione, inoltre da $0 \in X$ segue che $\hat{0} = 1 \in X$, e quindi anche $2 = \hat{1} \in X$, e così via. Per garantire l'esistenza di tali insiemi, occorre un apposito assioma, l'ottavo della nostra lista.

Assioma 8: Infinito.

$$\exists X \text{ “} X \text{ induttivo”}.$$

Osserviamo che l'assioma dell'insieme *vuoto* è adesso ridondante perché segue dall'assioma dell'infinito più lo schema di *separazione*; infatti, preso un qualunque insieme induttivo X , si ha $\emptyset = \{x \in X \mid x \neq x\}$.

Come abbiamo visto, dentro un fissato insieme induttivo X troviamo gli elementi $0, 1, 2, 3, \text{etc.}$, ma in generale dobbiamo aspettarci di trovare anche altri elementi. Questa *euristica* suggerisce la seguente

DEFINIZIONE 3.3. n si dice *numero naturale* se appartiene a tutti gli insiemi induttivi X .

I nostri assiomi garantiscono che i numeri naturali formano un insieme.

PROPOSIZIONE 3.4. Esiste ed unico un insieme ω i cui elementi sono tutti e soli i numeri naturali:

$$\omega = \{n \mid \text{"}n \text{ è un numero naturale"}\}.$$

Inoltre un tale insieme ω è esso stesso induttivo, e dunque è il “più piccolo” insieme induttivo.

DIM. Si prenda un qualunque insieme induttivo X , che esiste per l'assioma dell'*infinito*. Per *separazione*, esiste l'insieme

$$\omega = \{x \in X \mid \text{"}x \text{ è un numero naturale"}\}.$$

Per definizione, ogni numero naturale appartiene necessariamente ad X che è induttivo, e quindi ω contiene tutti e soli i numeri naturali. Per *estensionalità*, un tale ω è necessariamente unico.

Vediamo ora che ω stesso è un insieme induttivo. Questo segue direttamente dalle definizioni. Infatti $0 = \emptyset$ è un numero naturale (cioè appartiene ad ogni induttivo), dunque $0 \in \omega$. Inoltre, se $x \in \omega$, cioè se $x \in X$ per ogni insieme induttivo X , allora si avrà anche $\hat{x} \in X$ per ogni insieme induttivo X , e quindi $\hat{x} \in \omega$. $\square$

Nella nostra definizione di numero naturale ci siamo uniformati alla consuetudine in teoria degli insiemi di includere anche 0 (mentre fin qui avevamo convenuto che $0 \notin \mathbb{N}$); non ci sarà comunque ambiguità perché useremo due scritture diverse.

NOTAZIONE 3.5.

- ω denota l'insieme dei numeri naturali garantito dalla proposizione di sopra (dove $0 \in \omega$).
- $\mathbb{N} = \omega \setminus \{0\} = \{1, 2, \dots\}$ denota l'insieme dei naturali diversi da zero.

Qui di seguito, vedremo un po' alla volta che ω soddisfa le familiari proprietà che l'intuizione e la pratica matematica attribuiscono all'insieme dei numeri naturali. Questo giustificherà la nostra “strana” definizione di numero naturale, un po' come la proprietà fondamentale $(a, b) = (a', b') \leftrightarrow (a = a' \wedge b = b')$ aveva giustificato la nostra “strana” definizione di coppia ordinata $(a, b) = \{\{a\}, \{a, b\}\}$.⁸

La proprietà qua sotto, che è diretta conseguenza della minimalità di ω , riveste un ruolo fondamentale.

⁸ Uno dei criteri per valutare la validità fondazionale di una teoria degli insiemi è la possibilità di definire al suo interno opportuni insiemi che “codificano” in modo soddisfacente i principali oggetti della matematica, cioè che ne soddisfano le proprietà caratterizzanti come mostrate dalla pratica matematica.

TEOREMA 3.6 (Principio di induzione).

Sia $P(x, y_1, \dots, y_k)$ una formula, dove $x, y_1, \dots, y_k$ sono tutte e sole le sue variabili libere. Siano $A_1, \dots, A_k$ insiemi fissati (parametri), e supponiamo che valgano le due condizioni:

- Base induttiva: $P(0, A_1, \dots, A_k)$;
- Passo induttivo: Per ogni $n \in \omega$, $P(n, A_1, \dots, A_k) \Rightarrow P(\hat{n}, A_1, \dots, A_k)$.

Allora $P(n, A_1, \dots, A_k)$ vale per ogni $n \in \omega$.

DIM. Per ogni $A_1, \dots, A_k$, l'insieme $A = \{n \in \omega \mid P(n, A_1, \dots, A_k)\} \subseteq \omega$ esiste per separazione. Le ipotesi ci dicono che A è un insieme induttivo. Visto che ω è il più piccolo degli insiemi induttivi, deve necessariamente essere $A = \omega$, e questo dimostra la tesi. $\square$

Anche se la formulazione in termini di insiemi $\hat{x}$ potrebbe lasciare perplessi, tra poco risulterà chiaro che questo principio corrisponde esattamente al principio di induzione sui numeri naturali cui siamo abituati. Intanto cominciamo ad usarlo per dimostrare un paio di semplici proprietà che ci risulteranno utili nel seguito.

PROPOSIZIONE 3.7.

- (1) Se $x \neq 0$ è un numero naturale, allora $0 \in x$.
- (2) Siano $x, y \in \omega$ numeri naturali. Se $x \in y$ allora $\hat{x} \in \hat{y}$.

DIM. (1). Dimostriamo per induzione che per ogni $x \in \omega$, vale la proprietà $P(x)$: $(x \neq 0) \rightarrow (0 \in x)$. $P(0)$ è banalmente vera, perchè l'ipotesi " $0 \neq 0$ " non vale. Assumiamo ora $P(x)$ e dimostriamo $P(\hat{x})$. Se $x = 0$, allora $0 \in \{0\} = \hat{x}$. Se $x \neq 0$, per ipotesi induttiva $0 \in x$, e dunque anche $0 \in \hat{x}$.

(2). Procedendo per induzione, dimostriamo che per ogni $y \in \omega$ vale la proprietà $P(y)$: $\forall x \in \omega (x \in y) \rightarrow (\hat{x} \in \hat{y})$. Se $y = 0$ la proprietà è vera a vuoto perchè l'ipotesi $x \in y$ non è mai realizzata. Al passo induttivo, assumiamo $P(y)$ e dimostriamo $P(\hat{y})$. Supponiamo che $x \in \omega$ sia tale che $x \in \hat{y} = y \cup \{y\}$; dobbiamo mostrare che allora $\hat{x} \in \hat{\hat{y}}$. Si hanno due casi: se $x \in y$, per ipotesi induttiva $\hat{x} \in \hat{y}$, e quindi $\hat{x} \in \hat{\hat{y}}$; se invece $x = y$, allora $\hat{x} = \hat{y} \in \hat{\hat{y}}$. $\square$

ESERCIZIO 3.8. Dimostrare che $a = \{\{\emptyset\}\}$ e $b = \{\emptyset, \{\{\emptyset\}\}\}$ non sono numeri naturali.

Possiamo finalmente dimostrare una proprietà fondamentale dei numeri naturali.

TEOREMA 3.9.

La relazione di appartenenza $\in$ è una relazione di ordine lineare stretto su ω . Infatti valgono le seguenti proprietà:

- (1) Antiriflessività: $\forall x \in \omega (x \notin x)$;
- (2) Transitività: $\forall x, y, z \in \omega (x \in y \wedge y \in z) \rightarrow x \in z$;
- (3) Tricotomia: $\forall x, y \in \omega$, vale una ed una sola delle proprietà seguenti:
 $x \in y$, $x = y$, $y \in x$.

DIM. (2). Procediamo per induzione su z , e consideriamo la seguente proprietà (con parametro ω):

$$P(z) : \quad \forall x, y \in \omega (x \in y \wedge y \in z) \rightarrow x \in z.$$

Notiamo che $P(0)$ è banalmente vera. Infatti l'ipotesi $(x \in y \wedge y \in z)$ non è mai verificata (non esistono y tali che $y \in 0$!). Supponiamo ora vera la proprietà $P(z)$. Vogliamo dimostrare che vale

$$P(\hat{z}) : \quad \forall x, y \in \omega \ (x \in y \wedge y \in \hat{z}) \rightarrow x \in \hat{z}.$$

Assumiamo dunque $x \in y$ e $y \in \hat{z}$. Dimosteremo che $x \in z$, e quindi $x \in \hat{z}$. Da $y \in \hat{z} = z \cup \{z\}$, segue che $y \in z$ o $y = z$. Nel primo caso, abbiamo $(x \in y \wedge y \in z)$ e quindi, per ipotesi induttiva, $x \in z$. Nel secondo caso, $x \in y$ equivale a $x \in z$, cioè quanto voluto.

(1). Per induzione su x . Banalmente $0 \notin 0$. Vediamo adesso il passo induttivo $(x \notin x) \rightarrow (\hat{x} \notin \hat{x})$ o, equivalentemente, $(\hat{x} \in \hat{x}) \rightarrow (x \in x)$. Se $\hat{x} \in \hat{x} = x \cup \{x\}$, allora $\hat{x} \in x$ o $\hat{x} = x$. Nel primo caso, visto che $x \in \hat{x}$, per la proprietà transitiva (2) appena dimostrata, possiamo concludere che $x \in x$; e anche nel secondo caso vale $x \in x$ perché $x \in \hat{x} = x$.

(3). Osserviamo intanto che può verificarsi al più una di quelle tre possibilità. Infatti se $x \in y$ e $x = y$, allora $x \in x$ contro la (1). Analogamente se $y \in x$ e $x = y$. Inoltre, se $x \in y$ e $y \in x$, per la (2) avremmo che $x \in x$, di nuovo contro la (1).

Resta da vedere che almeno una di quelle tre eventualità si verifica sempre. Diciamo che $y \in \omega$ è *confrontabile* (con ogni $x \in \omega$) se vale la seguente proprietà:

$$P(y) : \quad \forall x \in \omega \ (x \in y \vee x = y \vee y \in x).$$

Vogliamo dimostrare che tutti i numeri naturali sono confrontabili. Procediamo per induzione su y . La base induttiva $P(0)$ è la proprietà:

$$\forall x \in \omega \ (x \in 0 \vee x = 0 \vee 0 \in x).$$

Visto che $x \in 0$ non è mai verificata, $P(0)$ equivale al punto (1) della Proposizione precedente. Consideriamo ora il passo induttivo. Supponiamo dunque che y sia confrontabile, e dimostriamo che anche $\hat{y}$ lo è. Sia $x \in \omega$ qualunque. Per ipotesi induttiva:

$$(x \in y \vee x = y \vee y \in x).$$

Sia nel primo caso $x \in y$ che nel secondo caso $x = y$, banalmente $x \in \hat{y}$, e quindi $\hat{y}$ è confrontabile con x . Nel terzo caso, per la (2) della Proposizione precedente, da $y \in x$ segue che $\hat{y} \in \hat{x}$. Ma allora $\hat{y} \in x$ o $\hat{y} = x$, e anche in questo caso $\hat{y}$ è confrontabile con x . $\square$

PROPOSIZIONE 3.10. $\hat{n}$ è il *successore* di $n \in \omega$ nell'insieme ordinato $(\omega, \in)$, cioè $\hat{n}$ è il più piccolo dei numeri naturali maggiori di n .

DIM. Supponiamo per assurdo che esista $m \in \omega$ tale che $n \in m \in \hat{n}$; quindi $m \in n$ oppure $m = n$. Nel primo caso avremmo $n \in m \in n$, da cui $n \in n$ per transitività, ma questo contraddice l'antiriflessività; nel secondo caso avremmo direttamente $n \in n$, di nuovo contraddicendo l'antiriflessività. $\square$

Anche se non abbiamo ancora definito la somma tra numeri naturali, per seguire l'uso comune da qui in avanti useremo la seguente

NOTAZIONE 3.11. Se $n \in \omega$ è un numero naturale, denotiamo $\hat{n} = n + 1$.

PROPOSIZIONE 3.12. La funzione “successore” $S : n \mapsto n + 1$ è una *bigezione* tra ω e $\omega \setminus \{0\}$.

DIM. Notiamo anzitutto che l'esistenza della funzione S è garantita dall'assioma di *separazione*:

$$S = \{(n, m) \in \omega \times \omega \mid m = n + 1\}.$$

Chiaramente S è una relazione univoca. Per vedere l'iniettività, supponiamo $n+1 = m+1$. Da $n \in n+1 = m+1$ segue che $n \in m$ o $n = m$; analogamente, da $m \in m+1 = n+1$ segue che $m \in n$ o $m = n$. Se per assurdo fosse $n \neq m$, avremmo allora sia $n \in m$ che $m \in n$, contro la proprietà di tricotomia di $(\omega, \in)$. La suriettività è immediata, perché afferma che ogni numero naturale diverso da 0 è un successore, e questo fa parte del principio di induzione. Formalmente, si dimostra banalmente per induzione che la seguente proprietà vale per ogni $n \in \omega$:

$$P(n) : n \neq 0 \rightarrow (\exists m \in n \ m + 1 = n).$$

□

ESERCIZIO 3.13. Dimostrare per induzione le seguenti proprietà relative a numeri naturali n, m :

- (1) $n \in m$ se e solo se $n \subsetneq m$;
- (2) L'intersezione di due numeri naturali è un numero naturale, e precisamente $n \cap m = \min\{n, m\}$;
- (3) L'unione di due numeri naturali è un numero naturale, e precisamente $n \cup m = \max\{n, m\}$.
- (4) Ogni elemento di un numero naturale è un numero naturale, cioè $(x \in n \in \omega) \rightarrow (x \in \omega)$;
- (5) Se $\hat{x} \in \omega$ allora $x \in \omega$;

Il prossimo teorema riguarda forme equivalenti del principio di induzione, cioè la cosiddetta “induzione forte” e il principio del “buon ordinamento”, una nozione centrale della teoria degli insiemi che indagheremo a fondo più avanti.

TEOREMA 3.14.

Sia $(N, <)$ un insieme totalmente ordinato avente un elemento minimo 0. Allora le due proprietà seguenti sono equivalenti:

- (1) Buon Ordinamento: Ogni sottoinsieme non vuoto $X \subseteq N$ ha minimo;
- (2) Induzione Forte: Sia $P(x)$ una proprietà.⁹ Supponiamo:
 - (I) $P(0)$;
 - (II) Per ogni $x \neq 0$ in N , vale l'implicazione $(\forall y < x \ P(y)) \rightarrow P(x)$.¹⁰
 Allora $\forall x \in N \ P(x)$.

Se inoltre ogni elemento $x \in N$ ha un successore $x+1$ e tutti gli $x \neq 0$ sono successori¹¹, vale anche l'equivalenza con:

- (3) Induzione: Sia $P(x)$ una proprietà. Supponiamo:
 - (I)' $P(0)$;
 - (II)' Per ogni $x \in N$, vale l'implicazione $P(x) \rightarrow P(x+1)$.

⁹ Qui per “proprietà” va intesa nel senso più generale, e non soltanto nel senso di proprietà formalizzabile in una fissato linguaggio del primo ordine. In altre parole, assumiamo che ad ogni sottoinsieme $A \subseteq N$ corrisponda una proprietà $P(x)$ tale che $\{x \in N \mid P(x)\} = A$.

¹⁰ Seguendo l'uso comune, con abuso di notazione abbiamo scritto “ $\forall y < x \ P(y)$ ” per intendere “ $\forall y (y < x \rightarrow P(y))$ ”.

¹¹ In un insieme ordinato $(A, <)$, un elemento a' si dice *successore* di a se $a < a'$ e non esistono elementi x tali che $a < x < a'$.

Allora $\forall x \in N \ P(x)$.

Visto che $(\omega, \in)$ soddisfa tutte le ipotesi richieste in (3), in particolare dal principio di induzione segue che in ω valgono anche il principio di *induzione forte* e la proprietà di *buon ordinamento*.

DIM. (1) $\Rightarrow$ (2). Per assurdo supponiamo che esista una proprietà $P(x)$ che soddisfa le condizioni (I) e (II) ma tale che non valga $\forall x \in N \ P(x)$. Dunque l'insieme $X = \{x \in N \mid \neg P(x)\}$ è non vuoto e quindi, per il buon ordinamento, ammetterà un elemento minimo ξ . Chiaramente $\xi \neq 0$ perché vale $P(0)$. Per definizione di minimo, tutti gli elementi $y < \xi$ non appartengono ad X , cioè vale la proprietà $\forall y < \xi \ P(y)$. Per la (II) avremmo allora $P(\xi)$, contro il fatto che $\xi \in X$.

(2) $\Rightarrow$ (1). Per assurdo sia $X \subseteq N$ un sottoinsieme non vuoto senza minimo, e consideriamo la proprietà $P(x) : x \notin X$. Certamente vale $P(0)$, altrimenti $0 \in X$ sarebbe il minimo. Supponiamo ora $\forall y < x \ P(y)$, cioè che ogni y minore di x non appartenga ad X . Ma allora anche $x \notin X$, cioè vale $P(x)$, altrimenti avremmo che $x = \min X$. Abbiamo così verificato (I) e (II). Per Induzione Forte seguirebbe allora $P(x)$ per ogni $x \in X$, cioè $X = \emptyset$, contro l'ipotesi.

Non appena sappiamo che ogni elemento x ha successore $x + 1$, l'implicazione (2) $\Rightarrow$ (3) vale banalmente (per questo la (2) è chiamata *induzione forte*). Infatti fissiamo una proprietà $P(x)$. Se le condizioni (I)' e (II)' sono soddisfatte, a maggior ragione sono soddisfatte le corrispondenti condizioni (I) e (II) della induzione forte. Dunque, applicando (2) si può concludere $\forall x \in N \ P(x)$, come voluto.

L'implicazione (3) $\Rightarrow$ (1) si dimostra esattamente come (2) $\Rightarrow$ (1), considerando la proprietà: $P'(x) : \forall y \leq x \ y \notin X$, ed usando l'ipotesi che ogni $x \neq 0$ è successore $x = y + 1$ di qualche $y \in N$. $\square$

Nel passo induttivo di alcune dimostrazioni, per giungere a dimostrare la proprietà $P(n + 1)$ è talvolta utile assumere come ipotesi induttiva non soltanto la proprietà $P(n)$, ma *tutte* le proprietà “precedenti” $P(1), P(2), \dots, P(n)$. In questo caso, è “più facile” dimostrare il passo induttivo. È infatti evidente che assumere un maggior numero di ipotesi, cioè $P(1), P(2), \dots, P(n)$ anziché soltanto $P(n)$, rende “più facile” verificare $P(n + 1)$. Di conseguenza, con questa forma di induzione, è “più facile” dimostrare la tesi $\forall n \ P(n)$, il che significa che abbiamo uno strumento dimostrativo più potente. Per questo si parla di *induzione forte*.

4. Il teorema di ricorsione numerabile

Le definizioni per ricorrenza sui numeri naturali sono uno strumento molto usato in matematica. Il prossimo teorema ne dà una piena giustificazione a partire dagli assiomi già dati della teoria degli insiemi.

TEOREMA 4.1 (Ricorsione Numerabile). *Siano dati un insieme A , un elemento $a \in A$, ed una funzione $g : \omega \times A \rightarrow A$. Allora esiste ed unica successione $f : \omega \rightarrow A$ tale che*

$$\begin{cases} f(0) = a \\ f(n + 1) = g(n, f(n)). \end{cases}$$

Naturalmente, l'analogo risultato vale se consideriamo, al posto di ω , l'insieme $\mathbb{N} = \omega \setminus \{0\}$ dei naturali diversi da zero.

Un esempio molto familiare di definizione per ricorsione è il seguente.

ESEMPIO 4.2. L'esistenza ed unicità della funzione *fattoriale* $f(n) = n!$ segue dal teorema di ricorsione (assumiamo qui di conoscere già la definizione di prodotto tra numeri naturali, che vedremo più avanti). Infatti, considerando come insieme $A = \mathbb{N}$, come elemento $a = 1 \in \mathbb{N}$, e come $g : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ la funzione $g : (n, m) \mapsto (n + 1) \cdot m$, otteniamo l'esistenza ed unicità di una funzione $f : \mathbb{N} \rightarrow \mathbb{N}$ tale che:

$$(\star) \quad \begin{cases} f(1) = 1 \\ f(n+1) = (n+1) \cdot f(n) = g(n, f(n)). \end{cases}$$

Prima di dimostrare il teorema di ricorsione numerabile, ci è utile chiarire alcuni aspetti che riguardano l'unione di funzioni. Intanto, l'unione di un insieme di relazioni binarie è ancora una relazione binaria, in quanto è un insieme di coppie ordinate. La stessa proprietà non vale però in generale per le funzioni. Ad esempio, se $f(a) = b$ e $g(a) = b'$ dove $b \neq b'$, allora l'unione di coppie ordinate $f \cup g$ *non* è una funzione, cioè non è una relazione univoca. Tuttavia l'unione di una famiglia di funzioni è una funzione nel caso in cui valga un'opportuna ipotesi di compatibilità.

DEFINIZIONE 4.3. Due funzioni φ e ψ sono *compatibili* se assumono gli stessi valori sull'intersezione dei rispettivi domini:

$$\forall \varphi, \psi \in \mathcal{F} \quad \forall x \in \text{dom}(\varphi) \cap \text{dom}(\psi) \quad \varphi(x) = \psi(x).$$

Equivalentemente, in termini puramente insiemistici, le funzioni φ e ψ sono compatibili se $\varphi \cap \psi$ è una funzione.

ESERCIZIO 4.4. Sia $\mathcal{F}$ un insieme di funzioni. Allora l'unione $\Phi = \bigcup_{\varphi \in \mathcal{F}} \varphi$ è una funzione se e solo se le funzioni in $\mathcal{F}$ sono a due a due compatibili. In questo caso, $\text{dom}(\Phi) = \bigcup_{\varphi \in \mathcal{F}} \text{dom}(\varphi)$.

Occupiamoci finalmente della dimostrazione del teorema di ricorsione numerabile.

DIM. Diciamo che φ è una *approssimazione finita* (in breve AF) se $\varphi : k \rightarrow A$ è una funzione che ha come dominio un numero naturale positivo k , ed è tale che $\varphi(0) = a$ e $\varphi(n+1) = g(n, \varphi(n))$ per ogni naturale $n+1 < k$. Ad esempio, la funzione $\varphi : 1 = \{0\} \rightarrow A$ dove $\varphi(0) = a$, è banalmente una AF. Notiamo ogni AF è un sottoinsieme di $\omega \times A$. Per *separazione* possiamo allora considerare l'insieme di *tutte* le AF:

$$\mathcal{F} = \{\varphi \in \mathcal{P}(\omega \times A) \mid \varphi \text{ è una AF}\}.$$

Il nostro scopo è adesso quello di “rincollare” le varie AF per formare una funzione $f : \omega \rightarrow A$ che soddisfi la $(\star)$. Vogliamo dimostrare che valgono le proprietà:

- (1) Le funzioni di $\mathcal{F}$ sono a due a due compatibili, cioè:

$$\forall \varphi, \psi \in \mathcal{F} \quad \forall x \in \text{dom}(\varphi) \cap \text{dom}(\psi) \quad \varphi(x) = \psi(x).$$

- (2) Per ogni $n \in \omega$, esiste $\varphi \in \mathcal{F}$ tale che $\text{dom}(\varphi) = n+1 = \{0, \dots, n\}$.

Una volta verificate le due proprietà di sopra, l'esistenza della funzione cercata si ottiene prendendo $f = \bigcup_{\varphi \in \mathcal{F}} \varphi$. Infatti, per l'Esercizio 4.4 di sopra, f è una funzione con $\text{dom}(f) = \bigcup_{\varphi \in \mathcal{F}} \text{dom}(\varphi) = \omega$. Inoltre, per ogni $\varphi \in \mathcal{F}$ e per ogni $n \in \text{dom}(\varphi)$, si ha $f(n) = \varphi(n)$, e le proprietà $(\star)$ seguono direttamente dal fatto che tutte le funzioni $\varphi \in \mathcal{F}$ sono AF.

Per dimostrare la (1), procediamo per induzione considerando la proprietà

$$P(n) : \quad \forall \varphi, \psi \in \mathcal{F} \quad (n \in \text{dom}(\varphi) \cap \text{dom}(\psi)) \rightarrow \varphi(n) = \psi(n).$$

Quando $n = 0$ la cosa è banale, perchè tutte le AF assumono il valore a per $n = 0$. Per il passo induttivo, supponiamo che un successore $n + 1 \in \text{dom}(\varphi) \cap \text{dom}(\psi)$ appartenga al dominio di due AF; notiamo che allora anche $n \in \text{dom}(\varphi) \cap \text{dom}(\psi)$. Usando l'ipotesi induttiva $\varphi(n) = \psi(n)$, dalle proprietà di AF si ottengono le uguaglianze:

$$\varphi(n + 1) = g(n, \varphi(n)) = g(n, \psi(n)) = \psi(n + 1).$$

Anche per dimostrare la (2) procediamo per induzione. Per $n = 0$ basta considerare $\varphi = \{(0, a)\}$, che è banalmente una AF con $\text{dom}(\varphi) = \{0\} = 1$. Inoltre, se $\varphi \in \mathcal{F}$ e $\text{dom}(\varphi) = n + 1 = \{0, 1, \dots, n\}$, anche $\psi = \varphi \cup \{(n + 1, b)\}$ dove $b = g(n, \varphi(n))$ è una AF con $\text{dom}(\psi) = \{0, 1, \dots, n, n + 1\} = n + 2$.

Occupiamoci infine della questione dell'*unicità*, e supponiamo che f_1 che f_2 entrambe soddisfino le proprietà $(\star)$. Per induzione su n , mostriamo che $f_1(n) = f_2(n)$. Per $n = 0$ questo è immediato perché $f_1(0) = a = f_2(0)$. Nel passo induttivo, basta notare che dall'ipotesi $f_1(n) = f_2(n)$ segue che $f_1(n + 1) = g(n, f_1(n)) = g(n, f_2(n)) = f_2(n + 1)$. $\square$

In alcune definizioni per ricorsione, il valore al passo successore $n + 1$ è determinato non solo dal valore nel predecessore n , ma anche da valori precedenti. Ad esempio, la *successione di Fibonacci* è definita per ricorsione ponendo: $a_1 = a_2 = 1$, e $a_{n+1} = a_n + a_{n-1}$ per $n \geq 2$. Per giustificare questo tipo di definizioni, occorre una forma più forte del teorema di ricorsione. Precisamente:

TEOREMA 4.5 (Ricorsione Numerabile II).

Per ogni insieme A , per ogni $a \in A$, e per ogni funzione $g : \omega \times \text{FSeq}(A) \rightarrow A$,¹² esiste ed unica funzione $f : \omega \rightarrow A$ tale che:

$$(\star) \quad \begin{cases} f(0) & = a \\ f(n + 1) & = g(n, f|_{n+1}). \end{cases}$$

Ovviamente anche questa versione del teorema di ricorsione vale se sostituiamo $\mathbb{N}$ al posto di ω .

La dimostrazione di questa forma di ricorsione numerabile è una semplice modifica della dimostrazione precedente, ed è lasciata per esercizio.

Siamo finalmente pronti a dimostrare un importante risultato sull'equipotenza che già abbiamo usato ripetutamente.

TEOREMA 4.6 (Cantor-Bernstein).

Se $|X| \leq |Y|$ e $|Y| \leq |X|$ allora $|X| = |Y|$.

¹² Ricordiamo che con $\text{FSeq}(A) = \{\sigma \mid \exists n \in \mathbb{N} \sigma : \{1, \dots, n\} \rightarrow A\}$ si denotava l'insieme delle *sequenze finite* di elementi di A .

Vista la particolare importanza di questo teorema, ne diamo due dimostrazioni.

DIM. 1. Prendiamo $f : X \rightarrow Y$ e $g : Y \rightarrow X$ funzioni iniettive. Chiaramente f determina una bigezione tra X e l'insieme immagine $f(X)$; e g determina una bigezione tra Y e $g(Y)$, e una bigezione tra $f(X)$ e $g(f(X))$. Abbiamo dunque $g(f(X)) \subseteq g(Y) \subseteq X$ dove $|g(f(X))| = |f(X)| = |X|$ e $|g(Y)| = |Y|$. La tesi segue allora dal lemma seguente, prendendo $A = X$, $B = g(Y)$, e $C = g(f(X))$. $\square$

LEMMA 4.7. *Siano $A \supseteq B \supseteq C$ dove $|A| = |C|$. Allora $|A| = |B| = |C|$.*

DIM. Fissiamo una bigezione $\varphi : A \rightarrow C$. Sia $D = A \setminus B$, e definiamo una successione di sottoinsiemi di C come segue:

$$\begin{cases} E_1 &= \varphi(D) \\ E_{n+1} &= \varphi(E_n) \end{cases}$$

Osserviamo che l'esistenza della successione $(E_n \mid n \in \mathbb{N})$ è garantita dal Teorema di ricorsione numerabile.¹³ Sia $E = \bigcup_{n \in \mathbb{N}} E_n$ l'unione di tutti questi insiemi, e definiamo la funzione $\psi : A \rightarrow B$ ponendo $\psi = \varphi|_{D \cup E} \cup \text{id}_{B \setminus E}$, cioè:

$$\psi(a) = \begin{cases} \varphi(a) & \text{se } a \in D \cup E \\ a & \text{altrimenti, cioè se } a \in B \setminus E. \end{cases}$$

Verifichiamo che ψ è la bigezione cercata. Vediamo prima la suriettività. Dalla definizione, segue direttamente che $\text{imm}(\psi) = \text{imm}(\varphi|_{D \cup E}) \cup \text{imm}(\text{id}_{B \setminus E})$. Visto che banalmente $\text{imm}(\text{id}_{B \setminus E}) = B \setminus E$, basta vedere che $E \subseteq \text{imm}(\varphi|_{D \cup E})$ (in realtà vale l'uguaglianza). Se $b \in E_0$, allora $b = \varphi(a) = \psi(a)$ con $a \in D$. Se invece $b \in E_{n+1}$ per qualche n , allora $b = \varphi(a) = \psi(a)$ per un $a \in E_n$. Per l'iniettività, notiamo che le restrizioni $\psi|_{D \cup E}$ e $\psi|_{B \setminus E}$ sono entrambe iniettive, perché uguali rispettivamente a $\varphi|_{D \cup E}$ e alla funzione identità $\text{id}_{B \setminus E}$. Per concludere che ψ è iniettiva basta allora osservare che $\varphi|_{D \cup E}$ e $\text{id}_{B \setminus E}$ hanno immagini disgiunte, e questo è immediato perché $\text{imm}(\varphi|_{D \cup E}) = E$. $\square$

DIM. 2. Definiamo per ricorsione numerabile:

$$X_0 = X; Y_0 = Y; X_{n+1} = g(Y_n); Y_{n+1} = f(X_n).$$

Formalmente, stiamo definendo la successione $a_n = (X_n, Y_n)$ ponendo $a_0 = (X, Y)$ e $a_{n+1} = F(a_n)$, dove $F : \mathcal{P}(X) \times \mathcal{P}(Y) \rightarrow \mathcal{P}(X) \times \mathcal{P}(Y)$ è la funzione tale che $F(Z, W) = (g(W), f(Z))$.

Notiamo anzitutto che le sequenze di insiemi $(X_n \mid n \in \omega)$ e $(Y_n \mid n \in \omega)$ sono debolmente decrescenti:

- Per ogni n , $X_{n+1} \subseteq X_n$ e $Y_{n+1} \subseteq Y_n$.

Questo si verifica facilmente per induzione. Se $n = 0$, $X_1 = g(Y) \subseteq X = X_0$ e $Y_1 = f(X) \subseteq Y = Y_0$. Consideriamo ora il passo induttivo $k + 1$. Per ipotesi induttiva $X_{k+1} \subseteq X_k$ e dunque $Y_{k+2} = f(X_{k+1}) \subseteq f(X_k) = Y_{k+1}$. Analogamente, dall'ipotesi $Y_{k+1} \subseteq Y_k$ segue che $X_{k+2} \subseteq X_{k+1}$.

¹³ Precisamente, si applica il Teorema di ricorsione numerabile considerando l'insieme $\mathcal{P}(C)$, l'elemento $\varphi(D) \in \mathcal{P}(C)$, e la funzione $g : \omega \times \mathcal{P}(C) \rightarrow \mathcal{P}(C)$ dove $g(n, X) = \varphi(X)$.

Partizioniamo gli insiemi X e Y considerando rispettivamente le “fette”

$$X_0 \setminus X_1; X_1 \setminus X_2; X_2 \setminus X_3; \dots; \tilde{X} = \bigcap_{n \in \mathbb{N}} X_n.$$

$$Y_0 \setminus Y_1; Y_1 \setminus Y_2; Y_2 \setminus Y_3; \dots; \tilde{Y} = \bigcap_{n \in \mathbb{N}} Y_n.$$

Visto che f è iniettiva, $f(\tilde{X}) = f(\bigcap_{n \in \omega} X_n) = \bigcap_{n \in \omega} f(X_n) = \bigcap_{n \in \omega} Y_{n+1} = \tilde{Y}$. Inoltre, usando l'iniettività di f e di g , si hanno le uguaglianze

$$f(X_n \setminus X_{n+1}) = f(X_n) \setminus f(X_{n+1}) = Y_{n+1} \setminus Y_{n+2}.$$

$$g(Y_n \setminus Y_{n+1}) = g(Y_n) \setminus g(Y_{n+1}) = X_{n+1} \setminus X_{n+2}.$$

Ne segue che per ogni n abbiamo le bigezioni:

$$f_n = f|_{X_n \setminus X_{n+1}} : X_n \setminus X_{n+1} \rightarrow Y_{n+1} \setminus Y_{n+2}$$

$$g_n = g|_{Y_n \setminus Y_{n+1}} : Y_n \setminus Y_{n+1} \rightarrow X_{n+1} \setminus X_{n+2}.$$

La bigezione cercata $\varphi : X \rightarrow Y$ si ottiene “rincollando” tutte le f_n con n pari e tutte le inverse g_n^{-1} con n dispari con la restrizione $f|_{\tilde{X}}$. Precisamente, poniamo:

$$\varphi(x) = \begin{cases} f_n(x) & \text{se } x \in X_n \setminus X_{n+1} \text{ con } n \text{ pari} \\ g_{n-1}^{-1}(x) & \text{se } x \in X_n \setminus X_{n+1} \text{ con } n \text{ dispari} \\ f(x) & \text{se } x \in \tilde{X}. \end{cases}$$

La verifica in dettaglio che la funzione φ definita sopra è effettivamente una bigezione tra X e Y è lasciata per esercizio. $\square$

L'aritmetica di Peano e gli insiemi numerici

1. Gli insiemi finiti

Grazie ai numeri naturali, si può usare la nozione di equipotenza per definire in modo rigoroso il concetto di insieme finito.

DEFINIZIONE 1.1. Un insieme A si dice *finito* se esiste un numero naturale n tale che $|A| = |n|$, cioè se esiste una bigezione $f : n \rightarrow A$ per qualche $n \in \omega$. Un insieme si dice *infinito* se non è finito.

Ci sono molte proprietà degli insiemi finiti che vengono usualmente assunte come evidenti. Qui di seguito, invece, le enunceremo esplicitamente e ne daremo una dimostrazione. Cominciamo col dimostrare che l'antico principio secondo il quale *il tutto è maggiore della parte* vale tra insiemi finiti. In particolare, seguirà che un sottoinsieme di un insieme finito è finito.

PROPOSIZIONE 1.2. Se $|B| = |n|$ è un insieme finito, e $A \subset B$ è un suo sottoinsieme proprio, allora $|A| = |m|$ per un opportuno $m < n$.

DIM. Prendiamo una bigezione $f : B \rightarrow n$. Chiaramente, se $A \subset B$ è un suo sottoinsieme proprio di A allora $X = f(A)$ è un sottoinsieme proprio di n , e $|A| = |f(A)|$. Per raggiungere la tesi, basta allora verificare che per ogni sottoinsieme proprio $X \subset n$ di un numero naturale n , esiste $m < n$ con $|X| = |m|$. Procediamo per induzione su n .

Quando $n = 0$, la proprietà è vera a vuoto perché $\emptyset$ non ha alcun sottoinsieme proprio. Supponiamo ora che $X \subset n + 1 = \{0, 1, \dots, n\}$, e distinguiamo due casi.

1) $n \notin X$. In questo caso $X \subseteq n = \{0, 1, \dots, n-1\}$. Se $X = n$, allora banalmente $|X| = |n|$ dove $n < n + 1$; se invece $X \subset n$ è un sottoinsieme proprio, dall'ipotesi induttiva segue che $|X| = |m|$ per qualche $m < n$, e dunque $m < n + 1$.

2) $n \in X$. In questo caso, $X' = X \setminus \{n\}$ è un sottoinsieme proprio di n e dunque, per ipotesi induttiva, $|X'| = |m|$ dove $m < n$. A questo punto, basta notare che da $|X'| = |m|$ segue che $|X| = |X' \cup \{n\}| = |m \cup \{m\}| = |m + 1|$, e inoltre $m < n \Rightarrow m + 1 < n + 1$, come voluto. $\square$

COROLLARIO 1.3. Sottoinsiemi di insiemi finiti sono insiemi finiti, e soprainsiemi di insiemi infiniti sono insiemi infiniti.

DIM. La prima proprietà segue direttamente dalla proposizione precedente. La seconda proprietà è la contro-nominale della prima; infatti se $A \subseteq B$, l'implicazione " B finito $\Rightarrow A$ finito" equivale all'implicazione " A non finito $\Rightarrow B$ non finito". $\square$

Un'importante strumento della combinatoria finita è il cosiddetto *principio dei cassetti*: "Se sono stati distribuiti n oggetti in m cassetti dove $m < n$, allora c'è un cassetto dove trovo almeno due oggetti". In termini più formali:

PROPOSIZIONE 1.4 (Principio dei cassetti). *Siano n, m numeri naturali. Se $n > m$ allora non esistono funzioni iniettive $f : n \rightarrow m$. Equivalentemente, se $|n| \leq |m|$ allora $n \leq m$.*

DIM. Mostriamo che vale l'implicazione $|n| \leq |m| \Rightarrow n \leq m$ procedendo per induzione su n . La base $n = 0$ è vera a vuoto, perché la tesi $0 \leq m$ è sempre vera.¹ Consideriamo ora il passo induttivo, e supponiamo che esista una funzione iniettiva $f : n + 1 \rightarrow m$. La restrizione $f|_n : n \rightarrow X$ dove $X = m \setminus \{f(n)\}$ è ancora iniettiva. Inoltre, visto che $X \subset m$ è un sottoinsieme proprio, per la Proposizione precedente esiste $k < m$ ed una bigezione $g : X \rightarrow k$. Ma allora la composizione $g \circ f|_n : n \rightarrow k$ è iniettiva e dunque, per l'ipotesi induttiva, $n \leq k < m$, e quindi $n + 1 \leq m$. $\square$

Come diretta conseguenza otteniamo la naturale proprietà che due numeri naturali sono equipotenti se e solo se sono uguali.

PROPOSIZIONE 1.5. *Due numeri naturali diversi non sono equipotenti.*

DIM. Se $n \neq m$, allora uno è maggiore dell'altro, ad esempio $n > m$. L'esistenza di una bigezione $g : n \rightarrow m$ contraddirebbe il principio dei cassetti. $\square$

COROLLARIO 1.6. Se A è un insieme finito e $B \subset A$ è un suo sottoinsieme proprio, allora $|A| \neq |B|$.

DIM. Sia $|A| = |n|$. Per la Proposizione 1.2, esiste $m < n$ con $|B| = |m|$ e quindi, per la proposizione precedente, $|A| = |n| \neq |m| = |B|$. $\square$

ESERCIZIO 1.7. Sia $f : A \rightarrow A$ una funzione dove A è un insieme finito. Senza usare l'assioma di scelta, dimostrare che le seguenti proprietà sono equivalenti:

- (1) f è iniettiva.
- (2) f è suriettiva.
- (3) f è biunivoca.

Per quanto visto sopra, la seguente definizione è ben posta.

DEFINIZIONE 1.8. Si dice *cardinalità* di un insieme finito A quell'unico numero naturale n tale che $|A| = |n|$. In tal caso scriviamo direttamente $|A| = n$.

Dunque prenderemo i numeri naturali come i *cardinali finiti*, cioè come i rappresentanti canonici delle classi di equipotenza di insiemi finiti. Definire i cardinali infiniti, cioè rappresentanti canonici delle classi di equipotenza di insiemi infiniti, sarà più complicato e richiederà lo sviluppo della teoria degli ordinali, che tratteremo più avanti.

La seguente nozione ha un'importanza storica, perché Dedekind la adottò come definizione di insieme infinito.

DEFINIZIONE 1.9. Un insieme A si dice *Dedekind-infinito* se è equipotente ad una sua parte propria, e si dice *Dedekind-finito* se non è Dedekind-infinito.

¹ Ricordiamo che un'implicazione $P \Rightarrow Q$ è vera quando l'ipotesi P è falsa (con Q qualunque); ed è vera quando la tesi Q è vera (con P qualunque).

PROPOSIZIONE 1.10. Se A è Dedekind-infinito allora A è infinito. Inoltre, assumendo (AC), vale anche il viceversa.²

DIM. Abbiamo già visto nel Corollario 1.6 che si ottiene direttamente che un insieme finito *non* può essere equipotente ad una sua parte propria. Viceversa, usando (AC), abbiamo dimostrato nel Teorema ?? che se A è infinito, allora esiste una funzione iniettiva $f : \mathbb{N} \rightarrow A$. La seguente funzione $g : A \rightarrow A \setminus \{f(1)\}$ è una bigezione tra A e una sua parte propria:

$$g(a) = \begin{cases} f(n+1) & \text{se } a = f(n) \text{ per qualche } n \in \mathbb{N} \\ a & \text{se } a \notin \text{imm}(f). \end{cases}$$

□

Come diretta conseguenza, dimostriamo finalmente l'esistenza di insiemi infiniti.

PROPOSIZIONE 1.11. *L'insieme ω dei numeri naturali è infinito.*

DIM. Basta notare che ω è Dedekind-infinito. Infatti, la funzione “successore” $S : n \mapsto n + 1$ è una bigezione tra ω e il suo sottoinsieme proprio $\omega \setminus \{0\}$. □

ESERCIZIO 1.12.

- (1) Se A e B sono finiti, allora anche $A \cap B$, $A \cup B$, $A \times B$, B^A e $\mathcal{P}(A)$ sono finiti;
- (2) Se R è una relazione (binaria) finita, allora anche il dominio $\text{dom}(R)$ e l'immagine $\text{imm}(R)$ sono finiti. In particolare, se $f : X \rightarrow Y$ è una funzione e X è finito, allora anche l'immagine $\text{imm}(f) = \{f(x) \mid x \in X\}$ è finita.

ESERCIZIO 1.13. Sia $\mathcal{F}$ una famiglia di insiemi. Allora:

- (1) Se $\mathcal{F}$ è una famiglia finita di insiemi finiti, allora anche l'unione $\bigcup_{F \in \mathcal{F}} F$ è un insieme finito.
- (2) Se $\mathcal{F}$ è infinita allora l'unione $\bigcup_{A \in \mathcal{F}} A$ è infinita.
- (3) Se per ogni $n \in \omega$ esiste $A \in \mathcal{F}$ con $|A| > n$, allora l'unione $\bigcup_{A \in \mathcal{F}} A$ è infinita.

Grazie al teorema di ricorsione, e all'assioma di scelta, possiamo finalmente dimostrare a partire dai nostri assiomi un'importante proprietà che già avevamo visto nella prima parte di teoria “ingenua” degli insiemi.

ESERCIZIO 1.14. (AC) Formalizzare nel dettaglio la dimostrazione del Teorema ??: “Se A è un insieme infinito, allora $|\mathbb{N}| \leq |A|$ ”.

² Se non si assume l'assioma di scelta, è consistente assumere l'esistenza di insiemi che non sono in bigezione con alcuna parte propria, e che allo stesso tempo non sono neanche in bigezione con alcun numero naturale.

2. Gli assiomi di Peano

Come abbiamo visto, l'insieme ω soddisfa il principio di induzione, e inoltre permette di formalizzare in modo rigoroso e soddisfacente la fondamentale nozione di finitezza. Vedremo di seguito che ω soddisfa anche le consuete proprietà algebriche che caratterizzano i numeri naturali. Per cominciare, definiremo le operazioni di *somma* e *prodotto*, facendo uso delle operazioni insiemistiche di unione disgiunta e di prodotto cartesiano.

Intuitivamente, il concetto di somma tra numeri naturali è strettamente collegato a quello di unione. Infatti, informalmente possiamo pensare alla somma $n + m$ come al numero di elementi dell'unione di un insieme avente n elementi con un insieme avente m elementi, purché siano disgiunti. Il prodotto $n \cdot m$ può essere pensato come la somma iterata $n + \dots + n$ di n con se stesso per m volte. Notiamo che un prodotto cartesiano $A \times B$ è in realtà una unione $A \times B = \bigcup_{b \in B} A \times \{b\}$ di tante copie disgiunte di A quanti sono gli elementi di B . Questo suggerisce di pensare al prodotto $n \cdot m$ di numeri naturali, come al numero di elementi di un prodotto cartesiano tra un insieme con n elementi ed uno con m elementi. Tutte queste intuizioni, sono formalizzate nella seguente

DEFINIZIONE 2.1. Se $n, m \in \omega$, poniamo:

- $n + m = |A \cup B|$ dove $|A| = n$, $|B| = m$, e $A \cap B = \emptyset$;
- $n \cdot m = |A \times B|$ dove $|A| = n$ e $|B| = m$.

Il fatto che la definizione data sopra è ben posta, segue da alcune proprietà. Anzitutto, unioni e prodotti cartesiani di insiemi finiti sono ancora insiemi finiti. Notiamo poi che per ogni $n, m \in \omega$, esistono sempre almeno due insiemi *disgiunti* A, B con $|A| = n$ e $|B| = m$. Non possiamo prendere direttamente m ed n , perché non sono disgiunti, ma il problema è facilmente risolvibile, ad esempio considerando $A = n$ e $B = m \times \{0\}$. Infine, occorre che le cardinalità $|A \cup B|$ e $|A \times B|$ non dipendano dalla particolare scelta degli insiemi A e B , ma solo dalle loro cardinalità, ma anche questa proprietà era già stata verificata nel primo capitolo.

Osserviamo che per ogni $n \in \omega$, la somma tra n ed 1 coincide con la cardinalità di $\hat{n} = n \cup \{n\}$ (si tratta infatti di un'unione disgiunta), e quindi la notazione $n + 1 = \hat{n}$ è coerente.

Il teorema di ricorsione numerabile garantisce che la seguente definizione è ben posta.

DEFINIZIONE 2.2. Per ogni $k \neq 0$, la *funzione esponenziale* con base k è definita ponendo:

$$\begin{cases} k^0 = 1 \\ k^{n+1} = k^n \cdot k. \end{cases}$$

ESERCIZIO 2.3. Per ogni $k \neq 0$, e per tutti gli $n, m \in \omega$, dimostrare che

- (1) $k^n \cdot k^m = k^{n+m}$.
- (2) $(k^n)^m = k^{n \cdot m}$.

ESERCIZIO 2.4. Dimostrare che se A è un insieme finito, allora $|\mathcal{P}(A)| = 2^{|A|}$.

Adesso che abbiamo definito l'insieme ω con le operazioni di somma e prodotto, vogliamo verificare che la struttura che ne risulta realizza in effetti tutte le proprietà che la comune intuizione attribuisce ai numeri naturali. Per formalizzare tali proprietà, considereremo la cosiddetta “aritmetica di Peano”, dal nome del matematico italiano che la introdusse nel 1889. Si tratta di una lista di assiomi che descrivono proprietà fondamentali della funzione successore $S(n) = n + 1$, delle operazioni di somma e prodotto, e che includono anche il principio di induzione. Gli assiomi di Peano hanno un contenuto intuitivo evidente, e tutte le fondamentali proprietà dei numeri naturali possono essere formalmente dimostrate a partire da essi. Per questo, il quadro assiomatico di Peano è universalmente adottato come il giusto riferimento per “definire” i numeri naturali.

DEFINIZIONE 2.5. Una struttura $(N, 0, S, +, \cdot)$ dove:

- N è un insieme;
- $0 \in N$ è un elemento fissato di N ;
- $S : N \rightarrow N$ è una funzione, detta *funzione successore*;
- $+$: $N \times N \rightarrow N$ è una funzione binaria, detta *somma*;
- $\cdot$: $N \times N \rightarrow N$ una funzione binaria, detta *prodotto*;

è un *sistema di numeri naturali* se soddisfa i seguenti *assiomi di Peano*:

(PA1) Tutti e soli i numeri diversi da zero sono successori.

$$\forall x (x \neq 0) \leftrightarrow (\exists y S(y) = x);$$

(PA2) La funzione successore è iniettiva.

$$\forall x, y (x \neq y) \rightarrow (S(x) \neq S(y));$$

(PA3) La somma $+$ soddisfa le seguenti proprietà:

$$(s1) \forall x x + 0 = x;$$

$$(s2) \forall x, y (x + S(y) = S(x + y)).$$

(PA4) Il prodotto $\cdot$ soddisfa le seguenti proprietà:

$$(p1) \forall x x \cdot 0 = 0;$$

$$(p2) \forall x, y (x \cdot S(y) = (x \cdot y) + x).$$

(PA5)₂ *Principio di induzione del secondo ordine.*

Sia A un sottoinsieme di N . Se $0 \in A$ ed A è chiuso per successore, cioè $\forall x (x \in A) \rightarrow (S(x) \in A)$, allora $A = N$.

Quella data sopra è l'assiomatizzazione di Peano al *secondo ordine* PA₂, che differisce da quella al *primo ordine* PA solo nella formulazione del principio di induzione. Precisamente, in PA si rimpiazza (PA5)₂ con il seguente schema di assiomi:

(PA5) *Principio di induzione del primo ordine.*

Sia $P(x)$ una proprietà espressa come formula nel linguaggio dell'aritmetica di Peano. Allora il seguente è un assioma:

$$(P(0) \wedge (\forall x P(x) \rightarrow P(S(x)))) \rightarrow \forall x P(x).$$

Osserviamo che l'induzione al primo ordine segue direttamente dall'induzione al secondo ordine: infatti, per ogni formula assegnata $P(x)$, basta considerare il corrispondente insieme $A = \{x \in N \mid P(x)\}$. Viceversa, non tutti i sottoinsiemi $A \subseteq N$ sono della forma $\{x \in N \mid P(x)\}$, come si può capire con un semplice ragionamento sulle cardinalità. Infatti, l'insieme N deve essere infinito visto che – in base

agli assiomi (PA1) e (PA2) – la funzione successore S è una bigezione tra N e il suo sottoinsieme proprio $N \setminus \{0\}$. Dunque i sottoinsiemi di N sono una quantità più che numerabile, mentre le possibili formule $P(x)$ nel linguaggio dell'aritmetica di Peano sono una quantità numerabile, perché le formule sono particolari stringhe finite formate usando una quantità finita di simboli.³ La conclusione è che l'induzione al secondo ordine è una proprietà strettamente più forte di quella al primo ordine. Abbiamo adottato qui l'assiomatizzazione più forte perché questa ci permetterà di dimostrare l'unicità dei modelli a meno di isomorfismi (vedi Teorema 2.10).

Come ulteriore distinzione, notiamo che l'induzione al secondo ordine (PA5)₂ *non* è formalizzabile usando formule del linguaggio dell'aritmetica; infatti non abbiamo simboli che denotino sottoinsiemi $A \subseteq N$; e *non* è ammissibile come formula la scrittura $\forall A \subseteq N \dots$. Viceversa, l'induzione al primo ordine (PA5) è formalizzabile usando infinite formule nel linguaggio dell'aritmetica, una per ogni fissata formula $\varphi(x)$; si tratta cioè di uno schema di assiomi, analogo all'assioma di separazione che abbiamo visto per la teoria degli insiemi ZFC.

A partire dagli assiomi di Peano si possono dimostrare ad una ad una tutte le proprietà che la pratica matematica attribuisce ai numeri naturali. A titolo di esempio, dimostriamo in dettaglio la proprietà commutativa.

PROPOSIZIONE 2.6. *La seguente proprietà è un teorema di PA:*

$$\forall x, y, z \quad x + y = y + x.$$

DIM. Per induzione su y , mostriamo che vale la seguente proprietà:

- $P(y)$: $\forall x \quad x + y = y + x$.

Cominciamo dimostrando il caso base:

- $P(0)$: $\forall x \quad x + 0 = 0 + x$.

Procediamo per induzione su x . Se $x = 0$, banalmente $0 + 0 = 0 + 0$. Al passo induttivo, notiamo che

$$S(x) + 0 \stackrel{(1)}{=} S(x) \stackrel{(2)}{=} S(x + 0) \stackrel{(3)}{=} S(0 + x) \stackrel{(4)}{=} 0 + S(x),$$

dove nelle uguaglianze (1), (2), (4) abbiamo usato l'assioma (PA3), e nell'uguaglianza (3) abbiamo usato l'ipotesi induttiva.

Adesso assumiamo $P(y)$ e dimostriamo che allora vale anche:

- $P(S(y))$: $\forall x \quad x + S(y) = S(y) + x$.

Anche in questo caso, procediamo per induzione su x . Quando $x = 0$, l'uguaglianza $0 + S(y) = S(y) + 0$ vale per la proprietà $P(0)$ vista sopra. Al passo induttivo, assumiamo che valga: " $x + S(y) = S(y) + x$ ". Allora abbiamo:

$$\begin{aligned} S(x) + S(y) &\stackrel{(1)}{=} S(S(x) + y) \stackrel{(2)}{=} S(y + S(x)) \stackrel{(3)}{=} S(S(y) + x) = \\ &\stackrel{(4)}{=} S(S(x) + y) \stackrel{(5)}{=} S(x + S(y)) \stackrel{(6)}{=} S(S(y) + x) \stackrel{(7)}{=} S(y) + S(x), \end{aligned}$$

dove nelle uguaglianze (1), (3), (5), (7) abbiamo usato l'assioma (PA3), nelle uguaglianze (2), (4) abbiamo usato la proprietà $P(y)$, e nell'uguaglianza (6) abbiamo usato l'ipotesi induttiva su x . $\square$

³ Le formule di PA vengono definite in modo analogo a come abbiamo definito le formule della teoria degli insiemi, considerando i simboli extra-logici $0, S, +, \cdot$ al posto del simbolo di appartenenza $\in$.

Altre proprietà fondamentali che seguono dagli assiomi di Peano sono raccolte nel seguente esercizio.

ESERCIZIO 2.7. Verificare che le seguenti proprietà sono teoremi di PA:⁴

- (1) Proprietà associativa della somma: $\forall x, y, z \quad x + (y + z) = (x + y) + z$;
- (2) Proprietà associativa del prodotto: $\forall x, y, z \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z$;
- (3) Proprietà commutativa del prodotto: $\forall x, y \quad x \cdot y = y \cdot x$;
- (4) Elemento neutro per il prodotto: $\forall x \quad x \cdot 1 = x$ dove $1 = S(0)$;
- (5) $\forall x \quad x + x = x \cdot 2$ dove $2 = S(S(0))$;
- (6) Proprietà distributiva: $\forall x, y, z \quad x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

L'ordinamento non è stato considerato nell'assiomatizzazione di Peano perché può essere definito a partire dalla somma, ponendo

$$x < y \iff \exists z \neq 0 \quad x + z = y.$$

Per induzione, si può poi verificare che quell'ordinamento ha le proprietà volute.

ESERCIZIO 2.8. Le seguenti proprietà sono teoremi di PA:

- La relazione $<$ definita sopra è un ordine totale;
- $\forall x, y, z \quad (x < y \Rightarrow x + z < y + z)$;
- $\forall x, y \quad \forall z \neq 0 \quad (x < y \Rightarrow x \cdot z < y \cdot z)$.

Non ci dilunghiamo qui sullo sviluppo dell'aritmetica di Peano, che pure è argomento di grande importanza in logica, perché ci condurrebbe fuori dagli scopi di questo corso. Mostriamo ora che l'insieme ω ci fornisce effettivamente un sistema di numeri naturali.

TEOREMA 2.9.

La struttura $(\omega, 0, S, +, \cdot)$ dove la funzione successore è definita da $S(n) = \hat{n} = n+1$, e le operazioni di somma e prodotto sono quelle della Definizione 2.1, soddisfa tutti gli assiomi dell'aritmetica di Peano al secondo ordine PA_2 .

DIM. (PA1) e (PA2) esprimono la proprietà che S è una bigezione tra ω e $\omega \setminus \{0\}$, e questo è stato già dimostrato.

(PA3). Per la (s1) basta notare che $|\emptyset| = 0$, e che se $|A| = n$, banalmente anche $|A \cup \emptyset| = |A| = n$. Prendiamo A, B tali che $|A| = |n|$, $|B| = |m|$, e $A \cap B = \emptyset$, e prendiamo $\star$ tale che $\star \notin A \cup B$ (ad esempio, otteniamo le proprietà richieste con $A = n$, $B = m \times \{0\}$, e $\star = \{\{\emptyset\}\}$).⁵ Abbiamo allora che:

$$n + S(m) = n + (m+1) = |A \cup (B \cup \{\star\})| = |(A \cup B) \cup \{\star\}| = (n+m)+1 = S(n+m),$$

e anche la (s2) è dimostrata.

(PA4). La (p1) segue dal fatto che per ogni A , il prodotto cartesiano $A \times \emptyset = \emptyset$. Per la (p2), notiamo che se $|A| = n$, $|B| = m$, e $\star \notin B$, allora $A \times B$ e $A \times \{\star\}$ sono disgiunti, e inoltre $|A \times \{\star\}| = |A| = n$. Dunque:

$$n \cdot S(m) = n \cdot (m+1) = |A \times (B \cup \{\star\})| = |(A \times B) \cup (A \times \{\star\})| = (n \cdot m) + n.$$

(PA5)₂ è la proprietà di induzione di ω , che abbiamo già dimostrato. $\square$

⁴ Cioè, si dimostrano a partire dagli assiomi dell'aritmetica di Peano al primo ordine.

⁵ Notiamo che invece $\{\{\emptyset\}\} = (0, 0) \in B$.

Per completare la discussione, resta da vedere il fondamentale teorema di unicità, secondo il quale tutti i sistemi di numeri che soddisfano gli assiomi di Peano al secondo ordine sono tra loro isomorfi. In altre parole, l'assiomatizzazione PA_2 “definisce” il sistema dei numeri naturali.

TEOREMA 2.10 (Unicità del sistema dei numeri naturali).

Ogni sistema $(N, 0', S', \oplus, \odot)$ che soddisfa gli assiomi di Peano PA_2 al secondo ordine è isomorfo a $(\omega, 0, S, +, \cdot)$, cioè esiste una funzione biunivoca $\Theta : \omega \rightarrow N$ tale che:

- (1) $\Theta(0) = 0'$;
- (2) $\forall n \in \omega \quad \Theta(S(n)) = S'(\Theta(n))$;
- (3) $\forall n, m \in \omega \quad \Theta(n + m) = \Theta(n) \oplus \Theta(m)$;
- (4) $\forall n, m \in \omega \quad \Theta(n \cdot m) = \Theta(n) \odot \Theta(m)$.

Dim. Grazie al teorema di ricorsione numerabile, esiste ed unica funzione $\Theta : \omega \rightarrow N$ tale che

$$\begin{cases} \Theta(0) = 0' \\ \Theta(n+1) = S'(\Theta(n)) \end{cases}$$

Le proprietà (1) e (2) valgono banalmente per la definizione di Θ . Dobbiamo vedere che Θ è biunivoca, e che soddisfa anche le proprietà (3) e (4).

Θ è suriettiva. Per dimostrare che l'immagine di Θ coincide con N , procediamo per induzione all'interno del sistema $(N, 0', S', \oplus, \odot)$. Intanto $0' = \Theta(0) \in \text{imm}(\Theta)$. Supponiamo ora che $x \in \text{imm}(\Theta)$, cioè che $x = \Theta(n)$ per un opportuno $n \in \omega$. Ma allora anche $S'(x) = S'(\Theta(n)) = \Theta(n+1) \in \text{imm}(\Theta)$.

Θ è iniettiva. Stavolta procediamo per induzione nel sistema $(\omega, 0, S, +, \cdot)$, e dimostriamo che la seguente “proprietà” vale per ogni $n \in \omega$:⁶

$$P(n) : \quad \forall m \quad \Theta(m) = \Theta(n) \Rightarrow m = n$$

Se $m \neq 0$ allora, in virtù dell'assioma (PA1) che vale in ω , sarà $m = m' + 1$ per un opportuno m' . In questo caso $\Theta(m) = \Theta(m' + 1) = S'(\Theta(m')) \neq 0' = \Theta(0)$, visto che (PA1) vale anche in N . Con questo abbiamo dimostrato che vale $P(0)$. Supponiamo ora vera $P(n)$, e supponiamo che $\Theta(m) = \Theta(n+1) = S'(\Theta(n))$. Chiaramente $m \neq 0$, altrimenti $\Theta(m) = \Theta(0) = 0' \neq S'(\Theta(n))$. Allora $m = m' + 1$ per un opportuno m' , e quindi $S'(\Theta(m')) = \Theta(m) = \Theta(n+1) = S'(\Theta(n))$. Dall'assioma (PA2) segue allora che $\Theta(m') = \Theta(n)$ e, applicando l'ipotesi induttiva, concludiamo che $m' = n$, da cui $m = n + 1$, come volevamo.

Occupiamoci ora della proprietà (3). Procediamo per induzione, e dimostriamo che la seguente “proprietà” vale per ogni $m \in \omega$:⁷

$$P(m) : \quad \forall n \quad \Theta(n + m) = \Theta(n) \oplus \Theta(m)$$

Il caso base $P(0)$ è una immediata applicazione della (s1) di (PA3); infatti $\Theta(n + 0) = \Theta(n) = \Theta(n) \oplus 0' = \Theta(n) \oplus \Theta(0)$. Per il caso successore, si usano

⁶ Notiamo che $P(n)$ non è una proprietà formalizzabile nel linguaggio dell'aritmetica di Peano, perché vi compare il parametro Θ . Più correttamente, avremmo dovuto considerare il corrispondente insieme $X = \{n \in \omega \mid \forall m \quad \Theta(m) = \Theta(n) \Rightarrow m = n\}$, che esiste per separazione, e dimostrare per induzione al secondo ordine che $X = \omega$.

⁷ Anche in questo caso valgono le considerazioni della nota precedente.

l'ipotesi induttiva, la definizione di Θ , e la (s2) di (PA3), che vale sia in ω che in N . Precisamente, si hanno le uguaglianze:

$$\begin{aligned}\Theta(n + (m + 1)) &= \Theta((n + m) + 1) = S'(\Theta(n + m)) = S'(\Theta(n) \oplus \Theta(m)) = \\ &= \Theta(n) \oplus S'(\Theta(m)) = \Theta(n) \oplus \Theta(m + 1).\end{aligned}$$

La proprietà (4) relativa al prodotto si dimostra in modo del tutto analogo alla proprietà (3), stavolta applicando l'assioma (PA4). $\square$

Da qui in avanti, per seguire l'uso comune, talvolta scriveremo $\mathbb{N}$ per denotare l'insieme $\omega \setminus \{0\}$ dei naturali positivi; e scriveremo $\mathbb{N}_0$ per denotare $\mathbb{N} \cup \{0\} = \omega$.

3. Gli interi e i razionali

Storicamente si è cercato di ricondurre i fondamentali insiemi numerici (interi, razionali, reali e complessi) al sistema dei numeri naturali, visto come una solida base alla quale riferirsi per evitare possibili contraddizioni ed errori. Cominciamo a sviluppare questo progetto *riduzionista*, considerando la seguente relazione $\sim$ sul prodotto cartesiano $\omega \times \omega$:

$$(a, b) \sim (c, d) \iff a + d = b + c.$$

L'idea intuitiva è quella di pensare alla coppia ordinata di numeri naturali (a, b) come al numero “ $a - b$ ”. Si può verificare facilmente che $\sim$ è una relazione di equivalenza. Diamo allora la:

DEFINIZIONE 3.1. Il sistema $(\mathbb{Z}, \leq, 0, +, \cdot)$ dei numeri interi è il sistema dove:

- $\mathbb{Z}$ è l'insieme quoziente $(\omega \times \omega) / \sim$;
- 0 è la classe di equivalenza $[(0, 0)]$;
- $[(a, b)] \leq [(c, d)] \iff a + d \leq b + c$;
- La *somma* tra elementi di $\mathbb{Z}$ è definita ponendo:

$$[(a, b)] + [(c, d)] = [(a + c, b + d)];$$

- Il *prodotto* tra elementi di $\mathbb{Z}$ è definito ponendo:

$$[(a, b)] \cdot [(c, d)] = [(a \cdot c + b \cdot d, a \cdot d + b \cdot c)].$$

Dobbiamo verificare che le definizioni date sopra sono ben poste, cioè non dipendono dai rappresentanti scelti nelle classi di equivalenza. Precisamente, occorre dimostrare che se $(a, b) \sim (a', b')$ e se $(c, d) \sim (c', d')$, allora:

- $a + d \leq b + c \iff a' + d' \leq b' + c'$;
- $(a + c, b + d) \sim (a' + c', b' + d')$;
- $(ac + bd, ad + bc) \sim (a'c' + b'd', a'd' + b'c')$.

Si tratta di verifiche dirette, che possono essere svolte come esercizio.

ESERCIZIO 3.2. Per ogni coppia ordinata $(a, b) \in \omega \times \omega$, si verifica una ed una sola delle seguenti due possibilità:

- $(a, b) \sim (0, 0)$;
- $(a, b) \sim (n, 0)$ per un unico naturale positivo $n \in \mathbb{N}$;
- $(a, b) \sim (0, m)$ per un unico naturale positivo $m \in \mathbb{N}$.

Nel primo caso, identifichiamo $[(a, b)] = [(0, 0)]$ con $0 \in \mathbb{N}_0$. Nel secondo caso, identifichiamo $[(a, b)] = [(n, 0)]$ con $n \in \mathbb{N}$, così da avere $\mathbb{N}_0 \subseteq \mathbb{Z}$. Infine, nel terzo caso, denotiamo l'elemento $[(a, b)] = [(0, m)] \in \mathbb{Z}$ con $-m$. In questo modo, ritroviamo la consueta scrittura adoperata per i numeri interi.

TEOREMA 3.3. *Il sistema dei numeri interi $(\mathbb{Z}, \leq, 0, 1, +, \cdot)$ è un anello ordinato discreto, la cui parte non-negativa è il sistema dei numeri naturali.*

Valgono la seguenti caratterizzazioni degli interi.

ESERCIZIO 3.4. A meno di isomorfismi, $(\mathbb{Z}, \leq, 0, 1, +, \cdot)$ è l'unico anello ordinato discreto dove tutti i sottoinsiemi non vuoti e limitati inferiormente hanno minimo.

ESERCIZIO 3.5. A meno di isomorfismi, $(\mathbb{Z}, 0, 1, +, \cdot)$ è l'unico anello con la proprietà universale: "Per ogni anello R con unità esiste un unico omomorfismo $\varphi: \mathbb{Z} \rightarrow R$ ".

La dimostrazione di questo teorema segue direttamente dalle definizioni, ed è lasciata per esercizio.

I numeri razionali sono introdotti in modo analogo agli interi. Precisamente si prende l'insieme $\mathbb{Z} \times \mathbb{N}$ delle coppie ordinate di interi la cui seconda componente è un intero positivo, e si considera la seguente relazione:

$$(a, b) \approx (c, d) \iff a \cdot d = b \cdot c.$$

Qui l'intuizione è quella di pensare ad una coppia ordinata (a, b) come al quoziente " a/b ". Si può facilmente verificare che $\approx$ è una relazione di equivalenza.

DEFINIZIONE 3.6. Il sistema $(\mathbb{Q}, \leq, 0, 1, +, \cdot)$ dei numeri razionali è il sistema dove:

- $\mathbb{Q}$ è l'insieme quoziente $(\mathbb{Z} \times \mathbb{N}) / \approx$;
- 0 è la classe di equivalenza $[(0, 1)]$;
- 1 è la classe di equivalenza $[(1, 1)]$;
- $[(a, b)] \leq [(c, d)] \iff a \cdot d \leq b \cdot c$;
- La *somma* tra elementi di $\mathbb{Q}$ è definita ponendo:

$$[(a, b)] + [(c, d)] = [(a \cdot d + b \cdot c, b \cdot d)];$$

- Il *prodotto* tra elementi di $\mathbb{Z}$ è definito ponendo:

$$[(a, b)] \cdot [(c, d)] = [(a \cdot c, b \cdot d)].$$

Anche in questo caso, è necessario dimostrare che le definizioni di sopra sono ben poste, cioè che se $(a, b) \approx (a', b')$ e se $(c, d) \approx (c', d')$, allora:

- $ad \leq bc \iff a'd' \leq b'c'$;
- $(ad + bc, bd) \approx (a'd' + b'c', b'd')$;
- $(ac + bd, ad + bc) \approx (a'c' + b'd', a'd' + b'c')$.

La verifica delle proprietà di sopra e la dimostrazione del seguente teorema, sono lasciate per esercizio.

TEOREMA 3.7. *Il sistema dei numeri razionali $(\mathbb{Q}, \leq, 0, 1, +, \cdot)$ è un campo ordinato.⁸ Inoltre:*

⁸ In linguaggio algebrico, $\mathbb{Q}$ è il campo delle frazioni dell'anello degli interi $\mathbb{Z}$.

- (1) $\mathbb{Q}$ è denso, cioè per ogni $q_1 < q_2$ esiste q con $q_1 < q < q_2$;
- (2) $\mathbb{Q}$ gode della “proprietà archimedeana”, cioè per ogni $0 < q_1 < q_2$ esiste $n \in \mathbb{N}$ con $q_1 \cdot n > q_2$.

4. I numeri reali

Dedichiamo questo paragrafo all'introduzione dei numeri reali $\mathbb{R}$, definiti a partire dall'insieme dei numeri razionali $\mathbb{Q}$. Successivamente, definiremo i numeri complessi $\mathbb{C}$ a partire da $\mathbb{R}$. Con questo ultimo passo, avremo così raggiunto l'obiettivo “riduzionista” che ci eravamo prefissati, cioè quello di definire tutti i fondamentali insiemi numerici a partire dal sistema dei numeri naturali.

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 fin qui. Infatti, le costruzioni coinvolte per le definizioni dei numeri interi e dei numeri razionali richiedevano soltanto l'uso di prodotti cartesiani e di loro quozienti rispetto ad opportune relazioni di equivalenza. Invece la costruzione dei reali richiederà un uso essenziale dell'*assioma delle parti*, che tra l'altro determinerà il salto di cardinalità dal numerabile al continuo.

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 4.1. 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*, cioè se $x' < x \in X$ allora anche $x' \in X$;
- (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 $\mathbb{Q}_q$ generato da un razionale $q \in \mathbb{Q}$, è un taglio di Dedekind:

$$\mathbb{Q}_q = \{q' \in \mathbb{Q} \mid q' < q\}.$$

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 $\sqrt{2}$.

ESERCIZIO 4.2. L'insieme $X = \{q \in \mathbb{Q} \mid (q \leq 0) \vee (q^2 < 2)\}$ è un taglio di Dedekind, ed inoltre $X \neq \mathbb{Q}_q$ per ogni $q \in \mathbb{Q}$.

ESERCIZIO 4.3. Sia X un taglio di Dedekind. Allora per ogni razionale $\varepsilon > 0$, esistono $x \in X$ e $y \notin X$ aventi distanza $y - x < \varepsilon$.

DEFINIZIONE 4.4. L'insieme dei *numeri reali* è l'insieme

$$\mathbb{R} = \{X \in \mathcal{P}(\mathbb{Q}) \mid X \text{ taglio di Dedekind}\}.$$

Identifichiamo ogni numero razionale $q \in \mathbb{Q}$ con il corrispondente taglio di Dedekind $\mathbb{Q}_q \in \mathbb{R}$, così da avere $\mathbb{Q} \subset \mathbb{R}$.

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 4.5.

- (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 $q \leq q' \Leftrightarrow \mathbb{Q}_q \leq \mathbb{Q}_{q'}$. Dunque, vista l'identificazione di ogni $q \in \mathbb{Q}$ con il corrispondente taglio di Dedekind $\mathbb{Q}_q \in \mathbb{R}$, $(\mathbb{Q}, \leq)$ è un sottoinsieme ordinato di $(\mathbb{R}, \leq)$;
- (3) $\mathbb{Q}$ è denso in $(\mathbb{R}, \leq)$, cioè per ogni $X, Y \in \mathbb{R}$ con $X < Y$, esiste $q \in \mathbb{Q}$ con $X < q < Y$;
- (4) $(\mathbb{R}, \leq)$ è completo, cioè ogni sottoinsieme non vuoto $A \subset \mathbb{R}$ che sia superiormente limitato, ammette estremo superiore:

$$\sup A = \min\{x \in \mathbb{R} \mid x > a \text{ per ogni } a \in A\}.$$

DIM. (1). La proprietà *riflessiva*, cioè " $X \subseteq X$ ", e la proprietà *simmetrica*, cioè " $(X \subseteq Y \wedge Y \subseteq X) \rightarrow X = Y$ " sono banalmente soddisfatte. Per verificare la proprietà *tricotomica*, supponiamo che $X \neq Y$ siano due tagli di Dedekind diversi; allora esiste un elemento che appartiene ad uno ma non all'altro, ad esempio un elemento $x_0 \in X$ con $x_0 \notin Y$ (se esiste $y_0 \in Y$ con $y_0 \notin X$ la dimostrazione è del tutto simile). Da $x_0 \notin Y$ segue che $x_0 > y$ per ogni $y \in Y$, visto che Y è un segmento iniziale; ma allora $Y \subset X$, visto che X è un segmento iniziale, ed abbiamo $X < Y$.

(2). Siano $q < q'$ due numeri razionali. Banalmente $\mathbb{Q}_q \subseteq \mathbb{Q}_{q'}$. Dobbiamo vedere che $\mathbb{Q}_q \neq \mathbb{Q}_{q'}$, e questo segue subito dalla densità di $(\mathbb{Q}, \leq)$. Infatti se prendiamo $\tilde{q}$ con $q < \tilde{q} < q'$, chiaramente $\tilde{q} \in \mathbb{Q}_{q'}$ mentre $\tilde{q} \notin \mathbb{Q}_q$. Il viceversa " $\mathbb{Q}_q < \mathbb{Q}_{q'} \Rightarrow q < q'$ " segue direttamente da quanto appena dimostrato (se per assurdo fosse $q \geq q'$, allora $\mathbb{Q}_{q'} \supseteq \mathbb{Q}_q$).

(3). Siano $X < Y$. Allora esiste $q \in Y \setminus X$. Osserviamo che non si può escludere che $X = \mathbb{Q}_q$. Per definizione di taglio di Dedekind, Y non ha massimo, dunque esiste $q' \in Y$ con $q < q'$. Così $q \in \mathbb{Q}_{q'} \setminus X$, e dunque $X < \mathbb{Q}_{q'}$. Inoltre da $q' \in Y$ segue subito che $\mathbb{Q}_{q'} < Y$.

(4). Sia $A \subset \mathbb{R}$ 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 $Y' \supseteq \bigcup_{X \in A} X = Y$.

Vediamo intanto Y è un sottoinsieme *non banale* di $\mathbb{Q}$. Per ipotesi $A \neq \emptyset$, dunque esiste un taglio di Dedekind $X \in A$ e quindi $\emptyset \neq X \subseteq Y$. Inoltre A è superiormente limitato, dunque esiste $Z \in \mathbb{R}$ con $X \subseteq Z$ per ogni $X \in A$, da cui $Y = \bigcup_{X \in A} X \subseteq Z \neq \mathbb{Q}$. Per vedere che Y è un segmento iniziale, consideriamo $y' < y$ dove $y \in Y$. Prendiamo $X \in A$ con $y \in X$. Poiché X è un taglio di Dedekind, da $y' < y \in X$ segue che $y' \in X \subseteq Y$, come voluto. Resta infine da controllare che Y non ha massimo. Se $y \in Y$, prendiamo $X \in A$ con $y \in X$. Allora esiste $y' \in X \subseteq Y$ con $y < y'$. $\square$

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 $(P, \leq)$ senza massimo né minimo, possiamo considerare l'insieme $\tilde{P}$ dei suoi tagli di Dedekind. Con gli stessi argomenti visti sopra, si dimostra che $(\tilde{P}, \subseteq)$ è un insieme ordinato completo senza massimo né minimo che ha (una copia di) P come sottoinsieme denso. Questo procedimento di *completamento* è unico a meno di isomorfismi. Precisamente, si può dimostrare che se $(P', \leq)$ è un insieme ordinato completo privo di massimo e minimo e avente $P \subseteq P'$ come sottoinsieme denso, allora esiste una bigezione $\Theta : P' \rightarrow \tilde{P}$ che preserva l'ordine: " $p_1 < p_2 \Leftrightarrow \Theta(p_1) < \Theta(p_2)$ ". In altre parole, a meno di cambiare i "nomi" agli elementi, $(\tilde{P}, \subseteq)$ e $(P', \leq)$ sono lo stesso insieme ordinato. Non dimostriamo qui questo teorema generale di unicità del completamento; il caso che ci interessa, cioè quello di $\mathbb{Q}$ ed $\mathbb{R}$, seguirà come corollario del teorema di unicità dei reali come campo ordinato completo che vedremo più avanti.

Il nostro obbiettivo adesso è quello di dare una struttura algebrica di campo all'insieme dei numeri reali. Cominciamo definendo l'operazione di *somma* tra tagli di Dedekind (di razionali):

$$X + Y = \{x + y \mid (x \in X) \wedge (y \in Y)\}.$$

ESERCIZIO 4.6.

- (1) Siano $a, x, y \in \mathbb{Q}$ tre numeri razionali con $a < x + y$. Allora $a = x' + y'$ per opportuni $x', y' \in \mathbb{Q}$ dove $x' < x$ e $y' < y$;
- (2) Se X, Y sono tagli di Dedekind, allora anche $X + Y$ è un taglio di Dedekind;
- (3) L'operazione di somma tra tagli di Dedekind è coerente con la somma tra razionali, cioè per ogni $q, q' \in \mathbb{Q}$ si ha $\mathbb{Q}_q + \mathbb{Q}_{q'} = \mathbb{Q}_{q+q'}$.

Chiaramente, la somma tra tagli è una operazione *commutativa e associativa*.

Occupiamoci ora dell'*opposto*. Per i tagli di Dedekind originati da razionali, poniamo $-(\mathbb{Q}_q) = \mathbb{Q}_{-q}$. Se invece X non è della forma $\mathbb{Q}_q$, cioè quando $\mathbb{Q} \setminus X$ non ha minimo, allora poniamo:

$$-X = \{q \in \mathbb{Q} \mid -q \notin X\}.$$

Denotiamo direttamente con 0 il taglio $\mathbb{Q}_0 = \{q \in \mathbb{Q} \mid q < 0\}$.

ESERCIZIO 4.7. Sia X un taglio di Dedekind. Allora:

- (1) $-X$ è un taglio di Dedekind;
- (2) $(X) + (-X) = 0$;
- (3) $X < 0$ se e solo se $-X > 0$.

Per definire il *prodotto*, consideriamo prima il caso di tagli positivi $X, Y > X_0$. In questo caso $X^+ = \{x \in X \mid x > 0\}$ e $Y^+ = \{y \in Y \mid y > 0\}$ sono non vuoti, e si pone:

$$X \cdot Y = \{x \cdot y \mid (x \in X^+) \wedge (y \in Y^+)\} \cup \{q \in \mathbb{Q} \mid q \leq 0\}.$$

ESERCIZIO 4.8. Siano $a, x, y \in \mathbb{Q}^+$ tre numeri razionali positivi con $a < x \cdot y$. Allora $a = x' \cdot y'$ per opportuni $x', y' \in \mathbb{Q}$ dove $0 < x' < x$ e $0 < y' < y$.

Utilizzando la proprietà di quest'ultimo esercizio, si verificano i seguenti risultati.

ESERCIZIO 4.9.

- (1) Se $X, Y > 0$ sono tagli di Dedekind positivi, allora anche $X \cdot Y$ è un taglio di Dedekind (positivo);
- (2) L'operazione di prodotto tra tagli di Dedekind positivi è coerente con il prodotto tra razionali, cioè per ogni $q, q' \in \mathbb{Q}^+$ si ha $\mathbb{Q}_q \cdot \mathbb{Q}_{q'} = \mathbb{Q}_{q \cdot q'}$.

Chiaramente, il prodotto sopra definito tra tagli positivi è una operazione *commutativa* e *associativa*. Il prodotto tra tagli qualunque è definito facendo uso dell'opposto. Precisamente:

- Se $X = 0$ o $Y = 0$, si pone: $X \cdot Y = Y \cdot X = 0$;
- Se $X > 0$ e $Y < 0$, si pone: $X \cdot Y = Y \cdot X = -(X \cdot (-Y))$;
- Se $X < 0$ e $Y < 0$, si pone: $X \cdot Y = (-X) \cdot (-Y)$.

Osserviamo che, per la (3) dell'Esercizio 4.7, le definizioni di sopra sono ben poste perché si riconducono al prodotto tra tagli di Dedekind positivi. Segue poi direttamente dall'esercizio precedente che anche il prodotto tra tagli qualunque è una operazione *commutativa* e *associativa*.

ESERCIZIO 4.10.

- (1) Vale la proprietà *distributiva*: $X \cdot (Y + Z) = X \cdot Y + X \cdot Z$;
- (2) Le operazioni di somma e prodotto tra tagli di Dedekind sono coerenti con l'ordinamento: $X \leq Y$ e $Z \geq 0 \Rightarrow X + Z \leq Y + Z$ e $X \cdot Z \leq Y \cdot Z$.

Proseguiamo definendo l'*inverso* di ogni taglio positivo $X > 0$.

Se $X = \mathbb{Q}_q$ è generato da un razionale $q > 0$, poniamo $1/\mathbb{Q}_q = \mathbb{Q}_{1/q}$. Se invece $X > 0$ non è della forma $\mathbb{Q}_q$, poniamo

$$1/X = \{1/q \mid q \notin X\}.$$

Si verifica facilmente che anche $1/X > 0$ è un taglio di Dedekind positivo. Per $X < 0$ negativi, poniamo $1/X = -(1/(-X))$.

ESERCIZIO 4.11. Per ogni $X \neq 0$, $X \cdot (1/X) = 1$ è il taglio generato da 1.

Abbiamo così finalmente introdotto tutta la struttura dei reali, che ricapitoliamo nella seguente

DEFINIZIONE 4.12. Il sistema dei *numeri reali* è il sistema $(\mathbb{R}, \leq, 0, 1, +, \cdot)$ dove:

- $\mathbb{R} = \{X \subset \mathbb{Q} \mid X \text{ è un taglio di Dedekind}\}$;
- $X \leq Y$ se e solo se $X \subseteq Y$;
- Ogni numero razionale $q \in \mathbb{Q}$ è identificato con il corrispondente taglio $X_q = \{q' \in \mathbb{Q} \mid q' < q\}$. In particolare $0 = X_0$ e $1 = X_1$;
- La somma e il prodotto tra tagli sono definiti come visto sopra.

Mettendo insieme i risultati presentati negli ultimi esercizi, si ottiene una dimostrazione del:

TEOREMA 4.13. *Il sistema dei numeri reali $(\mathbb{R}, \leq, 0, 1, +, \cdot)$ è un campo ordinato completo.*

Sia ora F un campo ordinato qualunque. Visto che il campo $\mathbb{Q}$ è generato da $\{0, 1\}$, esiste ed è unico omomorfismo di campi $\psi : \mathbb{Q} \rightarrow F$ tale che $\psi(0) = 0_F$ e $\psi(1) = 1_F$, dove 0_F e 1_F sono gli elementi neutri della somma e del prodotto di F , rispettivamente. Precisamente, se $n, m \in \mathbb{N}$ con $m > 0$, $\psi(\pm \frac{n}{m}) = \pm \frac{n_F}{m_F}$, dove $n_F = 1_F + \dots + 1_F$ è la somma iterata di 1_F con se stesso per n volte. Si può verificare facilmente che ψ è un omomorfismo iniettivo di campi ordinati.⁹ Visto che ψ determina un isomorfismo con la sua immagine $\mathbb{Q} \cong \psi(\mathbb{Q})$, possiamo assumere direttamente che $\mathbb{Q} \subseteq F$ sia un sottocampo ordinato di F .

Il prossimo teorema ci mostrerà che la proprietà di essere un campo ordinato completo caratterizza (a meno di isomorfismi) il sistema dei numeri reali.

TEOREMA 4.14 (Unicità dei reali).

Ogni campo ordinato completo è isomorfo al sistema dei numeri reali $(\mathbb{R}, \leq, 0, 1, +, \cdot)$.

DIM. Sia F un qualunque campo ordinato completo. Abbiamo visto sopra che si può direttamente assumere $\mathbb{Q} \subset F$. Per evitare confusioni, denotiamo con $\leq_F$ la relazione d'ordine su F , e con $\leq_R$ la relazione d'ordine su $\mathbb{R}$ data dall'inclusione tra tagli di Dedekind. Sui numeri razionali $q, q' \in \mathbb{Q}$ le due relazioni coincidono, e in questo caso scriveremo semplicemente $q < q'$. Denotiamo infine con $\sup_F$ l'estremo superiore calcolato in F .

Notiamo che se $X \in \mathbb{R}$ è un taglio di Dedekind, allora X è superiormente limitato anche in F . Risulta così ben definita la funzione:

$$\psi : \mathbb{R} \rightarrow F \quad \text{dove} \quad \psi(X) = \sup_F X.$$

La funzione ψ preserva l'ordine, ed è quindi iniettiva. Infatti se $X \subset Y$, per densità esiste $q \in \mathbb{Q}$ con $X <_R q <_R Y$, e dunque

$$\psi(X) = \sup_F X \leq q < \sup_F Y = \psi(Y).$$

Occupiamoci ora della suriettività, e prendiamo un generico $x \in F$. È facile verificare che l'insieme di razionali $F_x = \{q \in \mathbb{Q} \mid q <_F x\}$ è un taglio di Dedekind. Per la densità di $\mathbb{Q}$ in F , si ha $x = \sup_F F_x = \psi(F_x)$.

Resta da vedere che ψ è un omomorfismo di campi, cioè che per ogni $X, Y \in \mathbb{R}$, valgono le uguaglianze $\psi(X + Y) = \psi(X) + \psi(Y)$ e $\psi(X \cdot Y) = \psi(X) \cdot \psi(Y)$. Denotiamo con:

$$\xi = \psi(X) = \sup_F X, \quad \eta = \psi(Y) = \sup_F Y.$$

Se $x \in X$ e $y \in Y$, chiaramente $x < \xi$ e $y < \eta$, dunque $x + y < \xi + \eta$, e quindi

$$\psi(X + Y) = \sup_F \{x + y \mid (x \in X) \wedge (y \in Y)\} \leq \xi + \eta.$$

Fissiamo ora $a <_F \xi + \eta$. Per definizione di estremo superiore, esistono $x \in X$ e $y \in Y$ con $x >_F \xi - \varepsilon$ e $y >_F \eta - \varepsilon$, dove abbiamo preso $\varepsilon = \frac{\xi + \eta - a}{2} > 0$. Ma allora $x + y >_F \xi + \eta - 2\varepsilon = a$. Questo dimostra che

$$\psi(X + Y) = \sup_F \{x + y \mid (x \in X) \wedge (y \in Y)\} \geq \sup_F \{a \mid a <_F \xi + \eta\} = \xi + \eta.$$

⁹ Notiamo che il campo F ha necessariamente caratteristica zero perché è ordinato.

Con il prodotto la dimostrazione è analoga. Supponiamo prima che $X, Y > 0$. Una delle due disuguaglianze è banale:

$$\psi(X \cdot Y) = \sup_F \{x \cdot y \mid (x \in X^+) \wedge (y \in Y^+)\} \leq \xi \cdot \eta.$$

Fissiamo ora un elemento $a <_F \xi \cdot \eta$ positivo. Per densità, possiamo prendere un razionale q con $\frac{a}{\xi \cdot \eta} < q < 1$. Per la (1) dell'Esercizio 4.9, possiamo scrivere $q = q_1 q_2$ come prodotto di due razionali positivi $q_1, q_2 < 1$. Visto che $\xi \cdot q_1 < \xi$ e $\eta \cdot q_2 < \eta$, per definizione di estremo superiore, esistono $x \in X$ e $y \in Y$ tali che $x > \xi \cdot q_1$ e $y > \eta \cdot q_2$. Dunque abbiamo $x \cdot y > \xi \cdot \eta \cdot (q_1 q_2) > \xi \cdot \eta \cdot \frac{a}{\xi \cdot \eta} = a$. Possiamo così concludere che vale anche l'altra disuguaglianza:

$$\psi(X \cdot Y) = \sup_F \{x \cdot y \mid (x \in X) \wedge (y \in Y)\} \geq \sup_F \{a \mid a <_F \xi \cdot \eta\} = \xi \cdot \eta.$$

Infine, per il caso generale di tagli non necessariamente positivi, osserviamo che:

$$\psi(-X) = \sup_F \{q \in \mathbb{Q} \mid -q \notin X\} = -\inf_F \{q \in \mathbb{Q} \mid q \notin X\} = -\sup_F \{q \in \mathbb{Q} \mid q \in X\}.$$

Dunque $\psi(-X) = -\psi(X)$, e ci si può ricondurre al caso visto sopra di tagli positivi. $\square$

Ricordiamo l'importante proprietà archimedeana.

PROPOSIZIONE 4.15. Sia F un campo ordinato qualunque. Allora le seguenti condizioni sono equivalenti:

- (1) F soddisfa la *proprietà archimedeana*:
"Sia $x > 0$. Allora per ogni $\varepsilon > 0$ esiste $n \in \mathbb{N}$ tale che $n \cdot \varepsilon > x$ ".
- (2) $\mathbb{Q}$ è denso in F ;
- (3) Non esistono *infinitesimi* $\delta \neq 0$, cioè elementi $\delta \neq 0$ tali che $-1/n < \delta < 1/n$ per ogni $n \in \mathbb{N}^+$.
- (4) $\mathbb{N}$ è illimitato in F , cioè per ogni $x \in F$ esiste $n \in \mathbb{N}$ con $x < n$.

Inoltre, quando F è completo, tutte le condizioni di sopra sono verificate.

DIM. Per vedere l'equivalenza delle quattro condizioni, dimostriamo in sequenza le implicazioni $(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (1)$.

$(1) \Rightarrow (2)$. Siano $0 < x < y$ due elementi positivi di F . Per la proprietà archimedeana, esiste $m \in \mathbb{N}$ tale che $m \cdot 1 > \frac{1}{y-x}$, cioè $\frac{1}{m} < y - x$. Di nuovo per la proprietà archimedeana, l'insieme $A = \{n \in \mathbb{N} \mid n \cdot \frac{1}{m} > x\} \neq \emptyset$, e per il principio del buon ordinamento dei numeri naturali, esisterà $n = \min A$. Chiaramente $(n-1) \cdot \frac{1}{m} \notin A$, e quindi:

$$x < \frac{n}{m} = (n-1) \cdot \frac{1}{m} + \frac{1}{m} \leq x + \frac{1}{m} < x + (y-x) = y.$$

Dunque $\frac{n}{m}$ è la frazione cercata. Il caso $x < 0 < y$ è banale perché $0 \in \mathbb{Q}$. Infine, se $x < y < 0$, per il caso già dimostrato esiste $\frac{n}{m}$ con $0 < -y < \frac{n}{m} < -x$, e quindi $x < -\frac{n}{m} < y$.

$(2) \Rightarrow (3)$. Per assurdo sia $\delta \neq 0$ un infinitesimo. Possiamo supporre $\delta > 0$ (altrimenti prendiamo $-\delta$). Per ogni $n, m \in \mathbb{N}^+$ si ha $0 < \delta < \frac{n}{m}$, visto che $\delta < \frac{1}{m}$ per definizione di infinitesimo. Ne seguirebbe che $\mathbb{Q}$ non è denso in F .

(3) $\Rightarrow$ (4). Se $\mathbb{N}$ fosse limitato, esisterebbe $x \in F$ tale che $x > n$ per ogni $n \in \mathbb{N}$. Ma allora $\frac{1}{x}$ sarebbe un infinitesimo positivo.

(4) $\Rightarrow$ (1). Per ipotesi, esiste $n \in \mathbb{N}$ tale che $\frac{x}{\varepsilon} < n$, dunque $n \cdot \varepsilon > x$.

Per concludere la dimostrazione, basta vedere che se una delle quattro condizioni (equivalenti) di sopra *non* vale, allora F *non* è completo. Supponiamo dunque che (4) non valga, cioè che $\mathbb{N}$ sia limitato in F . È facile verificare che se x è un maggiorante di $\mathbb{N}$, allora anche $x - 1$ lo è. Dunque $\sup \mathbb{N}$ non esiste. $\square$

Un primo esempio di campo archimedeo (non completo) è il campo $\mathbb{Q}$ dei numeri razionali. Vediamo ora un esempio di campo non-archimedeo.

ESERCIZIO 4.16. Sia

$$\mathbb{Q}(x) = \left\{ \frac{A(x)}{B(x)} \mid A(x), B(x) \in \mathbb{Q}[x], B(x) \neq 0 \right\}$$

il campo delle frazioni dell'anello dei polinomi $\mathbb{Q}[x]$ a coefficienti razionali. Poniamo:

$$\frac{a_0 + a_1x + \dots + a_nx^n}{b_0 + b_1x + \dots + b_mx^m} \prec 0 \Leftrightarrow \frac{a_n}{b_m} < 0 \quad \text{e} \quad \frac{A(x)}{B(x)} \prec \frac{C(x)}{D(x)} \Leftrightarrow \frac{A(x)}{B(x)} - \frac{C(x)}{D(x)} \prec 0$$

Dimostrare che:

- (1) $(\mathbb{Q}(x), \preceq, 0, 1, +, \cdot)$ è un campo ordinato;
- (2) Tutti gli elementi $\frac{a_0 + a_1x + \dots + a_nx^n}{b_0 + b_1x + \dots + b_mx^m}$ dove $n < m$ sono infinitesimi.

ESERCIZIO 4.17. Il campo $\mathbb{Q}(x)$ (con l'ordine $\preceq$ definito sopra) è il più piccolo campo non-archimedeo, nel senso che ogni campo non-archimedeo ha un sotto-campo isomorfo a $\mathbb{Q}(x)$.

Concludiamo questo capitolo definendo i numeri complessi. I numeri interi e i numeri razionali sono stati definiti come opportuni insiemi quoziente di coppie ordinate. L'idea di considerare coppie ordinate viene usata anche per definire i numeri complessi a partire dai numeri reali. Precisamente, si dà la seguente

DEFINIZIONE 4.18. Il sistema $(\mathbb{C}, 0, 1, +, \cdot)$ dei *numeri complessi* è il sistema dove:

- $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ è l'insieme delle coppie ordinate di numeri reali;
- 0 è la coppia $(0, 0)$ e 1 è la coppia $(1, 0)$;
- La somma è definita ponendo: $(a, b) + (c, d) = (a + c, b + d)$;
- Il prodotto è definito ponendo: $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.

Nella pratica si introduce il simbolo i , detto *unità immaginaria*, e si usa la notazione $z = a + ib$ per indicare $z = (a, b) \in \mathbb{C}$. Il numero reale a , cioè la prima componente della coppia ordinata, viene chiamato *parte reale* di z , mentre il numero reale b , cioè la seconda componente, viene chiamato *parte immaginaria* di z . Coerentemente con la definizione di sopra, dati due numeri complessi $z = a + ib$ e $w = c + id$, la somma si calcola sommando le rispettive parti reali e immaginarie:

$$(a + ib) + (c + id) = (a + c) + i(b + d).$$

Per il prodotto, si procede come nei prodotti tra polinomi con incognita i , adottando la convenzione che $i^2 = -1$. Dunque:

$$(a + ib) \cdot (c + id) = ac + iad + ibc + i^2bd = (ac - bd) + i(ad + bc).$$

Identificando ogni numero reale $a \in \mathbb{R}$ con il numero complesso $(a, 0) = a + i \cdot 0$, il campo dei reali $\mathbb{R}$ risulta un sottocampo di $(\mathbb{C}, 0, 1, +, \cdot)$. Inoltre vale la seguente ben nota proprietà, per la quale rimandiamo ad un corso di algebra.

TEOREMA 4.19. *Il sistema dei numeri complessi $(\mathbb{C}, 0, 1, +, \cdot)$ è la chiusura algebrica del campo dei numeri reali.*

Buoni ordini e ordinali

1. Buoni ordini

Ci concentriamo ora sullo studio degli insiemi bene ordinati. Si tratta di un tipo speciale di insiemi ordinati che in un senso preciso generalizzano l'insieme dei numeri naturali. L'intuizione è questa: così come i numeri naturali si ottengono a partire dall'elemento minimo 0 applicando un numero finito di volte la funzione successore $S(n) = n + 1$, così gli elementi di un insieme bene ordinato si ottengono a partire dal suo elemento minimo, applicando un numero "transfinito" di volte la funzione successore.

Ad esempio, applicando infinite volte la funzione successore all'elemento 0, si può pensare di ottenere un nuovo elemento $\star$, che sta dopo tutti i numeri naturali (in un certo senso, $\star$ è il successore dell'insieme di tutti i numeri naturali). Se iteriamo poi l'applicazione della funzione successore anche a $\star$, si ottiene il seguente insieme *bene ordinato*:

$$0 < 1 < 2 < \dots < n + 1 < \dots < \star < \star + 1 < \dots < \star + n < \star + n + 1 < \dots$$

Possiamo poi andare avanti con questa procedura, ed ottenere un nuovo elemento $\star'$ che sta dopo tutti gli elementi di sopra, poi considerare $\star' + 1 < \star' + 2 < \dots$ e così via. L'intuizione è che in questo modo si ottengano (a meno di isomorfismo) tutti gli insiemi bene ordinati.

Come è evidente, le considerazioni fatte sopra sono del tutto informali; dobbiamo ora dare definizioni precise e rigorose che catturino quelle intuizioni. La proprietà fondamentale dei numeri naturali è l'*induzione* o, equivalentemente, il *principio del minimo*: "ogni sottoinsieme non vuoto di numeri naturali, ammette minimo". Useremo proprio quest'ultima proprietà per definire i bene ordinati.

DEFINIZIONE 1.1. Un insieme ordinato $(A, <)$ si dice *bene ordinato* se ogni suo sottoinsieme non vuoto ha minimo.

Osserviamo che gli insiemi ordinati introdotti informalmente sopra, sono in effetti bene ordinati.

Una prima immediata proprietà degli insiemi bene ordinati è che ogni elemento (tranne l'eventuale massimo) ha un successore immediato.

DEFINIZIONE 1.2. Sia $(A, <)$ un insieme bene ordinato, e sia $a \in A$. Se a non è il massimo di A , il *successore* di a è l'elemento $a^+ = \min\{a' \in A \mid a' > a\}$.

Quando ciò non determina confusione, il successore di un elemento a si denota anche scrivendo $a + 1$.

ESERCIZIO 1.3. Dimostrare che se $A \subseteq \mathbb{R}$ è bene ordinato con l'ordinamento indotto da $\mathbb{R}$, allora $|A| \leq \aleph_0$.

PROPOSIZIONE 1.4. Sia $(A, <)$ un insieme ordinato. Allora ogni sottoinsieme $X \subseteq A$ finito non vuoto ammette massimo e minimo.

DIM. Per induzione su $n = |X|$. Se $n = 1$ la tesi è banale. Al passo induttivo dove $|X| = n + 1$, prendiamo un elemento $a_0 \in X$. L'insieme $X' = X \setminus \{a_0\}$ ha cardinalità $|X'| = n$ e quindi, per ipotesi induttiva, esistono $m' = \min X'$ e $M' = \max X'$. È immediato che $m := \min\{m', a_0\}$ e $M' = \max\{M, a_0\}$ sono rispettivamente il minimo e il massimo di X . $\square$

COROLLARIO 1.5. *Ogni insieme ordinato $(A, <)$ dove il supporto A è finito è bene ordinato.*

DIM. Sia $X \subseteq A$ non vuoto. Notiamo che X è finito in quanto sottoinsieme di un insieme finito. Allora per la Proposizione precedente X ha un elemento minimo, come richiesto. $\square$

In particolare, tutti i numeri naturali $(n, \in)$ ordinati dall'appartenenza sono buoni ordini.

PROPOSIZIONE 1.6. *Sia $(A, <)$ un insieme ordinato finito. Allora $(A, <) \cong (n, \in)$ dove $n = |A|$.*

DIM. Procediamo per induzione su $n = |A|$. Se $n = 1$, la tesi è banale, quindi occupiamoci del passo induttivo quando $|A| = n + 1$. Visto che ogni insieme ordinato finito ha massimo, prendiamo $a = \max A$ e consideriamo $A' = A \setminus \{a\}$. Applicando l'ipotesi induttiva all'insieme A' che ha cardinalità n , abbiamo l'esistenza di un isomorfismo $\psi : (A', <) \rightarrow (n, \in)$. Se si estende ψ ponendo $\psi(a) = n$, si ottiene infine l'isomorfismo cercato tra $(A, <)$ e $(n + 1, \in)$. $\square$

Come immediata conseguenza, otteniamo il seguente

COROLLARIO 1.7. *Due insiemi ordinati $(A, <)$ e $(B, <)$ dove i supporti A e B sono insiemi finiti equipotenti, sono tra loro isomorfi: $(A, <) \cong (B, <)$.*

Come abbiamo visto dal principio del buon ordinamento, i numeri naturali ω sono il prototipo di insieme infinito bene ordinato. Viceversa, i numeri interi $\mathbb{Z}$, i numeri razionali $\mathbb{Q}$, e i numeri reali $\mathbb{R}$ non sono bene ordinati (ad esempio non hanno minimo).

Un'utile caratterizzazione della proprietà di buon ordinamento è la seguente.

PROPOSIZIONE 1.8. *(AC) Un insieme ordinato $(A, <)$ è bene ordinato se e solo se non esistono catene discendenti*

$$a_0 > a_1 > \dots > a_n > a_{n+1} > \dots$$

DIM. Una implicazione è immediata perché chiaramente una catena discendente è un esempio di insieme non vuoto privo di minimo.

Per l'implicazione inversa occorre l'assioma di scelta. Supponiamo che A non sia bene ordinato, e sia $X \subseteq A$ un suo sottoinsieme non vuoto privo di minimo. Fissiamo una funzione di scelta f su X , e definiamo una catena discendente per ricorsione numerabile in questo modo:

$$\begin{cases} a_0 = f(X) \\ a_{n+1} = f(\{x \in X \mid x < a_n\}) \end{cases}$$

La definizione data è ben posta. Infatti, visto che X non ha minimo, per ogni n l'insieme $\{x \in X \mid x < a_n\}$ è non vuoto. $\square$

DEFINIZIONE 1.9. Un sottoinsieme S di un insieme ordinato A si dice *segmento iniziale* se è “chiuso verso il basso”, cioè se $x < s \in S \Rightarrow x \in S$. Il *segmento iniziale generato* da un elemento $a \in A$ è il segmento

$$A_a = \{x \in A \mid x < a\}.$$

Anche l'insieme vuoto è considerato un segmento iniziale; e notiamo che $\emptyset = A_a$ è generato da un elemento a se e solo se $a = \min A$.

Chiaramente se $(A, <)$ è bene ordinato, per ogni $a \in A$ anche $(A_a, <)$ è bene ordinato, con la relazione indotta da quella di A .

Per quanto sia banale, è bene tenere a mente che se $a' < a$ sono elementi di A , allora il segmento iniziale di $(A_a, <)$ determinato da a' coincide con il segmento iniziale di A determinato da a' , cioè: $(A_a)_{a'} = A_{a'}$.

Vale la seguente caratterizzazione.

PROPOSIZIONE 1.10. *Un insieme ordinato $(A, <)$ è bene ordinato se e solo se ogni segmento iniziale $S \neq A$ è generato da un elemento $a \in A$, cioè $S = A_a$ per un opportuno $a \in A$.¹*

DIM. Visto che $S \neq A$, l'insieme $A \setminus S$ non è vuoto, e quindi ammetterà elemento minimo $a = \min(A \setminus S)$. Se $x < a$, allora $x \notin (A \setminus S)$, cioè $x \in S$. Se $x \geq a$ allora $x \notin S$, altrimenti, per la proprietà di segmento iniziale, si avrebbe che anche $a \in S$. Abbiamo così verificato che $S = A_a$.

Viceversa, dato $X \subseteq A$ non vuoto, consideriamo l'insieme dei suoi minoranti stretti $S = \{a \in A \mid \forall x \in X (a < x)\}$. Notiamo che se $a' < a \in S$, allora $x < a$ per ogni $x \in X$, quindi anche $a' < x$ per ogni $x \in X$, e perciò $a' \in S$; questo mostra che S è un segmento iniziale. Inoltre, se $x \in X$ allora $x \notin S$, visto che $x \not< x$; quindi $S \neq A$ visto che $X \neq \emptyset$. Possiamo allora applicare l'ipotesi per ottenere l'esistenza di un elemento $\bar{a}$ che genera S , cioè $S = A_{\bar{a}}$. Verifichiamo che $\bar{a} = \min X$. Notiamo che gli elementi più piccoli di $\bar{a}$ non appartengono ad X , visto che sono elementi di S . Quindi $\bar{a} \leq x$ per ogni $x \in X$. Inoltre non è possibile che valga la disuguaglianza stretta $\bar{a} < x$ per ogni $x \in X$, altrimenti avremmo che $\bar{a} \in S = A_{\bar{a}}$. Quindi $\bar{a} = x$ per un opportuno $x \in X$, cioè $\bar{a} \in X$. $\square$

ESERCIZIO 1.11. Sia $(A, <)$ un insieme ordinato. Dimostrare che esiste un insieme $\mathfrak{A} \subseteq \mathcal{P}(A)$ tale che $(A, <) \cong (\mathfrak{A}, \subsetneq)$.

Come abbiamo visto nel Capitolo 1, una catena di insiemi totalmente ordinati è ancora un insieme totalmente ordinato (Proposizione ??). La stessa proprietà *non* si estende ai buoni ordini.

ESEMPIO 1.12. Per ogni $k \in \mathbb{Z}$, l'insieme $[k, +\infty)_{\mathbb{Z}} = \{x \in \mathbb{Z} \mid x \geq k\}$ è un sottoinsieme bene ordinato di $\mathbb{Z}$ (è infatti isomorfo ad ω). L'unione della catena di buoni ordini $\mathcal{F} = \{[k, +\infty)_{\mathbb{Z}} \mid k \in \mathbb{Z}\}$ è $(\mathbb{Z}, <)$, che *non* è bene ordinato.

Tuttavia, con un'opportuna ipotesi più forte, anche la proprietà di buon ordinamento si conserva passando all'unione.

¹ Per questa caratterizzazione, è essenziale aver incluso l'insieme vuoto tra i possibili segmenti iniziali $S \neq A$. Ad esempio, $(\mathbb{Z}, <)$ non è bene ordinato ma ogni suo segmento iniziale *non vuoto* $S \neq \mathbb{Z}$ è generato da un elemento. La stessa proprietà vale per i reali $(\mathbb{R}, <)$, e più in generale per ogni insieme ordinato *completo*, se ci limitiamo ai segmenti $S \neq \mathbb{R}$ privi di massimo; in questo caso infatti $S = \mathbb{R}_r$ dove $r = \sup S$.

PROPOSIZIONE 1.13. *Sia $\mathcal{F}$ una catena di insiemi bene ordinati. Se gli elementi di $\mathcal{F}$ sono uno segmento iniziale dell'altro, cioè se per ogni $(A, <_A), (B, <_B) \in \mathcal{F}$, si ha che $(A, <_A)$ è un segmento iniziale di $(B, <_B)$ o viceversa, allora l'unione è un insieme bene ordinato.*

DIM. Sia $(X, <)$ l'insieme ordinato ottenuto come unione di $\mathcal{F}$, e sia $Y \subseteq X$ un suo sottoinsieme non vuoto. Fissiamo un elemento $y_0 \in Y$, e sia $(A, <_A) \in \mathcal{F}$ tale che $y_0 \in A$. Se $y_0 = \min Y$ abbiamo finito. Altrimenti, per ogni $x < y_0$, prendiamo $(B, <_B) \in \mathcal{F}$ con $x \in B$. Dall'ipotesi sappiamo che $(A, <_A)$ è un segmento iniziale di $(B, <_B)$ o viceversa; in ogni caso segue che anche $x \in A$. Dunque $X_{y_0} = \{x \in X \mid x < y_0\} \subseteq A$, e quindi anche $Y' = \{y \in Y \mid y < y_0\} \subseteq A$. Concludiamo la dimostrazione osservando che il minimo di Y in $(X, <)$ coincide con il minimo di Y' in $(A, <_A)$. $\square$

Cominciamo a vedere le prime proprietà degli insiemi bene ordinati. Una semplice ma utile osservazione è la seguente.

PROPOSIZIONE 1.14. *Sia $(A, <)$ un insieme bene ordinato. Se $\varphi : A \rightarrow A$ preserva l'ordine, cioè se $a < a' \Rightarrow \varphi(a) < \varphi(a')$, allora φ è non decrescente, cioè $\varphi(a) \geq a$ per ogni $a \in A$.*

DIM. Se per assurdo la tesi fosse falsa, esisterebbe $x = \min\{a \in A \mid \varphi(a) < a\}$. Ma allora $\varphi(x) < x \Rightarrow \varphi(\varphi(x)) < \varphi(x)$ e quindi $\varphi(x) \in \{a \in A \mid \varphi(a) < a\}$, contro la minimalità di x . $\square$

Come immediate conseguenze, otteniamo le seguenti proprietà:

PROPOSIZIONE 1.15. *Sia $(A, <)$ un insieme bene ordinato.*

- (1) *A non è isomorfo ad alcun suo segmento iniziale proprio, cioè $A_a \not\cong A$ per ogni $a \in A$;*
- (2) *Segmenti iniziali propri diversi non sono isomorfi, cioè $a \neq a' \Rightarrow A_a \not\cong A_{a'}$;*
- (3) *L'unico automorfismo $\varphi : A \rightarrow A$ è l'identità.*

DIM. (1) Non possono esistere funzioni $\varphi : A \rightarrow A_a$ che preservano l'ordine, perché si avrebbe $\varphi(a) \in A_a$, cioè $\varphi(a) < a$, contro la Proposizione 1.14.

(2) Basta notare che se $a' < a$ allora $A_{a'}$ è un segmento iniziale dell'insieme bene ordinato A_a , ed applicare la (1).

(3) Sia $\varphi : A \rightarrow A$ una funzione che preserva l'ordine. Dimostriamo che se φ è diversa dall'identità, allora non è un isomorfismo. A questo scopo, prendiamo $x = \min\{a \in A \mid \varphi(a) \neq a\}$. Se $a < x$, chiaramente $\varphi(a) = a < x$. Se $a > x$, per la Proposizione 1.14 si ha $\varphi(a) \geq a > x$. Visto che anche $\varphi(x) \neq x$, si conclude che x non appartiene all'immagine di φ , che quindi non può essere un isomorfismo.

Un modo equivalente, e più breve, per dimostrare questa proprietà è il seguente. Se $\varphi : A \rightarrow A$ è un isomorfismo, allora anche l'inversa $\varphi^{-1} : A \rightarrow A$ è un isomorfismo. Usando la Proposizione 1.14, sappiamo che per ogni $a \in A$ si ha $\varphi(a) \geq a$, e quindi $a = \varphi^{-1}(\varphi(a)) \geq \varphi(a) \geq a$, da cui $\varphi(a) = a$. $\square$

ESERCIZIO 1.16. Dati due insiemi bene ordinati $(A, <)$ e $(B, <)$, esiste al più un isomorfismo $\varphi : A \rightarrow B$.

Per quanto molto semplice, il prossimo risultato è importante e sarà usato ripetutamente nel seguito.

PROPOSIZIONE 1.17. *Sia $\varphi : (A, <) \rightarrow (B, <)$ un isomorfismo tra insiemi ordinati. Allora per ogni $a \in A$, la restrizione $\varphi|_{A_a} : A_a \rightarrow B_{\varphi(a)}$ è un isomorfismo tra il segmento iniziale di A generato da a , e il segmento iniziale di B generato da $\varphi(a)$.*

DIM. Visto che φ preserva l'ordine, certamente $\varphi[A_a] \subseteq B_{\varphi(a)}$. Resta da vedere che vale anche l'altra inclusione $B_{\varphi(a)} \subseteq \varphi[A_a]$. Sia $b < \varphi(a)$; per la suriettività di φ esiste $a' \in A$ con $\varphi(a') = b$. Deve essere $a' < a$, perché φ preserva l'ordine. $\square$

Una proprietà fondamentale degli insiemi bene ordinati è che sono sempre “confrontabili”, cioè (a meno di isomorfismi) sono sempre uno segmento iniziale dell'altro.

TEOREMA 1.18 (Tricotomia degli insiemi bene ordinati).

Siano $(A, <)$ e $(B, <)$ due insiemi bene ordinati. Allora vale una ed una sola delle seguenti tre possibilità:

- (1) $A \cong B$;
- (2) $A \cong B_b$ per un opportuno $b \in B$;
- (3) $B \cong A_a$ per un opportuno $a \in A$.

DIM. Vediamo anzitutto che può verificarsi al più una delle tre possibilità di sopra. Se valessero sia la (1) che la (2), B sarebbe isomorfo ad un suo segmento proprio B_b , contro la Proposizione 1.15. Analogamente, da (1) e (3) seguirebbe l'assurdo $A \cong A_a$. Supponiamo infine che valgano (2) e (3) e sia $\psi : B \rightarrow A_a$ un isomorfismo. La restrizione $\psi|_{B_b}$ è un isomorfismo tra B_b e $A_{a'}$, dove $a' = \psi(b)$. Ma allora si otterrebbe l'assurdo che $A \cong A_{a'}$.

Sia ora $\Gamma = \{(a, b) \in A \times B \mid A_a \cong B_b\}$. Le coppie di Γ formeranno (il grafico di) una funzione, che ci darà l'isomorfismo cercato. Notiamo che se $0_A = \min A$ e $0_B = \min B$, allora $(0_A, 0_B) \in \Gamma$, perché entrambi i corrispondenti segmenti iniziali sono vuoti, dunque banalmente isomorfi. Se 1_A è il successore di 0_A e 1_B è il successore di 0_B , allora anche $(1_A, 1_B) \in \Gamma$, perché i corrispondenti segmenti iniziali sono rispettivamente $\{0_A\}$ e $\{0_B\}$; e così via. Vogliamo dimostrare che in questo modo si ottiene una funzione $0_A \mapsto 0_B$, $1_A \mapsto 1_B$ ecc., che è l'isomorfismo cercato.

Se $(a, b), (a, b') \in \Gamma$, cioè se $A_a \cong B_b$ e $A_a \cong B_{b'}$, allora $B_b \cong B_{b'}$, e quindi $b = b'$ per la Proposizione 1.15. Questo dimostra che Γ è effettivamente una funzione. Possiamo dunque usare la consueta notazione $\Gamma(a)$ per indicare quell'unico elemento b tale che $(a, b) \in \Gamma$.

Supponiamo ora che $\Gamma(a) = b$ e sia $\varphi : A_a \rightarrow B_{\Gamma(a)}$ un isomorfismo. Se $a' < a$, la restrizione $\varphi|_{A_{a'}} : A_{a'} \rightarrow B_{\varphi(a')}$ è ancora un isomorfismo, e perciò anche $a' \in \text{dom}(\Gamma)$ e inoltre $\Gamma(a') = \varphi(a') < b$. Questo dimostra che $\text{dom}(\Gamma)$ è un segmento iniziale di A (eventualmente coincidente con tutto A), e che Γ preserva l'ordine. Se $b' < b$, allora la restrizione $\varphi|_{A_{a'}} : A_{a'} \rightarrow B_{b'}$ è un isomorfismo, dove a' è l'elemento tale che $\varphi(a') = b'$. Dunque $\Gamma(a') = b'$, e resta verificato che $\text{imm}(\Gamma)$ è un segmento di B .

Per quanto dimostrato sopra, la funzione $\Gamma : A' \rightarrow B'$ è un isomorfismo tra un segmento iniziale $A' = \text{dom}(\Gamma)$ di A ed un segmento iniziale $B' = \text{imm}(\Gamma)$ di B . Notiamo che non può accadere che $A' = A_a$ e $B' = B_b$ siano entrambi segmenti propri. Infatti, se così fosse, $\Gamma : A_a \cong B_b$ sarebbe un isomorfismo, dunque $(a, b) \in \Gamma$,

e si avrebbe $a \in \text{dom}(\Gamma) = A_a$ e $b \in \text{imm}(\Gamma) = B_b$, il che è assurdo. Restano così le tre possibilità elencate nell'enunciato del teorema, cioè:

- (1) $A' = A$ e $B' = B$, dunque $\Gamma : A \cong B$.
- (2) $A' = A$ e $B' = B_b$ è un segmento iniziale proprio, dunque $\Gamma : A \cong B_b$.
- (3) $A' = A_a$ è un segmento iniziale proprio e $B' = B$, dunque $\Gamma : A_a \cong B$.

□

In conseguenza della tricotomia, possiamo dare una relazione d'ordine tra *tipi d'ordine* ("order types") degli insiemi bene ordinati.

NOTAZIONE 1.19. Siano A e B insiemi bene ordinati. Scriviamo:

- $\text{ot}(A) = \text{ot}(B)$ quando $A \cong B$;
- $\text{ot}(A) < \text{ot}(B)$ quando $A \cong B_b$ per qualche $b \in B$;
- $\text{ot}(A) \leq \text{ot}(B)$ quando $\text{ot}(A) = \text{ot}(B)$ oppure $\text{ot}(A) < \text{ot}(B)$.

È immediato verificare questa relazione " $\leq$ " tra tipi di buon ordine soddisfa le proprietà riflessiva, simmetrica e transitiva, oltre alla tricotomia. Dunque, abbiamo una relazione d'ordine totale tra le classi di isomorfismo (cioè tra i tipi d'ordine) degli insiemi bene ordinati. Inoltre, vale anche la proprietà di buon ordinamento.

PROPOSIZIONE 1.20. *Sia $\mathcal{F}$ una famiglia non vuota di insiemi bene ordinati. Allora esiste $A \in \mathcal{F}$ che ha tipo d'ordine minimo, cioè tale che $\text{ot}(A) \leq \text{ot}(B)$ per ogni $B \in \mathcal{F}$.*

DIM. Fisso un generico elemento $X \in \mathcal{F}$. Se $\text{ot}(X) \leq \text{ot}(B)$ per ogni $B \in \mathcal{F}$, ho già quanto voluto. Altrimenti, per ogni $B \in \mathcal{F}$ non isomorfo a X , esiste un unico elemento $x_B \in X$ tale che $B \cong X_{x_B}$. Prendo $x_A \in X$ il minimo tra tutti gli elementi x_B al variare di $B \neq X$. Segue direttamente dalla definizione che il corrispondente $A \in \mathcal{F}$ è l'insieme con tipo d'ordine minimo che cercavamo. □

PROPOSIZIONE 1.21. *Sia A bene ordinato. Se $B \subseteq A$ allora $\text{ot}(B) \leq \text{ot}(A)$.*

DIM. Se per assurdo fosse $\text{ot}(B) > \text{ot}(A)$, allora esisterebbe un isomorfismo $\psi : A \rightarrow B_b$ per un opportuno $b \in B$. Visto che ψ è una funzione definita su A a valori in A che preserva l'ordine, si avrebbe $\psi(b) \geq b \notin B_b$, una contraddizione. □

Attenzione! Può accadere che sottoinsiemi propri abbiano lo stesso tipo d'ordine di tutto l'insieme. Ad esempio i numeri pari $\{2n \mid n \in \omega\} \subset \omega$ sono un sottoinsieme proprio di ω che è isomorfo ad ω .

ESERCIZIO 1.22. (AC) Sia $(A, <)$ un insieme ordinato infinito. Dimostrare che sono proprietà equivalenti:

- (1) $(A, <) \cong (\omega, \in)$;
- (2) Ogni segmento iniziale di A è finito;
- (3) Ogni sottoinsieme infinito di A è privo di massimo.

Abbiamo già visto che ogni tipo di buon ordine finito ha un rappresentante canonico, cioè il numero naturale dato dalla sua cardinalità (vedi Proposizione 1.6). È poi immediato verificare che $\text{ot}(n) < \text{ot}(m)$ se e solo se $n < m$. Tra gli insiemi bene ordinati infiniti, il tipo d'ordine più piccolo è quello dell'insieme dei numeri naturali.

PROPOSIZIONE 1.23. $ot(\omega)$ è il più piccolo tipo di buon ordine infinito.

DIM. Se per assurdo $(A, <)$ fosse un buon ordine infinito con $ot(A) < ot(\omega)$, allora A sarebbe isomorfo ad un segmento iniziale proprio di ω . Questo non è possibile perché i segmenti iniziali propri di ω sono tutti finiti (sono i numeri naturali n). Per la tricotomia, segue allora che $ot(\omega) \leq ot(A)$, come volevamo. $\square$

2. Somma, prodotto ed esponenziazione di buoni ordini

In questo paragrafo vedremo tre operazioni fondamentali che si possono definire tra insiemi ordinati, e cioè la somma, il prodotto, e l'esponenziazione.

Assegnati due insiemi ordinati, il modo più naturale di combinarli ed ottenerne uno nuovo è quello di disporre in fila tutti gli elementi del primo insieme, seguiti da tutti gli elementi del secondo insieme. Strettamente parlando, questo tipo di operazione presuppone che i due insiemi siano disgiunti, ma con un semplice trucco possiamo estenderla anche al caso generale.

DEFINIZIONE 2.1. L'unione disgiunta $A \sqcup B$ di due insiemi A e B è definita ponendo

$$A \sqcup B = (A \times \{0\}) \cup (B \times \{1\}) = \{(a, 0) \mid a \in A\} \cup \{(b, 1) \mid b \in B\}$$

Dunque $A \sqcup B$ è l'insieme ottenuto “attaccando” ad ogni elemento $a \in A$ l'etichetta 0, e “attaccando” ad ogni elemento $b \in B$ l'etichetta 1, così da ottenere copie disgiunte di A e di B . Per semplicità, nel caso in cui A e B siano già insiemi disgiunti, nella definizione di sopra identificheremo A con $A \times \{0\}$ e B con $B \times \{1\}$, in modo da avere $A \sqcup B = A \cup B$.

DEFINIZIONE 2.2. La somma $A + B$ di due insiemi ordinati $(A, <_A)$ e $(B, <_B)$ è l'insieme ordinato $(A \sqcup B, <)$ dove l'ordine è definito ponendo:

- $(a, 0) < (a', 0) \Leftrightarrow a <_A a'$ per ogni $a, a' \in A$,
- $(b, 1) < (b', 1) \Leftrightarrow b <_B b'$ per ogni $b, b' \in B$,
- $(a, 0) < (b, 1)$ per ogni $a \in A$ e $b \in B$.

È immediato verificare che $(A + B, <)$ è in effetti un ordine totale. Inoltre:

PROPOSIZIONE 2.3. Siano A e B insiemi ordinati. Allora $A + B$ è bene ordinato se e solo se sia A che B sono bene ordinati.

DIM. Supponiamo prima che $A + B$ sia bene ordinato. Dato un sottoinsieme $X \subseteq A$ non vuoto, se $(a, 0)$ è il minimo dell'insieme $X \times \{0\}$ in $A + B$, allora $a = \min X$. Nello stesso modo, per ogni insieme non vuoto $Y \subseteq B$, se $(b, 1)$ è il minimo di $Y \times \{1\}$ in $A + B$, allora $b = \min Y$.

Viceversa, supponiamo che A e B siano bene ordinati, e consideriamo un insieme non vuoto $Z \subseteq A + B$. Se esiste $a \in A$ con $(a, 0) \in Z$, allora $\min Z = (\tilde{a}, 0)$ dove $\tilde{a} = \min\{a \in A \mid (a, 0) \in Z\}$. Altrimenti $Z \subseteq B \times \{1\}$, e $\min Z = (\tilde{b}, 1)$ dove $\tilde{b} = \min\{b \in B \mid (b, 1) \in Z\}$. $\square$

Notiamo che la somma tra insiemi ordinati determina anche una somma tra tipi d'ordine, perché è coerente per isomorfismo. Si ha infatti:

ESERCIZIO 2.4. Se $A \cong A'$ e $B \cong B'$ allora $A + B \cong A' + B'$.

In base alla nostra definizione, l'unione disgiunta *non* è un'operazione associativa, perchè in generale $(A \sqcup B) \sqcup C \neq A \sqcup (B \sqcup C)$. Di conseguenza anche $(A + B) + C \neq A + (B + C)$. Se però guardiamo alla sostanza, cioè al tipo d'ordine, la somma tra insiemi ordinati è associativa.

ESERCIZIO 2.5. Per tutti gli insiemi ordinati A, B, C , si ha un isomorfismo

$$(A + B) + C \cong A + (B + C)$$

A meno di isomorfismo, la somma tra buoni ordini soddisfa la proprietà associativa. Di conseguenza, Per semplificare la notazione, nel seguito ometteremo le parentesi nel caso di somme di più insiemi ordinati,

NOTA BENE 2.6. In senso stretto, la notazione $A_1 + A_2 + \dots + A_n$ relativa alla somma di più di due insiemi ordinati è ambigua, perché dipende dal posizionamento delle parentesi. Tuttavia abbiamo visto che, a meno di isomorfismo, la somma tra ordini soddisfa la proprietà associativa e quindi, al variare di tutti i possibili modi in cui si possono piazzare le parentesi, si ottengono buoni ordini che sono tutti isomorfi tra loro. Per questo, per semplificare la notazione, nel seguito ometteremo le parentesi nel caso di somme di più insiemi ordinati, convenendo che quelle somme sono da intendersi come somme tra tipi d'ordine.

ESERCIZIO 2.7. Mostrare che per tutti gli $n, m \in \omega$ pensati come insiemi (bene) ordinati dall'appartenenza $\in$, si ha che $n + m \cong n + m$.

ESERCIZIO 2.8. Trovare un sottoinsieme di $(\mathbb{Q}, <)$ isomorfo a $\omega + \omega$.

Analogamente a quanto succedeva con i numeri naturali, anche i tipi di buon ordine hanno successore.

PROPOSIZIONE 2.9. Sia A un insieme bene ordinato e sia $\{\star\}$ un singoletto. Allora $ot(A + \{\star\})$ è il più piccolo tra i tipi d'ordine maggiori di $ot(A)$.

DIM. Senza perdita di generalità, possiamo assumere che $\star \notin A$, ed identificare $A \sqcup \{\star\} = A \cup \{\star\}$. Supponiamo che $ot(B) < ot(A \cup \{\star\})$; allora esiste un opportuno $\xi \in A \cup \{\star\}$ tale che $B \cong (A + \{\star\})_\xi$. Se $\xi = \star$, allora $(A + \{\star\})_\xi = A$ e quindi $ot(B) = ot(A)$. Se invece $\xi \in A$, allora $(A + \{\star\})_\xi = A_\xi$ e quindi $ot(B) = ot(A_\xi) < ot(A)$. $\square$

NOTAZIONE 2.10. Per ogni insieme bene ordinato $(A, <)$, denotiamo con

$$ot(A) + 1 = ot(A + \{\star\})$$

il tipo di buon ordine *successore* di $ot(A)$.

Almeno inizialmente, i tipi d'ordine bene ordinati si dispongono quindi come avevamo informalmente visto all'inizio del paragrafo:

$$ot(0) < ot(1) < ot(2) < \dots < ot(n) < ot(n+1) < \dots < ot(\omega) < ot(\omega + \{\star\}) < \dots$$

Attenzione! La somma tra tipi d'ordine *non* è commutativa. Ad esempio, se ω è l'insieme bene ordinato dei numeri naturali, allora si verifica facilmente che $\{\star\} + \omega \cong \omega$ per ogni singoletto $\{\star\}$. Abbiamo dunque:

$$ot(\{\star\} + \omega) = ot(\omega) < ot(\omega + \{\star\}).$$

In aritmetica, il prodotto $n \cdot m$ si può pensare come somma iterata di n con se stesso per m volte:

$$n \cdot m = \underbrace{n + n + \dots + n}_{m \text{ volte}}$$

In modo analogo, un'idea di prodotto tra due insiemi ordinati A e B è quella di sommare A a se stesso per “ B volte”. Per dare un senso preciso a questa intuizione, consideriamo prima l'esempio più semplice, cioè la somma $A + A$. In base alla nostra definizione, si prendono due copie disgiunte di A , e si considera l'ordine che dispone prima tutti gli elementi della prima copia $A \times \{0\}$, seguiti da tutti gli elementi della seconda copia $A \times \{1\}$. Infatti $A + A$ non è altro che il prodotto cartesiano $A \times \{0, 1\}$ dove la copia di A al “livello 0” precede la copia di A al “livello 1”. Se al posto di $\{0, 1\}$ mettiamo in verticale gli elementi di un qualunque insieme ordinato B , per analogia arriviamo alla seguente nozione generale di prodotto tra A e B .

DEFINIZIONE 2.11. Il *prodotto* $A \times B$ di due insiemi ordinati $(A, <_A)$ e $(B, <_B)$ è l'insieme ordinato $(A \times B, <)$ con l'ordine *anti-lessicografico*:²

$$(a, b) < (a', b') \iff b < b' \text{ oppure } b = b' \text{ \& } a < a'.$$

La verifica che la relazione $<$ definita sopra è in effetti un ordine totale è immediata. Un modo equivalente di pensare al prodotto $A \times B$ è immaginare di rimpiazzare ogni elemento di B con una copia di A .

ESERCIZIO 2.12. Sia A un insieme ordinato, e sia $B = \{b_1 < \dots < b_k\}$ un insieme ordinato finito con k elementi. Allora

$$A \times B \cong \underbrace{A + A + \dots + A}_{k \text{ volte}}$$

Analogamente alla somma, anche il prodotto preserva il buon ordinamento.

PROPOSIZIONE 2.13. *Siano A e B insiemi ordinati. Allora $A \times B$ è bene ordinato se e solo se sia A che B sono bene ordinati.*

DIM. È molto simile alla dimostrazione vista per la somma. Nell'ipotesi che $A \times B$ sia bene ordinato, per ogni $X \subseteq A$ non vuoto prendiamo $(a, 0)$ il minimo dell'insieme $X \times \{0\}$ in $A \times B$. È immediato verificare che allora $a = \min X$. Dato $Y \subseteq B$ non vuoto, se $(0, b)$ è il minimo di $\{0\} \times B$ in $A \times B$, allora $b = \min Y$.

Supponiamo ora che A e B siano bene ordinati. Dato $Z \subseteq A \times B$ non vuoto, prendiamo $\tilde{b}$ il minimo “livello” di una coppia in Z , cioè

$$\tilde{b} = \min\{b \in B \mid \exists a \in A (a, b) \in Z\} = \min(\text{imm}(Z)).$$

Allora $\min Z = (\tilde{a}, \tilde{b})$ dove $\tilde{a} = \min\{a \in A \mid (a, \tilde{b}) \in Z\}$. □

Anche il prodotto è coerente per isomorfismo, e quindi determina un prodotto tra tipi d'ordine.

ESERCIZIO 2.14. Se $A \cong A'$ e $B \cong B'$ allora $A \times B \cong A' \times B'$.

² Questo ordine si chiama *anti-lessicografico* perchè, al contrario dell'ordine alfabetico delle parole, le coppie (a, b) sono messe in fila “leggendole” nel verso contrario da destra a sinistra. Dunque, prima si considera la seconda componente, e quando due coppie hanno la stessa seconda componente, si ordina in base alla prima componente.

Così come per la somma, a meno di isomorfismo anche il prodotto tra insiemi ordinati è associativo.

ESERCIZIO 2.15. Per tutti gli insiemi ordinati A, B, C , si ha un isomorfismo

$$(A \times B) \times C \cong A \times (B \times C)$$

Esattamente come fatto per le somme (vedi Nota Bene 2.6) nel seguito ometteremo le parentesi nel caso di prodotti di più insiemi ordinati, che saranno intesi come prodotti tra tipi d'ordine.

ESERCIZIO 2.16. Mostrare che per tutti gli $n, m \in \omega$ pensati come insiemi ordinati dall'appartenenza $\in$, si ha che $n \times m \cong n \cdot m$.

ESERCIZIO 2.17. Trovare un sottoinsieme di $(\mathbb{Q}, <)$ isomorfo a $\omega \times \omega$.

Attenzione! Così come accade per la somma, anche il prodotto tra tipi d'ordine *non* è commutativo. Ad esempio, la funzione f tale che $f(0, n) = 2n$ e $f(1, n) = 2n + 1$ è un isomorfismo $f : \{0, 1\} \times \omega \cong \omega$. Per contro, $\omega \not\cong \omega + \omega \cong \omega \times \{0, 1\}$. Abbiamo dunque che

$$\text{ot}(\{0, 1\} \times \omega) = \text{ot}(\omega) < \text{ot}(\omega + \omega) = \text{ot}(\omega \times \{0, 1\}).$$

Ragionando informalmente, l'insieme ordinato $A \times (B + C)$ si ottiene disponendo tante copie disgiunte di A una dopo l'altra per “ $B + C$ volte”. Visto che $B + C$ si ottiene disponendo prima gli elementi di B e poi gli elementi di C , possiamo concludere che $A \times (B + C)$ si ottiene mettendo in fila “ B copie” di A seguite da altre “ C copie” di A . Formalizzando questo ragionamento, si ottiene la

PROPOSIZIONE 2.18. *Vale la proprietà distributiva a destra per tipi d'ordine:*

$$A \times (B + C) \cong (A \times B) + (A \times C).$$

DIM. Per ogni $a \in A$, per ogni $b \in B$, e per ogni $c \in C$, poniamo

$$f(a, (b, 0)) = ((a, b), 0) \quad \text{e} \quad f(a, (c, 1)) = ((a, c), 1).$$

Segue direttamente dalle definizioni che la $f : A \times (B \sqcup C) \rightarrow (A \times B) \sqcup (A \times C)$ così definita è un isomorfismo. $\square$

Attenzione! Non vale la proprietà distributiva a *sinistra*. Ad esempio:

$$(\{0\} + \{1\}) \times \omega \cong \{0, 1\} \times \omega \cong \omega < \omega + \omega \cong (\{0\} \times \omega) + (\{1\} \times \omega).$$

L'ordine della *minima differenza* che avevamo definito sull'insieme $\text{Fun}(\mathbb{N}, \mathbb{N})$ (vedi Esempio ?? del Capitolo 1), può essere considerato anche nel caso generale di insiemi di funzioni $\text{Fun}(A, B)$, purché A sia bene ordinato, e B sia ordinato. Si può infatti verificare che, sotto queste ipotesi, la relazione

$$f < g \iff f(\tilde{a}) < g(\tilde{a}) \quad \text{dove} \quad \tilde{a} = \min\{a \in A \mid f(a) \neq g(a)\}.$$

è una relazione d'ordine totale. Questa relazione non preserva però il buon ordinamento.

ESEMPIO 2.19. Pur assumendo che A e B siano entrambi bene ordinati, l'ordine della minima differenza su $\text{Fun}(A, B)$ *non* è in generale un buon ordine. Ad esempio, se per ogni naturale n denotiamo con χ_n la funzione caratteristica del singoletto $\{n\}$ (cioè, $\chi_n(n) = 1$ e $\chi_n(m) = 0$ per $m \neq n$), allora abbiamo la seguente catena discendente in $\text{Fun}(\omega, \{0, 1\})$:

$$\chi_1 > \chi_2 > \dots > \chi_n > \chi_{n+1} > \dots$$

Riusciremo ad ottenere un buon ordine restringendoci alle funzioni che assumono valore non nullo solo in un numero finito di punti.

NOTAZIONE 2.20. Siano X e Y insiemi bene ordinati, e sia $0 = \min X$.

- Il *supporto* di una funzione $f : X \rightarrow Y$ è l'insieme

$$\text{Supp}(f) = \{x \in X \mid f(x) \neq 0\}.$$

- L'insieme di tutte le funzioni da X in Y aventi supporto finito:

$$\text{Fun}_0(X, Y) = \{f : X \rightarrow Y \mid \text{Supp}(f) \text{ è finito}\}.$$

DEFINIZIONE 2.21. L'*esponenziale* $\text{Exp}(A, B)$ tra due insiemi bene ordinati $(A, <_A)$ e $(B, <_B)$ è l'insieme ordinato $(\text{Fun}_0(B, A), <)$ con l'ordine della *massima differenza*:

$$f < g \iff f(\tilde{b}) < g(\tilde{b}) \text{ dove } \tilde{b} = \max\{b \in B \mid f(b) \neq g(b)\}.$$

Notiamo che l'insieme $\{b \in B \mid f(b) \neq g(b)\}$ è finito perché è incluso nell'unione $\text{Supp}(f) \cup \text{Supp}(g)$; dunque ha sicuramente un elemento massimo (quando $f \neq g$) e la definizione di sopra è ben posta. Osserviamo che – a differenza della somma e del prodotto che sono definite per insiemi ordinati qualunque – l'esponenziale è definita soltanto tra buoni ordini.

Possiamo pensare ad una funzione $f : B \rightarrow A$ come alla stringa di “lunghezza B ” ottenuta disponendo in fila i suoi valori secondo l'ordine di B . Ad esempio, se $B = \omega$ allora possiamo vedere $f : \omega \rightarrow A$ come la stringa di “lunghezza ω ”:

$$f(0)f(1)f(2)f(3)\dots f(n)f(n+1)\dots$$

In questo senso, una funzione ha supporto finito se e solo se la corrispondente stringa contiene solo un numero finito di elementi diversi da zero. Con questa interpretazione, l'ordine della massima differenza non è altro che l'ordine anti-lessicografico. Questo indica che l'esponenziale definita sopra sia una sorta di prodotto iterato. Vale infatti il seguente risultato.

PROPOSIZIONE 2.22. Sia $B = \{b_1 < \dots < b_k\}$ un insieme ordinato finito con k elementi, e sia A bene ordinato. Allora l'esponenziale

$$\text{Exp}(A, B) \cong \underbrace{A \times A \times \dots \times A}_{k \text{ volte}}$$

DIM. Visto che B è finito, banalmente *tutte* le funzioni $f : B \rightarrow A$ hanno supporto finito. Adesso, ad ogni funzione $f : \{b_1 < \dots < b_k\} \rightarrow A$ facciamo corrispondere la k -upla $(f(b_1), \dots, f(b_k))$. Questa bigezione tra $\text{Fun}(B, A) = \text{Fun}_0(B, A)$ e A^k è l'isomorfismo cercato perché, come abbiamo notato sopra, l'ordine della massima differenza corrisponde all'ordine anti-lessicografico. $\square$

Dobbiamo ancora verificare che l'ordine della massima differenza è effettivamente un buon ordine.

PROPOSIZIONE 2.23. Siano A e B due insiemi bene ordinati. Allora il loro esponenziale $\text{Exp}(A, B)$ è un insieme bene ordinato.

DIM. Per vedere che l'ordine della massima differenza è un ordine, l'unica cosa non banale da verificare è la proprietà transitiva. Supponiamo $f < g < h$, e siano $b_1 = \max\{b \mid f(b) \neq g(b)\}$ e $b_2 = \max\{b \mid g(b) \neq h(b)\}$. Distinguiamo tre casi.

- Se $b_1 < b_2$, allora $h(b_2) > g(b_2) = f(b_2)$, ed inoltre $h(b) = g(b) = f(b)$ per ogni $b > b_2$. Dunque $h > f$.
- Se $b_1 = b_2$, allora $h(b_2) > g(b_2) > f(b_2)$, dunque $h(b_2) > f(b_2)$, ed inoltre $h(b) = g(b) = f(b)$ per $b > b_2$. Anche in questo caso $h > f$.
- Se $b_1 > b_2$, allora $h(b_1) = g(b_1) > f(b_1)$, ed inoltre $h(b) = g(b) = f(b)$ per ogni $b > b_1$. Dunque $h > f$.

Occupiamoci ora della proprietà del buon ordine. Per ogni $f \in \text{Fun}_0(B, A)$, denotiamo con $\chi(f)$ la coppia $(a, b) \in A \times B$ dove $b = \max \text{Supp}(f)$ e $a = f(b)$. Useremo la seguente proprietà, che collega l'ordinamento di $\text{Exp}(A, B)$ con quello del prodotto $A \times B$. La dimostrazione segue direttamente dalle definizioni ed è lasciata come esercizio.

$$(\star) \quad \chi(f) < \chi(g) \Rightarrow f < g \Rightarrow \chi(f) \leq \chi(g).$$

Supponiamo per assurdo che $\text{Exp}(A, B)$ non sia bene ordinato, e prendiamo una catena discendente

$$f_0 > f_1 > \dots > f_n > \dots$$

dove il valore $\chi(f_0) = (a, b)$ del termine iniziale sia il minimo possibile (qui stiamo usando la proprietà di buona fondatezza di $A \times B$). Per ogni $n > 0$, dalla $(\star)$ segue che $\chi(f_n) \leq (a, b)$. D'altra parte, se fosse $\chi(f_n) < (a, b)$, la catena discendente $f_n > f_{n+1} > \dots$ contraddirebbe la minimalità di (a, b) . Quindi, per ogni n abbiamo che $\chi(f_n) = (a, b)$, cioè $\max \text{Supp}(f_n) = b$ e $f_n(b) = a$. Definiamo adesso

$$g_n(x) = \begin{cases} f_n(x) & \text{se } x < b \\ 0 & \text{se } x \geq b. \end{cases}$$

È facile verificare che $g_0 > g_1 > \dots$ è una catena discendente dove $\max(\text{Supp}(g_0)) < b$, e dunque $\chi(g_0) < (a, b)$, contro la minimalità di (a, b) . $\square$

ESERCIZIO 2.24. Trovare un sottoinsieme di $(\mathbb{Q}, <)$ isomorfo a $\text{Exp}(\omega, \omega)$.

3. Ordinali

Introduciamo ora una speciale classe di insiemi bene ordinati, cioè gli *ordinali*. Come vedremo, si tratta di insiemi che generalizzano i numeri naturali. Il risultato fondamentale che dimostreremo è che ogni insieme bene ordinato è isomorfo ad uno ed un solo ordinale. Dunque potremo prendere gli ordinali come i rappresentanti canonici dei tipi d'ordine bene ordinati.

Per definire gli ordinali, dobbiamo introdurre prima un'importante nozione insiemistica.

DEFINIZIONE 3.1. Un insieme A si dice *transitivo* se $a' \in a \in A \Rightarrow a' \in A$; equivalentemente, se $A \subseteq \mathcal{P}(A)$.

ESERCIZIO 3.2. Sia $\mathcal{F}$ una famiglia di insiemi transitivi. Allora anche l'intersezione $\bigcap_{A \in \mathcal{F}} A$ e l'unione $\bigcup_{A \in \mathcal{F}} A$ sono insiemi transitivi.

DEFINIZIONE 3.3. Un insieme α è un *ordinale* se:

- (1) $(\alpha, \in)$ è un insieme bene ordinato dalla relazione di appartenenza;

(2) α è un insieme *transitivo*.³

Abbiamo già incontrato esempi di ordinali.

ESEMPIO 3.4.

- (1) Tutti i numeri naturali n sono ordinali;
- (2) ω è un ordinale.

È facile trovare esempi di insiemi che, pur essendo bene ordinati dall'appartenenza, non sono ordinali. Ad esempio sia $A = \{2n \mid n \in \omega\}$ l'insieme dei numeri naturali pari. Chiaramente $(A, \in)$ è bene ordinato in quanto sottoinsieme dell'insieme bene ordinato $(\omega, \in)$. Tuttavia l'insieme A non è transitivo perchè, ad esempio, $1 \in 2 \in A$ ma $1 \notin A$.

Tranne che per gli ordinali finiti, seguendo la consuetudine, denoteremo sempre gli ordinali con lettere greche:

$$\alpha, \beta, \gamma, \delta, \dots, \xi, \eta, \zeta, \dots$$

Come conseguenza diretta della transitività degli ordinali, ricaviamo la seguente utile proprietà.

PROPOSIZIONE 3.5. *Non esistono catene discendenti di ordinali:*

$$\alpha_0 \ni \alpha_1 \ni \dots \ni \alpha_n \ni \alpha_{n+1} \ni \dots$$

DIM. Dalla transitività dell'ordinale α_0 , segue che $X = \{\alpha_n \mid n \geq 1\} \subseteq \alpha_0$ è un sottoinsieme non vuoto di α_0 . Ma X non ha elemento minimo rispetto alla relazione di appartenenza, e questo contraddice l'ipotesi che $(\alpha_0, \in)$ è bene ordinato. $\square$

In un ordinale, visto che la relazione d'ordine considerata è la relazione $\in$ di appartenenza, i segmenti iniziali generati da un elemento coincidono con l'elemento stesso. Precisamente vale la seguente equivalenza.

PROPOSIZIONE 3.6. *Sia $(\alpha, \in)$ un insieme bene ordinato dalla relazione di appartenenza. Allora sono proprietà equivalenti:*

- (i) α è un insieme transitivo;
- (ii) Per ogni $a \in \alpha$, il segmento iniziale generato da a coincide con a stesso, cioè: $\alpha_a = \{a' \in \alpha \mid a' < a\} = a$.

In particolare, se α è un ordinale allora $\alpha_a = a$ per ogni $a \in \alpha$.

DIM. Visto che la relazione d'ordine è l'appartenza, per ogni $a \in \alpha$ si ha che:

$$\alpha_a =: \{a' \in \alpha \mid a' \in a\} = a \cap \alpha.$$

Osserviamo poi che seguenti proprietà sono tra loro equivalenti.

- α è un insieme transitivo.
- Per ogni $a \in \alpha$ si ha che $a \subseteq \alpha$.
- Per ogni $a \in \alpha$ si ha che $a = a \cap \alpha = \alpha_a$.

$\square$

Osserviamo che elementi di ordinali sono ordinali.

³ Attenzione a non confondere la proprietà di *transitività insiemistica*, con la proprietà transitiva degli ordini. Anche se nel caso particolare degli ordinali queste due proprietà coincidono (visto che la relazione d'ordine considerata è quella di appartenenza), in generale si tratta di due concetti diversi, anche se analoghi.

PROPOSIZIONE 3.7. *Se α è un ordinale e $\beta \in \alpha$, allora anche β è un ordinale.*

DIM. Poiché α è un insieme transitivo, da $\beta \in \alpha$ segue che $\beta \subseteq \alpha$, e dunque $(\beta, \in)$ è bene ordinato perché $(\alpha, \in)$ lo è. Inoltre, se $\gamma \in \beta' \in \beta$, di nuovo per il fatto che α è un insieme transitivo, abbiamo che $\beta' \in \alpha$, e quindi anche $\gamma \in \alpha$. Infine, visto che α è totalmente ordinato da $\in$ e che γ, β', β sono suoi elementi, da $\gamma \in \beta'$ e $\beta' \in \beta$ segue che $\gamma \in \beta$, per la proprietà transitiva dell'ordine su α . $\square$

Intersezione di ordinali è un ordinale. (Più avanti vedremo che anche le unioni di ordinali sono ordinali.)

PROPOSIZIONE 3.8. *Sia $\{\alpha_i \mid i \in I\}$ una famiglia non vuota di ordinali. Allora anche $\bigcap_{i \in I} \alpha_i$ è un ordinale.*

DIM. Notiamo che $\beta := \bigcap_{i \in I} \alpha_i$ è un insieme transitivo perché intersezione di insiemi transitivi. Inoltre, fissato un qualunque ordinale α_{i_0} della famiglia, banalmente $\beta \subseteq \alpha_{i_0}$, e quindi $(\beta, \in)$ è bene ordinato perché $(\alpha_{i_0}, \in)$ lo è. $\square$

Sugli ordinali, le relazioni di appartenenza e di inclusione stretta coincidono.

PROPOSIZIONE 3.9. *Siano α e β ordinali. Sono proprietà equivalenti:*

- (1) $\alpha \in \beta$;
- (2) α è un segmento iniziale proprio di β ;
- (3) $\alpha \subsetneq \beta$.

DIM. (1) $\Rightarrow$ (2). Se $\alpha \in \beta$, allora il segmento iniziale proprio $\beta_\alpha = \alpha$ per la Proposizione precedente 3.6.

(2) $\Rightarrow$ (3) è banale.

(3) $\Rightarrow$ (1). Supponiamo $\alpha \subsetneq \beta$ e prendiamo $\xi = \min(\beta \setminus \alpha)$. Vogliamo mostrare che $\alpha = \xi$, e quindi $\alpha \in \beta$.

Per la transitività di β , da $\xi \in \beta$ segue che $\xi \subseteq \beta$; ma allora, per la minimalità di ξ , tutti gli elementi di ξ devono appartenere ad α . Questo mostra l'inclusione $\xi \subseteq \alpha$. Per l'altra inclusione, supponiamo che $\gamma \in \alpha$; dobbiamo vedere che $\gamma \in \xi$. Notiamo intanto che $\gamma, \xi \in \beta$, quindi sono confrontabili per la proprietà di ordine di $(\beta, \in)$. Chiaramente $\xi \neq \gamma$, altrimenti $\xi = \gamma \in \alpha$ mentre $\xi \notin \alpha$; inoltre $\xi \notin \gamma$, altrimenti $\xi \in \gamma \in \alpha \Rightarrow \xi \in \alpha$ per la transitività di α , mentre $\xi \notin \alpha$. Allora non resta che la terza possibilità, cioè $\gamma \in \xi$, come volevamo. $\square$

Una fondamentale proprietà è il seguente teorema di unicità degli ordinali nelle classi di isomorfismo.

PROPOSIZIONE 3.10. *Siano α e β ordinali. Se $\alpha \cong \beta$, allora $\alpha = \beta$.*

DIM. Sia $\varphi : \alpha \rightarrow \beta$ un isomorfismo. Dimostriamo che φ è la funzione identità. Se per assurdo così non fosse, prendiamo

$$\xi = \min\{x \in \alpha \mid \varphi(x) \neq x\}.$$

Restringendo φ al segmento iniziale α_ξ , si ottiene un isomorfismo

$$\psi = \varphi|_{\alpha_\xi} : \alpha_\xi \rightarrow \beta_{\varphi(\xi)}.$$

Chiaramente ψ è la funzione identità, e quindi $\alpha_\xi = \beta_{\varphi(\xi)}$. Resta da notare che, per la (2)' nella definizione di ordinale, i segmenti iniziali $\alpha_\xi = \xi$ e $\beta_{\varphi(\xi)} = \varphi(\xi)$. Si concluderebbe così che $\xi = \varphi(\xi)$, contro la definizione di ξ . $\square$

Mettendo insieme alcuni dei risultati visti fin qui, ricaviamo il

TEOREMA 3.11 (Tricotomia degli Ordinali). *Siano α e β due ordinali. Allora vale una ed una sola delle seguenti tre eventualità:*

$$(1) \alpha = \beta ; \quad (2) \alpha \in \beta ; \quad (3) \beta \in \alpha .$$

Diamo due dimostrazioni di questo risultato.

DIM 1. È conseguenza diretta della tricotomia degli insiemi bene ordinati (Teorema 1.18). Infatti, $\alpha \cong \beta \Leftrightarrow \alpha = \beta$, per la Proposizione 3.10. Inoltre, se $\alpha \cong \beta_\gamma = \gamma$ per qualche $\gamma \in \beta$, allora $\alpha = \beta_\gamma = \gamma \in \beta$; e analogamente, se $\beta \cong \alpha_\delta = \delta$ per qualche $\delta \in \alpha$, si ha $\beta = \alpha_\delta = \delta \in \alpha$. $\square$

DIM. 2. In questa dimostrazione alternativa, *non* facciamo uso del teorema sulla tricotomia dei buoni ordini, ma useremo ripetutamente l'equivalenza tra appartenenza e inclusione stretta tra ordinali, data dalla la Proposizione 3.9.

Dati due ordinali $\alpha \neq \beta$, consideriamo l'intersezione $\gamma = \alpha \cap \beta$. Chiaramente γ è un ordinale. Per raggiungere la tesi, basta mostrare che $\gamma = \alpha$ o $\gamma = \beta$. Infatti se $\gamma = \alpha \cap \beta = \alpha$ allora $\alpha \subsetneq \beta$, e quindi $\alpha \in \beta$; e analogamente, se $\gamma = \alpha \cap \beta = \beta$ allora $\beta \subsetneq \alpha$, e quindi $\beta \in \alpha$.

Se per assurdo fosse $\gamma \subsetneq \alpha$ e $\gamma \subsetneq \beta$, allora si avrebbe che $\gamma \in \alpha$ e $\gamma \in \beta$, dunque $\gamma \in \alpha \cap \beta$, cioè $\gamma \in \gamma$, una contraddizione. $\square$

Riassumendo alcuni dei risultati visti sopra, si ottiene il seguente:

TEOREMA 3.12. *La relazione di appartenenza $\in$ soddisfa tutte le proprietà di ordine totale sulla collezione degli ordinali:*

- (1) Irriflessiva: *Per ogni α ordinale, $\alpha \notin \alpha$;*
- (2) Asimmetrica: *Per tutti gli ordinali α e β , $\alpha \in \beta \Rightarrow \beta \notin \alpha$;*
- (3) Transitiva: *Per tutti gli ordinali α, β, γ , $(\alpha \in \beta \wedge \beta \in \gamma) \Rightarrow \alpha \in \gamma$;*
- (4) Ordine totale: *Per tutti gli ordinali α e β , vale una ed una sola delle seguenti: $\alpha \in \beta$, $\alpha = \beta$, $\beta \in \alpha$;*

DIM. (1). Se fosse $\alpha \in \alpha$, allora non varrebbe la proprietà antiriflessiva dell'insieme ordinato $(\alpha, \in)$.

(2) Se per assurdo si avesse $\alpha \in \beta$ e $\beta \in \alpha$ allora, per la transitività di α , si avrebbe $\alpha \in \alpha$, contraddicendo la (1).

(3) afferma che ogni ordinale γ è un insieme transitivo, e questo fa parte della definizione di ordinale.

(4) è la proprietà tricotomica degli ordinali (Teorema 3.11). $\square$

Visto il Teorema 3.12, da qui in avanti useremo il simbolo d'ordine $<$ tra ordinali. Precisamente, se α e β sono ordinali, scriveremo:

- $\alpha < \beta$ per intendere che $\alpha \in \beta$ (equivalentemente, $\alpha \subsetneq \beta$);
- $\alpha \leq \beta$ per intendere che $\alpha \in \beta$ o $\alpha = \beta$ (equivalentemente, $\alpha \subseteq \beta$).

PROPOSIZIONE 3.13. *Se α è un ordinale, allora anche $\alpha \cup \{\alpha\}$ è un ordinale, e il suo tipo d'ordine è il più piccolo tipo di buon ordine tra quelli maggiori di α .*

DIM. La transitività di $\alpha \cup \{\alpha\}$ segue direttamente dalla transitività di α . Inoltre $(\alpha \cup \{\alpha\}, \in)$ è bene ordinato perché è isomorfo a $\alpha + \{\star\}$. Infine, ricordiamo che $ot(\alpha + \{\star\})$ è il tipo di buon ordine successore di $ot(\alpha)$. $\square$

NOTAZIONE 3.14. Per analogia con i numeri naturali, si denota

$$\alpha + 1 = \alpha \cup \{\alpha\}.$$

Possiamo finalmente dimostrare che la relazione di appartenenza sugli ordinali soddisfa anche la proprietà di buon ordine.

PROPOSIZIONE 3.15. *Sia X un insieme non vuoto di ordinali. Allora l'intersezione $\xi = \bigcap X$ è l'elemento minimo di X rispetto alla relazione di appartenenza.*

DIM. Per la definizione di ξ , per ogni $\alpha \in X$ si ha che $\xi \leq \alpha$ (cioè $\xi \subseteq \alpha$). Dunque ξ è un minorante di X . Osserviamo infine che $\xi \in X$, e quindi è il minimo elemento di X . Infatti, se così non fosse, avremmo $\xi < \alpha$ per ogni $\alpha \in X$, da cui $\xi + 1 \leq \alpha$ per ogni $\alpha \in X$, e quindi $\xi \subsetneq \xi + 1 \subseteq \bigcap X$, il che è assurdo. $\square$

Mettendo insieme il Teorema 3.12 con la proposizione precedente, si ottiene il seguente

COROLLARIO 3.16. *Sia Λ un insieme di ordinali. Allora $(\Lambda, \in)$ è un insieme bene ordinato.*

Come conseguenza di quanto già visto per i buoni ordini, abbiamo la seguente proprietà degli ordinali.

PROPOSIZIONE 3.17. *Non esistono catene discendenti di ordinali:*

$$\alpha_1 \supset \alpha_2 \supset \dots \supset \alpha_n \supset \alpha_{n+1} \supset \dots$$

DIM. Altrimenti, $\Lambda := \{\alpha_n \mid n \in \mathbb{N}\}$ sarebbe un insieme di ordinali *non* bene ordinato. $\square$

PROPOSIZIONE 3.18. *Sia X un insieme di ordinali. Allora X è un ordinale se e solo se X è un insieme transitivo.*

DIM. Se X è un ordinale, allora per definizione X è un insieme transitivo, ed inoltre i suoi elementi sono ordinali per la Proposizione 3.7. Viceversa, se X è un insieme transitivo di ordinali, allora X è un ordinale perché $(X, \in)$ è bene ordinato, per il Corollario 3.16. $\square$

Abbiamo già visto che la collezione di Russell $R = \{x \mid x \notin x\}$ e la collezione universale di tutti gli insiemi $V = \{x \mid x = x\}$ *non* possono essere insiemi. Un ulteriore importante esempio di questo tipo di collezioni si ottiene considerando gli ordinali.

PROPOSIZIONE 3.19 (Paradosso di Burali-Forti). *La seguente collezione non è un insieme:*

$$ORD = \{\alpha \mid \text{"}\alpha \text{ è un ordinale"}\}.$$

DIM. Supponiamo per assurdo che ORD sia un insieme. Visto che elementi di ordinali sono ordinali, ORD sarebbe un insieme transitivo di ordinali, e dunque esso stesso un ordinale. Ma allora avremmo $ORD \in ORD$, il che è assurdo. $\square$

Dimostriamo finalmente il risultato che giustifica l'introduzione degli ordinali.

TEOREMA 3.20. *Ogni insieme bene ordinato è isomorfo ad un unico ordinale.*

DIM. L'unicità è già stata dimostrata nella Proposizione 3.10. Occupiamoci dunque dell'esistenza. Fissato l'insieme bene ordinato $(A, <)$, consideriamo l'insieme

$$X = \{a \in A \mid \text{il segmento iniziale proprio } A_a \text{ è isomorfo ad un ordinale}\}.$$

Consideriamo inoltre:

$$Y = \{\alpha \text{ ordinale} \mid \alpha \text{ è isomorfo ad un segmento iniziale proprio di } A\}.$$

Attenzione! Mentre l'insieme X esiste per l'assioma di *separazione*, gli assiomi di ZFC visti finora *non* possono garantire che un tale Y sia un insieme. A questo scopo, dovremo usare un nuovo assioma chiamato *rimpiazzamento*, che sarà introdotto e discusso nel prossimo capitolo. Assumiamo comunque per il momento l'esistenza dell'insieme Y , e proseguiamo con la dimostrazione.

Sia f la funzione $f : X \rightarrow Y$ dove $f(a)$ è quell'*unico* ordinale α tale che $\alpha \cong A_a$ (ricordiamo che due ordinali diversi non possono essere isomorfi). Dimostriamo ora due proprietà:

- (1) Sia $a \in X$. Se $b < a$, allora $b \in X$ e $f(b) \in f(a)$.
- (2) Sia $a \in X$. Se $\beta \in f(a)$, allora esiste $b \in X$ con $f(b) = \beta$;

Per definizione di f , esiste un isomorfismo $\psi : A_a \rightarrow f(a)$. Notiamo che per ogni $b < a$, il segmento iniziale generato da b in A_a coincide con il segmento iniziale generato da b in A , cioè

$$(A_a)_b = \{x \in A_a \mid x < b\} = \{x \in A \mid x < b\} = A_b.$$

Inoltre, visto che $f(a)$ è un ordinale, il segmento iniziale $f(a)_{\psi(b)}$ coincide con $\psi(b)$. Allora, restringendo ψ ad A_b otteniamo un isomorfismo $\psi|_{A_b} : A_b \rightarrow \psi(b)$. Questo dimostra che $b \in X$ e che $f(b) = \psi(b) \in f(a)$, cioè la (1). Adesso, dato $\beta \in f(a)$, prendiamo $b \in A_a$ tale che $\psi(b) = \beta$. Per quanto visto sopra, restringendo ψ ad A_b , si ottiene un isomorfismo $A_b \cong \psi(b) = \beta$, e questo dimostra la (2).

In conseguenza delle due proprietà di sopra, X è un segmento iniziale di A , $Y = \text{imm}(f) = \gamma$ è un ordinale in quanto insieme transitivo di ordinali, e $f : X \rightarrow \gamma$ è un isomorfismo d'ordine. Se X fosse un segmento iniziale proprio, allora $X = A_a$ per un opportuno $a \in A$. Ma abbiamo appena visto che $f : A_a \rightarrow \gamma$ è un isomorfismo, e quindi avremmo che $a \in X = A_a$, il che è assurdo. Concludiamo che $X = A$ e che $f : A \rightarrow \gamma$ è l'isomorfismo cercato. $\square$

Stabilito che gli ordinali sono rappresentanti canonici nelle classi di isomorfismo dei buoni ordini, da qui in avanti ci concentreremo sugli ordinali. Infatti le loro proprietà descrivono, senza perdita di generalità, le proprietà di tutti i buoni ordini.

PROPOSIZIONE 3.21. *Un ordinale α ha massimo se e solo se esiste un ordinale β con $\alpha = \beta + 1$.*

DIM. Vediamo prima che se α ha un elemento massimo β , allora $\alpha = \beta \cup \{\beta\}$. Un'inclusione segue immediatamente dalla definizione di massimo, perchè per ogni $\gamma \in \alpha$ si ha $\gamma \leq \beta$, cioè $\gamma \in \beta$ o $\gamma = \beta$. L'altra inclusione $\beta \cup \{\beta\} \subseteq \alpha$ si ottiene per la transitività insiemistica di α , visto che da $\beta \in \alpha$ segue che $\beta \subseteq \alpha$.

Viceversa, se $\alpha = \beta \cup \{\beta\}$, allora per ogni $\gamma \in \alpha$ si ha $\gamma \in \beta$ o $\gamma = \beta$, cioè $\gamma \leq \beta$. Dunque $\beta \in \alpha$ è l'elemento massimo di α . $\square$

Grazie a questa proposizione, la seguente definizione è ben posta.

DEFINIZIONE 3.22. Un ordinale $\alpha \neq 0$ si dice *successore* se ha massimo (cioè se è della forma $\alpha = \beta + 1$), e si dice *limite* altrimenti.

Per transitività, se α è un ordinale allora $\gamma \in \alpha \Rightarrow \gamma \subseteq \alpha$, e quindi $\bigcup \alpha \subseteq \alpha$. L'inclusione inversa vale se e solo se l'ordinale è limite.

PROPOSIZIONE 3.23. Un ordinale λ è limite se e solo se $\bigcup \lambda = \lambda$.

DIMOSTRAZIONE. Come abbiamo osservato sopra, visto che λ è un insieme transitivo, si ha l'inclusione $\bigcup \lambda \subseteq \lambda$. Poi basta notare che le seguenti proprietà sono ognuna equivalente alla successiva:

- $\lambda \subseteq \bigcup \lambda$;
- Per ogni $\beta \in \lambda$ esiste $\gamma \in \lambda$ tale che $\beta \in \gamma$;
- $(\lambda, \in)$ non ha massimo.

□

Ricordiamo che ogni insieme non vuoto di ordinali X ha un elemento minimo dato dall'intersezione $\xi = \bigcap X$. Non sempre un insieme di ordinali ha massimo, ma ha sempre un estremo superiore.

PROPOSIZIONE 3.24. Sia X un insieme non vuoto di ordinali. Allora l'unione $\eta = \bigcup X$ è un ordinale, ed inoltre $\eta = \sup X$.

DIM. Dati $\gamma \in \beta \in \bigcup X$, prendiamo $\alpha \in X$ tale che $\beta \in \alpha$. Allora β è un ordinale in quanto elemento di un ordinale; inoltre $\gamma \in \alpha$ perché α è transitivo, e quindi $\gamma \in \bigcup X$. Questo mostra che X è un insieme transitivo di ordinali, e quindi è esso stesso un ordinale $\eta = \bigcup X$. Chiaramente $\alpha \leq \eta$ per ogni $\alpha \in X$, visto che $\alpha \subseteq \bigcup X$. Inoltre, se ζ è un maggiorante di X , cioè se $\zeta \geq \alpha$ per ogni $\alpha \in X$, allora $\zeta \supseteq \alpha$ per ogni $\alpha \in X$, e quindi $\zeta \supseteq \bigcup X = \eta$, cioè $\zeta \leq \eta$. Concludiamo che η è il minimo dei maggioranti di X . □

Uno strumento tipico della teoria degli insiemi è l'induzione transfinita, che estende la familiare induzione sui numeri naturali a tutta la classe degli ordinali. Notiamo che mentre tutti numeri naturali $n \neq 0$ sono successori, esistono ordinali infiniti $\alpha \neq 0$ che *non* lo sono. Per questo, in una formulazione dell'induzione, si distinguono tre casi: il caso *base* $\alpha = 0$, il caso *successore* $\alpha = \beta + 1$, e il caso *limite*.

TEOREMA 3.25 (Induzione Transfinita).

- Induzione forte: Sia $P(x)$ una formula, eventualmente con parametri. Supponiamo che per ogni ordinale β valga l'implicazione $(\forall \gamma < \beta P(\gamma)) \rightarrow P(\beta)$.⁴ Allora $P(\alpha)$ vale per ogni ordinale α .
- Induzione per casi: Sia $P(x)$ una formula, eventualmente con parametri. Supponiamo che valgano:
 - $P(0)$;
 - Per ogni ordinale β , vale implicazione $P(\beta) \rightarrow P(\beta + 1)$.
 - Per ordinale limite λ , vale l'implicazione $(\forall \gamma < \lambda P(\gamma)) \rightarrow P(\lambda)$.
 Allora $P(\alpha)$ vale per ogni ordinale α .

⁴ Notiamo che “ $\forall \gamma < 0 P(\gamma)$ ” è vera banalmente perchè non esistono ordinali $\gamma < 0$. Dunque, nel caso $\beta = 0$, l'ipotesi equivale a dire che $P(0)$ vale.

DIM. Chiaramente, se le ipotesi dell'induzione per casi sono soddisfatte allora anche le ipotesi dell'induzione forte sono soddisfatte; quindi, l'induzione per casi segue dall'induzione forte.

Per dimostrare quest'ultima, procediamo per assurdo e supponiamo che le ipotesi siano soddisfatte ma che esista un ordinale δ con $\neg P(\delta)$. In questo caso, $A = \{\alpha \leq \delta \mid \neg P(\alpha)\}$ sarebbe un insieme non vuoto dell'ordinale $\delta + 1$, e quindi avrebbe un elemento minimo, diciamo β . Per la minimalità di β , deve valere $P(\gamma)$ per ogni $\gamma < \beta$. Ma allora varrebbe anche $P(\beta)$, contro la nostra assunzione. $\square$

Il fondamentale risultato collegato all'induzione transfinita, che vedremo nel prossimo capitolo, è il Teorema di ricorsione transfinita che estende il Teorema di ricorsione numerabile dai numeri naturali ω alla collezione ORD di tutti gli ordinali. Analogamente a come la ricorsione numerabile permette di definire sequenze $(a_n \mid n \in \mathbb{N})$, la ricorsione transfinita permetterà di definire "sequenze" $(\alpha_\alpha \mid \alpha \in \text{ORD})$ indicizzate su tutti gli ordinali. Ricordiamo che ORD non è un insieme, e quindi anche queste ultime sequenze non saranno insiemi; potremo tuttavia considerarle nella teoria ZFC usando opportuni accorgimenti.

Classi, rimpiazzamento, ricorsione transfinita

1. Classi in ZFC

Abbiamo già incontrato almeno tre diverse “collezioni” che è contraddittorio assumere come insiemi:

- *Paradosso di Russell*: La collezione $R = \{x \mid x \notin x\}$ di tutti gli insiemi che non appartengono a se stessi, non è un insieme.
- *Paradosso di Cantor*: La collezione universale $V = \{x \mid x = x\}$ di tutti gli insiemi non è un insieme.
- *Paradosso di Burali-Forti*: La collezione $\text{ORD} = \{x \mid x \text{ è un ordinale}\}$ di tutti gli ordinali non è un insieme.

Strettamente parlando, le collezioni di sopra non esistono nella nostra teoria assiomatica, perchè gli unici oggetti della teoria sono insiemi. Ciò nonostante nella pratica matematica si usano talvolta collezioni che non sono insiemi; in particolare, la collezione degli ordinali ha una speciale importanza. Come possiamo rimediare a questo inconveniente?

Una prima possibile strada è quella di mantenerci all'interno della teoria di Zermelo-Fraenkel, e considerare le classi come convenienti notazioni metalinguistiche, cioè come notazioni che si riferiscono ad oggetti che *non* fanno parte della teoria. Vedremo più avanti che un'altra possibile strada è quella di lavorare all'interno di una *teoria assiomatica delle classi*.

DEFINIZIONE 1.1 (Meta-definizione in ZFC). Una *classe* $\mathbf{C}$ è l'estensione di una formula $\varphi(x)$, eventualmente con parametri; cioè, $\mathbf{C}$ è la collezione di tutti gli insiemi x che soddisfano $\varphi(x)$. In questo caso, con abuso di notazione, scriviamo:

$$\mathbf{C} = \{x \mid \varphi(x)\}.$$

Riserveremo lettere in grassetto per indicare classi in ZFC.

Ovviamente ogni insieme A è una classe, perchè banalmente $A = \mathbf{C}_\varphi$ dove $\varphi(x)$ è la formula con parametro “ $x \in A$ ”.

Osserviamo che le tre collezioni elencate sopra relative ai paradossi sono tutte di questo tipo. Se $\mathbf{C}_\varphi$ è la classe estensione della formula φ , allora useremo le seguenti notazioni:

- “ $a \in \mathbf{C}_\varphi$ ” indica la formula “ $\varphi(a)$ ”;
- “ $a \in \mathbf{C}_\varphi \cap \mathbf{C}_\psi$ ” indica la formula “ $\varphi(a) \wedge \psi(a)$ ”;
- “ $a \in \mathbf{C}_\varphi \cup \mathbf{C}_\psi$ ” indica la formula “ $\varphi(a) \vee \psi(a)$ ”;
- “ $a \in \mathbf{C}_\varphi \setminus \mathbf{C}_\psi$ ” indica la formula “ $\varphi(a) \wedge \neg\psi(a)$ ”;
- “ $\mathbf{C}_\varphi \subseteq \mathbf{C}_\psi$ ” indica la formula “ $\forall x (\varphi(x) \rightarrow \psi(x))$ ”;

Ricordiamo comunque che in generale non possiamo applicare a tali collezioni le operazioni insiemistiche, perchè le classi *non sempre* sono insiemi.

2. Assioma di Rimpiazzamento

DEFINIZIONE 2.1. La formula $\varphi(x, y, a_1, \dots, a_k)$ con parametri gli insiemi $a_1, \dots, a_k$ si dice *formula funzionale* rispetto alle variabili x e y se vale:

$$\forall x \forall y \forall y' (\varphi(x, y, a_1, \dots, a_k) \wedge \varphi(x, y', a_1, \dots, a_k)) \rightarrow y = y'.$$

DEFINIZIONE 2.2. Se una classe di coppie ordinate

$$\mathbf{F} = \{(x, y) \mid \varphi(x, y)\}$$

è definita da una formula funzionale $\varphi(x, y)$ rispetto alle variabili x e y , allora $\mathbf{F}$ si dice *funzione-classe*. Il *dominio* e l'*immagine* di $\mathbf{F}$ sono rispettivamente le classi:

- $\text{dom}(\mathbf{F}) := \{x \mid \exists y \varphi(x, y)\},$
- $\text{imm}(\mathbf{F}) := \{y \mid \exists x \varphi(x, y)\}.$

Come per le usuali funzioni, si adotta la notazione $\mathbf{F} : \mathbf{A} \rightarrow \mathbf{B}$ per intendere che $\mathbf{F}$ è una funzione-classe con $\text{dom}(\mathbf{F}) = \mathbf{A}$ e $\text{imm}(\mathbf{F}) \subseteq \mathbf{B}$.

Inoltre, se $\mathbf{C} = \{x \mid \psi(x)\} \subseteq \mathbf{A}$ è una classe inclusa nel dominio, allora anche l'immagine di $\mathbf{C}$ mediante $\mathbf{F}$ è una classe:

- $\mathbf{F}[\mathbf{C}] = \{\mathbf{F}(x) \mid x \in \mathbf{C}\} = \{y \mid \exists x \psi(x) \wedge \varphi(x, y)\}.$

Assioma 9: Schema di Rimpiazzamento.

Per ogni formula $\varphi(x, y, z_1, \dots, z_k)$, il seguente è un assioma:

$$\forall a_1 \dots \forall a_k \text{ “}\varphi(x, y, a_1, \dots, a_k) \text{ funzionale in } x \text{ e } y\text{”} \rightarrow \\ \forall B \exists C \text{ “}C = \{y \mid \exists x \in B \varphi(x, y, a_1, \dots, a_k)\}\text{”}.$$

Usando le notazioni introdotte per le classi, possiamo informalmente enunciare l'assioma di rimpiazzamento in questo modo:

- **Rimpiazzamento:** Se $\mathbf{F}$ è una funzione-classe e B è un insieme allora anche $\mathbf{F}[B]$ è un insieme.

Applicando l'assioma di rimpiazzamento, possiamo finalmente concludere la dimostrazione del Teorema ??.

DIM. TEOREMA ?? (PARTE 2). Ricordiamo che restava da dimostrare l'esistenza dell'insieme

$$Y = \{\alpha \text{ ordinale} \mid \alpha \text{ è isomorfo ad un segmento iniziale proprio di } A\}.$$

Consideriamo la seguente formula (con parametro A):

$$\varphi(a, \alpha) : \text{ “}a \in A \text{ e l'ordinale } \alpha \text{ è isomorfo al segmento iniziale } A_a\text{”}.$$

La formula φ è funzionale nella variabile a perchè per ogni $a \in A$ esiste al più un ordinale $\alpha \cong A_a$. Ricordiamo che avevamo considerato l'insieme

$$X = \{a \in A \mid A_a \text{ è isomorfo ad un ordinale}\},$$

che esiste per l'assioma di *separazione*. Grazie all'assioma di *rimpiazzamento*, esiste allora l'insieme $\{\alpha \mid \exists x \in X \varphi(x, \alpha)\}$, che è precisamente l'insieme Y di cui volevamo dimostrare l'esistenza. $\square$

La nozione di restrizione si applica anche alle funzioni-classe nel modo ovvio.

DEFINIZIONE 2.3. Sia $\mathbf{F}$ una funzione-classe. Per ogni classe $\mathbf{A} \subseteq \text{dom}(\mathbf{F})$, la *restrizione* $\mathbf{F}|_{\mathbf{A}}$ è la funzione-classe tale che $\text{dom}(\mathbf{F}|_{\mathbf{A}}) = \mathbf{A}$ e $(\mathbf{F}|_{\mathbf{A}})(x) = \mathbf{F}(x)$ per ogni $x \in \mathbf{A}$. Più precisamente, se $\mathbf{F}$ è determinata dalla formula funzionale $\varphi(x, y)$ e se $\mathbf{A} = \{x \mid \psi(x)\}$, allora $\mathbf{F}|_{\mathbf{A}} = \{(x, y) \mid \psi(x) \wedge \varphi(x, y)\}$.

Un'utile caratterizzazione dell'assioma di *rimpiazzamento* è la seguente:

TEOREMA 2.4 (Meta-teorema di ZFC). *Lo schema di impiazzamento è equivalente alla seguente proprietà: Se $\mathbf{F}$ è una funzione-classe e $A \subseteq \text{dom}(\mathbf{F})$ è un insieme, allora la restrizione $\mathbf{F}|_A$ è un insieme (ed è una funzione).*

DIM. Sia $\varphi(x, y)$ la formula funzionale che definisce $\mathbf{F}$. Dallo schema di impiazzamento segue che l'immagine $\mathbf{F}[A] = \{y \mid \exists a \in A \varphi(a, y)\}$ è un insieme. Ma allora anche la restrizione $\mathbf{F}|_A = \{(x, y) \in A \times \mathbf{F}[A] \mid \varphi(x, y)\}$ è un insieme per l'assioma di *separazione*. Viceversa, data una funzione-classe $\mathbf{F}$ ed un insieme A , se la restrizione $f = \mathbf{F}|_A$ è un insieme, allora anche la sua immagine $\text{imm}(f) = \{f(a) \mid a \in A\} = \{\mathbf{F}(a) \mid a \in A\} = \mathbf{F}[A]$ è un insieme. $\square$

3. La teoria delle classi NGB di von Neumann-Gödel-Bernays

Un secondo modo per trattare collezioni di insiemi (che possono non essere esse stesse insiemi) è quello di formalizzarlo all'interno di una teoria assiomatica. Si tratta di estendere il concetto di *insieme* in modo che anche le collezioni di insiemi viste sopra siano effettivi oggetti della nostra teoria. A questo scopo, formuleremo qui un'opportuna teoria assiomatica, la *teoria delle classi* NGB di von Neumann-Gödel-Bernays. Come vedremo, questa teoria “ingloba” la teoria ZFC, ed ha il vantaggio di semplificare notevolmente alcuni argomenti più avanzati, e specialmente la ricorsione transfinita.

Gli oggetti della teoria NGB si chiamano *classi*. Come vedremo, alcune di quelle classi si dicono *insiemi*. Quelle classi che non sono insiemi si dicono *classi proprie*.

L'idea intuitiva è che le classi proprie siano talmente “grandi” che possano essere considerate solo come oggetti “in potenza” e non come entità pienamente realizzate; per questo sembra plausibile assumere che una classe propria non possa mai essere un elemento di un'altra classe. Viceversa, l'intuizione degli insiemi è che siano classi non troppo “grandi”, che quindi possiamo pensare come oggetti realizzati, conclusi, e che per questo possano essere elementi di altre classi. Per gli insiemi, cioè per le classi “piccole”, assumeremo tutti gli assiomi della teoria degli insiemi ZFC che abbiamo visto fin qui; ad essi aggiungeremo tre ulteriori assiomi che riguardano le classi in generale. Come fatto per ZFC, procederemo con cautela, permettendo tra le classi solo operazioni che non conducano direttamente a contraddizioni.

È importante far presente che nella nostra teoria NGB esisteranno come oggetti anche le collezioni “grandi” che abbiamo considerato nei paradossi di Russell, di Cantor, e di Burali-Forti, ricordati sopra. Ad esempio, la collezione

$$R := \{x \text{ insieme} \mid x \notin x\}$$

sarà una classe, quindi un legittimo oggetto della teoria NGB. Il paradosso di Russell ci dice che R non può essere un insieme; si tratta quindi di una classe propria che non può appartenere ad alcuna classe; in particolare, $R \notin R$. Notiamo che questo

non determina una contraddizione perché R non è un insieme, e quindi da $R \notin R$ non possiamo dedurre che $R \in R$.

Anche la collezione universale $V = \{x \text{ insieme} \mid x = x\}$ di tutti gli insiemi, e la collezione ORD di tutti gli ordinali, saranno classi nella teoria NGB. I paradossi di Cantor e di Burali-Forti dimostrano semplicemente che V e ORD *non* sono insiemi, e quindi sono classi proprie.

Diamo di seguito la definizioni formali relative alle teoria NGB di von Neumann-Gödel-Bernays (ricordiamo che gli oggetti di questa teoria si chiamano *classi*). Cominciamo specificando il linguaggio.

- Le formule della teoria NGB sono le stesse formule del linguaggio della teoria degli insiemi considerate per la teoria ZFC.¹

DEFINIZIONE 3.1. Una classe A si dice *insieme* se esiste una classe B tale che $A \in B$. Una classe che non è un insieme si dice *classe propria*.

Le seguenti sono comode abbreviazioni che useremo nel seguito.

NOTAZIONE 3.2.

- Scriviamo “ x è un insieme” per intendere la formula “ $\exists y \ x \in y$ ”.
- Scriviamo “ $\forall^I x \ \varphi(x)$ ” per intendere “ $\forall x \ (\text{“}x \text{ insieme”} \rightarrow \varphi(x))$ ”, cioè:

$$\forall x \ (\exists y \ x \in y \rightarrow \varphi(x))$$
.
- Scriviamo “ $\exists^I x \ \varphi(x)$ ” per intendere “ $\exists x \ (\text{“}x \text{ insieme”} \wedge \varphi(x))$ ”, cioè:

$$\exists x \ (\exists y \ x \in y \wedge \varphi(x))$$
.

Nelle formule di sopra, come y possiamo considerare una qualunque variabile purché *non* compaia nella formula φ .

Di solito, ma non sempre, con lettere maiuscole $A, B, C, \dots$ denoteremo generiche classi, e con lettere minuscole $a, b, c, \dots$ denoteremo insiemi. Analogamente, useremo lettere maiuscole $X, Y, Z, \dots$ per indicare variabili che sono classi, e lettere minuscole $x, y, z, \dots$ per indicare variabili che sono insiemi.²

Elenchiamo finalmente gli assiomi di NGB. Come prima proprietà che riguarda le classi, estendiamo la validità del fondamentale principio di estensionalità.

NGB 1: Estensionalità per classi.

Due classi sono uguali se e solo se hanno gli stessi elementi:

$$\forall A \forall B \ ((\forall x (x \in A \leftrightarrow x \in B)) \leftrightarrow A = B).$$

Ricordiamo il principio di *comprensione*, già introdotto nel primo capitolo quando abbiamo trattato la teoria “ingenua” degli insiemi.

Principio di Comprensione (o di Astrazione). Se P è una proprietà “ammissibile”, allora esiste la sua estensione, cioè una “collezione” X tale che:

$$X = \{x \mid P(x)\}.$$

¹ Vedi Definizione ??.

² In alcuni testi, le lettere minuscole denotano esclusivamente insiemi. Ad esempio, scrivendo “ $\forall x \ \varphi(x)$ ” intendono “ $\forall^I x \ \varphi(x)$ ”; mentre la quantificazione universale (non ristretta agli insiemi) viene scritta nella forma “ $\forall X \ \varphi(X)$ ”, dove per la variabile quantificata si usa una lettera maiuscola.

Come ci hanno mostrato i paradossi, quel principio è contraddittorio se per proprietà “ammissibili” intendiamo quelle formalizzate da formule nel linguaggio della teoria degli insiemi, e se per “collezioni” intendiamo gli insiemi della teoria ZFC. Tuttavia il principio di comprensione è molto utile, ed infatti abbiamo incluso una sua versione più debole tra gli assiomi di ZFC, cioè l’assioma di *separazione*. Ricordiamo che quell’assioma postula l’esistenza dell’estensione di ogni proprietà, purché ci si restringa ai soli oggetti che appartengono ad un insieme prefissato.

Anche nella teoria delle classi NGB c’è un’assioma che postula il principio di comprensione in una forma limitata, dove le proprietà “ammissibili” sono quelle formalizzabili da formule in cui i quantificatori variano solo su insiemi. Grazie a questo assioma, tutte le classi di ZFC (che erano informalmente definite come collezioni ottenute come estensioni di formule) saranno oggetti della teoria NGB. L’intuizione è che però l’universo di NGB sia più ricco, e contenga come oggetti anche collezioni “non definibili” di insiemi, cioè collezioni che non sono estensione di alcuna formula.

DEFINIZIONE 3.3. Una formula φ si dice *predicativa* se tutti i suoi quantificatori sono ristretti ad insiemi, cioè compaiono sempre nella forma “ $\forall^{\mathcal{I}}x \dots$ ” oppure “ $\exists^{\mathcal{I}}x \dots$ ”.

NGB 2: Comprensione (o Astrazione).

Se $\varphi(x, x_1, \dots, x_n)$ una formula *predicativa* dove $x, x_1, \dots, x_n$ sono tutte e sole le variabili libere, allora il seguente è un assioma:

$$\forall A_1, \dots, A_n \exists C \forall x (x \in C \leftrightarrow (“x \text{ è un insieme}” \wedge \varphi(x, A_1, \dots, A_n))).$$

Denoteremo la classe C di sopra nel modo seguente:

$$C = \{x \text{ insieme} \mid \varphi(x, A_1, \dots, A_n)\}.$$

L’assioma di rimpiazzamento per classi ha un enunciato più semplice.

NGB 3: Rimpiazzamento.

Se F è una funzione e $a \subseteq \text{dom}(F)$ è un insieme, allora anche l’immagine $F[a] := \{F(x) \mid x \in a\}$ è un insieme:

$$\forall F \forall^{\mathcal{I}}a (“F \text{ funzione}” \rightarrow (\exists^{\mathcal{I}}b “b = F[a]”)).$$

Vogliamo che la nostra teoria delle classi incorpori la teoria degli insiemi ZFC, in modo che tutte le classi di ZFC siano effettivi oggetti della teoria.

Quest’ultima proprietà è di immediata verifica. Infatti sia $\mathbf{C} = \{x \mid \varphi(x)\}$ la classe di ZFC definita come estensione della formula $\varphi(x)$. Per l’assioma di comprensione, esiste in NGB la classe $C = \{x \mid \varphi^{\mathcal{I}}(x)\}$, dove con $\varphi^{\mathcal{I}}$ abbiamo denotato la formula ottenuta da φ restringendo tutti i quantificatori agli insiemi.³ Chiaramente C coincide con la collezione $\mathbf{C}$.

Per “inglobare” in NGB la teoria ZFC, dobbiamo postulare la validità di tutte le formule corrispondenti ad assiomi di ZFC, nella forma ristretta ad insiemi. Ad esempio, abbiamo visto sopra che se A è una classe anche $\bigcup A$ è una classe; ma se vogliamo mantenere la validità dell’assioma dell’unione per insiemi, dobbiamo postulare che se la classe A è un insieme, allora anche la classe $\bigcup A$ è un insieme.

³ Cioè, dove tutti i quantificatori vengono posti nella forma $\forall x (x \text{ “insieme”} \rightarrow \dots)$ o $\exists x (x \text{ “insieme”} \wedge \dots)$.

NGB 4: Assiomi di ZFC ristretti ad insiemi.

- *Insieme vuoto*: $\exists^I x \forall y y \notin x$.
- *Coppia*: $\forall^I x \forall^I y \exists^I z "z = \{x, y\}"$.
- *Unione*: $\forall^I x \exists^I y "y = \bigcup x"$.
- *Insieme potenza*: $\forall^I x \exists^I y "y = \mathcal{P}(x)"$.
- *Infinito*: $\exists^I x "x \text{ induttivo}"$.
- *Scelta*: $\forall^I \mathcal{F} \exists^I f ("f \text{ funzione}" \wedge \forall F \in \mathcal{F} (F \neq \emptyset \rightarrow f(F) \in F))$.

Le abbreviazioni usate sopra sono le stesse usate nei capitoli precedenti; ad esempio:⁴

- " $z = \{x, y\}$ " denota la formula " $\forall t (t \in z \leftrightarrow (t = x \vee t = y))$ ".
- " $y = \bigcup x$ " denota la formula " $\forall t (t \in y \leftrightarrow (\exists z (z \in x \wedge t \in z)))$ ".
- " $y = \mathcal{P}(x)$ " denota la formula " $\forall t (t \in y \leftrightarrow (\forall z (z \in t \rightarrow z \in x)))$ ".

Qualche commento sul gruppo di assiomi NGB 4:

- In conseguenza dell'assioma di comprensione NGB 2 esiste la classe senza elementi $\{x \text{ insieme} \mid x \neq x\}$. Tale classe è unica, visto l'assioma di estensionalità NGB 1. Visto l'assioma dell'insieme vuoto in NGB 4, quella classe senza elementi è un insieme, che denotiamo " $\emptyset$ ".
- L'assioma della coppia di ZFC vale nella forma ristretta ad insiemi, come postulata in NGB 4. Tuttavia quell'assioma *non* vale nella forma generale non ristretta. Infatti, se almeno una tra le classi A e B è una classe propria allora *non* esiste la classe coppia $C := \{A, B\}$, visto che le classi proprie *non* appartengono ad alcuna classe.
- L'assioma dell'unione vale anche nella versione non ristretta; infatti, se A è una classe, grazie al principio di comprensione esiste la classe $\bigcup A = \{x \mid \exists y \in A x \in y\}$.
- Applicando il principio di comprensione, per ogni classe A si dimostra che esiste la classe $\mathcal{P}(A) = \{x \text{ insieme} \mid x \subseteq A\}$. Notiamo che se A è un insieme, allora la classe $\mathcal{P}(A)$ è un insieme, in base all'assioma delle parti incluso in NGB 4. Tuttavia non vale la versione non ristretta di quella proprietà; infatti, se A è una classe propria, allora *non* esiste la classe che contiene tutte le sottoclassi di A , perchè una classe non può contenere classi proprie.
- L'assioma di comprensione NGB 2 garantisce l'esistenza della classe di tutti gli insiemi induttivi. Tuttavia solo l'assioma dell'infinito in NGB 4 garantisce che quella classe non è vuota.

Notiamo che non è stato necessario includere in NGB 4 la lista completa degli assiomi di ZFC, perchè quelli mancanti sono conseguenza degli altri assiomi di NGB. Infatti, la restrizione dell'estensionalità ad insiemi è conseguenza diretta di NGB 1; inoltre – come vedremo di seguito – sia lo schema di separazione, sia lo schema di rimpiazzamento di ZFC sono dimostrabili nella teoria NGB.

ESERCIZIO 3.4. Dimostrare che se A, B sono classi, allora anche le seguenti sono classi:

⁴ Notiamo che in queste tre formule (usate all'interno di assiomi in NGB 4) non c'è bisogno di restringere i quantificatori $\forall t, \exists z, \forall z$ agli insiemi, perchè per ipotesi sia x che y sono insiemi.

- (1) $A \cup B := \{x \mid x \in A \vee x \in B\}.$
- (2) $A \cap B := \{x \mid x \in A \wedge x \in B\}.$
- (3) $A \setminus B := \{x \mid x \in A \wedge x \notin B\}.$
- (4) $A \times B := \{x \mid \exists a \in A \exists b \in B x = (a, b)\}.$
- (5) $\bigcup A := \{x \mid \exists y \in A x \in y\}.$
- (6) $\mathcal{P}(A) := \{x \text{ insieme} \mid x \subseteq A\}.$
- (7) $\text{dom}(A) := \{x \text{ insieme} \mid \exists y (x, y) \in A\}.$
- (8) $\text{imm}(A) := \{y \text{ insieme} \mid \exists x (x, y) \in A\}.$

ESERCIZIO 3.5.

- (1) La relazione di identità tra insiemi è una classe propria:⁵

$$\Delta := \{(x, x) \mid x \text{ insieme}\}.$$

- (2) La relazione di appartenenza tra insiemi è una classe propria:

$$E := \{(x, y) \mid x, y \text{ insieme} \wedge x \in y\}.$$

TEOREMA 3.6 (NGB). *Vale la*

- *Proprietà dell'intersezione:*

Se C è una classe e b è un insieme, allora anche $C \cap b$ è un insieme:

$$\forall C \forall^I b \exists^I a \forall x (x \in a \leftrightarrow (x \in C \wedge x \in b))$$

DIM. Se non esistono insiemi $x \in C$ tali che $x \in b$, allora la classe $C \cap b$ è l'insieme vuoto. Altrimenti possiamo prendere un elemento $\star \in C$ tale che $\star \in b$, e definire la funzione $F : V \rightarrow V$ ponendo

$$F(x) = \begin{cases} x & \text{se } x \in C \\ \star & \text{se } x \notin C. \end{cases}$$

Per il rimpiazzamento, l'immagine $F[b] = \{F(x) \mid x \in b\}$ è un insieme. È poi immediato verificare che $F[b] = C \cap b$, e quindi $C \cap b$ è un insieme. $\square$

Da NGB segue lo schema di rimpiazzamento di ZFC.

TEOREMA 3.7 (NGB). *Vale lo schema di rimpiazzamento di ZFC.*

DIM. Sia $\varphi(x, y)$ una formula funzionale. Notiamo che se x e y sono insiemi, allora anche la coppia ordinata di Kuratowski $(x, y) = \{\{x\}, \{x, y\}\}$ è un insieme (come fatto in ZFC, si usano l'assioma della coppia e l'assioma dell'unione per insiemi del gruppo NGB 4). Allora, per l'assioma di comprensione, esiste in NGB la funzione

$$F := \{t \mid \exists^I x \exists^I y t = (x, y) \wedge \varphi(x, y)\}.$$

Se A è un insieme, dal rimpiazzamento in NGB segue che anche

$$F[A] = \{F(x) \mid x \in A\} = \{y \mid \exists x \in A \varphi(x, y)\}$$

è un insieme. $\square$

⁵ Abbiamo usato la consueta notazione funzionale, per intendere

$$\Delta := \{t \mid \exists x t = (x, x)\} \quad \text{e} \quad E := \{t \mid \exists x \exists y x \in y \wedge t = (x, y)\}.$$

Si può dimostrare (ma non lo facciamo qui perché servirebbero strumenti che non abbiamo) che gli assiomi di coppia, di unione, e di potenza ristretti ad insiemi, *non* sono dimostrabili a partire dagli assiomi per classi NGB 1, NGB 3, e NGB 4.

Ricalcando quanto già visto in ZFC, gli assiomi dati permettono di dimostrare che la classe degli insiemi è chiusa rispetto alle fondamentali operazioni.

ESERCIZIO 3.8.

- (1) Se A, B sono insiemi, allora anche $A \cup B$ è un insieme.
- (2) Se R è un insieme, allora anche $\text{dom}(R)$ e $\text{imm}(R)$ sono insiemi;
- (3) Se a, b sono insiemi, allora anche la coppia ordinata (a, b) è un insieme;
- (4) Se A, B sono insiemi, allora anche $A \times B$ è un insieme;
- (5) Se una classe f è una funzione dove $\text{dom}(f)$ è un insieme, allora f è un insieme.

ESERCIZIO 3.9. Dimostrare che non esistono funzioni iniettive $F : C \rightarrow b$ da una classe propria C a valori in un insieme b .

ESERCIZIO 3.10. Dimostrare che per ogni insieme $a \neq \emptyset$, la sua classe di equipotenza $|a| := \{b \text{ insieme} \mid |b| = |a|\}$.

Alcuni autori includono tra gli assiomi della teoria di von Neumann-Gödel-Bernays anche il seguente:

- **Scelta globale:** *Esiste una funzione $F : V \rightarrow V$ definita sulla classe V di tutti gli insiemi tale che $F(x) \in x$ per ogni x insieme non vuoto x .*

Quella forte forma di scelta non è necessaria ai nostri scopi, e quindi non l'abbiamo inserita.

Una caratteristica importante della teoria delle classi NGB, dimostrata da Gödel, è il fatto che si tratta di una teoria *finitamente assiomatizzabile*. Questo significa che si può trovare una lista finita di assiomi (che Gödel ha fornito esplicitamente) che sono equivalenti a quelli di NGB.

Un fondamentale risultato in questo ambito che è dimostrabile con gli strumenti della logica matematica è il seguente:

- *Sia σ un enunciato (cioè una formula senza variabili libere) nel linguaggio della teoria degli insiemi, e sia σ^I la formula ottenuta da σ rimpiazzando ogni quantificatore $\forall x, \exists x$ con la sua restrizione $\forall^I x, \exists^I x$. Allora σ è un teorema di ZFC se e solo se σ^I è un teorema della teoria NGB.*

Come conseguenza, le teorie ZFC e NGB sono equiconsistenti, cioè sono entrambe non contraddittorie o sono entrambe contraddittorie.⁶

⁶ Naturalmente gli insiemisti credono nella prima ipotesi, che però sarebbe dimostrabile soltanto se le teorie fossero contraddittorie, a causa del *teorema di incompletezza* di Gödel. Ricordiamo che una teoria T è contraddittoria se dimostra sia σ che la sua negazione $\neg\sigma$ per un certo enunciato σ . Una teoria è contraddittoria se e solo se dimostra *tutti* gli enunciati σ , in accordo col motto di origine medioevale: *ex falso sequitur quodlibet*.

4. La ricorsione transfinita

Ricordiamo che un tipico procedimento per definire successioni (cioè funzioni con dominio $\mathbb{N}$) è la ricorsione numerabile. Tale proprietà garantisce l'esistenza ed unicità di una successione, una volta che sia stabilito in modo “definibile” quale deve essere il suo valore in un numero qualunque, se assumiamo come noti i suoi valori sui numeri più piccoli. Un esempio tipico è la funzione fattoriale $n \mapsto n!$ che è definita come l'unica successione $f : \omega \rightarrow \omega$ tale che $f(0) = 1$ e $f(n+1) = f(n) \cdot (n+1)$.

Nell'ambito della teoria degli insiemi, è utile avere a disposizione uno strumento analogo che più in generale permetta di definire funzioni definite su ordinali, o anche funzioni-classe definite sull'intera classe ORD degli ordinali. La formulazione dei teoremi di “ricorsione transfinita” è più semplice all'interno della teoria delle classi NGB; vedremo comunque in seguito come formulare correttamente quei teoremi anche nel linguaggio della teoria degli insiemi ZFC. In entrambi i casi, l'assioma di rimpiazzamento giocherà un ruolo cruciale.

TEOREMA 4.1 (NGB – Ricorsione transfinita su un ordinale). *Sia $G : V \rightarrow V$ una funzione definita per tutti gli insiemi. Allora per ogni ordinale α esiste ed è unica funzione f con dominio α e tale che per ogni $\gamma \in \alpha$ si ha:*

$$(\star) \quad f(\gamma) = G(f|_\gamma).$$

Notiamo che la funzione f la cui esistenza è garantita dal teorema di ricorsione transfinita è un insieme, visto che il suo dominio è un insieme.⁷

DIM. Per ogni ordinale $\beta \in \alpha$, chiamiamo β -*approssimazione* una funzione f_β avente come dominio $\text{dom}(f_\beta) = \beta$, e che soddisfa le proprietà $(\star)$ per ogni $\gamma \in \text{dom}(f_\beta)$. Procediamo per induzione transfinita e mostriamo che per ogni $\beta \in \alpha$, esiste ed è unica una β -approssimazione f_β .

Se $\beta = 0$, allora $f_0 = \emptyset$ è una 0-approssimazione, ed è banalmente unica.

Se $\beta = \gamma + 1$ è successore, prendiamo la γ -approssimazione f_γ che esiste ed è unica per ipotesi induttiva, ed estendiamo imponendo che il valore in γ sia quello imposto dalla condizione $(\star)$. Precisamente, definiamo $f_\beta := f_\gamma \cup \{(\gamma, G(f_\gamma))\}$. Chiaramente $\text{dom}(f_\beta) = \text{dom}(f_\gamma) \cup \{\gamma\} = \gamma \cup \{\gamma\} = \gamma + 1 = \beta$; inoltre segue direttamente dalla definizione che f_β soddisfa la proprietà $(\star)$, ed è quindi una β -approssimazione. Inoltre, se f e g sono due β -approssimazioni, allora le loro restrizioni $f|_\gamma$ e $g|_\gamma$ coincidono perchè sono due γ -approssimazioni, e le γ -approssimazioni sono uniche per ipotesi induttiva. Infine, anche $f(\gamma) = G(f|_\gamma) = G(g|_\gamma) = g(\gamma)$. Possiamo concludere che $f = g$, come volevamo.

Nel caso $\beta = \lambda$ limite, consideriamo la funzione (classe) F che associa ad ogni ordinale $\gamma < \lambda$ l'unica γ -approssimazione f_γ . Per l'assioma di *rimpiazzamento*, l'immagine $F[\lambda] = \{f_\gamma \mid \gamma < \lambda\}$ è un insieme. Se $\gamma' < \gamma < \lambda$, la restrizione di f_γ all'insieme γ' è una γ' -approssimazione e quindi coincide con $f_{\gamma'}$, vista l'unicità delle γ' -approssimazioni garantita dall'ipotesi induttiva. In altre parole, f_γ è un'estensione di $f_{\gamma'}$ e questo dimostra che $\{f_\gamma \mid \gamma < \lambda\}$ è una famiglia di funzioni a due a due compatibili, e quindi anche l'unione $f_\lambda := \bigcup_{\gamma < \lambda} f_\gamma$ è una funzione (vedi Proposizione ??). Infine, si verifica direttamente che tale f_λ è una λ -approssimazione, ed è unica.

⁷ Cfr. Esercizio 3.8 (3).

Infine, usando di nuovo l'assioma di rimpiazzamento e ragionando in modo del tutto simile a sopra, si ottiene l'esistenza dell'insieme $\{f_\gamma \mid \gamma \in \alpha\}$ di tutte le γ -approssimazioni, e quindi si ottiene l'esistenza della funzione $f = \bigcup_{\gamma \in \alpha} f_\gamma$ che ha le proprietà volute. $\square$

Già nel caso particolare $\alpha = \omega$, il Teorema di ricorsione transfinita rafforza il Teorema di ricorsione numerabile ???. Notiamo infatti che nella ricorsione numerabile era necessario partire da funzioni $g : \omega \times A \rightarrow A$ che assumevano valori in un insieme assegnato A ; col teorema di sopra possiamo estendere la validità di quella procedura e considerare più in generale arbitrarie funzioni (classe) $G : V \rightarrow V$.

Vediamo una prima applicazione del teorema di ricorsione transfinita nel caso $\alpha = \omega$.

DEFINIZIONE 4.2. Si dice *chiusura transitiva* di un insieme A l'insieme $\text{TC}(A) = \bigcup_{n \in \omega} A_n$, dove si pone per ricorsione su ω :

$$\begin{cases} A_0 = A \\ A_{n+1} = \bigcup A_n = \{y \mid \exists x \in A_n \ y \in x\} \end{cases}$$

L'esistenza della successione $\sigma = \langle A_n \mid n \in \omega \rangle$ segue per ricorsione transfinita su ω considerando come $G : V \rightarrow V$ una qualunque funzione tale che $G(\emptyset) = A$, e che associa ad ogni sequenza finita non vuota $\tau = \langle \tau(0), \tau(1), \dots, \tau(n) \rangle$ l'unione del suo ultimo termine, cioè $\bigcup \tau(n)$. Infatti in questo caso si ha che $\sigma(n+1) = A_{n+1} = G(\sigma|_{n+1}) = G(\langle A_0, \dots, A_n \rangle) = \bigcup A_n$, come richiesto.

Notiamo invece che il teorema di ricorsione numerabile *non* garantisce l'esistenza della successione $\sigma = \langle A_n \mid n \in \omega \rangle$; infatti, se non si assume già l'esistenza della chiusura transitiva di A , non abbiamo a disposizione un insieme B ed una funzione $g : \omega \times B \rightarrow B$ tale che $g(n+1, A_n) = \bigcup A_n$.

Il nome “chiusura transitiva” è giustificato dalla seguente proprietà:

PROPOSIZIONE 4.3. *La chiusura transitiva di un insieme è il più piccolo insieme transitivo che lo include.*

DIM. Sia A un insieme qualunque. Vediamo prima che $\text{TC}(A)$ è effettivamente un insieme transitivo. Dati $y \in x \in \text{TC}(A)$, prendiamo $n \in \omega$ tale che $x \in A_n$. Ma $y \in x \in A_n$ significa che $x \in \bigcup A_n = A_{n+1}$, e quindi anche $y \in A$.

Per ottenere la proprietà di minimalità dobbiamo verificare che se $T \supseteq A$ è un insieme transitivo che include A allora necessariamente $T \supseteq \text{TC}(A)$. Procediamo per induzione, e dimostriamo che $A_n \subseteq T$ per ogni $n \in \omega$. La base induttiva $A_0 = A \subseteq T$ è vera per ipotesi. Supponiamo ora che $A_n \subseteq T$. Dalla transitività di T segue che $y \in x \in A_n \subseteq T \Rightarrow y \in T$, e quindi $A_{n+1} = \bigcup A_n \subseteq T$. $\square$

La versione più generale della ricorsione transfinita garantisce l'esistenza di funzioni definite su tutta la classe degli ordinali.

TEOREMA 4.4 (NGB – Ricorsione transfinita su ORD). *Sia $G : V \rightarrow V$ una funzione definita per tutti gli insiemi. Allora esiste ed è unica funzione $F : \text{ORD} \rightarrow V$ tale che per ogni ordinale γ si ha:*

$$(\star) \quad f(\gamma) = G(f|_\gamma).$$

DIM. Dal teorema precedente (ricorsione transfinita per ordinali) sappiamo che per ogni ordinale α esiste ed unica α -approssimazione f_α , cioè una funzione f_α avente come dominio α e che soddisfa la proprietà $f_\alpha(\gamma) = G(f_\alpha|_\gamma)$ per ogni $\gamma \in \alpha$. Vista l'unicità, le approssimazioni sono una restrizione dell'altra, cioè se $\beta < \alpha$, allora $f_\alpha|_\beta = f_\beta$. Per comprensione, esiste la funzione Φ avente come dominio ORD e tale che $\Phi(\alpha) = f_\alpha$ per ogni α . La funzione F cercata è allora la funzione ottenuta come unione $F = \bigcup \text{imm}(\Phi) = \bigcup_{\alpha \in \text{ORD}} f_\alpha$, cioè quella definita dalla seguente formula funzionale:

$$\varphi(\alpha, y) : \quad \alpha \text{ è un ordinale} \wedge \text{“}\exists f_\alpha \text{ } \alpha\text{-approssimazione con } f_\alpha(\alpha) = y\text{”}.$$

□

Nella pratica, nelle definizioni per ricorsione transfinita spesso si distingue tra caso zero, caso successore e caso limite. Ecco la formulazione:

TEOREMA 4.5 (NGB – Ricorsione transfinita su ORD, formulazione per casi).
Sia A un insieme, e siano $G_1, G_2 : V \rightarrow V$ due funzioni. Allora esiste ed unica funzione $F : \text{ORD} \rightarrow V$ tale che:

$$(\star) \quad \begin{cases} F(0) &= A ; \\ F(\beta + 1) &= G_1(\beta, F(\beta)) ; \\ F(\lambda) &= G_2(\lambda, F|_\lambda) \text{ se } \lambda \text{ è limite.} \end{cases}$$

La formulazione della ricorsione transfinita “per casi” segue da quella generale.

ESERCIZIO 4.6. * Dimostrare il Teorema di ricorsione transfinita 4.4 come conseguenza del Teorema di ricorsione transfinita “per casi” 4.5.

Algebra ordinale

1. Somma, prodotto, ed esponenziazione di ordinali

Come primo esempio rilevante di applicazione del teorema di ricorsione nella sua forma più generale, definiamo le fondamentali operazioni algebriche di somma e prodotto tra ordinali.

DEFINIZIONE 1.1. Per ogni ordinale fissato α , per ricorsione transfinita su β poniamo:

$$\begin{cases} \alpha + 0 &= \alpha \\ \alpha + (\beta + 1) &= (\alpha + \beta) + 1 \\ \alpha + \lambda &= \bigcup_{\beta < \lambda} \alpha + \beta \text{ se } \lambda \text{ è limite.} \end{cases}$$

$$\begin{cases} \alpha \cdot 0 &= 0 \\ \alpha \cdot (\beta + 1) &= (\alpha \cdot \beta) + \alpha \\ \alpha \cdot \lambda &= \bigcup_{\beta < \lambda} \alpha \cdot \beta \text{ se } \lambda \text{ è limite.} \end{cases}$$

Le definizioni date sopra sono coerenti con le operazioni di somma e prodotto tra buoni ordini che avevamo definito in precedenza.

PROPOSIZIONE 1.2. *Siano α e β ordinali. Allora:*

- (1) *L'insieme bene ordinato $\alpha \mathbin{+} \beta$ è isomorfo alla somma ordinale $\alpha + \beta$;*
- (2) *L'insieme bene ordinato $\alpha \mathbin{\times} \beta$ è isomorfo al prodotto ordinale $\alpha \cdot \beta$.*

DIM. (1) Ricordiamo che $\alpha \mathbin{+} \beta = (\alpha \mathbin{\uplus} \beta, \prec)$ dove $\alpha \mathbin{\uplus} \beta$ è l'unione *disgiunta* di α e β , e dove l'ordine $\prec$ mantiene l'ordine tra coppie di elementi di α e tra coppie di elementi di β , e impone che $a \prec b$ se $a \in \alpha$ e $b \in \beta$.

Procediamo per induzione transfinita su β , e mostriamo che esiste un isomorfismo $\psi_\beta : \alpha \mathbin{+} \beta \rightarrow \alpha + \beta$.

Se $\beta = 0$, la tesi è banale. Supponiamo ora $\beta = \gamma + 1$ successore. Per ipotesi induttiva esiste un isomorfismo $\psi : \alpha \mathbin{+} \gamma \rightarrow \alpha + \gamma$. Ma allora $\psi' = \psi \cup \{(\gamma, \alpha + \gamma)\}$ è l'isomorfismo cercato tra l'insieme bene ordinato $\alpha \mathbin{+} (\gamma + 1) = \alpha \mathbin{+} (\gamma \cup \{\gamma\})$, e l'ordinale $\alpha + (\gamma + 1)$, che per definizione è uguale a $(\alpha + \gamma) + 1 = (\alpha + \gamma) \cup \{\alpha + \gamma\}$.

Se β è limite, allora $\beta = \bigcup_{\gamma < \beta} \gamma$ e quindi

$$\alpha \mathbin{+} \beta = (\alpha \times \{0\}) \cup \left(\bigcup_{\gamma < \beta} \gamma \times \{1\} \right) = \bigcup_{\gamma < \beta} ((\alpha \times \{0\}) \cup (\gamma \times \{1\})) = \bigcup_{\gamma < \beta} (\alpha \mathbin{+} \gamma).$$

Inoltre, per definizione di somma con un ordinale limite, $\alpha + \beta = \bigcup_{\gamma < \beta} (\alpha + \gamma)$. Per ipotesi induttiva, per ogni $\gamma < \beta$ esiste un isomorfismo $\psi_\gamma : \alpha \mathbin{+} \gamma \rightarrow \alpha + \gamma$. Vista l'unicità degli isomorfismi tra insiemi bene ordinati, necessariamente per ogni $\gamma' < \gamma < \beta$, la restrizione di ψ_γ all'insieme $\alpha \mathbin{+} \gamma'$ coincide con $\psi_{\gamma'}$. Dunque le funzioni in $\{\psi_\gamma \mid \gamma < \beta\}$ sono a due a due compatibili, e la loro unione $\psi = \bigcup_{\gamma < \beta} \psi_\gamma : \alpha \mathbin{+} \beta \rightarrow \alpha + \beta$ è l'isomorfismo cercato.

(2) Ricordiamo che $\alpha \mathbin{\times} \beta = (\alpha \times \beta, \prec)$ dove $\prec$ è l'ordine *antilexicografico*, cioè $(a, b) \prec (a', b')$ se $b < b'$ in β , oppure se $b = b'$ e $a < a'$ in α .

Per induzione transfinita su β , dimostriamo che gli insiemi bene ordinati $\alpha \times \beta$ e $\alpha \cdot \beta$ sono isomorfi.

Se $\beta = 0$, la tesi è banale perché $\alpha \times 0 = 0 = \alpha \cdot 0$ è l'insieme vuoto. Supponiamo ora $\beta = \gamma + 1$ successore. Informalmente, $\alpha \times (\gamma + 1)$ si ottiene disponendo in sequenza $\gamma + 1$ copie successive di α , cioè γ copie di α seguite da un'ultima copia di α . È dunque facile mostrare che esiste un isomorfismo $\alpha \times (\gamma + 1) \cong (\alpha \times \gamma) + \alpha$. Per ipotesi induttiva, quest'ultimo è isomorfo a $(\alpha \cdot \gamma) + \alpha$, il quale a sua volta, per quanto già dimostrato riguardo la somma, è isomorfo a $(\alpha \cdot \gamma) + \alpha$. Concludiamo notando che, per definizione, $(\alpha \cdot \gamma) + \alpha = \alpha \cdot (\gamma + 1)$.

Se β è limite, notiamo che $\alpha \times \beta = \alpha \times (\bigcup_{\gamma < \beta} \gamma) = \bigcup_{\gamma < \beta} (\alpha \times \gamma)$. Notiamo inoltre, per definizione di prodotto ordinale, $\alpha \cdot \beta = \bigcup_{\gamma < \beta} \alpha \cdot \gamma$. Si procede poi esattamente come nella dimostrazione del passo limite della somma, considerando l'unione $\bigcup_{\gamma < \beta} \psi_\gamma$ dove ψ_γ è (l'unico) isomorfismo dato dall'ipotesi induttiva tra $\alpha \times \gamma$ e $\alpha \cdot \gamma$. $\square$

ESERCIZIO 1.3. Dimostrare che per ogni ordinale α si ha $0 + \alpha = \alpha$ e $1 \cdot \alpha = \alpha$.

ESERCIZIO 1.4. Per ogni ordinale infinito α e per ogni $n \in \omega$ si ha che $n + \alpha = \alpha$.

Vale l'analoga proprietà per il prodotto? Cioè, se α è un ordinale infinito e $n \geq 1$ è un numero naturale allora necessariamente $n \cdot \alpha = \alpha$?

Ricordiamo che valgono le proprietà associative della somma e del prodotto fra buoni ordini (vedi Esercizi ?? e ??):

$$A + (B + C) \cong (A + B) + C; \quad A \times (B \times C) \cong (A \times B) \times C.$$

Come conseguenza diretta della proposizione precedente, si ottiene che anche la somma e il prodotto tra ordinali sono operazioni associative.

Analogamente, dalla proprietà distributiva del prodotto tra buoni ordini rispetto alla somma (vedi Proposizione ??):

$$A \times (B + C) \cong (A \times B) + (A \times C),$$

si ottiene la proprietà distributiva anche per gli ordinali.

Di seguito, dimostriamo direttamente quelle proprietà degli ordinali usando l'induzione transfinita, senza fare ricorso agli analoghi risultati dei buoni ordini.

PROPOSIZIONE 1.5. *Siano α, β, γ ordinali.*

- (1) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$;
- (2) $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$;
- (3) $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

DIM. Fissati α e β , dimostriamo tutte e tre le proprietà procedendo per induzione transfinita su γ .

(1). Il caso base $\gamma = 0$ è banale. Nel caso successore $\gamma = \delta + 1$ abbiamo:

$$\begin{aligned} \alpha + (\beta + \gamma) &= \alpha + (\beta + (\delta + 1)) \stackrel{1}{=} \alpha + ((\beta + \delta) + 1) \stackrel{2}{=} (\alpha + (\beta + \delta)) + 1 \stackrel{3}{=} \\ &\stackrel{3}{=} ((\alpha + \beta) + \delta) + 1 \stackrel{4}{=} (\alpha + \beta) + (\delta + 1) = (\alpha + \beta) + \gamma, \end{aligned}$$

dove nelle uguaglianze 1, 2, e 4 abbiamo usato la definizione di somma con un ordinale successore, e nell'uguaglianza 3 abbiamo usato l'ipotesi induttiva. Infine, nel caso limite $\gamma = \lambda$ abbiamo:

$$(\alpha + \beta) + \lambda \stackrel{1}{=} \bigcup_{\delta < \lambda} ((\alpha + \beta) + \delta) \stackrel{2}{=} \bigcup_{\delta < \lambda} (\alpha + (\beta + \delta)) \stackrel{3}{=} \bigcup_{\xi < \beta + \lambda} \alpha + \xi \stackrel{4}{=} \alpha + (\beta + \lambda).$$

dove nelle uguaglianze 1 e 4 abbiamo usato la definizione di somma con un ordinale limite, e nell'uguaglianza 2 abbiamo usato l'ipotesi induttiva. Inoltre, nell'uguaglianza 3, abbiamo usato il fatto che le unioni di ordinali corrispondono agli estremi superiori, che $(\beta + \delta \mid \delta < \lambda)$ è una sequenza infinita crescente illimitata in $\beta + \lambda$, e che quindi $\sup\{\alpha + (\beta + \delta) \mid \delta < \lambda\} = \sup\{\alpha + \xi \mid \xi < \beta + \lambda\}$.

(3). Il caso base $\gamma = 0$ è banale. Nel caso successore $\gamma = \delta + 1$ abbiamo:

$$\begin{aligned} \alpha \cdot (\beta + \gamma) &= \alpha \cdot (\beta + (\delta + 1)) \stackrel{1}{=} \alpha \cdot ((\beta + \delta) + 1) \stackrel{2}{=} \alpha \cdot (\beta + \delta) + \alpha \stackrel{3}{=} \\ &\stackrel{3}{=} (\alpha \cdot \beta + \alpha \cdot \delta) + \alpha \stackrel{4}{=} \alpha \cdot \beta + (\alpha \cdot \delta + \alpha) \stackrel{5}{=} \alpha \cdot \beta + (\alpha \cdot (\delta + 1)) = \alpha \cdot \beta + \alpha \cdot \gamma, \end{aligned}$$

dove nelle uguaglianze 1 e 5 abbiamo usato la definizione di somma con un ordinale successore, nell'uguaglianza 2 abbiamo usato la definizione di prodotto per un ordinale successore, nell'uguaglianza 3 abbiamo usato l'ipotesi induttiva, e nell'uguaglianza 4 abbiamo usato la proprietà associativa della somma vista sopra.

Nel caso limite $\gamma = \lambda$ abbiamo:

$$\alpha \cdot (\beta + \lambda) \stackrel{1}{=} \bigcup_{\xi < \beta + \lambda} \alpha \cdot \xi \stackrel{2}{=} \bigcup_{\delta < \lambda} \alpha \cdot (\beta + \delta) \stackrel{3}{=} \bigcup_{\delta < \lambda} (\alpha \cdot \beta + \alpha \cdot \delta) \stackrel{4}{=} \bigcup_{\eta < \alpha \cdot \lambda} (\alpha \cdot \beta + \eta) \stackrel{5}{=} \alpha \cdot \beta + \alpha \cdot \lambda,$$

dove nelle uguaglianze 1 e 5 abbiamo usato la definizione di somma con un ordinale limite, e nell'uguaglianza 3 abbiamo usato l'ipotesi induttiva. Inoltre, nelle uguaglianze 2 e 4 abbiamo usato il fatto che le unioni di ordinali corrispondono agli estremi superiori, che $(\beta + \delta \mid \delta < \lambda)$ e $(\alpha \cdot \delta \mid \delta < \lambda)$ sono sequenze infinite crescenti illimitate rispettivamente in $\beta + \lambda$ e in $\alpha \cdot \lambda$, e che quindi $\sup\{\alpha \cdot (\beta + \delta) \mid \delta < \lambda\} = \sup\{\alpha \cdot \xi \mid \xi < \beta + \lambda\}$, e $\sup\{\alpha \cdot \beta + \alpha \cdot \delta \mid \delta < \lambda\} = \sup\{\alpha \cdot \beta + \eta \mid \eta < \alpha \cdot \lambda\}$.

(2). Il caso base $\gamma = 0$ è banale. Nel caso successore $\gamma = \delta + 1$ abbiamo:

$$\begin{aligned} \alpha \cdot (\beta \cdot \gamma) &= \alpha \cdot (\beta \cdot (\delta + 1)) \stackrel{1}{=} \alpha \cdot ((\beta \cdot \delta) + \beta) \stackrel{2}{=} \alpha \cdot (\beta \cdot \delta) + \alpha \cdot \beta \stackrel{3}{=} \\ &\stackrel{3}{=} (\alpha \cdot \beta) \cdot \delta + \alpha \cdot \beta \stackrel{4}{=} (\alpha \cdot \beta) \cdot (\delta + 1) = (\alpha \cdot \beta) \cdot \gamma, \end{aligned}$$

dove nelle uguaglianze 1 e 4 abbiamo usato la definizione di prodotto con un ordinale limite, nell'uguaglianza 2 abbiamo usato la proprietà distributiva (3) vista sopra, e nell'uguaglianza 3 abbiamo usato l'ipotesi induttiva.

Nel caso limite $\gamma = \lambda$ abbiamo:

$$\alpha \cdot (\beta \cdot \lambda) \stackrel{1}{=} \bigcup_{\xi < \beta \cdot \lambda} \alpha \cdot \xi \stackrel{2}{=} \bigcup_{\delta < \lambda} (\alpha \cdot (\beta \cdot \delta)) \stackrel{3}{=} \bigcup_{\delta < \lambda} ((\alpha \cdot \beta) \cdot \delta) \stackrel{4}{=} (\alpha \cdot \beta) \cdot \lambda,$$

dove nelle uguaglianze 1 e 4 abbiamo usato la definizione di prodotto con un ordinale limite, e nell'uguaglianza 3 abbiamo usato l'ipotesi induttiva. Inoltre, nell'uguaglianza 2 abbiamo usato il fatto che le unioni di ordinali corrispondono agli estremi superiori, che $(\beta \cdot \delta \mid \delta < \lambda)$ è una sequenza infinita crescente illimitata in $\beta \cdot \lambda$, e che quindi $\sup\{\alpha \cdot (\beta \cdot \delta) \mid \delta < \lambda\} = \sup\{\alpha \cdot \xi \mid \xi < \beta \cdot \lambda\}$. $\square$

ESERCIZIO 1.6. Dimostrare che per β e per ogni $\gamma \geq 1$ si ha $\beta < \beta + \gamma$. Analogamente, dimostrare che per β e per ogni $\gamma \geq 2$ si ha $\beta < \beta \cdot \gamma$.

PROPOSIZIONE 1.7. Siano $\alpha, \beta \neq 0$ ordinali. Allora:

- (1) La somma $\alpha + \beta$ è un successore se e solo se β è un successore.
- (2) Il prodotto $\alpha \cdot \beta$ è un successore se e solo se sia α che β sono successori.
- (3) Se $\alpha \geq 2$, l'esponentiale α^β è un successore se e solo se $\beta \in \omega$ è un numero naturale.

DIM. FARE

□

Possiamo riassumere i risultati della proposizione precedente nella seguente tabella, dove “S” indica ordinale *successore*, e “L” indica ordinale *limite*.

α	β	$\alpha + \beta$	$\alpha \cdot \beta$	α^β
S	S	S	S	S se $\beta \in \omega$; L se $\beta \notin \omega$
S	L	L	L	L
L	S	S	L	L
L	L	L	L	L

Il primo importante risultato sull'algebra ordinale è il seguente.

TEOREMA 1.8 (Sottrazione a destra). *Se $\alpha < \beta$, allora esiste ed unico $\gamma > 0$ tale che $\alpha + \gamma = \beta$.*

DIM. Dimostriamo intanto questa semplice proprietà preliminare.

- Per tutti gli α, β ordinali si ha $\alpha + \beta \geq \beta$.

Procediamo per induzione su β . Il caso $\beta = 0$ è banale perchè $\alpha + 0 = \alpha \geq 0 = \beta$. Se $\beta = \delta + 1$ è successore, dall'ipotesi induttiva $\alpha + \delta \geq \delta$ segue direttamente che $\alpha + \beta = (\alpha + \delta) + 1 \geq \delta + 1 = \beta$. Infine se β è un ordinale limite, allora $\alpha + \beta = \bigcup_{\delta < \beta} \alpha + \delta \geq$ (per ipotesi induttiva) $\geq \bigcup_{\delta < \beta} \delta = \beta$.

Alternativamente, basta notare che la mappa $\psi : \gamma \mapsto \alpha + \gamma$ determina un isomorfismo tra $(\beta, \in)$ e $((\alpha + \beta) \setminus \alpha, \in)$. Visto che $(\alpha + \beta) \setminus \alpha \subseteq \alpha + \beta$ si ha che $\text{ot}(\beta) = \text{ot}((\alpha + \beta) \setminus \alpha) \leq \text{ot}(\alpha + \beta)$, e quindi $\beta \leq \alpha + \beta$.

La proprietà di sopra garantisce l'esistenza di ordinali ξ tali $\alpha + \xi > \beta$; ad esempio $\alpha + (\beta + 1) \geq \beta + 1 > \beta$. Prendiamo il minimo δ di tali ordinali ξ , cioè $\delta = \min\{\xi \mid \alpha + \xi > \beta\}$. Ovviamente $\delta \neq 0$ perchè $\alpha < \beta$. Osserviamo inoltre che δ non è un ordinale limite, altrimenti da $\beta < \alpha + \delta = \bigcup_{\eta < \delta} \alpha + \eta$ seguirebbe che $\beta < \alpha + \eta$ per un opportuno $\eta < \delta$, contro la minimalità di δ . Quindi $\delta = \gamma + 1$ è un successore, e si ha $\alpha + \gamma \leq \beta < \alpha + \gamma + 1$, e quindi $\beta = \alpha + \gamma$.

Per provare l'unicità della differenza, supponiamo che $\alpha + \gamma = \beta$ e $\alpha + \gamma' = \beta$. Se per assurdo γ e γ' fossero diversi, allora uno sarebbe maggiore dell'altro, ad esempio $\gamma > \gamma'$. Per quanto dimostrato sopra, allora esisterebbe una differenza η tale che $\gamma = \gamma' + \eta$. Ovviamente $\eta > 0$ perchè $\gamma > \gamma'$, e quindi avremmo che $\beta = \alpha + \gamma = \alpha + \gamma' + \eta = \beta + \eta > \beta$, assurdo. □

Somme e prodotti tra ordinali preservano le disuguaglianze deboli a sinistra, e preservano le disuguaglianze forti a destra.

PROPOSIZIONE 1.9. *Siano α, β, γ ordinali.*

- (1) *Se $\alpha \leq \beta$ allora $\alpha + \gamma \leq \beta + \gamma$;*
- (2) *Se $\alpha < \beta$ allora $\gamma + \alpha < \gamma + \beta$;*
- (3) *Se $\alpha \leq \beta$ allora $\alpha \cdot \gamma \leq \beta \cdot \gamma$;*
- (4) *Se $\alpha < \beta$ e $\gamma \geq 1$ allora $\gamma \cdot \alpha < \gamma \cdot \beta$.*

DIM. (1). Fissati $\alpha \leq \beta$, procediamo per induzione transfinita su γ . Il caso base è banale perchè $\alpha + 0 = \alpha \leq \beta = \beta + 0$. Se $\gamma = \delta + 1$ è successore, dall'ipotesi induttiva $\alpha + \delta \leq \beta + \delta$ segue subito che $\alpha + \gamma = \alpha + \delta + 1 \leq \beta + \delta + 1 = \beta + \gamma$.

Infine se γ è un ordinale limite, dalle definizioni di somma per un ordinale limite si ha che

$$\alpha + \gamma = \bigcup_{\delta < \gamma} \alpha + \delta \leq (\text{per ipotesi induttiva}) \leq \bigcup_{\delta < \gamma} \beta + \delta = \beta + \gamma.$$

Alternativamente, notiamo che la funzione $\psi : \alpha + \gamma \rightarrow \beta + \gamma$ dove $\psi(\delta) = \delta$ per ogni $\delta < \alpha$, e $\psi(\alpha + \varepsilon) = \beta + \varepsilon$ per ogni $\varepsilon < \gamma$, preserva l'ordine. Quindi $\alpha + \gamma = \text{ot}(\text{Imm}(\psi)) \leq \beta + \gamma$.

(2). Per il Teorema della differenza, esiste $\delta > 0$ tale che $\beta = \alpha + \delta$. Allora $\gamma + \alpha < \gamma + \alpha + \delta = \gamma + \beta$.

(3). Si procede in modo analogo ad (1) per induzione transfinita su γ . Il caso base è banale perché $\alpha \cdot 1 = \alpha \leq \beta = \beta \cdot 1$. Se $\gamma = \delta + 1$ è successore, dall'ipotesi induttiva $\alpha \cdot \delta \leq \beta \cdot \delta$ e dal fatto che le somme preservano le disuguaglianze deboli, si ottiene che

$$\alpha \cdot \gamma = \alpha \cdot \delta + \alpha \leq \beta \cdot \delta + \alpha \leq \beta \cdot \delta + \beta = \beta \cdot \gamma.$$

Infine se γ è un ordinale limite, dalle definizioni di prodotto per un ordinale limite si ha che

$$\alpha \cdot \gamma = \bigcup_{\delta < \gamma} \alpha \cdot \delta \leq (\text{per ipotesi induttiva}) \leq \bigcup_{\delta < \gamma} \beta \cdot \delta = \beta \cdot \gamma.$$

(4). Per il Teorema della differenza, esiste $\delta > 0$ tale che $\beta = \alpha + \delta$. Allora, usando la proprietà distributiva, si ha $\gamma \cdot \alpha < \gamma \cdot \alpha + \gamma \cdot \delta = \gamma \cdot (\alpha + \delta) = \gamma \cdot \beta$. Notiamo che avere la disuguaglianza stretta $\gamma \cdot \alpha < \gamma \cdot \alpha + \gamma \cdot \delta$ è necessaria l'ipotesi $\gamma > 0$. $\square$

NOTA BENE 1.10. Osserviamo che le somme e i prodotti a sinistra in generale non preservano gli ordini stretti. Ad esempio $2 < 3$ ma $2 + \omega = \omega = 3 + \omega$; e $2 \cdot \omega = \omega = 3 \cdot \omega$.

TEOREMA 1.11 (Divisione euclidea). *Per ogni α e per ogni $\beta \neq 0$, esistono ed unici γ e $\rho < \beta$ tali che $\alpha = \beta \cdot \gamma + \rho$.*

DIM. Dimostriamo prima l'esistenza. Osserviamo che esistono ordinali ξ tali che $\beta \cdot \xi > \alpha$. Infatti, ad esempio, $\beta \cdot (\alpha + 1) \geq 1 \cdot (\alpha + 1) = \alpha + 1 > \alpha$. Prendiamo allora il minimo δ di tali ordinali, cioè $\delta = \min\{\xi \mid \beta \cdot \xi > \alpha\}$. Chiaramente $\delta \neq 0$. Inoltre δ non è un ordinale limite, perché altrimenti da $\beta < \alpha \cdot \delta = \bigcup_{\eta < \delta} \alpha \cdot \eta$ seguirebbe che $\beta < \alpha \cdot \eta$ per un opportuno $\eta < \delta$, contro la minimalità di δ . Allora $\delta = \gamma + 1$ è un successore, e si ha $\beta \cdot \gamma \leq \alpha < \alpha \cdot (\gamma + 1)$. Per il Teorema della differenza, esiste $\rho \geq 0$ tale che $\alpha = \beta \cdot \gamma + \rho$. Osserviamo che il resto $\rho < \gamma$ altrimenti da $\rho \geq \gamma$ seguirebbe che $\alpha = \beta \cdot \gamma + \rho \geq \alpha \cdot \gamma + \gamma = \alpha \cdot (\gamma + 1)$.

Occupiamoci adesso dell'unicità e supponiamo che $\alpha = \beta \cdot \gamma + \rho$ e $\alpha = \beta \cdot \gamma' + \rho'$ dove $\rho < \gamma$ e $\rho' < \gamma'$. Se per assurdo γ e γ' fossero diversi, allora uno sarebbe maggiore dell'altro, ad esempio $\gamma > \gamma'$. Per il teorema sulla differenza esisterebbe allora $\delta > 0$ tale che $\gamma = \gamma' + \delta$ e si avrebbe

$$\alpha = \beta \cdot \gamma' + \rho' < \beta \cdot \gamma' + \gamma' = \beta \cdot (\gamma' + 1) \leq \beta \cdot (\gamma' + \delta) = \beta \cdot \gamma \leq \beta \cdot \gamma + \rho = \alpha,$$

contro l'ipotesi. Visto che $\gamma = \gamma'$, per l'unicità della differenza a destra tra α e $\beta \cdot \gamma$ si ottiene infine che $\rho = \rho'$. $\square$

Introduciamo adesso l'operazione di esponenziazione tra ordinali.

DEFINIZIONE 1.12. Per ogni ordinale fissato $\alpha \geq 1$, per ricorsione transfinita su β poniamo:

$$\begin{cases} \alpha^0 &= 1 \\ \alpha^{\beta+1} &= (\alpha^\beta) \cdot \alpha \\ \alpha^\lambda &= \bigcup_{\beta < \lambda} \alpha^\beta \text{ se } \lambda \text{ è limite.} \end{cases}$$

Osserviamo che banalmente $1^\beta = 1$ per ogni ordinale β .

ESERCIZIO 1.13. Dimostrare che per ogni base fissata $\alpha \geq 2$, la funzione classe $\beta \mapsto \alpha^\beta$ dalla classe degli ordinali in sé è strettamente crescente.

La definizione di sopra è coerente con l'esponenziazione tra buoni ordini che avevamo definito in precedenza.

ESERCIZIO 1.14. Siano α, β ordinali con $\alpha \geq 1$. Allora l'insieme bene ordinato $\text{Exp}(\alpha, \beta)$ è isomorfo all'esponenziale ordinale α^β .

ESERCIZIO 1.15. Dimostrare che, analogamente a somme e prodotti, anche le esponenziazioni tra ordinali preservano gli ordini deboli a sinistra e gli ordini stretti a destra:

- (1) Se $\alpha \leq \beta$ allora $\alpha^\gamma \leq \beta^\gamma$;
- (2) Se $\alpha < \beta$ e $\gamma \geq 2$ allora $\gamma^\alpha < \gamma^\beta$.

Le prossime due proprietà mettono in relazione l'esponenziale con somme e prodotti, e sono del tutto analoghe alle proprietà della usuale funzione esponenziale per numeri reali.

PROPOSIZIONE 1.16. Siano α, β, γ ordinali con $\alpha \geq 1$.

- (1) $\alpha^\beta \cdot \alpha^\gamma = \alpha^{\beta+\gamma}$;
- (2) $(\alpha^\beta)^\gamma = \alpha^{\beta \cdot \gamma}$.

DIM. Nel seguito assumeremo $\alpha \geq 2$, altrimenti la tesi è banale.

(1). Per α e β fissati, procediamo per induzione transfinita su γ . Il caso base $\gamma = 0$ è immediato perché $\alpha^\beta \cdot \alpha^\gamma = \alpha^\beta \cdot \alpha^0 = \alpha^\beta \cdot 1 = \alpha^\beta = \alpha^{\beta+0}$. Se $\gamma = \delta + 1$ è successore, allora $\alpha^\beta \cdot \alpha^{\delta+1} = \alpha^\beta \cdot \alpha^\delta \cdot \alpha = (\text{per ipotesi induttiva}) = \alpha^{\beta+\delta} \cdot \alpha = \alpha^{\beta+\delta+1} = \alpha^{\beta+\gamma}$. Consideriamo ora il caso in cui γ è limite. Ricordiamo che allora anche gli ordinali α^γ e $\beta + \gamma$ sono limite; inoltre $(\alpha^\delta \mid \delta < \gamma)$ è illimitato in α^γ e $(\alpha^{\beta+\delta} \mid \delta < \gamma)$ è illimitato in $\alpha^{\beta+\gamma}$. Abbiamo quindi:

$$\alpha^\beta \cdot \alpha^\gamma = \bigcup_{\eta < \alpha^\gamma} \alpha^\beta \cdot \eta = \bigcup_{\delta < \gamma} \alpha^\beta \cdot \alpha^\delta = (\text{ipotesi induttiva}) = \bigcup_{\delta < \gamma} \alpha^{\beta+\delta} = \bigcup_{\zeta < \beta+\gamma} \alpha^\zeta = \alpha^{\beta+\gamma}.$$

(2). Come sopra, per α e β fissati, procediamo per induzione transfinita su γ . Il caso base $\gamma = 0$ è immediato perché $(\alpha^\beta)^0 = 1 = \alpha^0 = \alpha^{\beta \cdot 0}$. Se $\gamma = \delta + 1$ è successore, allora $(\alpha^\beta)^{\delta+1} = (\alpha^\beta)^\delta \cdot \alpha^\beta \stackrel{1}{=} \alpha^{\beta \cdot \delta} \cdot \alpha^\beta \stackrel{2}{=} \alpha^{\beta \cdot \delta + \beta} = \alpha^{\beta \cdot (\delta+1)} = \alpha^{\beta \cdot \gamma}$, dove nell'uguaglianza 1 abbiamo usato l'ipotesi induttiva, e nell'uguaglianza 2 abbiamo usato la proprietà (1) di sopra. Consideriamo infine il caso in cui γ è limite. Ricordiamo che allora anche gli ordinali $\beta \cdot \gamma$ e $\alpha^{\beta \cdot \gamma}$ sono limite; e inoltre $(\alpha^{\beta \cdot \delta} \mid \delta < \gamma)$ è illimitato in $\alpha^{\beta \cdot \gamma}$. Abbiamo quindi:

$$(\alpha^\beta)^\gamma = \bigcup_{\delta < \gamma} (\alpha^\beta)^\delta = (\text{ipotesi induttiva}) = \bigcup_{\delta < \gamma} \alpha^{\beta \cdot \delta} = \bigcup_{\eta < \beta \cdot \gamma} \alpha^\eta = \alpha^{\beta \cdot \gamma}.$$

□

PROPOSIZIONE 1.17. *Per ogni ordinale $\alpha \neq 0$ esiste ed unico δ tale che*

$$\omega^\delta \leq \alpha < \omega^{\delta+1}.$$

DIM. Se $\alpha = 1$, chiaramente la proprietà richiesta è vera con $\delta = 0$. Se $\alpha > 1$, prendiamo $\xi = \min\{\eta \leq \alpha + 1 \mid \omega^\eta > \alpha\}$. Notiamo che la definizione è ben posta perché quell'insieme è non vuoto; ad esempio, $\omega^{\alpha+1} \geq \alpha + 1 > \alpha$. Un tale minimo ξ non può essere un limite, altrimenti da $\alpha < \omega^\xi = \bigcup_{\eta < \xi} \omega^\eta$ seguirebbe che $\alpha < \omega^\eta$ per qualche $\eta < \xi$, contro la minimalità di ξ . Allora $\xi = \delta + 1$ per un opportuno δ e quindi $\omega^\delta \leq \alpha < \omega^{\delta+1}$. $\square$

ESERCIZIO 1.18. Per ogni ordinale infinito α esistono ed unici ordinale δ e numero naturale positivo n tali che

$$\left(\omega^{(\omega^\delta)}\right)^n \leq \alpha < \left(\omega^{(\omega^{\delta+1})}\right)^{n+1}.$$

Il prossimo risultato ci mostra un'utile rappresentazione degli ordinali “in base ω ”.

TEOREMA 1.19 (Forma normale di Cantor). *Per ogni $\alpha > 0$ esistono ed unici $\beta_1 > \dots > \beta_k$ ordinali e $n_1, \dots, n_k \in \omega \setminus \{0\}$ numeri naturali non nulli tali che*

$$\alpha = \omega^{\beta_1} \cdot n_1 + \dots + \omega^{\beta_k} \cdot n_k.$$

DIM. Vediamo prima l'esistenza. Procediamo per induzione su $\alpha \geq 1$. La base è ovvia perché $1 = \omega^0 \cdot 1$ è una forma normale di Cantor. Se $\alpha > 1$, prendiamo δ tale che $\omega^\delta \leq \alpha < \omega^{\delta+1}$. Dividendo α per ω^δ si ottiene $\alpha = \omega^\delta \cdot \vartheta + \rho$ dove il resto $\rho < \omega^\delta$. Notiamo che il quoziente $\vartheta < \omega$ è un numero naturale, altrimenti $\vartheta \geq \omega \Rightarrow \alpha \geq \omega^\delta \cdot \omega = \omega^{\delta+1}$, contro l'assunzione su δ . Inoltre $\vartheta \neq 0$ altrimenti $\alpha = \rho < \omega^\delta$. Se $\rho = 0$ abbiamo già ottenuto la forma normale di Cantor. Altrimenti applichiamo l'ipotesi induttiva al resto ρ (che è minore di α) ed otteniamo l'esistenza di ordinali $\beta_2 > \dots > \beta_k$ e di numeri naturali non nulli $n_2, \dots, n_k$ tali che $\rho = \omega^{\beta_2} \cdot n_2 + \dots + \omega^{\beta_k} \cdot n_k$. Visto che $\rho < \omega^\delta$ e $\rho \geq \omega^{\beta_2}$, deve essere $\beta_2 < \delta$. Se poniamo $\beta_1 = \delta$ e $n_1 = \vartheta$, si ottiene la forma normale cercata:

$$\alpha = \omega^\delta \cdot \vartheta + \rho = \omega^{\beta_1} \cdot n_1 + \omega^{\beta_2} \cdot n_2 + \dots + \omega^{\beta_k} \cdot n_k.$$

Per vedere l'unicità, supponiamo di avere due forme normali di Cantor per lo stesso ordinale:

$$\alpha = \omega^{\beta_1} \cdot n_1 + \omega^{\beta_2} \cdot n_2 + \dots + \omega^{\beta_k} \cdot n_k.$$

$$\alpha = \omega^{\gamma_1} \cdot m_1 + \omega^{\gamma_2} \cdot m_2 + \dots + \omega^{\gamma_h} \cdot m_h.$$

Notiamo che n_1 è il quoziente della divisione euclidea di α con ω^{β_1} , ed il resto è $\rho = \omega^{\beta_2} \cdot n_2 + \dots + \omega^{\beta_k} \cdot n_k < \omega^{\beta_1}$. Infatti:

$$\rho \leq \omega^{\beta_2} \cdot n_2 + \dots + \omega^{\beta_k} \cdot n_k \leq \omega^{\beta_2} \cdot (n_2 + \dots + n_k) < \omega^{\beta_2} \cdot \omega = \omega^{\beta_2+1} \leq \omega^{\beta_1}.$$

(Se $k = 1$ si pone $\rho = 0$). Analogamente, m_1 è il quoziente della divisione euclidea di α con ω^{γ_1} , ed il resto è $\sigma = \omega^{\gamma_2} \cdot m_2 + \dots + \omega^{\gamma_h} \cdot m_h$ (se $h = 1$ si pone $\sigma = 0$). Osserviamo che $\beta_1 = \gamma_1$, altrimenti da $\beta_1 < \gamma_1$ seguirebbe che

$$\alpha = \omega^{\beta_1} \cdot n_1 + \rho < \omega^{\beta_1} \cdot n_1 + \omega^{\beta_1} < \omega^{\beta_1+1} \leq \omega^{\gamma_1} \leq \alpha.$$

Un'analogha contraddizione si otterrebbe assumendo $\beta_1 > \gamma_1$. Ma allora, dall'unicità del quoziente e del resto nella divisione euclidea di α con $\omega^{\beta_1} = \omega^{\gamma_1}$, segue che le due forme normali di Cantor necessariamente coincidono. $\square$

ESERCIZIO 1.20. Dimostrare che la forma normale del teorema di Cantor vale anche se si rimpiazzano le potenze di ω con le potenze di un ordinale fissato $\beta \geq 2$. Precisamente:

- Per ogni ordinale $\alpha \geq 1$ e per ogni ordinale $\beta \geq 2$ esistono ed unici $\gamma_1 > \dots > \gamma_k$ e $0 < c_1, \dots, c_k < \beta$ tali che $\alpha = \beta^{\gamma_1} \cdot c_1 + \dots + \beta^{\gamma_k} \cdot c_k$.

Ricordiamo che alcuni ordinali “assorbono” le somme a sinistra con ordinali più piccoli di loro. L'esempio fondamentale è fornito da ω perché, come abbiamo già più volte osservato, per ogni $n < \omega$ si ha $n + \omega = \omega$. Il prossimo risultato afferma che questi fenomeni di assorbimento a sinistra si verificano per tutti e soli gli ordinali che sono potenze di ω .

PROPOSIZIONE 1.21. Per ogni ordinale $\alpha > 0$, le seguenti condizioni sono equivalenti:

- (1) α è additivamente chiuso, cioè se $\beta, \gamma < \alpha$ allora anche $\beta + \gamma < \alpha$;
- (2) α assorbe additivamente a sinistra, cioè per ogni $\beta < \alpha$, si ha $\beta + \alpha = \alpha$;
- (3) Esiste δ tale che $\alpha = \omega^\delta$.

DIM. (2) $\Rightarrow$ (1). Se $\beta, \gamma < \alpha$, banalmente $\beta + \gamma < \beta + \alpha = \alpha$ per ipotesi.

(1) $\Rightarrow$ (3). 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 $\omega^{\delta+1} = \omega^\delta \cdot \omega = \sup_{n < \omega} \omega^\delta \cdot n$, è facile verificare che l'intervallo aperto di estremi ω^δ e $\omega^{\delta+1}$:

$$(\omega^\delta, \omega^{\delta+1}) = \bigcup_{n \geq 1} (\omega^\delta \cdot n, \omega^\delta \cdot (n+1)]$$

è unione di intervalli aperti a sinistra e chiusi a destra. Quindi esiste $n \geq 1$ con $\omega^\delta \cdot n < \alpha \leq \omega^\delta \cdot (n+1)$. Ma allora $\omega^\delta, \omega^\delta \cdot n < \alpha$, mentre

$$\omega^\delta + \omega^\delta \cdot n = \omega^\delta \cdot (n+1) \geq \alpha,$$

contro l'ipotesi (1).

(3) $\Rightarrow$ (2). Fissiamo $\beta < \alpha = \omega^\delta$. Distinguiamo tre casi. Se $\delta = 0$, allora $\alpha = 1$ e $\beta = 0$, dunque banalmente $\beta + \alpha = \alpha$. Se $\delta = \zeta + 1$ è successore, da $\beta < \omega^{\zeta+1} = \omega^\zeta \cdot \omega = \sup_{n < \omega} \omega^\zeta \cdot n$ segue che $\beta < \omega^\zeta \cdot n$ per qualche $n < \omega$. Allora deve essere $\beta + \alpha = \alpha$, in quanto

$$\alpha \leq \beta + \alpha = \beta + \omega^{\zeta+1} \leq \omega^\zeta \cdot n + \omega^\zeta \cdot \omega = \omega^\zeta(n + \omega) = \omega^\zeta \cdot \omega = \alpha.$$

(Qua abbiamo usato la proprietà $n + \omega = \omega$ per ogni $n < \omega$. Più in generale, si può dimostrare che $n + \alpha = \alpha$ per ogni ordinale infinito α .)

Se $\delta = \lambda$ è limite, $\beta < \alpha \Rightarrow \beta < \omega^\gamma$ per qualche $\gamma < \lambda$. Per il Teorema della differenza, esiste $\xi > 0$ tale che $\gamma + \xi = \lambda$, e quindi

$$\alpha \leq \beta + \alpha = \beta + \omega^\lambda \leq \omega^\gamma + \omega^\lambda = \omega^\gamma \cdot (1 + \omega^\xi) = \omega^\gamma \cdot \omega^\xi = \omega^\lambda = \alpha.$$

Notiamo che ω^ξ è un ordinale infinito perché $\xi > 0$, e quindi $1 + \omega^\xi = \omega^\xi$. $\square$

Il prossimo risultato è l'analogo moltiplicativo della proposizione precedente.

PROPOSIZIONE 1.22. Per ogni ordinale infinito α , le seguenti condizioni sono equivalenti:

- (1) α è moltiplicativamente chiuso, cioè se $\beta, \gamma < \alpha$ allora anche $\beta \cdot \gamma < \alpha$;
- (2) α assorbe moltiplicativamente a sinistra, cioè per ogni $0 < \beta < \alpha$, si ha $\beta \cdot \alpha = \alpha$;

(3) *Esiste δ tale che $\alpha = \omega^{(\omega^\delta)}$.*

DM. La dimostrazione è del tutto simile a quella della proposizione precedente.

(2) $\Rightarrow$ (1). Se $\beta = 0$, la tesi è banale. Se $\beta > 0$ e $\beta, \gamma < \alpha$, banalmente $\beta \cdot \gamma < \beta \cdot \alpha$ e per ipotesi sappiamo che $\beta \cdot \alpha = \alpha$.

(1) $\Rightarrow$ (3). Notiamo prima che per ogni ordinale infinito α esiste un ordinale δ tale che $\omega^{(\omega^\delta)} \leq \alpha < \omega^{(\omega^{\delta+1})}$. (La dimostrazione è del tutto analoga a quella della Proposizione ??.) Per raggiungere la tesi, mostriamo che per ogni δ , se $\omega^{(\omega^\delta)} < \alpha < \omega^{(\omega^{\delta+1})}$, allora α non è moltiplicativamente chiuso.

Visto che $\omega^{(\omega^{\delta+1})} = \omega^{(\omega^\delta) \cdot \omega} = \sup_{n < \omega} \omega^{(\omega^\delta \cdot n)}$, possiamo prendere $1 \leq n < \omega$ con $\omega^{(\omega^\delta \cdot n)} < \alpha \leq \omega^{(\omega^\delta \cdot (n+1))}$. Ma allora:

$$\omega^{(\omega^\delta \cdot n)} \cdot \omega^{(\omega^\delta)} = \omega^{(\omega^\delta \cdot n + \omega^\delta)} = \omega^{(\omega^\delta \cdot (n+1))} \geq \alpha,$$

e quindi α non è moltiplicativamente chiuso.

(3) $\Rightarrow$ (2). Sia $\beta < \alpha = \omega^{(\omega^\delta)}$. Distinguiamo tre casi. Se $\delta = 0$, allora $\alpha = \omega$ e $\beta < \omega$ è un numero naturale, ed abbiamo già osservato che $n \cdot \omega = \omega$ per ogni $n \in \omega$. Se $\delta = \eta + 1$ è successore, da $\beta < \omega^{(\omega^{\eta+1})} = \omega^{(\omega^\eta \cdot \omega)} = (\omega^{(\omega^\eta)})^\omega = \sup_{n < \omega} (\omega^{(\omega^\eta)})^n$ segue che $\beta < (\omega^{(\omega^\eta)})^n = \omega^{(\omega^\eta \cdot n)}$ per qualche $n < \omega$. Allora deve essere $\beta \cdot \alpha = \alpha$, in quanto

$$\begin{aligned} \alpha \leq \beta \cdot \alpha &= \beta \cdot \omega^{(\omega^{\eta+1})} \leq \omega^{(\omega^\eta \cdot n)} \cdot \omega^{(\omega^\eta \cdot \omega)} = \\ &= \omega^{(\omega^\eta \cdot n + \omega^\eta \cdot \omega)} = \omega^{(\omega^\eta \cdot (n + \omega))} = \omega^{(\omega^\eta \cdot \omega)} = \omega^{(\omega^{\eta+1})} = \alpha. \end{aligned}$$

Infine, se $\delta = \lambda$ è limite, $\alpha = \omega^{(\omega^\lambda)} = \sup_{\xi < \omega^\lambda} \omega^\xi = \sup_{\gamma < \lambda} \omega^{(\omega^\gamma)}$ e quindi $\beta < \alpha \Rightarrow \beta < \omega^{(\omega^\gamma)}$ per qualche $\gamma < \lambda$. Allora abbiamo che

$$\alpha \leq \beta \cdot \alpha \leq \omega^{(\omega^\gamma)} \cdot \omega^{(\omega^\lambda)} = \omega^{(\omega^\gamma + \omega^\lambda)} = \omega^{(\omega^\lambda)} = \alpha.$$

Notiamo che ω^λ è additivamente chiuso per la proposizione precedente, e quindi $\omega^\gamma + \omega^\lambda = \omega^\lambda$ per ogni $\gamma < \lambda$. $\square$

I cardinali

1. Il primo ordinale non numerabile: ω_1 .

Notiamo che gli esempi espliciti di ordinali che abbiamo considerato fin qui sono tutti al più numerabili. Ad esempio tutti gli ordinali $\omega + n$ con $n \in \omega$ sono chiaramente numerabili; l'ordinale $\omega + \omega$ è numerabile, perché isomorfo all'insieme bene ordinato $\omega + \omega$ che è ottenuto ordinando opportunamente l'unione disgiunta $\omega \sqcup \omega = \omega \times \{0\} \cup \omega \times \{1\}$ (vedi Definizione ??); l'ordinale $\omega \cdot \omega$ è numerabile, perché è isomorfo all'insieme bene ordinato $\omega \times \omega$ (vedi Definizione ??); l'ordinale ω^ω è numerabile perché è isomorfo all'insieme bene ordinato $\text{EXP}(\omega, \omega)$ che è ottenuto ordinando l'insieme numerabile delle funzioni a supporto finito $\{f : \omega \rightarrow \omega \mid \{n \in \omega \mid f(n) \neq 0\} \text{ finito}\}$ (vedi Definizione ??); e così via.

Per ottenere il primo esempio canonico di ordinale non numerabile l'idea è semplice: prendiamo la collezione di tutti gli ordinali al più numerabili. Dovremo però verificare che una tale collezione è in effetti un insieme.

DEFINIZIONE 1.1. $\omega_1 = \{\alpha \text{ ordinale} \mid |\alpha| \leq |\omega|\}$.

Gli assiomi della nostra teoria ci garantiscono la seguente proprietà fondamentale di ω_1 . Osserviamo che la sua dimostrazione non richiede l'assioma di scelta.

PROPOSIZIONE 1.2 (ZF). ω_1 è il più piccolo degli ordinali non numerabili.

DIM. Come prima cosa dobbiamo verificare che ω_1 è in effetti un insieme, e non una classe propria. A questo scopo consideriamo la seguente classe:

$$\Gamma(\omega) := \{(A, \prec) \text{ buon ordine} \mid A \subseteq \omega\}.$$

Osserviamo che ogni elemento $(A, \prec) \in \Gamma(\omega)$ è una coppia ordinata dove $A \subseteq \omega$, e dove l'insieme di coppie dato dalla relazione d'ordine $\prec$ è un sottoinsieme di $\omega \times \omega$. Dunque $\Gamma(\omega) \subseteq \mathcal{P}(\omega) \times \mathcal{P}(\omega \times \omega)$ è una sottoclasse di un insieme, e quindi è un insieme per l'assioma di separazione.

Sia adesso $\mathbf{F}$ una funzione-classe che associa ad ogni insieme bene ordinato $(A, \prec)$ quell'unico ordinale α tale che $(A, \prec) \cong (\alpha, \in)$. Visto che $\Gamma(\omega)$ è un insieme, per l'assioma di rimpiazzamento anche

$$\mathbf{F}[\Gamma(\omega)] = \{\mathbf{F}(A, \prec) \mid (A, \prec) \in \Gamma(\omega)\}$$

è un insieme. Verifichiamo che $\mathbf{F}[\Gamma(\omega)] = \omega_1$.

Un'inclusione è ovvia perché se un ordinale α è isomorfo ad un buon ordine $(A, \prec) \in \Gamma(\omega)$, allora $|\alpha| = |A| \leq |\omega|$. Viceversa, se $|\alpha| \leq |\omega|$, allora possiamo prendere una funzione iniettiva $f : \alpha \rightarrow \omega$. Sull'insieme immagine $A := \text{Imm}(f)$ definiamo una relazione d'ordine $\prec$ ponendo $f(\beta) \prec f(\gamma) \Leftrightarrow \beta \in \gamma$. Osserviamo che la definizione è ben posta perché f è iniettiva. È immediato dalla definizione di $\prec$ che $f : (\alpha, \in) \cong (A, \prec)$ è un isomorfismo d'ordine. Quindi, visto che $A \subseteq \omega$, si ha $(A, \prec) \in \Gamma(\omega)$ e che $\mathbf{F}(A, \prec) = \alpha$.

Per mostrare che ω_1 è un ordinale basta osservare che si tratta di un insieme di ordinali che è transitivo. Questo si verifica facilmente: se $\beta \in \alpha \in \omega_1$, allora $\beta \subset \alpha$

dove $|\alpha| \leq |\omega|$, quindi anche $|\beta| \leq |\omega|$ e perciò $\beta \in \omega_1$. Osserviamo che ω_1 non è numerabile, altrimenti avremmo che $\omega_1 \in \omega_1$, una contraddizione.

Infine, se γ è un ordinale non numerabile, allora per ogni ordinale al più numerabile α non è possibile che $\gamma \subseteq \alpha$; quindi, per la tricotomia degli ordinali, deve essere $\alpha \in \gamma$. Questo significa che $\omega_1 \subseteq \gamma$, e quindi ω_1 ha la proprietà di minimalità voluta. $\square$

2. Cardinali come ordinali iniziali

Percorrendo la retta transfinita degli ordinali, si incontrano degli speciali ordinali quando avviene un “cambio” di cardinalità. Ad esempio, percorrendo tutti gli ordinali a partire da ω , il primo ordinale in cui si ha un cambio di cardinalità è ω_1 .

DEFINIZIONE 2.1. Un *cardinale* è un *ordinale iniziale*, cioè un ordinale κ con la proprietà che per ogni $\alpha < \kappa$ si ha $|\alpha| \neq |\kappa|$ (e quindi $|\alpha| < |\kappa|$).

Osserviamo che tutti i naturali $n \in \omega$ sono cardinali, perché se $n < m$ non esistono biezioni tra n ed m . Anche ω è un cardinale, perché è il più piccolo degli ordinali infiniti (se $n < \omega$, chiaramente n non è in biezione con ω). Come abbiamo osservato sopra, il primo cardinale più grande di ω è ω_1 .

ESERCIZIO 2.2. Se κ e ν sono cardinali, allora $|\kappa| \leq |\nu| \Leftrightarrow \kappa \leq \nu$.

PROPOSIZIONE 2.3. Ogni cardinale infinito è un ordinale limite.

DIM. Un ordinale successore infinito $\alpha + 1$ non è un ordinale iniziale perché $|\alpha| = |\alpha + 1|$. Infatti, se $\alpha + 1$ è infinito allora $\omega \subseteq \alpha$, ed è immediato vedere che esiste una biezione $f : \alpha + 1 \rightarrow \alpha$. Ad esempio si può definire $f(n) = n + 1$ se $n \in \omega$, e $f(\beta) = \beta$ se $\omega \leq \beta < \alpha$, e $f(\alpha) = 0$. $\square$

Osserviamo che non vale l’implicazione inversa nella proposizione precedente. Ad esempio, $\omega + \omega$ è un ordinale limite, ma non è un ordinale iniziale perché $\omega < \omega + \omega$ e $|\omega| = |\omega + \omega|$.

PROPOSIZIONE 2.4. Ogni ordinale è in biezione con un unico cardinale.

DIM. Dato un ordinale α , prendiamo κ il minimo ordinale tale che $|\kappa| = |\alpha|$. Un tale κ è un cardinale per minimalità; infatti se $\beta < \gamma$ allora $|\beta| \neq |\gamma|$. Infine, non possono esistere due cardinali diversi $\kappa < \kappa'$ entrambi equipotenti ad α , altrimenti si avrebbe che $|\kappa| = |\kappa'|$, contro la definizione di ordinale iniziale. $\square$

Come vedremo nella prossima sezione, gli ordinali iniziali saranno presi come rappresentanti canonici nelle classi di equipotenza.

Ricordiamo che l’unione di ordinali corrispondeva all’estremo superiore e l’intersezione di ordinale corrispondeva al minimo. La stessa proprietà vale anche per i cardinali.

PROPOSIZIONE 2.5. Sia $\mathcal{K}$ un insieme non vuoto di cardinali. Allora:

- L' unione $\bigcup \mathcal{K} = \bigcup_{\kappa \in \mathcal{K}} \kappa = \sup \mathcal{K}$ è un cardinale;
- L' intersezione $\bigcap \mathcal{K} = \bigcap_{\kappa \in \mathcal{K}} \kappa = \min \mathcal{K}$ è un cardinale.

DIM. Per esercizio. $\square$

3. La funzione-classe di Hartogs

Facciamo presente che in ZF (senza assioma di scelta) non è possibile trovare una buona definizione di cardinale come rappresentante canonico in ogni classe di equipotenza. Precisamente vale il seguente risultato, che enunciamo in modo “informale”.¹ Non lo dimostriamo perchè richiede tecniche che vanno al di là degli scopi di questo corso.

TEOREMA 3.1. (*Pincus 1974*). *In ZF non esiste alcuna funzione-classe $\mathbf{F}$ definita per tutti gli insiemi che soddisfi le seguenti due proprietà:*

- (i) $|\mathbf{F}(A)| = |A|$;
- (ii) $\mathbf{F}(A) = \mathbf{F}(B) \Leftrightarrow |A| = |B|$.

Esistono invece rappresentanti canonici nelle classi di equipotenza degli insiemi *bene ordinabili*, cioè di quegli insiemi A per i quali esiste una relazione di buon ordine $\prec$ su A .

DEFINIZIONE 3.2. Per ogni insieme bene ordinabile A , la *cardinalità* di A è l'unico cardinale κ equipotente ad A . In questo caso scriviamo:

$$\kappa = |A|.$$

Si osservi infatti che se $\prec$ è un buon ordinamento su A , allora si prende l'unico ordinale α isomorfo ad $(A, \prec)$, ed infine l'unico cardinale κ equipotente ad α .

Grazie all'assioma di scelta, vedremo che ogni insieme è bene ordinabile, e quindi ad ogni insieme corrisponderà il suo cardinale.²

TEOREMA 3.3 (Zermelo). *Ogni insieme è bene ordinabile.*

Generalizziamo adesso la costruzione usata per la definizione di ω_1 .

DEFINIZIONE 3.4. Per ogni insieme A , sia

$$\mathbb{H}(A) = \{\alpha \text{ ordinale} \mid |\alpha| \leq |A|\}$$

il suo *numero di Hartogs*.

La seguente fondamentale proprietà dei numeri di Hartogs è dimostrabile senza alcun uso dell'assioma di scelta. È importante evidenziare questo fatto perché la useremo più avanti per dimostrare alcune equivalenze dell'assioma di scelta.

TEOREMA 3.5 (ZF). (*Hartogs 1915*) $\mathbb{H}(A)$ è un cardinale, ed è il più piccolo ordinale tale che $|\mathbb{H}(A)| \not\leq |A|$.

DIM. Come prima cosa verifichiamo che la classe $\mathbb{H}(A)$ è un insieme.

Sia $\mathbf{F}$ la funzione-classe così definita: se $x = (B, \prec)$ è un buon ordinamento dove $B \subseteq A$, allora $\mathbf{F}(x)$ è l'unico ordinale ad esso isomorfo; altrimenti si pone $\mathbf{F}(x) = 0$. Per l'assioma di separazione, la seguente collezione è un insieme:

$$\Gamma(A) = \{(B, \prec) \in \mathcal{P}(A) \times \mathcal{P}(A \times A) \mid (B, \prec) \text{ buon ordine}\}.$$

¹ Un più corretto enunciato è il seguente: “Non esiste alcuna formula $\varphi(x, y)$ della teoria degli insiemi per cui ZF dimostra che φ determina una funzione-classe $\mathbf{F}$ definita per tutti gli insiemi e che soddisfa le proprietà (i) e (ii)”.

² Per la dimostrazione del teorema di Zermelo si veda la sezione dedicata all'assioma di scelta.

In modo del tutto analogo a quanto fatto nella dimostrazione del Teorema 1.2, si dimostra che l'immagine di $\Gamma(A)$ mediante $\mathbf{F}$ coincide con $\mathbb{H}(A)$, cioè $\mathbf{F}(\Gamma(A)) = \mathbb{H}(A)$. Per rimpiazzamento, si ottiene allora che $\mathbb{H}(A)$ è un insieme.

Osserviamo che $\mathbb{H}(A)$ è un ordinale in quanto insieme transitivo di ordinali. Infatti se $\beta \in \alpha \in \mathbb{H}(A)$, per definizione esiste una funzione iniettiva $f : \alpha \rightarrow A$. Ma $\beta \in \alpha \Rightarrow \beta \subset \alpha$; dunque anche la restrizione $f|_\beta : \beta \rightarrow A$ è iniettiva, e perciò $\beta \in \mathbb{H}(A)$. Inoltre si ha $|\mathbb{H}(A)| \not\leq |A|$, altrimenti da $|\mathbb{H}(A)| \leq |A|$, e dal fatto che $\mathbb{H}(A)$ è un ordinale, seguirebbe che $\mathbb{H}(A) \in \mathbb{H}(A)$, una contraddizione.

Per vedere che l'ordinale $\mathbb{H}(A)$ è un cardinale, supponiamo per assurdo che esista $\alpha < \mathbb{H}(A)$, cioè $\alpha \in \mathbb{H}(A)$, tale che $|\alpha| = |\mathbb{H}(A)|$. Per definizione di numero di Hartogs, $\alpha \in \mathbb{H}(A)$ se e solo se $|\alpha| \leq |A|$, e quindi avremmo che $|\mathbb{H}(A)| = |\alpha| \leq |A|$, contro quanto visto sopra. $\square$

COROLLARIO 3.6. *Se β è un ordinale, allora $\mathbb{H}(\beta)$ è il più piccolo cardinale maggiore di β .*

DIM. Banalmente $|\beta| \leq |\beta|$, e quindi $\beta \in \mathbb{H}(\beta)$, cioè $\beta < \mathbb{H}(\beta)$. Inoltre, se $\kappa > \beta$ è un cardinale allora $\mathbb{H}(\beta) \leq \kappa$, altrimenti si avrebbe $\kappa < \mathbb{H}(\beta)$ e quindi $|\kappa| \leq |\beta|$ mentre $|\beta| < |\kappa|$. $\square$

ESERCIZIO 3.7. * Senza usare l'assioma di scelta, dimostrare che per ogni insieme A esiste una funzione suriettiva $\theta : \mathcal{P}(\mathcal{P}(A)) \rightarrow \mathbb{H}(A)$, e quindi si ha $|\mathbb{H}(A)| \leq |\mathcal{P}(\mathcal{P}(\mathcal{P}(A)))|$.³

Il teorema di Hartogs ci permetterà di chiarire il ruolo dell'assioma di scelta riguardo la nozione di cardinalità.

Una fondamentale nozione in teoria degli insiemi è la sequenza degli *alephs*.

DEFINIZIONE 3.8. La sequenza degli *alephs* è definita per ricorsione transfinita come segue:

$$\begin{cases} \aleph_0 = \omega; \\ \aleph_{\alpha+1} = \mathbb{H}(\aleph_\alpha); \\ \aleph_\lambda = \bigcup_{\gamma < \lambda} \aleph_\gamma \text{ se } \lambda \text{ è limite.} \end{cases}$$

PROPOSIZIONE 3.9. *La sequenza degli aleph è una sequenza strettamente crescente di cardinali infiniti.*

DIM. Procediamo per induzione transfinita. Al passo base basta notare che $\aleph_0 = \omega$ è un cardinale infinito.

Al passo successore, per le proprietà del numero di Hartogs sappiamo che $\aleph_{\alpha+1} = \mathbb{H}(\aleph_\alpha) > \aleph_\alpha$ è un cardinale. Inoltre per ogni $\gamma < \alpha$, per ipotesi induttiva $\aleph_\gamma < \aleph_\alpha$, e quindi anche $\aleph_\gamma < \aleph_{\alpha+1}$.

Al passo limite, abbiamo che $\aleph_\lambda = \bigcup_{\gamma < \lambda} \aleph_\gamma$ è un cardinale perché unione di cardinali. Notiamo che per ogni $\gamma < \lambda$, anche $\gamma + 1 < \lambda$, e per ipotesi induttiva $\aleph_\gamma < \aleph_{\gamma+1}$; inoltre $\aleph_{\gamma+1} \leq \aleph_\lambda$ perché $\aleph_{\gamma+1} \subseteq \aleph_\lambda$. Possiamo allora concludere che vale la disuguaglianza stretta $\aleph_\gamma < \aleph_\lambda$. $\square$

³ Ricordiamo che vale questo risultato generale, dimostrabile senza l'uso dell'assioma di scelta:

- Se esiste una funzione suriettiva $g : X \rightarrow Y$, allora esiste una funzione iniettiva $f : Y \rightarrow \mathcal{P}(X)$.

Infatti basta porre $f(y) = \{x \in X \mid g(x) = y\}$.

In vista del prossimo teorema ci occorre questo

LEMMA 3.10. Per ogni ordinale α , si ha $\alpha \leq \aleph_\alpha$.

DIM. Procediamo per induzione transfinita. La base $\alpha = 0$ è banale. Al passo successore, per ipotesi induttiva sappiamo che $\beta \leq \aleph_\beta$, dunque $|\beta| \leq |\aleph_\beta|$ e perciò $\beta \in \mathbb{H}(\aleph_\beta) = \aleph_{\beta+1}$ e dunque anche $\beta + 1 < \aleph_{\beta+1}$ (ricordiamo che gli alephs sono cardinali infiniti, dunque ordinali limite). Infine al passo limite λ , per ipotesi induttiva sappiamo che $\gamma \leq \aleph_\gamma$ per ogni $\gamma < \lambda$, e quindi $\lambda = \bigcup_{\gamma < \lambda} \gamma \leq \bigcup_{\gamma < \lambda} \aleph_\gamma = \aleph_\lambda$. $\square$

Attenzione! Nell'enunciato del Lemma qua sopra non si può mettere la disuguaglianza stretta; infatti esistono cardinali κ tali che $\kappa = \aleph_\kappa$.

ESEMPIO 3.11. Definiamo per ricorsione numerabile la successione di cardinali $(\kappa_n \mid n \in \omega)$ ponendo:

$$\begin{cases} \kappa_0 = \aleph_0; \\ \kappa_{n+1} = \aleph_{\kappa_n}. \end{cases}$$

Allora il cardinale $\kappa = \bigcup_{n \in \omega} \kappa_n$ è tale che $\kappa = \aleph_\kappa$.

Per verificarlo, osserviamo intanto che vale la disuguaglianza $\kappa \leq \aleph_\kappa$, mostrata nel Lemma precedente. Per l'altra disuguaglianza, notiamo che κ è un cardinale infinito perché unione di cardinali infiniti; dunque κ è un ordinale limite e per definizione $\aleph_\kappa = \bigcup_{\gamma < \kappa} \aleph_\gamma$. Per ogni $\gamma < \kappa = \bigcup_{n \in \omega} \kappa_n$ esiste $n \in \omega$ con $\gamma \in \kappa_n$. Dalla crescita degli alephs segue allora che $\aleph_\gamma < \aleph_{\kappa_n} = \kappa_{n+1} \leq \kappa$. Visto che questa disuguaglianza vale per ogni $\gamma < \kappa$, concludiamo che $\aleph_\kappa = \bigcup_{\gamma < \kappa} \aleph_\gamma \leq \kappa$, come volevamo.

ESERCIZIO 3.12. Dimostrare che la sequenza $(\kappa_n \mid n \in \omega)$ definita nell'Esempio 3.11 è strettamente crescente.

ESERCIZIO 3.13. Dimostrare che la sequenza degli alephs ha punti fissi arbitrariamente grandi, cioè per ogni ordinale α esiste $\kappa > \alpha$ tale che $\aleph_\kappa = \kappa$.

La sequenza degli alephs enumera tutti i cardinali infiniti.

TEOREMA 3.14. *Gli alephs sono tutti e soli i cardinali infiniti.*

DIM. Abbiamo già osservato che tutti gli alephs sono cardinali infiniti. Dobbiamo vedere che vale anche il viceversa, cioè che per ogni cardinale infinito κ esiste un ordinale α tale che $\kappa = \aleph_\alpha$.

Abbiamo visto che $\kappa \leq \aleph_\kappa$; inoltre, vista la crescita della funzione aleph, $\aleph_\kappa < \aleph_{\kappa+1}$, dove $\kappa + 1$ è l'ordinale successore di κ . Esistono quindi ordinali γ per i quali vale la disuguaglianza stretta $\kappa < \aleph_\gamma$. Sia β il minimo di questi ordinali. Notiamo che un tale β non può essere 0, altrimenti avrei $\kappa < \aleph_0$, mentre κ è per ipotesi un cardinale infinito. Inoltre un tale β non può essere limite, altrimenti da $\kappa < \aleph_\beta = \bigcup_{\gamma < \beta} \aleph_\gamma$ seguirebbe l'esistenza di un $\gamma < \beta$ tale che $\kappa < \aleph_\gamma$, contro la minimalità di β . Allora necessariamente $\beta = \alpha + 1$ è un successore, e pertanto si ha $\aleph_\beta \leq \kappa < \aleph_{\beta+1}$. Infine osserviamo che $\kappa \in \aleph_{\beta+1} = \mathbb{H}(\aleph_\beta)$ significa che $|\kappa| \leq |\aleph_\beta|$, e quindi $\kappa \leq \aleph_\beta$, trattandosi di cardinali. Concludiamo quindi che $\kappa = \aleph_\beta$. $\square$

TEOREMA 3.15. *Ogni insieme infinito bene ordinabile è equipotente ad un unico aleph.*

DIM. Sia B un insieme bene ordinabile, e sia $\prec$ un buon ordine su B . Allora esiste (ed unico) ordinale α tale che $(B, \prec) \cong (\alpha, \in)$. In particolare $|B| = |\alpha|$. Se $\kappa = \min\{\beta \leq \alpha \mid |\beta| = |\alpha|\}$ allora κ è un cardinale e $|\kappa| = |\alpha| = |B|$. Visto che ogni cardinale infinito è un aleph, la dimostrazione è conclusa. $\square$

COROLLARIO 3.16 (ZF). Il Teorema di Zermelo è equivalente alla proprietà: “Ogni insieme infinito è equipotente ad un aleph”.

DIM. Se vale il Teorema di Zermelo, ogni insieme infinito è bene ordinabile e dunque, per il teorema precedente, ogni insieme infinito è equipotente ad un aleph. Viceversa, basta notare che se esiste una bigezione $f : A \rightarrow \aleph_\alpha$ da un insieme A in un aleph (che è bene ordinato), allora A è bene ordinabile; basta infatti definire $a < a' \Leftrightarrow f(a) < f(a')$. $\square$

Esattamente come accadeva per gli ordinali, anche i cardinali si dividono in cardinali successori e cardinali limite.

DEFINIZIONE 3.17. Un cardinale κ si dice *successore* se esiste il massimo dei cardinali $\mu < \kappa$. Un cardinale $\kappa \neq 0$ si dice *limite* altrimenti.

Notiamo che ogni numero naturale $n \neq 0$ è un cardinale successore. Inoltre:

PROPOSIZIONE 3.18. Sia κ un cardinale infinito. Allora κ è *successore* se e solo se $\kappa = \aleph_\alpha$ dove $\alpha = \beta + 1$ è un ordinale successore; e κ è *limite* se e solo se $\kappa = \aleph_\lambda$ dove λ è un ordinale limite.

DIM. Per esercizio. $\square$

Il prossimo risultato fornirà una proprietà fondamentale dell'algebra cardinale, e ci consentirà anche di dimostrare alcune formulazioni equivalenti dell'assioma di scelta AC in termine di proprietà di cardinalità.

TEOREMA 3.19 (ZF). Per ogni ordinale α , si ha $|\aleph_\alpha \times \aleph_\alpha| = |\aleph_\alpha|$.

DIM. Procediamo per induzione transfinita. Abbiamo già visto che $|\omega \times \omega| = |\omega|$, e dunque la base di induzione $\alpha = 0$ vale.

Consideriamo ora un aleph $\aleph_\alpha$ con $\alpha > 0$ e definiamo un buon ordinamento sul prodotto cartesiano $\aleph_\alpha \times \aleph_\alpha$ come segue:

- $(\xi, \eta) \prec (\xi', \eta')$ se $\max\{\xi, \eta\} < \max\{\xi', \eta'\}$;
oppure se $\max\{\xi, \eta\} = \max\{\xi', \eta'\}$ e $\xi < \xi'$;
oppure infine se $\max\{\xi, \eta\} = \max\{\xi', \eta'\}$ e $\xi = \xi'$ e $\eta < \eta'$.

Si verifica facilmente che si tratta di un buon ordinamento. È immediato che $|\aleph_\alpha| \leq |\aleph_\alpha \times \aleph_\alpha|$. Se per assurdo fosse $|\aleph_\alpha| < |\aleph_\alpha \times \aleph_\alpha|$, per la tricotomia dei buoni ordini avremmo che $\aleph_\alpha$ sarebbe isomorfo ad un segmento iniziale proprio $S = (\aleph_\alpha \times \aleph_\alpha)_{(\xi, \eta)}$ di $(\aleph_\alpha \times \aleph_\alpha, \prec)$. Sia $\zeta = \max\{\xi, \eta\}$; osserviamo che se $(\xi', \eta') \prec (\xi, \eta)$ allora $\max\{\xi', \eta'\} \leq \zeta$, e quindi $S \subseteq (\zeta + 1) \times (\zeta + 1)$. Poichè $\zeta < \aleph_\alpha$, anche $\zeta + 1 < \aleph_\alpha$ e quindi $|\zeta + 1| = \aleph_\beta$ per qualche $\beta < \alpha$. Otteniamo quindi la contraddizione:

$$|\aleph_\alpha| = |S| \leq |(\zeta + 1) \times (\zeta + 1)| = |\aleph_\beta \times \aleph_\beta| = (\text{per ipotesi induttiva}) = |\aleph_\beta| < |\aleph_\alpha|.$$

$\square$

Formulazioni equivalenti dell'assioma di scelta

Ci sono proprietà in matematica che possono essere equivalentemente riformulate in modi diversi apparentemente molto distanti l'uno dall'altro; quando questo accade, ciò è considerato un segno della rilevanza di tali proprietà.

In questo capitolo ci concentreremo sull'assioma di scelta, e ne dimosteremo cinque diverse formulazioni equivalenti tra le più significative. Naturalmente, nel dimostrare quelle equivalenze, dovremo fare molta attenzione a lavorare sempre all'interno della teoria ZF, senza mai usare né l'assioma di scelta, né alcuna delle sue conseguenze.

È bene precisare che lo studio delle varie forme di assioma di scelta è stato molto approfondito ed ha permesso di isolare centinaia di formulazioni equivalenti, oltre che di una miriade di principi più deboli, ma comunque non dimostrabili senza l'assioma di scelta.¹

1. Il Lemma di Zorn, il Teorema di Zermelo, e la confrontabilità

Una formulazione equivalente dell'assioma di scelta è data dal seguente principio, che ha larga applicazione in diverse aree della matematica.

Lemma di Zorn.

Sia $(P, \leq)$ un insieme parzialmente ordinato. Se ogni catena ammette maggioranti allora esistono elementi massimali.

Ricordiamo che un sottoinsieme $C \subseteq P$ si dice *catena* se la restrizione dell'ordine parziale a C è un ordine totale, cioè se per tutti i $c, c' \in C$ si ha $c \leq c'$ o $c' \leq c$. Un elemento $p \in P$ si dice *maggiorante* dell'insieme $X \subseteq P$ se $p \geq x$ per ogni $x \in X$. Un elemento $p \in P$ si dice *massimale* se non esistono elementi $q \in P$ con $p < q$. Nel caso di un ordine totale, un elemento massimale è necessariamente il massimo di P . Tuttavia, nel caso di ordini parziali P , possono esistere elementi massimali distinti (e quindi inconfrontabili).

TEOREMA 1.1 (ZF). “Assioma di scelta” $\Rightarrow$ “Lemma di Zorn”.

Diamo di questo risultato due diverse dimostrazioni. La prima è piuttosto elaborata, ma ha il vantaggio di non richiedere conoscenze specifiche di teoria degli insiemi. La seconda, più breve e diretta, si basa sulla ricorsione transfinita.

DIM.1. Sia $(P, \leq)$ un insieme parzialmente ordinato dove ogni catena ammette maggioranti. Vogliamo trovare un elemento massimale. L'idea della dimostrazione è quella di costruire una catena bene ordinata $C \subseteq P$ il “più lunga possibile”, in modo che l'unico maggiorante di C sia in realtà il massimo di C ed un elemento massimale per tutto $(P, \leq)$.

¹ Si veda ad esempio il volume “*Consequences of the Axiom of Choice*” di P. Howard e J.E. Rubin (American Mathematical Society, 1998). Il numero di proprietà considerato è talmente grande che era stato preparato un sito web per consultare velocemente l'esistenza di implicazioni tra le varie formulazioni: <http://www.math.purdue.edu/~hrubin/JeanRubin/Papers/conseq.html>. Purtroppo al momento della scrittura di questa dispensa quella pagina non è più funzionante.

Fissiamo una funzione di scelta $f : \mathcal{P}(P) \setminus \{\emptyset\} \rightarrow P$. Diciamo che un sottoinsieme non vuoto $A \subseteq P$ è una *f-catena* se:

- $(A, \leq)$ è bene ordinato;
- Per ogni $a \in A$, si ha $a = f(A^a)$ dove $A^a = \{p \in P \mid p > a\}$ è l'insieme dei maggioranti *stretti* del segmento iniziale $A_a = \{a' \in A \mid a' < a\}$.²

Ragioniamo informalmente per capire meglio l'idea che guida la dimostrazione. Se $p_0 = f(P)$, allora $A = \{p_0\}$ è una *f-catena*. Infatti il segmento iniziale A_{p_0} è vuoto, e banalmente l'insieme dei suoi maggioranti stretti $A^{p_0} = P$, quindi $f(A^{p_0}) = p_0$. Se p_0 è elemento massimale, abbiamo finito. Altrimenti $A^{p_0} \neq \emptyset$ e possiamo prendere $p_1 = f(A^{p_0})$. È facile verificare che anche $\{p_0 < p_1\}$ è una *f-catena*. Di nuovo, se p_1 è un elemento massimale di P , la tesi è raggiunta. Altrimenti possiamo iterare il procedimento e, se non troviamo elementi massimali, arriviamo a definire una *f-catena* infinita $A = \{p_0 < p_1 < p_2 < \dots < p_n < p_{n+1} < \dots\}$.

Adesso, per ipotesi ogni catena ammette maggioranti, dunque possiamo prendere l'elemento $p_\omega = f(\{p \in P \mid p > A\})$ ed aggiungerlo alla *f-catena* A . Si osservi che anche $A' = A \cup \{p_\omega\}$ è una *f-catena*, visto che il segmento iniziale $(A')_{p_\omega} = A$, che $(A')^{p_\omega} = \{p \in P \mid p > A\}$, e che quindi $p_\omega = f((A')^{p_\omega})$. Proseguiamo in questo modo, e “allunghiamo” la catena finché ciò è possibile, cioè fin quando esistono maggioranti stretti.

Per rendere rigorosa questa costruzione informale, ci occorre intanto la seguente proprietà.

($\star$) Se A e B sono due *f-catene*, allora una è segmento iniziale dell'altra.

Visto che A e B sono buoni ordini, uno dei due è isomorfo ad un segmento iniziale dell'altro. Ad esempio, supponiamo che $\theta : A \rightarrow B$ sia un isomorfismo, dove S è un segmento iniziale (non necessariamente proprio) di B . Vogliamo dimostrare che θ è l'identità. Procediamo per assurdo, e consideriamo $a = \min\{x \in A \mid \theta(x) \neq x\}$. I segmenti iniziali A_a e $B_{\theta(a)}$ coincidono, dunque anche i corrispondenti insiemi di maggioranti stretti $A^a = B^{\theta(a)}$ sono uguali. Ma allora si avrebbe che $a = f(A^a) = f(B^{\theta(a)}) = \theta(a)$, contro l'ipotesi.

Sappiamo che l'unione di un insieme di buoni ordini che sono uno segmento iniziale dell'altro è ancora un buon ordine. Dunque l'unione $(C, \leq)$ di tutte le *f-catene* è un sottoinsieme bene ordinato di P . Inoltre è facile verificare che C stesso è una *f-catena*, e quindi C è la *f-catena* massima. In particolare, non esistono maggioranti stretti di C , altrimenti la catena C potrebbe essere estesa. Da questo segue che un elemento maggiorante della catena C è necessariamente il massimo di C , ed è inoltre un elemento massimale per P . $\square$

DIM.2. Sia $(P, \leq)$ un insieme parzialmente ordinato dove ogni catena ammette maggioranti. Fissiamo una funzione di scelta $f : \mathcal{P}(P) \setminus \{\emptyset\} \rightarrow P$, e prendiamo un elemento $\star \notin P$. Per ricorsione transfinita, definiamo $p_0 = f(P)$, e per $\alpha > 0$:

$$p_\alpha = \begin{cases} f(P^\alpha) & \text{se } \star \notin \{p_\beta \mid \beta < \alpha\} \text{ e } P^\alpha = \{p \in P \mid \forall \beta < \alpha \ p > p_\beta\} \neq \emptyset \\ \star & \text{altrimenti.} \end{cases}$$

Con questa definizione, costruiamo una sequenza strettamente crescente di elementi di P , fino a che ciò è possibile. Notiamo che se arriviamo ad un passo α dove l'insieme P^α dei maggioranti *stretti* di $\{p_\beta \mid \beta < \alpha\}$ è vuoto, allora $p_\alpha = \star$. Inoltre,

² Se $X \subseteq P$ è un insieme, scriviamo $p > X$ per intendere $p > x$ per tutti i $x \in X$.

se questo accade, dalla definizione segue immediatamente che allora avremo $p_\beta = \star$ per tutti gli ordinali $\beta > \alpha$.

Verifichiamo che esistono effettivamente indici α tali che $p_\alpha = \star$. Se così non fosse, ogni $p_\alpha = f(P^\alpha) \in P^\alpha \subseteq P$, e dunque la funzione-classe $\mathbb{F} : \alpha \mapsto p_\alpha$, che è definita sulla classe propria degli ordinali, sarebbe strettamente crescente, quindi iniettiva. Ma allora anche la sua immagine $\{p_\alpha \mid \alpha \in \mathbf{ORD}\}$ sarebbe una classe propria, e questo è impossibile perché si tratta di un sottoinsieme di P .

Sia adesso α il più piccolo indice con $p_\alpha = \star$. Se per assurdo α fosse un ordinale limite, ogni maggiorante della catena crescente $\{p_\beta \mid \beta < \alpha\}$ sarebbe anche un maggiorante stretto, e quindi un elemento di P^α . Ma allora dovrebbe essere $p_\alpha = f(P^\alpha) \in P$, contro l'ipotesi $p_\alpha = \star \notin P$. Concludiamo allora che $\alpha = \beta + 1$ è un successore, e quindi p_β è l'ultimo elemento della sequenza diverso da $\star$. È adesso facile verificare che p_β è un elemento massimale in $(P, \leq)$, perché un eventuale $p > p_\beta$ apparterebbe a $P^{\beta+1}$, e sarebbe $p_{\beta+1} \neq \star$. $\square$

TEOREMA 1.2 (ZF). (*Teorema di Zermelo*) “*Lemma di Zorn*” $\Rightarrow$ “*Ogni insieme è bene ordinabile*”.

DIM. Dato un insieme X , consideriamo la collezione di tutti i possibili buoni ordini ottenuti con suoi sottoinsiemi:

$$\mathcal{B} = \{(B, \leq_B) \text{ buon ordine} \mid B \subseteq X\}.$$

Il fatto che $\mathcal{B}$ è effettivamente un insieme segue per separazione, notando che ogni elemento di $\mathcal{B}$ appartiene a $\mathcal{P}(X) \times \mathcal{P}(X \times X)$.³ Su $\mathcal{B}$ definiamo la seguente relazione:

$$(B, \leq_B) \preceq (B', \leq_{B'}) \text{ se e solo se } (B, \leq_B) \text{ è un segmento iniziale di } (B', \leq_{B'}).$$

Più precisamente, richiediamo che $B \subseteq B'$, che la relazione d'ordine $\leq_{B'}$ ristretta ad elementi di B coincida con $\leq_B$, ed infine che se $x \leq_{B'} b$ dove $b \in B$, allora anche $x \in B$. È immediato verificare che $\preceq$ è un ordinamento parziale su $\mathcal{B}$. Inoltre, ogni catena C di $\mathcal{B}$ ammette maggiorante (basta considerare l'unione $\bigcup C$ e ricordare che unione di bene ordinati che sono uno segmento iniziale dell'altro è ancora un buon ordine). Possiamo allora applicare il *Lemma di Zorn* e ricavare l'esistenza di un elemento massimale $(B, \leq_B) \in \mathcal{B}$. Per concludere la dimostrazione, resta da verificare che $B = X$. Se così non fosse, potremmo prendere un elemento $\xi \in X \setminus B$, e sull'insieme $B \cup \{\xi\}$ considerare il buon ordinamento $\leq$ dove ξ viene posto “dopo” tutti gli elementi di B , cioè $x \leq y$ se e solo se $x, y \in B$ e $x \leq_B y$, oppure $y = \xi$. Allora $(B \cup \{\xi\}, \leq)$ sarebbe un buon ordine avente B come segmento iniziale generato da ξ , contro la massimalità di $(B, \leq_B)$. $\square$

La proprietà del buon ordinamento di Zermelo implica direttamente l'assioma di scelta.

TEOREMA 1.3 (ZF). “*Ogni insieme è bene ordinabile*” $\Rightarrow$ “*Assioma di scelta*”.

DIM. Sia X un insieme non vuoto fissato. Per ipotesi, esiste un buon ordinamento $\leq$ su X . Una funzione di scelta $f : \mathcal{P}(X) \setminus \{\emptyset\} \rightarrow X$ si può allora definire ponendo $f(A) = \min A$ per ogni $A \subseteq X$ non vuoto. $\square$

³ Ricordiamo che gli insiemi ordinati $(B, \leq_B)$ sono coppie ordinate, dove B è un insieme e la relazione d'ordine $\leq_B$ è uno speciale insieme di coppie ordinate di elementi di B .

Combinando i tre teoremi di questa sezione, otteniamo le seguenti equivalenze:

TEOREMA 1.4 (ZF). *Le seguenti proprietà sono equivalenti:*

- (1) *Assioma di scelta.*
- (2) *Lemma di Zorn.*
- (3) *Proprietà di Zermelo: “Ogni insieme è bene ordinabile”.*

2. Uso della funzione-classe di Hartogs

Il teorema di Hartogs ci permetterà di chiarire il ruolo dell’assioma di scelta riguardo la nozione di cardinalità.

Introduciamo due proprietà relative alla nozione di equipotenza fra insiemi che mostreremo essere equivalenti all’assioma di scelta. La prima riguarda l’ordine fra cardinalità.

- *Confrontabilità delle cardinalità:*

“Per tutti gli insiemi A, B esiste una funzione iniettiva $f : A \rightarrow B$ o esiste una funzione iniettiva $g : B \rightarrow A$, cioè si ha $|A| \leq |B|$ o $|B| \leq |A|$ ”.

Abbiamo già dimostrato (senza usare AC) che $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, e che $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$. Vedremo che l’estensione di questa proprietà a tutti gli insiemi infiniti è una forma equivalente dell’assioma di scelta.

- *Idempotenza delle cardinalità infinite:*

“Ogni insieme infinito X è equipotente al prodotto cartesiano con se stesso, cioè $|X \times X| = |X|$ ”.

Grazie allo strumento della funzione-classe di Hartogs, possiamo mostrare l’equivalenza con AC delle proprietà relative alla cardinalità introdotte sopra.

TEOREMA 2.1 (ZF). *Le seguenti proprietà sono equivalenti:*⁴

- (1) *Proprietà di Zermelo: “ogni insieme è bene ordinabile”.*
- (2) *Confrontabilità delle cardinalità.*
- (3) *Idempotenza delle cardinalità infinite.*

DIM. (1) $\Rightarrow$ (2). Per la proprietà di Zermelo, esiste un buon ordine $<_A$ su A ed esiste un buon ordine $<_B$ su B . Per il teorema di tricotomia dei buoni ordini, $(A, <_A)$ è isomorfo ad un segmento iniziale di $(B, <_B)$ o viceversa. Visto che isomorfismi di ordine sono in particolare bigezioni, concludiamo che A è equipotente ad un sottoinsieme di B o viceversa, e quindi $|A| \leq |B|$ o $|B| \leq |A|$.

(2) $\Rightarrow$ (1). Dal Teorema di Hartogs sappiamo che $|\mathbb{H}(A)| \not\leq |A|$. Allora, per la confrontabilità delle cardinalità, deve essere $|A| \leq |\mathbb{H}(A)|$, cioè esiste una funzione iniettiva $f : A \rightarrow \mathbb{H}(A)$. Ma $\mathbb{H}(A)$ è un cardinale, dunque bene ordinato, e perciò A “eredita” mediante f un buon ordinamento. Precisamente, se si pone $a < a' \Leftrightarrow f(a) <_A f(a')$ per tutti gli $a, a' \in A$, allora dall’iniettività di f segue che $(A, <_A) \cong (\text{imm}(f), <)$, e quindi $(A, <_A)$ è bene ordinato in quanto isomorfo ad un sottoinsieme ordinato di $\mathbb{H}(A)$.

(1) $\Rightarrow$ (3). Come abbiamo visto nel capitolo sui cardinali (vedi Teorema ??), ogni insieme infinito bene ordinabile è equipotente ad un aleph. Quindi, per la

⁴ L’equivalenza tra AC e la confrontabilità delle cardinalità è attribuita ad Hartogs, 1915. L’equivalenza tra AC e l’idempotenza delle cardinalità infinite è attribuita a Tarski, 1924.

proprietà di Zermelo, ogni insieme infinito X è equipotente ad un $\aleph_\alpha$. La tesi segue allora dalla proprietà $|\aleph_\alpha \times \aleph_\alpha| = |\aleph_\alpha|$ (vedi Teorema ??).

(3) $\Rightarrow$ (1). Visto che ogni insieme finito è banalmente bene ordinabile, possiamo assumere che A sia infinito. Inoltre, a meno di rimpiazzare A con $A' = A \times \{0\}$, possiamo supporre che A non contenga ordinali, e quindi che $A \cap \mathbb{H}(A) = \emptyset$. Per l'ipotesi $A \cup \mathbb{H}(A)$ è equipotente al prodotto cartesiano $(A \cup \mathbb{H}(A)) \times (A \cup \mathbb{H}(A))$. Visto che quest'ultimo è un soprainsieme di $A \times \mathbb{H}(A)$, esiste allora una funzione iniettiva $\varphi : A \times \mathbb{H}(A) \rightarrow A \cup \mathbb{H}(A)$. Per ogni $a \in A$, la restrizione $\varphi_a : \mathbb{H}(A) \rightarrow A \cup \mathbb{H}(A)$ dove $\alpha \mapsto \varphi(a, \alpha)$ è anch'essa iniettiva. Ma allora $\text{imm}(\varphi_a) \not\subseteq A$, altrimenti avremmo che $|\mathbb{H}(A)| \leq |A|$, contro il Teorema di Hartogs. Dunque $\mathbb{H}(A) \cap \text{imm}(\varphi_a) \neq \emptyset$ e possiamo prendere $\theta(a) = \min \mathbb{H}(A) \cap \text{imm}(\varphi_a)$. In questo modo resta definita una funzione $\theta : A \rightarrow \mathbb{H}(A)$. Visto che φ è iniettiva, è immediato verificare che anche θ è iniettiva, e quindi A “eredita” un buon ordine da $\mathbb{H}(A)$ ponendo $a < a' \Leftrightarrow f(a) < f(a')$ per tutti $a, a' \in A$. $\square$

Ci sono molte altre proprietà relative alle cardinalità che sono equivalenti all'assioma di scelta. Ad esempio:

TEOREMA 2.2 (ZF). (*Tarski 1924*). *Le seguenti proprietà sono equivalenti:*

- (1) *Proprietà di Zermelo.*
- (2) $|A \times B| = |A \cup B|$ per tutti gli insiemi infiniti A, B tali che $A \cap B = \emptyset$.
- (3) $|A \times A| = |B \times B| \Rightarrow |A| = |B|$ per tutti gli insiemi infiniti A, B .
- (4) *Per ogni insieme infinito A esiste un insieme B tale che $|A| = |B \times B|$ (cioè ogni cardinalità infinita ha una radice quadrata).*

DIM. Per esercizio. $\square$

3. Uso del Lemma di Zorn

In questa sezione mostriamo come si possano dimostrare direttamente a partire dal Lemma di Zorn sia la confrontabilità delle cardinalità, sia l'idempotenza dei cardinali infiniti. Anche se si tratta di proprietà già dimostrate con l'uso della funzione-classe di Hartogs, e il percorso in questo caso diventa più tortuoso, si tratta però di esempi significativi di uso del Lemma di Zorn, che può essere istruttivo vedere.

TEOREMA 3.1 (ZF). “*Lemma di Zorn*” $\Rightarrow$ “*Confrontabilità delle cardinalità*”.

DIM. Consideriamo l'insieme parzialmente ordinato $(\mathcal{F}, \preceq)$ dove

$$\mathcal{F} = \{f : X \rightarrow B \mid X \subseteq A, f \text{ iniettiva}\}$$

e dove $f \preceq g$ se e solo se $f \subseteq g$, cioè se g è una estensione di f . È facile verificare che ogni catena $\mathcal{C} \subseteq \mathcal{F}$ ammette maggiorante; infatti, per la proprietà di catena, $\mathcal{C}$ contiene funzioni che sono una estensione dell'altra e quindi l'unione $\varphi = \bigcup \mathcal{C}$ è una funzione iniettiva $\varphi : \tilde{X} \rightarrow B$ dove $\tilde{X} = \bigcup \{\text{dom}(f) \mid f \in \mathcal{C}\} \subseteq A$ che estende ogni $f \in \mathcal{C}$. Per l'ipotesi, possiamo prendere allora un elemento massimale $F : X \rightarrow B$. Se $X = A$ abbiamo $|A| \leq |B|$. Se F è suriettiva, abbiamo una bigezione tra il sottoinsieme $X \subseteq A$ e B , e quindi $|B| \leq |A|$.

Per completare la dimostrazione, mostriamo che la terza eventualità, cioè che $X \neq A$ e $\text{imm}(F) \neq B$, non può accadere. In questo caso infatti potremmo prendere

un elemento $a \in A \setminus X$, un elemento $b \in B \setminus \text{imm}(F)$, e considerare la funzione $G : X \cup \{a\} \rightarrow B$ che estende F ponendo $G(a) = b$. Chiaramente G è iniettiva e $G \succ F$, contro la massimalità di F . $\square$

Vediamo una prima conseguenza della confrontabilità delle cardinalità.

PROPOSIZIONE 3.2 (ZF). *Se vale la confrontabilità: “Per tutti gli insiemi A, B si ha $|A| \leq |B|$ o $|B| \leq |A|$ ”, allora per ogni X infinito si ha $|\mathbb{N}| \leq |X|$.”⁵*

DIM. Vista l’ipotesi, basta verificare che $|X| < |\mathbb{N}|$ è impossibile. Supponiamo per assurdo che esista $f : X \rightarrow \mathbb{N}$ iniettiva; chiaramente $|X| = |\text{imm}(f)|$. Se $\text{imm}(f) \subseteq \mathbb{N}$ fosse infinito allora avremmo che $|\text{imm}(f)| = |\mathbb{N}|$, contro l’assunzione $|\mathbb{N}| \neq |X|$.⁶ Allora $\text{imm}(f)$ deve essere finito, ma anche questo non è possibile perché un insieme finito non può essere equipotente a $\mathbb{N}$.⁷ $\square$

ESERCIZIO 3.3. Senza usare né l’assioma di scelta, né la confrontabilità, mostrare direttamente che: “Lemma di Zorn” $\Rightarrow$ “per ogni X infinito si ha $|\mathbb{N}| \leq |X|$ ”.

PROPOSIZIONE 3.4 (ZF). *Sia X un insieme infinito e supponiamo che $|X \times X| = |X|$. Se $|A_1| = \dots = |A_k| = |X|$ allora anche $|A_1 \cup \dots \cup A_k| = |X|$.*

PROOF. Per ogni $i = 1, \dots, k$, fissiamo una bigezione $f_i : A_i \rightarrow X$, e definiamo la funzione $F : A_1 \cup \dots \cup A_k \rightarrow X \times \{1, \dots, k\}$ ponendo $F(a) = (f_s(a), s)$ dove $s = \min\{i \mid x \in A_i\}$. Chiaramente F è iniettiva. Inoltre banalmente $|\{1, \dots, k\}| \leq |X|$ perché X è infinito. La tesi si ottiene applicando il Teorema di Cantor-Bernstein a partire dalle seguenti disuguaglianze:

$$|X| = |A_1| \leq |A_1 \cup \dots \cup A_k| \leq |X \times \{1, \dots, k\}| \leq |X \times X| = |X|.$$

$\square$

TEOREMA 3.5 (ZF). *Lemma di Zorn $\Rightarrow |A \times A|$ per ogni insieme infinito A .*

DIM. Visto che banalmente $|A| \leq |A \times A|$, per il Teorema di Cantor-Bernstein basta mostrare l’esistenza di una funzione iniettiva $f : A \times A \rightarrow A$. Consideriamo l’insieme parzialmente ordinato $(\mathcal{F}, \preceq)$ dove

$$\mathcal{F} = \{f : X \times X \rightarrow X \mid X \subseteq A \text{ infinito, } f \text{ iniettiva}\}$$

e dove $f \preceq g$ se e solo se $f \subseteq g$, cioè g è una estensione di f . Notiamo anzitutto che $\mathcal{F} \neq \emptyset$. Infatti dalla Proposizione 3.2 sappiamo che esiste una funzione iniettiva $\theta : \mathbb{N} \rightarrow A$, e quindi un sottoinsieme $X = \text{imm}(\theta) \subseteq A$ con $|X| = |\mathbb{N}|$. Senza usare AC, abbiamo visto $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$. Allora abbiamo che $|X \times X| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}| = |X|$; più esplicitamente, se $\psi : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ è una bigezione, allora la funzione $f : X \times X \rightarrow X$ dove $f(\theta(n), \theta(m)) = \theta(\psi(n, m))$ è una bigezione, e quindi appartiene ad $\mathcal{F}$.

Procedendo in modo analogo alla dimostrazione del Teorema 3.1 di sopra, è facile verificare che ogni catena $\mathcal{C} \subseteq \mathcal{F}$ ha come maggiorante l’unione $\bigcup_{f \in \mathcal{C}} f$. Per il Lemma di Zorn esiste allora un elemento massimale $F : X \times X \rightarrow X$. Notiamo che per Cantor-Bernstein deve essere $|X \times X| = |X|$.

⁵ Ricordiamo che avevamo già dimostrato questa proprietà degli insiemi infiniti usando però l’assioma di scelta (vedi Teorema ??).

⁶ Qui abbiamo usato la Proposizione ??, che era stata dimostrata senza usare l’assioma di scelta.

⁷ Qui abbiamo usato la Proposizione ??, con la quale abbiamo mostrato, senza usare l’assioma di scelta, che $\mathbb{N}$ non è equipotente ad alcun insieme finito

Visto che $X \subseteq A$, banalmente $|X| \leq |A|$. Se $|X| = |A|$, allora $|A \times A| = |X \times X| = |X| = |A|$, come voluto. Per completare la dimostrazione, resta da vedere che $|X| < |A|$ è impossibile.

Supponiamo allora per assurdo che $|X| < |A|$, e consideriamo il complemento $A \setminus X$. La disuguaglianza $|A \setminus X| \leq |X|$ non può valere, altrimenti si avrebbe

$$|A| = |X \cup (A \setminus X)| \leq |(X \times \{1\}) \cup (X \cup \{2\})| = |X \times \{1, 2\}| \leq |X \times X| = |X| < |A|.$$

Allora, per la confrontabilità (che segue dal Lemma di Zorn, vedi Teorema 3.1) deve valere la disuguaglianza $|X| < |A \setminus X|$. Possiamo allora prendere un sottoinsieme $X' \subseteq A \setminus X$ con $|X'| = |X|$. Il nostro scopo è adesso quello di estendere F ad una funzione iniettiva $G : (X \cup X') \times (X \cup X') \rightarrow X \cup X'$, contraddicendo così la massimalità di F .

Notiamo che $(X \cup X') \times (X \cup X')$ è dato dall'unione disgiunta di $(X \times X)$ con $Y = (X \times X') \cup (X' \times X) \cup (X' \times X')$. Adesso, $|X \times X'| = |X' \times X| = |X' \times X'| = |X \times X| = |X|$ e quindi $|X| \leq |Y| = |X \times \{1, 2, 3\}| \leq |X \times X| = |X|$. Possiamo prendere allora una bigezione $F' : Y \rightarrow X'$, e definire $G = F \cup F'$. È immediato verificare che $G : (X \cup X') \times (X \cup X') \rightarrow X \cup X'$ è iniettiva, in quanto unione disgiunta di due funzioni iniettive. $\square$

Algebra cardinale e cofinalità

1. Somme, prodotti, esponenziazioni

Ricordiamo ora alcune nozioni riguardanti la cardinalità che avevamo presentato nella parte “intuitiva” della teoria degli insiemi.

Se A è finito, avevamo denotato con $|A|$ quell'unico numero naturale $n \in \omega$ equipotente ad A , e quindi scrivevamo $|A| = n$. Possiamo adesso fare una cosa analoga per tutti gli insiemi, anche infiniti, grazie ai cardinali.

DEFINIZIONE 1.1. (AC) Per ogni insieme A , denotiamo con $|A|$ quell'unico cardinale κ tale che $|\kappa| = |A|$. In questo caso scriviamo

$$|A| = \kappa.$$

NOTA BENE 1.2. Senza usare AC, la definizione di sopra ha senso per ogni insieme bene ordinabile, ma non in generale. Ad esempio, se non assumiamo che l'insieme dei numeri reali $\mathbb{R}$ sia bene ordinabile, non potremmo avere l'esistenza di un cardinale ad esso equipotente.

Attenzione. Da qui in avanti assumeremo sempre l'assioma di scelta, salvo indicazione contraria.

DEFINIZIONE 1.3. Siano μ, ν cardinali. Diciamo che $\mu \leq \nu$ se esiste una funzione iniettiva $f : \mu \rightarrow \nu$.

Chiaramente, la relazione d'ordine $\leq$ definita sopra coincide con la relazione d'ordine tra ordinali; in particolare, da $\kappa \leq \mu$ e $\mu \leq \kappa$ segue che $\kappa = \mu$. In conseguenza di questa banale osservazione, possiamo ottenere una dimostrazione alternativa del teorema di Cantor-Bernstein, che però richiede l'assunzione che ogni insieme sia equipotente ad un cardinale, e quindi l'intera potenza dell'assioma di scelta.

Introduciamo finalmente l'algebra cardinale, definendo le operazioni di somma, prodotto, ed esponenziazione tra cardinali.

DEFINIZIONE 1.4. Siano μ, ν cardinali. Allora

- $\mu + \nu = |A \cup B|$ dove A, B sono insiemi disgiunti con $|A| = \mu$ e $|B| = \nu$;
- $\mu \cdot \nu = |A \times B|$ dove A, B sono insiemi con $|A| = \mu$ e $|B| = \nu$;
- $\mu^\nu = |\text{Fun}(A, B)|$ dove A, B sono insiemi con $|A| = \nu$ e $|B| = \mu$.¹

Che le definizioni di sopra sono ben poste, segue dalle proprietà raccolte nel seguente esercizio, che in realtà abbiamo già considerato nel capitolo ??.²

ESERCIZIO 1.5. Supponiamo che $|A| = |A'|$ e $|B| = |B'|$. Allora:

- (1) $|A \cup B| = |A' \cup B'|$ se $A \cap B = A' \cap B' = \emptyset$.
- (2) $|A \times B| = |A' \times B'|$.
- (3) $|\text{Fun}(A, B)| = |\text{Fun}(A', B')|$.

¹ Ricordiamo che con $\text{Fun}(A, B)$ oppure con B^A si denota l'insieme delle funzioni con dominio A a valori in B .

² Vedi Esercizio ??.

ESERCIZIO 1.6. Per ogni cardinale κ e per ogni naturale positivo n si ha:

$$\kappa \cdot n = \underbrace{\kappa + \dots + \kappa}_{n \text{ volte}} \quad e \quad \kappa^n = \underbrace{\kappa \cdot \dots \cdot \kappa}_{n \text{ volte}}.$$

Le prime fondamentali proprietà delle operazioni cardinali di somma, prodotto, ed esponenziazione cardinale sono raccolte nella seguente proposizione.

PROPOSIZIONE 1.7. *Siano $\kappa, \kappa', \mu, \mu', \nu$ cardinali. Allora valgono:*

- (1) *Proprietà associative della somma e del prodotto:*
 - $\kappa + (\mu + \nu) = (\kappa + \mu) + \nu.$
 - $\kappa \cdot (\mu \cdot \nu) = (\kappa \cdot \mu) \cdot \nu.$
- (2) *Proprietà commutative della somma e del prodotto:*
 - $\kappa + \mu = \mu + \kappa.$
 - $\kappa \cdot \mu = \mu \cdot \kappa.$
- (3) *Proprietà distributiva della somma rispetto al prodotto:*
 - $\kappa \cdot (\mu + \nu) = (\kappa \cdot \mu) + (\kappa \cdot \nu).$
- (4) *Proprietà di monotonìa della somma, del prodotto, e dell'esponenziazione:*
 - Se $\kappa' \leq \kappa$ e $\mu' \leq \mu$ allora $\kappa' + \mu' \leq \kappa + \mu.$
 - Se $\kappa' \leq \kappa$ e $\mu' \leq \mu$ allora $\kappa' \cdot \mu' \leq \kappa \cdot \mu.$
 - Se $\kappa' \leq \kappa$ e $\mu' \leq \mu$ allora $(\kappa')^{\mu'} \leq \kappa^\mu.$

DIM. Per esercizio.³

□

Valgono inoltre le seguenti proprietà tipiche dell'esponenziazione:

PROPOSIZIONE 1.8. *Siano κ, μ, ν cardinali. Allora:*

- (1) $\kappa^{\mu+\nu} = \kappa^\mu \cdot \kappa^\nu.$
- (2) $(\kappa^\mu)^\nu = \kappa^{\mu \cdot \nu}.$
- (3) $(\kappa \cdot \mu)^\nu = \kappa^\nu \cdot \mu^\nu.$

DIM. Per esercizio.

□

Segue direttamente dalle definizioni che per ogni cardinale $\kappa \neq 0$ si ha:

- $\kappa + 0 = \kappa$
- $\kappa \cdot 0 = 0$
- $\kappa \cdot 1 = \kappa.$
- $\kappa^1 = \kappa.$
- $1^\kappa = 1.$

ESERCIZIO 1.9. Sia n un naturale positivo. Allora $n + \aleph_0 = n \cdot \aleph_0 = (\aleph_0)^n = \aleph_0.$

Ricordiamo che in base al Teorema di Cantor si ha $|\mathcal{P}(A)| > |A|$ per ogni insieme A . Come abbiamo già osservato nel capitolo ??, c'è una bigezione naturale tra $\mathcal{P}(A)$ e $\text{Fun}(A, \{0, 1\})$ che si ottiene associando ad ogni sottoinsieme $X \subseteq A$ la corrispondente funzione caratteristica $1_X : A \rightarrow \{0, 1\}$. Quindi, per ogni cardinale κ si ha $|\mathcal{P}(k)| = |\text{Fun}(\kappa, \{0, 1\})|$, e perciò:

- $2^k > \kappa.$

In particolare, la cardinalità del *continuo* è più che numerabile:

- $\mathfrak{c} := |\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0} > \aleph_0.$

³ La proprietà (4) è già stata considerata nel capitolo ??, Esercizio ??.

NOTA BENE 1.10. Gli assiomi di ZFC non permettono di stabilire quale tra i cardinali maggiori di κ sia uguale a 2^κ . A questo riguardo, valgono i seguenti importanti risultati, che sono stati dimostrati usando strumenti avanzati di logica matematica.

- (Gödel 1938). Gli assiomi di ZFC non consentono di refutare la seguente proprietà, nota come *ipotesi generalizzata del continuo* (GCH):
 - Per ogni cardinale infinito κ , si ha che $2^\kappa = \kappa^+$ è il cardinale successore di κ .

In particolare, è consistente con ZFC assumere che $\mathfrak{c} = \aleph_1$.

- (Cohen 1963). Gli assiomi di ZFC non consentono di dimostrare la seguente proprietà, nota come *ipotesi del continuo* (CH):
 - $2^{\aleph_0} = \aleph_1$.

In particolare, è consistente con ZFC assumere che $\mathfrak{c} > \aleph_1$.

ESERCIZIO 1.11. Sia n un naturale positivo. Allora:

$$n + \mathfrak{c} = \aleph_0 + \mathfrak{c} = n \cdot \mathfrak{c} = \aleph_0 \cdot \mathfrak{c} = \mathfrak{c}^n = \aleph_0^{\aleph_0} = \mathfrak{c}^{\aleph_0} = \mathfrak{c}.$$

Il Teorema ??, in base al quale $|\aleph_\alpha \times \aleph_\alpha| = |\aleph_\alpha|$ per ogni α , ci dice che:

- $\kappa \cdot \kappa = \kappa$ per ogni cardinale infinito κ .

Come conseguenza dell'idempotenza del prodotto tra cardinali infiniti $\kappa \cdot \kappa = \kappa$, l'algebra cardinale relativa a somme e prodotti si rivela banale, come mostra la seguente

PROPOSIZIONE 1.12. Siano $\kappa, \mu \neq 0$ cardinali dove almeno uno dei due è infinito. Allora

$$\kappa + \mu = \kappa \cdot \mu = \max\{\kappa, \mu\}.$$

DIM. Senza perdita di generalità supponiamo $\kappa \geq \mu$, dunque κ è infinito e $\max\{\kappa, \mu\} = \kappa$. Se $\mu = 1$ la tesi è banale perché $\kappa + 1 = \kappa$ (visto che κ è infinito) e $\kappa \cdot 1 = \kappa$. Altrimenti, quando $\mu \geq 2$ abbiamo la seguente catena di disuguaglianze:

$$\kappa \leq \kappa + \mu \leq \kappa + \kappa = \kappa \cdot 2 \leq \kappa \cdot \mu \leq \kappa \cdot \kappa = \kappa.$$

□

Come corollario si ricava il seguente risultato generale sui complementi relativi. Ricordiamo che i casi particolari per la cardinalità numerabile $\aleph_0$ e la cardinalità del continuo $\mathfrak{c}$ sono già stati dimostrati nel capitolo ??, senza usare l'assioma di scelta.⁴

PROPOSIZIONE 1.13. Sia $A \subseteq B$ dove B è un insieme infinito. Se $|A| < |B|$ allora $|B \setminus A| = |B|$.

DIM. Se A è vuoto la tesi è banale. Se $|A| \neq 0$, possiamo applicare la proposizione precedente, ed otteniamo:

$$|B| = |B \setminus A| + |A| = \max\{|B \setminus A|, |A|\}.$$

Visto che $|A| < |B|$, deve essere $|B| = |B \setminus A|$. □

ESERCIZIO 1.14. Siano $\kappa \geq \nu$ cardinali infiniti. Allora i seguenti insiemi hanno cardinalità κ^ν :

⁴ Vedi Proposizione ?? e Esercizio ??.

- $[\kappa]^{\leq \nu} := \{A \subseteq \kappa \mid |A| \leq \nu\}$.
- $[\kappa]^\nu := \{A \subseteq \kappa \mid |A| = \nu\}$.

ESERCIZIO 1.15. Siano α, β ordinali infiniti. Allora

$$|\alpha + \beta| = |\alpha \cdot \beta| = |\alpha^\beta| = \max\{|\alpha|, |\beta|\}.$$

Quando la base è “piccola” rispetto all’esponente “grande”, l’esponenziazione tra cardinali coincide con la cardinalità dell’insieme delle parti dell’insieme “grande”.

PROPOSIZIONE 1.16. Sia κ un cardinale infinito e supponiamo che $2 \leq \mu \leq 2^\kappa$. Allora $\mu^\kappa = 2^\kappa$. In particolare, $\kappa^\kappa = 2^\kappa$ per ogni cardinale infinito.

DIM. Vale la catena di disuguaglianze: $2^\kappa \leq \mu^\kappa \leq (2^\kappa)^\kappa = 2^{\kappa \cdot \kappa} = 2^\kappa$. $\square$

2. La sequenza dei beth e i limiti forti

DEFINIZIONE 2.1. La sequenza degli *beth* è definita per ricorsione transfinita come segue:

$$\begin{cases} \beth_0 = \aleph_0; \\ \beth_{\alpha+1} = 2^{\beth_\alpha}; \\ \beth_\lambda = \bigcup_{\gamma < \lambda} \beth_\gamma \text{ se } \lambda \text{ è limite.} \end{cases}$$

Notiamo che, rispetto alla definizione della sequenza degli aleph, al passo successore qua si considera la cardinalità dell’insieme delle parti $\beth_{\alpha+1} = 2^{\beth_\alpha} = |\mathcal{P}(\beth_\alpha)|$ anziché il cardinale successore $\aleph_{\alpha+1} = \mathbb{H}(\aleph_\alpha) = (\aleph_\alpha)^+$. Per il Teorema di Cantor, sappiamo che per ogni cardinale κ si ha $2^\kappa > \kappa$, e quindi $2^\kappa \geq \kappa^+$. Di conseguenza, è immediato verificare per induzione transfinita che vale la disuguaglianza:

OSSERVAZIONE 2.2. Per ogni ordinale α si ha $\aleph_\alpha \leq \beth_\alpha$.

Ricordiamo che l’ipotesi generalizzata del continuo GCH afferma che $2^\kappa = \kappa^+$ è il cardinale successore di κ , per ogni cardinale infinito κ . Sotto questa ipotesi la sequenza dei beth e la sequenza degli aleph coincidono.

PROPOSIZIONE 2.3. Le seguenti proprietà sono equivalenti:

- (1) *Ipotesi generalizzata del continuo (GCH):*
 $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ per ogni ordinale α .
- (2) $\aleph_\alpha = \beth_\alpha$ per ogni ordinale α .

DIM. Per esercizio. $\square$

ESERCIZIO 2.4.

- (1) La sequenza dei beth ha punti fissi arbitrariamente grandi, cioè per ogni ordinale α esiste $\beta > \alpha$ tale che $\beth_\beta = \beta$.
- (2) La classe $\text{Fix}(\beth) = \{\alpha \in \mathbf{ORD} \mid \beth_\alpha = \alpha\}$ è una classe propria.

DEFINIZIONE 2.5. Un cardinale κ si dice *limite forte* se per tutti i cardinali $\mu, \nu < \kappa$ si ha $\mu^\nu < \kappa$.

OSSERVAZIONE 2.6. Se il cardinale κ è limite forte allora κ è un cardinale *limite*.

DIM. Intanto notiamo che $\kappa = \aleph_0$ è sia limite forte che limite. Se $\kappa > \aleph_0$ non è un cardinale limite, allora $\kappa = \aleph_{\alpha+1}$ per un opportuno α . Visto che $2^{\aleph_\alpha} \geq \aleph_{\alpha+1} = \kappa$ dove $2, \aleph_\alpha < \kappa$, concludiamo che κ non è un limite forte. $\square$

Il prossimo risultato fornisce una caratterizzazione dei limiti forti come punti limite della sequenza dei beth.

PROPOSIZIONE 2.7. *Un cardinale $\kappa > \aleph_0$ è limite forte se e solo se è un punto limite della sequenza dei beth, cioè $\kappa = \beth_\lambda$ dove λ è un ordinale limite.*

DIM. Visto che $\alpha \leq \beth_\alpha$, la sequenza dei beth è illimitata, e quindi possiamo considerare $\gamma := \min\{\beta \mid \kappa < \beth_\beta\}$. Osserviamo che $\gamma \neq 0$ perché $\kappa > \aleph_0$. Inoltre γ non è limite, altrimenti $\kappa < \beth_\gamma = \bigcap_{\gamma < \alpha} \beth_\alpha$ implicherebbe $\kappa < \beth_\gamma$ per un opportuno $\gamma < \alpha$, contro la minimalità di α . Allora $\alpha = \beta + 1$ deve essere un successore, e si ha $\beth_\beta \leq \kappa < \beth_{\beta+1}$. Non è possibile che $\beth_\beta < \kappa$, altrimenti $2^{\beth_\beta} = \beth_{\beta+1} = \kappa$, contro l'ipotesi di κ limite forte. Resta quindi dimostrato che $\kappa = \beth_\beta$. Infine osserviamo che per ogni α , il cardinale $\beth_{\alpha+1}$ non è limite forte, perché $2^{\beth_\alpha} = \beth_{\alpha+1}$ dove $2, \beth_\alpha < \beth_{\alpha+1}$. Per esclusione, deve allora essere $\kappa = \beth_\beta$ dove β è limite. $\square$

ESERCIZIO 2.8. Il cardinale $\aleph_\omega$ è limite forte se e solo se $\aleph_\omega = \beth_\omega$.

3. Somme infinite

Come abbiamo visto, le somme e i prodotti di cardinali si possono calcolare in modo semplicissimo, perché corrispondono al massimo dei due cardinali considerati. Più interessante è la nozione di somma infinita di cardinali, che vediamo in questa sezione, e quella di prodotto infinito di cardinali, che vedremo nella prossima.

Esattamente come per la somma di due cardinali, la somma infinita di cardinali è definita mediante unioni disgiunte.

DEFINIZIONE 3.1. Sia $(\kappa_i \mid i \in I)$ una sequenza infinita di cardinali. La *somma infinita* è definita ponendo:

$$\sum_{i \in I} \kappa_i = \left| \bigcup_{i \in I} A_i \right|$$

dove gli insiemi $|A_i| = \kappa_i$ sono a due a due disgiunti.

ESERCIZIO 3.2. Verificare che la definizione di sopra è ben posta, cioè che per ogni sequenza infinita $(\kappa_i \mid i \in I)$ di cardinali, si ha:

- Esiste una sequenza di insiemi $(A_i \mid i \in I)$ tali che $|A_i| = \kappa_i$ e $A_i \cap A_j \neq \emptyset$ per $i \neq j$.
- Se $(A_i \mid i \in I)$ e $(B_i \mid i \in I)$ sono due sequenze di insiemi tali che $|A_i| = |B_i|$ e $A_i \cap A_j = B_i \cap B_j = \emptyset$ per $i \neq j$, allora $|\bigcup_{i \in I} A_i| = |\bigcup_{i \in I} B_i|$.

ESEMPIO 3.3. $\sum_{n < \omega} \aleph_n = \aleph_\omega$. Infatti banalmente $\aleph_m < \sum_{n < \omega} \aleph_n$ per ogni $m < \omega$, e quindi $\aleph_\omega = \sup_{m < \omega} \aleph_m \leq \sum_{n \in \omega} \aleph_n$. Per l'altra disuguaglianza, osserviamo che

$$\sum_{n \in \omega} \aleph_n = \left| \bigcup_{n \in \omega} (\aleph_n \times \{n\}) \right| \leq |\aleph_\omega \times \omega| = \aleph_\omega \cdot \aleph_0 = \aleph_\omega.$$

Le seguenti proprietà fondamentali delle somme infinite di cardinali seguono direttamente dalle definizioni, e la loro dimostrazione è lasciata per esercizio.

ESERCIZIO 3.4. Nel caso di somme infinite dove tutti gli addendi sono uguali:

$$\sum_{i \in I} \kappa = \kappa \cdot |I|.$$

In particolare, $\sum_{i \in I} 1 = |I|$.

Anche le somme infinite sono coerenti rispetto alle disuguaglianze deboli.

ESERCIZIO 3.5. Siano $(\kappa_i \mid i \in I)$ e $(\mu_i \mid i \in I)$ due sequenze infinite di cardinali dove $\kappa_i \leq \mu_i$ per ogni $i \in I$. Allora $\sum_{i \in I} \kappa_i \leq \sum_{i \in I} \mu_i$.

Abbiamo già visto che unioni numerabili di insiemi al più numerabili è numerabile. Abbiamo anche visto che un'analogia proprietà vale relativamente alla cardinalità del continuo.

ESERCIZIO 3.6. Sia $\{A_i \mid i \in I\}$ una famiglia di insiemi (non necessariamente a due a due disgiunti). Sia κ un cardinale infinito e supponiamo che $|A_i| \leq \kappa$ per ogni $i \in I$ e $|I| \leq \kappa$. Allora $|\bigcup_{i \in I} A_i| \leq \kappa$.

ESERCIZIO 3.7. Sia $(I, <)$ un insieme ordinato infinito e sia $(A_i \mid i \in I)$ una sequenza di insiemi (non necessariamente a due a due disgiunti). Allora:

$$\left| \bigcup_{i \in I} A_i \right| \leq \sum_{i \in I} |A_i|.$$

Il risultato seguente ci fornisce una semplice formula per il calcolo delle somme infinite di cardinali.

TEOREMA 3.8. Sia $(\kappa_i \mid i \in I)$ una sequenza infinita di cardinali diversi da 0. Allora

$$\sum_{i \in I} \kappa_i = \max \left\{ \sup_{i \in I} \kappa_i, |I| \right\}.$$

DIM. Per comodità, denotiamo con $\kappa := \sup_{i \in I} \kappa_i$. Per ogni $j \in I$ si ha che $\sum_{i \in I} \kappa_i \geq \kappa_j$, e quindi $\sum_{i \in I} \kappa_i \geq \kappa$. Inoltre, $\sum_{i \in I} \kappa_i \geq \sum_{i \in I} 1 = |I|$. Concludiamo allora che $\sum_{i \in I} \kappa_i \geq \max\{\kappa, |I|\}$. Per l'altra disuguaglianza, basta osservare che $\sum_{i \in I} \kappa_i \leq \sum_{i \in I} \kappa = \kappa \cdot |I| = \max\{\kappa, |I|\}$. $\square$

ESERCIZIO 3.9. Sia $(I, <)$ un insieme ordinato infinito e sia $(A_i \mid i \in I)$ una sequenza di insiemi. Se $A_i \supsetneq \bigcup_{j < i} A_j$ per ogni $i \in I$ allora $|\bigcup_{i \in I} A_i| = \sum_{i \in I} |A_i|$.

ESERCIZIO 3.10. Sia $(I, <)$ un insieme ordinato senza massimo e sia $(A_i \mid i \in I)$ una sequenza di insiemi.

- (1) Se $(I, <)$ è bene ordinato e la sequenza è crescente, cioè $A_i \subsetneq A_j$ per tutti gli $i < j$, allora $|\bigcup_{i \in I} A_i| = \sum_{i \in I} |A_i|$.
- (2) Vale la proprietà (1) senza l'ipotesi di $(I, <)$ bene ordinato?

Concludiamo questa sezione con un significativo esempio di applicazione degli ordinali e del calcolo delle cardinalità di unioni infinite. Mostreremo che la cardinalità dei sottoinsiemi Boreliani di $\mathbb{R}$ (o più in generale di $\mathbb{R}^n$) ha la cardinalità $\mathfrak{c}$ del continuo. Di conseguenza, non solo esistono insiemi che non sono Boreliani, ma la famiglia degli insiemi non Boreliani ha la stessa cardinalità $2^{\mathfrak{c}}$ della famiglia di tutti i sottoinsiemi di $\mathbb{R}$.

DEFINIZIONE 3.11. La famiglia dei *Boreliani* $\mathcal{B}(\mathbb{R})$ è la più piccola σ -algebra di sottoinsiemi di $\mathbb{R}$ che contiene tutti gli aperti.⁵

PROPOSIZIONE 3.12. *La famiglia dei Boreliani $\mathcal{B}(\mathbb{R})$ ha la cardinalità del continuo $\mathfrak{c}$.*

DIM. Per ricorsione transfinita, definiamo la seguente sequenza crescente di insiemi:

$$\begin{cases} \mathcal{B}_0 = \{X \subseteq \mathbb{R} \mid X \text{ è aperto}\} \\ \mathcal{B}_{\alpha+1} = \mathcal{B}_\alpha \cup \{X^c \mid X \in \mathcal{B}_\alpha\} \cup \{\bigcup_{n < \omega} X_n \mid X_n \in \mathcal{B}_\alpha\} \cup \{\bigcap_{n < \omega} X_n \mid X_n \in \mathcal{B}_\alpha\} \\ \mathcal{B}_\lambda = \bigcup_{\alpha < \lambda} \mathcal{B}_\alpha \text{ se } \lambda \text{ è limite.} \end{cases}$$

Poniamo poi $\tilde{\mathcal{B}} = \bigcup_{\alpha < \omega_1} \mathcal{B}_\alpha$. Visto che $\mathcal{B}(\mathbb{R})$ contiene tutti gli aperti, ed è una σ -algebra, è immediato verificare per induzione transfinita che $\mathcal{B}_\alpha \subseteq \mathcal{B}(\mathbb{R})$ per ogni $\alpha < \omega_1$; dunque $\tilde{\mathcal{B}} \subseteq \mathcal{B}(\mathbb{R})$. Osserviamo inoltre che $\tilde{\mathcal{B}}$ stessa è una σ -algebra che contiene tutti gli aperti e quindi, per minimalità, deve essere $\tilde{\mathcal{B}} = \mathcal{B}(\mathbb{R})$. Verifichiamo in dettaglio questa proprietà.

Se $A \in \tilde{\mathcal{B}} = \bigcup_{\alpha < \omega_1} \mathcal{B}_\alpha$, allora esiste $\alpha < \omega_1$ con $A \in \mathcal{B}_\alpha$, e quindi il complementare $A^c \in \mathcal{B}_{\alpha+1} \subseteq \bigcup_{\alpha < \omega_1} \mathcal{B}_\alpha$. Inoltre, se $\{A_n \mid n \in \mathbb{N}\} \subseteq \bigcup_{\alpha < \omega_1} \mathcal{B}_\alpha$ è una famiglia numerabile, per ogni $n \in \mathbb{N}$ definisco $\gamma_n = \min\{\alpha \mid A_n \in \mathcal{B}_\alpha\}$, e considero $\gamma = \sup_n \gamma_n = \bigcup_n \gamma_n$. Osserviamo che γ è numerabile, visto che è unione numerabile di ordinali numerabili, e quindi $\gamma \in \omega_1$. Dunque $\{A_n \mid n \in \mathbb{N}\} \subseteq \mathcal{B}_\gamma$, e perciò $\bigcup_n A_n, \bigcap_n A_n \in \mathcal{B}_{\gamma+1} \subseteq \tilde{\mathcal{B}}$, come volevamo.

Adesso procediamo per induzione transfinita, e dimostriamo che $|\mathcal{B}_\alpha| = \mathfrak{c}$ per ogni $\alpha < \omega_1$. Abbiamo già visto che la famiglia $\mathcal{B}_0$ di tutti gli aperti di $\mathbb{R}$ ha la cardinalità del continuo $\mathfrak{c}$ (vedi Esercizio ??), e quindi vale la base di induzione. Al passo successore $\alpha + 1$, consideriamo le funzioni:

$$\psi : \mathcal{B}_\alpha \times \{0, 1\} \rightarrow \mathcal{B}_{\alpha+1} \quad \text{e} \quad \theta : \text{Fun}(\mathbb{N}, \mathcal{B}_\alpha) \times \{0, 1\} \rightarrow \mathcal{B}_{\alpha+1},$$

dove $\psi(A, 0) = A$, $\psi(A, 1) = A^c$, $\theta(\sigma, 0) = \bigcup_n \sigma(n)$ e $\theta(\sigma, 1) = \bigcap_n \sigma(n)$. Osserviamo che l'immagine di ψ consiste di tutti gli elementi di $\mathcal{B}_\alpha$ e dei loro complementi, e l'immagine di θ consiste di tutte le unioni e intersezioni numerabili di elementi di $\mathcal{B}_\alpha$. Ma allora, usando l'ipotesi induttiva $|\mathcal{B}_\alpha| = \mathfrak{c}$, si ha:

$$|\mathcal{B}_{\alpha+1}| = |\text{imm}(\psi) \cup \text{imm}(\theta)| \leq |\mathcal{B}_\alpha \times \{0, 1\}| + |\text{Fun}(\mathbb{N}, \mathcal{B}_\alpha) \times \{0, 1\}| = \mathfrak{c} + \mathfrak{c}^{\aleph_0} = \mathfrak{c}.$$

Il caso limite $\lambda < \omega_1$ segue facilmente notando che:

$$\mathfrak{c} = |\mathcal{B}_0| \leq |\mathcal{B}_\lambda| \leq \sum_{\alpha < \lambda} |\mathcal{B}_\alpha| = \max\{|\lambda|, \sup_{\alpha < \lambda} |\mathcal{B}_\alpha|\} = \max\{\aleph_0, \mathfrak{c}\} = \mathfrak{c}.$$

Possiamo infine concludere che:

$$\mathfrak{c} = |\mathcal{B}_0| \leq |\tilde{\mathcal{B}}| \leq \sum_{\alpha < \omega_1} |\mathcal{B}_\alpha| = \max\{|\omega_1|, \sup_{\alpha < \omega_1} |\mathcal{B}_\alpha|\} = \max\{\aleph_1, \mathfrak{c}\} = \mathfrak{c}.$$

□

⁵ Ricordiamo che una σ -algebra è una famiglia di insiemi chiusa per complementi, e chiusa per intersezioni e unioni numerabili.

4. Prodotti infiniti

Analogamente al prodotto di due cardinali, il prodotto infinito di cardinali è definito mediante prodotti cartesiani. Osserviamo che è necessario l'assioma di scelta per rendere non banale la seguente definizione, visto che altrimenti potremmo avere sequenze di insiemi non vuoti il cui prodotto cartesiano infinito è vuoto.

DEFINIZIONE 4.1. Sia $(\kappa_i \mid i \in I)$ una sequenza infinita di cardinali diversi da 0. Il *prodotto infinito* è definita ponendo:

$$\prod_{i \in I} \kappa_i = \left| \prod_{i \in I} A_i \right|$$

dove gli insiemi $|A_i| = \kappa_i$.

ESERCIZIO 4.2. Verificare che la definizione di sopra è ben posta, cioè che per ogni sequenza infinita $(\kappa_i \mid i \in I)$ di cardinali, si ha:

- Se $(A_i \mid i \in I)$ e $(B_i \mid i \in I)$ sono due sequenze di insiemi tali che $|A_i| = |B_i|$ per ogni $i \in I$, allora $|\prod_{i \in I} A_i| = |\prod_{i \in I} B_i|$.

Le seguenti proprietà fondamentali delle somme infinite di cardinali seguono direttamente dalle definizioni, e la loro dimostrazione è lasciata per esercizio.

ESERCIZIO 4.3. Nel caso di prodotti infiniti dove tutti i fattori sono uguali:

$$\prod_{i \in I} \kappa = \kappa^{|I|}.$$

I prodotti infiniti sono coerenti rispetto alle disuguaglianze deboli.

ESERCIZIO 4.4. Siano $(\kappa_i \mid i \in I)$ e $(\mu_i \mid i \in I)$ due sequenze infinite di cardinali dove $0 < \kappa_i \leq \mu_i$ per ogni $i \in I$. Allora $\prod_{i \in I} \kappa_i \leq \prod_{i \in I} \mu_i$.

ESERCIZIO 4.5. Vale la seguente proprietà commutativa generalizzata. Per ogni sequenza infinita $(\kappa_i \mid i \in I)$ di cardinali diversi da 0 e per ogni permutazione $\sigma : I \rightarrow I$, si ha:

$$\prod_{i \in I} \kappa_i = \prod_{i \in I} \kappa_{\sigma(i)}.$$

ESERCIZIO 4.6. Vale la seguente proprietà associativa generalizzata. Per ogni sequenza infinita $(\kappa_i \mid i \in I)$ di cardinali diversi da 0 e per ogni partizione $I = \bigcup_{s \in S} I_s$ si ha:⁶

$$\prod_{i \in I} \kappa_i = \prod_{s \in S} \left(\prod_{i \in I_s} \kappa_i \right).$$

Un primo semplice esempio di prodotto infinito si ottiene considerando la sequenza dei cardinali finiti diversi da 0.

ESEMPIO 4.7. $\prod_{0 < n < \omega} n = \mathfrak{c}$. Infatti $\prod_{0 < n < \omega} n = \prod_{2 \leq n < \omega} n \geq \prod_{2 \leq n < \omega} 2 = 2^{\aleph_0} = \mathfrak{c}$; inoltre $\prod_{0 < n < \omega} n \leq \prod_{0 < n < \omega} \aleph_0 = (\aleph_0)^{\aleph_0} = \mathfrak{c}$.

Un esempio più interessante è il seguente.

⁶ Ricordiamo che $I = \bigcup_{s \in S} I_s$ è una partizione se i pezzi I_s sono a due a due disgiunti.

ESEMPIO 4.8. $\prod_{n < \omega} \aleph_n = (\aleph_\omega)^{\aleph_0}$.⁷ Poiché ogni $\aleph_n < \aleph_\omega$ per ogni n , si ha subito la disuguaglianza: $\prod_{n < \omega} \aleph_n \leq \prod_{n < \omega} \aleph_\omega = (\aleph_\omega)^{\aleph_0}$. L'altra disuguaglianza non è immediata. Per ottenerla, partizioniamo $\omega = \bigcup_{k < \omega} I_k$ in infiniti pezzi infiniti; ad esempio se $\{p_1 < \dots < p_k < \dots\}$ è l'insieme dei numeri primi, per $k \geq 1$ si può prendere come I_k l'insieme delle potenze del k -esimo primo p_k , e come I_0 il complementare di $\bigcup_{1 \leq k < \omega} I_k$. Osserviamo che per ogni $k \in \omega$, il prodotto infinito $\prod_{n \in I_k} \aleph_n$ è maggiore o uguale di ciascuno dei suoi fattori, e quindi $\prod_{n \in I_k} \aleph_n \geq \sup_{n \in I_k} \aleph_n$; osserviamo inoltre che $\sup_{n \in I_k} \aleph_n = \aleph_\omega$, visto che I_k è infinito e quindi è illimitato in ω . Infine, usando la proprietà associativa generalizzata, si ottiene che: $\prod_{n < \omega} \aleph_n = \prod_{k \in \omega} \left(\prod_{n \in I_k} \aleph_n \right) \geq \prod_{k \in \omega} \aleph_\omega = (\aleph_\omega)^{\aleph_0}$.

Generalizzando l'idea sviluppata nell'esempio precedente, siamo in grado di dimostrare una formula generale per il calcolo di prodotti infiniti di cardinali.

TEOREMA 4.9. *Sia ν un cardinale infinito, e sia $(\kappa_\alpha \mid \alpha \in \nu)$ una sequenza non-decrescente di cardinali $\kappa_\alpha \neq 0$. Allora*

$$\prod_{\alpha \in \nu} \kappa_\alpha = \left(\sup_{\alpha \in \nu} \kappa_\alpha \right)^\nu.$$

DIM. Denotiamo con $\kappa := \sup_{\alpha < \nu} \kappa_\alpha$. Banalmente per ogni $\alpha < \nu$ si ha $\kappa_\alpha \leq \kappa$, e quindi $\prod_{\alpha < \nu} \kappa_\alpha \leq \prod_{\alpha < \nu} \kappa = \kappa^\nu$.

Per vedere l'altra disuguaglianza, partizioniamo $\nu = \bigcup_{\beta < \nu} A_\beta$ in ν pezzi ognuno di cardinalità $|A_\beta| = \nu$. Per vedere che questo è possibile ricordiamo che, essendo ν è un cardinale infinito, si ha $\nu = \nu \cdot \nu$ e quindi c'è una bigezione $\varphi : \nu \times \nu \rightarrow \nu$. Se prendiamo $A_\beta := \{\varphi(\alpha, \beta) \mid \alpha \in \nu\}$, allora per l'iniettività di φ si ha $|A_\beta| = \nu$; inoltre $A_\beta \cap A_\gamma = \emptyset$ per $\beta \neq \gamma$; infine $\bigcup_{\alpha < \nu} A_\alpha = \text{imm}(\varphi) = \nu$ per la suriettività di φ .

Adesso osserviamo che da $|A_\alpha| = \nu$ segue che $A_\alpha \subset \nu$ è illimitato (vedi Esercizio ??). Di conseguenza, visto che la sequenza $(\kappa_\alpha \mid \alpha < \nu)$ è non-decrescente, si ha $\sup_{\alpha \in A_\beta} \kappa_\alpha = \sup_{\alpha < \nu} \kappa_\alpha = \kappa$. Osserviamo anche che per ogni $\gamma \in A_\beta$, banalmente $\prod_{\alpha \in A_\beta} \kappa_\alpha \geq \kappa_\gamma$, e quindi $\prod_{\alpha \in A_\beta} \kappa_\alpha \geq \sup_{\gamma \in A_\beta} \kappa_\gamma = \kappa$. Infine, usando la proprietà associativa generalizzata, si ottiene la disuguaglianza voluta:

$$\prod_{\alpha < \nu} \kappa_\alpha = \prod_{\beta < \nu} \left(\prod_{\alpha \in A_\beta} \kappa_\alpha \right) \geq \prod_{\beta < \nu} \kappa = \kappa^\nu.$$

□

NOTA BENE 4.10. Data una sequenza di cardinali $(\kappa_\alpha \mid \alpha < \nu)$ è sempre possibile riordinare gli elementi in modo da formare una sequenza non-decrescente. Si potrebbe pensare allora che, valendo la proprietà commutativa generalizzata per i prodotti infiniti, la richiesta di avere una successione non-decrescente possa sempre essere soddisfatta. Tuttavia non è così perché la sequenza “riordinata” potrebbe non essere più indicizzabile su un cardinale. Vediamo un semplice esempio per chiarire.

Sia $(\kappa_n \mid n \in \aleph_0)$ la sequenza dove $\kappa_{2n} = \aleph_n$ e $\kappa_{2n+1} = \aleph_{\omega+n}$ per ogni $n \in \omega$. Se riordiniamo la sequenza assegnata $\aleph_0, \aleph_\omega, \aleph_1, \aleph_{\omega+1}, \dots, \aleph_n, \aleph_{\omega+n}, \dots$ in modo

⁷ Vedremo più avanti che $(\aleph_\omega)^{\aleph_0} > \aleph_\omega$.

crescente, otteniamo:

$$\aleph_0 < \aleph_1 < \dots < \aleph_n < \dots < \aleph_\omega < \aleph_{\omega+1} < \dots < \aleph_{\omega+n} < \dots$$

Notiamo però che in questo caso avremmo $(\aleph_\alpha \mid \alpha < \omega + \omega)$, dove l'insieme degli indici non è un cardinale.

Come mostrano i seguenti due esercizi, entrambe le ipotesi nel Teorema di sopra sono necessarie.

ESERCIZIO 4.11. Trovare una sequenza di cardinali $(\kappa_\alpha \mid \alpha < \nu)$ indicizzata su un cardinale tale che $\prod_{\alpha < \nu} \kappa_\alpha < (\sup_{\alpha < \nu} \kappa_\alpha)^\nu$.

ESERCIZIO 4.12. Trovare una sequenza di cardinali $(\kappa_\alpha \mid \alpha < \beta)$ non-decrescente indicizzata su un ordinale β tale che $\prod_{\alpha < \beta} \kappa_\alpha < (\sup_{\alpha < \beta} \kappa_\alpha)^\nu$.

Vale la seguente disuguaglianza (debole) tra somme infinite e prodotti infiniti.

PROPOSIZIONE 4.13. Sia $(\kappa_i \mid i \in I)$ una sequenza infinita di cardinali $\kappa_i \geq 2$. Allora $\sum_{i \in I} \kappa_i \leq \prod_{i \in I} \kappa_i$.

DIM. Osserviamo che per ogni $j \in I$ si ha $\prod_{i \in I} \kappa_i \geq \kappa_j$. Infatti se prendiamo la sequenza $(\kappa'_i \mid i \in I)$ dove $\kappa'_j = \kappa_j$ e $\kappa'_i = 1$ per $j \neq i$, banalmente $\kappa'_i \leq \kappa_i$ per ogni $i \in I$, e allora $\prod_{i \in I} \kappa_i \geq \prod_{i \in I} \kappa'_i = \kappa_j$. Questo dimostra che $\prod_{i \in I} \kappa_i \geq \sup_{i \in I} \kappa_i$. Inoltre $\prod_{i \in I} \kappa_i \geq \prod_{i \in I} 2 = 2^{|I|} > |I|$. Possiamo così concludere che $\prod_{i \in I} \kappa_i \geq \max\{\sup_{i \in I} \kappa_i, |I|\} = \sum_{i \in I} \kappa_i$. $\square$

Concludiamo questa sezione con il Teorema di König, che è una forte generalizzazione del Teorema di Cantor: $\kappa < 2^\kappa$. Si tratta dell'unico risultato relativo a disuguaglianze strette tra cardinalità.

TEOREMA 4.14 (König). Siano $(\mu_i \mid i \in I)$ e $(\kappa_i \mid i \in I)$ due sequenze infinite di cardinali dove $\mu_i < \kappa_i$ per ogni $i \in I$. Allora vale la disuguaglianza stretta:

$$\sum_{i \in I} \mu_i < \prod_{i \in I} \kappa_i.$$

DIM. Prendiamo una famiglia $\{A_i \mid i \in I\}$ di insiemi a due a due disgiunti e tali che $|A_i| = \mu_i$ per ogni $i \in I$, in modo da avere $\sum_{i \in I} \mu_i = |\bigcup_{i \in I} A_i|$. Usando la Proposizione 4.13, otteniamo la disuguaglianza debole $\sum_{i \in I} \mu_i \leq \sum_{i \in I} \kappa_i \leq \prod_{i \in I} \kappa_i$, quindi basta vedere che non esistono funzioni suriettive $\varphi : \bigcup_{i \in I} A_i \rightarrow \prod_{i \in I} \kappa_i$. Per ogni $j \in I$ denotiamo con $\varphi_j = \varphi|_{A_j} : A_j \rightarrow \prod_{i \in I} \kappa_i$ la restrizione di φ all'insieme A_j ; e denotiamo con $\pi_j : \prod_{i \in I} \kappa_i \rightarrow \kappa_j$ la proiezione sulla j -esima componente.⁸ Per l'ipotesi $|A_j| = \mu_j < \kappa_j$, la funzione $\pi_j \circ \varphi_j : A_j \rightarrow \kappa_j$ non può essere suriettiva, e quindi possiamo prendere un elemento $\xi_j \in \kappa_j$ tale che $\xi_j \notin \text{imm}(\pi_j \circ \varphi_j)$. Osserviamo che $\vec{\xi} = (\xi_j \mid j \in I) \in \prod_{i \in I} \kappa_i$ non appartiene all'immagine di φ , e quindi φ non è suriettiva. Infatti se per assurdo esistesse $a \in \bigcup_{i \in I} A_i$ con $\varphi(a) = \vec{\xi}$, allora prendendo $j \in I$ l'indice tale che $a \in A_j$, avremmo che $(\pi_j \circ \varphi_j)(a) = \xi_j$, contro il fatto che $\xi_j \notin \text{imm}(\pi_j \circ \varphi_j)$. $\square$

Come caso particolare, ritroviamo il Teorema di Cantor.

COROLLARIO 4.15. Per ogni cardinale infinito κ si ha $2^\kappa > \kappa$.

⁸ Ricordiamo che, per definizione, $\prod_{i \in I} \kappa_i := \{(x_i \mid i \in I) \mid x_i \in \kappa_i \text{ per ogni } i \in I\}$. Quindi la proiezione j -esima è la funzione $\pi_j(x_i \mid i \in I) = x_j$.

DIM. Consideriamo le due sequenze infinite $(1 \mid i \in \kappa)$ e $(2 \mid i \in \kappa)$. Per il teorema di König si ha che $\kappa = \sum_{i \in I} 1 < \prod_{i \in \kappa} 2 = 2^\kappa$. $\square$

5. Cofinalità, cardinali regolari e cardinali singolari

Un concetto cruciale nello studio dell'algebra cardinale è quello di cofinalità che, intuitivamente, misura quando “lungo” è un cardinale per lo studio delle cardinalità

DEFINIZIONE 5.1. Chiamiamo *cofinalità* di un insieme ordinato $(A, <)$ la più piccola cardinalità di un suo sottoinsieme illimitato:

$$\text{cof}(A) = \min\{|X| \mid X \subseteq A \text{ illimitato}\}.$$

Possiamo pensare alla cardinalità di un insieme come una sorta di misura della sua “grandezza”. Analogamente, possiamo pensare alla cofinalità di un insieme ordinato come ad una misura della sua “lunghezza”.

Banalmente, $\text{cof}(A) \leq |A|$, ma ci sono casi in cui vale la disuguaglianza stretta. Osserviamo inoltre che se $(A, <)$ ha massimo, allora $\text{cof}(A) = 1$; e se A non ha massimo allora $\text{cof}(A) \geq \aleph_0$.

ESEMPIO 5.2. Come sappiamo l'insieme $\mathbb{R}$ dei numeri reali ha cardinalità più che numerabile. Tuttavia la cofinalità $\text{cof}(\mathbb{R}) = \aleph_0$ è numerabile, perché $\mathbb{R}$ non ha massimo, e $\mathbb{N} \subset \mathbb{R}$ è un sottoinsieme illimitato.

ESEMPIO 5.3. Se un insieme $A \subseteq \omega_1$ è numerabile, allora $\sup A = \bigcup_{\alpha \in A} \alpha$ è un ordinale numerabile, in quanto è unione numerabile di insiemi al più numerabili.⁹ Quindi $\sup A < \omega_1$, cioè A è limitato. Concludiamo allora che $\text{cof}(\omega_1) = \aleph_1$.

ESEMPIO 5.4. Per ogni ordinale α , la cofinalità $\text{cof}(\alpha + \omega) = \aleph_0$. Infatti $\alpha + \omega$ non ha massimo, e l'insieme numerabile $A = \{\alpha + n \mid n \in \omega\}$ è illimitato in $\alpha + \omega$.

ESERCIZIO 5.5. Per ogni insieme ordinato A , si ha $\text{cof}(\text{cof}(A)) = \text{cof}(A)$.

ESERCIZIO 5.6. Per ogni ordinale $\alpha > 1$ e per ogni ordinale limite λ , si ha:

$$\text{cof}(\alpha + \lambda) = \text{cof}(\alpha \cdot \lambda) = \text{cof}(\alpha^\lambda) = \text{cof}(\lambda).$$

Il prossimo risultato ci mostra che nella definizione di cofinalità, potevamo equivalentemente considerare funzioni illimitate o funzioni illimitate crescenti definite su ordinali.

PROPOSIZIONE 5.7.

- (1) $\text{cof}(A) = \min\{\alpha \text{ ordinale} \mid \exists f : \alpha \rightarrow A \text{ funzione illimitata}\}.$
- (2) $\text{cof}(A) = \min\{\alpha \text{ ordinale} \mid \exists f : \alpha \rightarrow A \text{ funzione illimitata crescente}\}.$

DIM. Denotiamo con

- $\text{cof}_1(A) = \min\{\alpha \text{ ordinale} \mid \exists f : \alpha \rightarrow A \text{ funzione illimitata}\};$
- $\text{cof}_2(A) = \min\{\alpha \text{ ordinale} \mid \exists f : \alpha \rightarrow A \text{ funzione illimitata crescente}\}.$

⁹ Ricordiamo che per definizione della funzione di Hartogs, gli ordinali in $\omega_1 = \mathbb{H}(\omega)$ sono al più numerabili.

Se $f : \alpha \rightarrow A$ è una funzione illimitata, allora $X = \text{imm}(f)$ è un sottoinsieme illimitato di A avente cardinalità $|X| \leq |\alpha| \leq \alpha$, e dunque $\text{cof}(A) \leq \text{cof}_1(A)$. La disuguaglianza $\text{cof}_1(A) \leq \text{cof}_2(A)$ vale banalmente perché le funzioni illimitate crescenti sono un sottoinsieme delle funzioni illimitate. Resta da vedere che $\text{cof}_2(A) \leq \text{cof}(A)$.

Intanto possiamo supporre che A non abbia massimo, altrimenti la tesi è banale. Sia $\kappa = \text{cof}(A)$, e sia $X \subseteq A$ un insieme illimitato di cardinalità κ . Possiamo allora enumerare $X = \{x_\alpha \mid \alpha < \kappa\}$. Per ricorsione transfinita, definiamo una funzione $f : \kappa \rightarrow A$ in questo modo. Alla base induttiva poniamo $f(0) = \sigma(0)$. Per $\beta > 0$, osserviamo che l'insieme $Y_\beta = \{f(\delta) \mid \delta < \beta\} \cup \{x_\beta\}$ è limitato in A . Infatti $|Y_\beta| \leq |\beta| + 1 < \kappa$, e κ è la minima cardinalità di un insieme illimitato. Esistono allora elementi di X più grandi di ogni elemento di Y_β , e quindi possiamo definire $f(\beta) = x_\gamma$ dove γ è il minimo ordinale tale $x_\gamma > Y_\beta$ (cioè $x_\gamma > y$ per ogni $y \in Y_\beta$). Segue direttamente dalla definizione che f è strettamente crescente. Inoltre f è illimitata perché $f(\beta) \geq x_\beta$ per ogni β . Concludiamo che $\text{cof}_2(A) \leq \kappa = \text{cof}(A)$, e la tesi è raggiunta. $\square$

DEFINIZIONE 5.8. Un cardinale κ si dice *regolare* se $\text{cof}(\kappa) = \kappa$, cioè se non ha sottoinsiemi illimitati aventi cardinalità più piccola. Un cardinale si dice *singolare* se non è regolare.

Chiaramente ogni cardinale finito n è regolare. Notiamo che anche $\aleph_0$ è un cardinale regolare.

ESEMPIO 5.9. $\aleph_1$ è un cardinale regolare. Infatti, come abbiamo osservato nell'Esempio 5.4, si ha che $\text{cof}(\omega_1) = \aleph_1$.

ESEMPIO 5.10. $\aleph_\omega$ è un cardinale singolare perché $\text{cof}(\aleph_\omega) = \aleph_0 < \aleph_\omega$. Infatti, l'insieme numerabile $A = \{\aleph_n \mid n \in \omega\}$ è illimitato in $\aleph_\omega$.

ESERCIZIO 5.11. Sia κ un cardinale regolare, e sia $(\xi_\alpha \mid \alpha \in \kappa)$ una sequenza crescente di ordinali. Se $\xi = \sup_{\alpha \in \kappa} \xi_\alpha$ allora $\text{cof}(\xi) = \kappa$.

L'esempio di $\aleph_1$ cardinale regolare si generalizza a tutti i cardinali successivi.

PROPOSIZIONE 5.12. *Ogni cardinale successore è regolare.*

DIM. Sia $A \subseteq \aleph_{\alpha+1}$ un sottoinsieme illimitato. Questo significa che $\aleph_{\alpha+1} = \sup A = \bigcup_{\beta \in A} \beta$. Notiamo che ogni elemento $\beta \in A$ appartiene al cardinale $\aleph_{\alpha+1} = \mathbb{H}(\aleph_\alpha)$, dunque la sua cardinalità $|\beta| \leq \aleph_\alpha$. Abbiamo:

$$\aleph_{\alpha+1} = \left| \bigcup_{\beta \in A} \beta \right| \leq \sum_{\beta \in A} |\beta| = \max \left\{ \sup_{\beta \in A} |\beta|; |A| \right\} = \max\{\aleph_\alpha; |A|\}.$$

Ma allora deve necessariamente essere $|A| = \aleph_{\alpha+1}$, cioè la tesi. $\square$

Sorge spontaneo chiedersi se valga anche l'implicazione inversa, cioè se ogni cardinale regolare $> \aleph_0$ sia necessariamente un successore. La risposta è tutt'altro che semplice. Da un lato è consistente con ZFC che non esistano cardinali limite regolari; dall'altro l'esistenza di tali cardinali non solo non è dimostrabile con gli assiomi di ZFC, ma non è neppure possibile dimostrare che è consistente (a meno che ZFC sia contraddittorio!). Torneremo più avanti su questo tipo di considerazioni.

Riguardo i cardinali limite, vale la seguente proprietà:

PROPOSIZIONE 5.13. *Se λ è un ordinale limite, allora $\text{cof}(\aleph_\lambda) = \text{cof}(\lambda)$ e $\text{cof}(\beth_\lambda) = \text{cof}(\lambda)$.*

DIM. Visto che λ è un ordinale limite, $\aleph_\lambda = \bigcup_{\gamma < \lambda} \aleph_\gamma$. Sia ora $X \subseteq \lambda$ un sottoinsieme illimitato dove $|X| = \text{cof}(\lambda)$. Notiamo che l'insieme $Y := \{\aleph_\xi \mid \xi \in X\}$ è illimitato in $\aleph_\lambda$, e quindi $\text{cof}(\aleph_\lambda) \leq |Y| = |X| = \text{cof}(\lambda)$. Infatti, se $\beta \in \aleph_\lambda$ allora esiste $\gamma < \lambda$ tale che $\beta \in \aleph_\gamma$; visto che X è illimitato possiamo prendere $\xi \in X$ con $\xi \geq \gamma$, e quindi $\aleph_\xi \in Y$ è tale che $\aleph_\xi \geq \aleph_\gamma > \beta$.

Viceversa, sia $Y \subseteq \aleph_\lambda$ è un sottoinsieme illimitato dove $|Y| = \text{cof}(\aleph_\lambda)$, e consideriamo l'insieme $X := \{\xi_y \mid y \in Y\}$ dove $\xi_y := \min\{\beta \in \lambda \mid \aleph_\beta > y\}$. Notiamo che X è illimitato in λ . Infatti se $\gamma < \lambda$, prendo $y \in Y$ tale che $\aleph_\gamma < y$, e allora da $\aleph_{\xi_y} > y$ segue che $\xi_y > \gamma$. Abbiamo allora:

$$\text{cof}(\aleph_\lambda) = |Y| \geq |X| \geq \text{cof}(\lambda).$$

La dimostrazione per la la sequenza dei beth è del tutto simile. $\square$

Un'altra utile caratterizzazione della cofinalità è la seguente:

ESERCIZIO 5.14. Per ogni cardinale infinito ν regolare, esiste un punto fisso $\kappa = \aleph_\kappa$ di cofinalità ν . La stessa proprietà vale per la sequenza dei beth.

PROPOSIZIONE 5.15. *Sia κ un cardinale. Allora $\text{cof}(\kappa)$ è il più piccolo cardinale ν tale che esiste una sequenza $(\kappa_i \mid i \in \nu)$ di cardinali $\kappa_i < \kappa$ con $\sum_{i \in \nu} \kappa_i = \kappa$.*

DIM. Sia $\nu = \text{cof}(\kappa)$, e sia $f : \nu \rightarrow \kappa$ una funzione illimitata. Consideriamo la sequenza di cardinali $(\kappa_i \mid i \in \nu)$ dove $\kappa_i = |f(i)| < \kappa$. Se κ è singolare, allora κ è limite, e in questo caso

$$\sup_{i \in \nu} \kappa_i = \sup_{i \in \nu} |f(i)| = \sup\{\mu \text{ cardinale} \mid \mu < \kappa\} = \kappa.$$

Se invece κ è regolare, allora $\nu = \kappa$. In entrambi i casi, si ha che

$$\sum_{i \in \nu} \kappa_i = \max \left\{ \sup_{i \in \nu} \kappa_i, \nu \right\} = \max \left\{ \sup_{i \in \nu} |f(i)|, \nu \right\} = \kappa.$$

Infine, notiamo che $\text{cof}(\kappa)$ è il più piccolo cardinale con quella proprietà. Infatti, supponiamo per assurdo che esista una sequenza di cardinali $(\kappa_i \mid i \in \mu)$ tale che $\kappa = \sum_{i \in \mu} \kappa_i = \max\{\sup_{i \in \mu} \kappa_i, \mu\}$, dove $\mu < \text{cof}(\kappa)$ e dove $\kappa_i < \kappa$. Allora dovremmo avere $\sup_{i \in \mu} \kappa_i = \kappa$; quindi $\{\kappa_i \mid i \in \mu\}$ sarebbe illimitato in κ , e allora $\mu \geq \text{cof}(\kappa)$, una contraddizione. $\square$

ESERCIZIO 5.16. Se κ è un cardinale limite e $\text{cof}(\kappa) = \nu$, allora esiste una successione crescente di cardinali $(\kappa_i \mid i \in \nu)$ dove ogni $\kappa_i < \kappa$ è un successore e dove $\kappa = \sup_{i \in \nu} \kappa_i$. In particolare, $\kappa = \sum_{i \in \nu} \kappa_i$.

ESERCIZIO 5.17. Se κ è un limite forte, allora $\kappa^{\text{cof}(\kappa)} = 2^\kappa$.

6. Cofinalità ed esponenziazioni

In questa sezione vedremo come usando la nozione di cofinalità, sia possibile stabilire alcune importanti proprietà relative alle esponenziazioni di cardinali.

Cominciamo con due utili risultati relativi alla cofinalità delle esponenziazioni. Si tratta di due disuguaglianze strette, che seguono dal teorema di König.

TEOREMA 6.1. *Per ogni cardinale infinito κ si ha:*

- (1) $\kappa^{\text{cof}(\kappa)} > \kappa$.
- (2) $\text{cof}(\mu^\kappa) > \kappa$ per ogni $\mu \geq 2$.

DIM. (1). Siano $\kappa_i < \kappa$ cardinali tali che $\kappa = \sum_{i \in \text{cof}(\kappa)} \kappa_i$. Allora applicando la disuguaglianza di König si ottiene:

$$\kappa = \sum_{i \in \text{cof}(\kappa)} \kappa_i < \prod_{i \in \text{cof}(\kappa)} \kappa = \kappa^{\text{cof}(\kappa)}.$$

(2). Supponiamo per assurdo che $\nu := \text{cof}(\mu^\kappa) \leq \kappa$. Visto che $\mu \geq 2$, il cardinale μ^κ è infinito e possiamo applicare il punto precedente, ottenendo una contraddizione:

$$\mu^\kappa < (\mu^\kappa)^\nu \leq (\mu^\kappa)^\kappa = \mu^{\kappa \cdot \kappa} = \mu^\kappa.$$

□

Gli assiomi di ZFC non permettono di stabilire il valore del continuo. Tuttavia è possibile dare la seguente restrizione, che in realtà è l'unica possibile.¹⁰

COROLLARIO 6.2. *Per ogni ordinale limite λ di cofinalità numerabile si ha $\mathfrak{c} \neq \aleph_\lambda$. In particolare $\mathfrak{c} \neq \aleph_\omega$.*

DIM. Notiamo che $\text{cof}(\mathfrak{c}) = \text{cof}(2^{\aleph_0}) > \aleph_0$, mentre $\text{cof}(\aleph_\lambda) = \text{cof}(\lambda) = \aleph_0$. □

Ragionare in termini di cofinalità è cruciale per la dimostrazione del seguente classico risultato, in base al quale è possibile ricondurre le esponenziazioni con base un cardinale successore ad esponenziazioni con base un cardinale limite.¹¹

TEOREMA 6.3 (Hausdorff). *Siano κ e ν cardinali infiniti. Allora $(\kappa^+)^nu = \max\{\kappa^\nu, \kappa^+\}$.*

DIM. Se $\kappa^+ \leq \nu$, cioè quando la base è “piccola” rispetto all’esponente, allora per quanto già visto nella Proposizione 1.16, si ha $\kappa^\nu = (\kappa^+)^nu = 2^\nu > \nu \geq \kappa^+$, da cui la tesi $(\kappa^+)^nu = \max\{\kappa^\nu, \kappa^+\} = 2^\nu$.

Supponiamo ora $\nu < \kappa^+$. Visto che κ^+ è regolare in quanto cardinale successore, ogni funzione $f : \nu \rightarrow \kappa^+$ ha immagine limitata, e dunque esiste un ordinale $\gamma < \kappa^+$ tale che $\text{imm}(f) \subseteq \gamma$; in altre parole, $f \in \text{Fun}(\nu, \gamma)$ per un opportuno $\gamma < \kappa^+$. Abbiamo quindi:

$$\text{Fun}(\nu, \kappa^+) = \bigcup_{\gamma < \kappa^+} \text{Fun}(\nu, \gamma).$$

Ricordiamo che se $\gamma < \kappa^+$, allora $|\gamma| \leq \kappa$ e quindi $|\text{Fun}(\nu, \gamma)| = |\gamma|^\nu \leq \kappa^\nu$. Valgono le disuguaglianze:

$$\begin{aligned} (\kappa^+)^nu &= |\text{Fun}(\nu, \kappa^+)| = \left| \bigcup_{\gamma < \kappa^+} \text{Fun}(\nu, \gamma) \right| \leq \\ &\leq \sum_{\gamma < \kappa^+} |\text{Fun}(\nu, \gamma)| \leq \sum_{\gamma < \kappa^+} \kappa^\nu = \max\{\kappa^\nu, \kappa^+\}. \end{aligned}$$

L'altra disuguaglianza $\max\{\kappa^\nu, \kappa^+\} \leq (\kappa^+)^nu$ è immediata. □

¹⁰ Per ogni cardinale κ con $\text{cof}(\kappa) > \aleph_0$, è consistente avere $\mathfrak{c} = \kappa$ (cioè esistono modelli di ZFC dove $\mathfrak{c} = \kappa$).

¹¹ Ricordiamo che se $\kappa = \aleph_\alpha$ è un cardinale infinito, si denota con $\kappa^+ = \aleph_{\alpha+1}$ il suo successore.

Ricordiamo che ogni ordinale $\alpha > 0$ si può scrivere nella forma $\alpha = \lambda + n$ dove n è un naturale positivo, e dove $\lambda = 0$ oppure λ è un ordinale limite.¹² Iterando un numero finito di volte il Teorema di Hausdorff, si ottiene la seguente formula che si applica a tutti cardinali successivi:

COROLLARIO 6.4. *Per ogni ordinale λ e per ogni naturale $n \in \omega$ si ha $(\aleph_{\lambda+n})^{\aleph_\beta} = \max\{(\aleph_\lambda)^{\aleph_\beta}, \aleph_{\lambda+n}\}$.*

DIM. Per induzione su $n \in \omega$. Quando $n = 0$ la tesi è banale. Nel caso successore $n + 1$ basta applicare prima il Teorema di Hausdorff e poi l'ipotesi induttiva:

$$\begin{aligned} (\aleph_{\lambda+n+1})^{\aleph_\beta} &= \max\{(\aleph_{\lambda+n})^{\aleph_\beta}, \aleph_{\lambda+n+1}\} = \\ &= \max\{\max\{(\aleph_\lambda)^{\aleph_\beta}, \aleph_{\lambda+n}\}, \aleph_{\lambda+n+1}\} = \max\{(\aleph_\lambda)^{\aleph_\beta}, \aleph_{\lambda+n+1}\}. \end{aligned}$$

□

Ad esempio:

- $(\aleph_{17})^{\aleph_{11}} = \max\{(\aleph_0)^{\aleph_{11}}, \aleph_{17}\} = \max\{2^{\aleph_{11}}, \aleph_{17}\}.$
- $(\aleph_{\omega+13})^{\aleph_\omega} = \max\{(\aleph_\omega)^{\aleph_\omega}, \aleph_{\omega+13}\} = \max\{2^{\aleph_\omega}, \aleph_{\omega+13}\}.$

Occupiamoci ora di esponenziazioni con esponente un cardinale limite.

NOTAZIONE 6.5. Se ν è un cardinale infinito, per ogni $\kappa \geq 2$ è consuetudine denotare

$$\kappa^{<\nu} := \sup\{\kappa^\xi \mid \xi < \nu\}.$$

TEOREMA 6.6. *Sia ν un cardinale limite e sia $\kappa \geq 2$. Allora*

$$\kappa^\nu = (\kappa^{<\nu})^{\text{cof}(\nu)}.$$

DIM. Scriviamo $\nu = \sum_{i \in \text{cof}(\nu)} \nu_i$ dove $(\nu_i \mid i \in \text{cof}(\nu))$ è una sequenza crescente di cardinali $\nu_i < \nu$. Usando la formula per i prodotti infiniti, si ottengono le uguaglianze:

$$\kappa^\nu = \kappa^{\sum_{i \in \text{cof}(\nu)} \nu_i} = \prod_{i \in \text{cof}(\nu)} \kappa^{\nu_i} = \left(\sup_{i \in \text{cof}(\nu)} \kappa^{\nu_i} \right)^{\text{cof}(\nu)} = (\kappa^\nu)^{\text{cof}(\nu)}.$$

□

ESEMPIO 6.7. Se $2^{\aleph_n} < \aleph_\omega$ per ogni $n \in \omega$, allora $2^{\aleph_\omega} = (\aleph_\omega)^{\aleph_0}$. Infatti, sotto questa ipotesi, $2^{<\aleph_\omega} = \aleph_\omega$.

ESERCIZIO 6.8. Siano κ, ν cardinali infiniti. Se ν è singolare, e se la sequenza $(\kappa^\xi \mid \xi < \nu)$ è definitivamente costante, allora $\kappa^\nu = \kappa^{<\nu}$.

Riguardo le esponenziazioni che hanno come base un cardinale limite, vale il seguente risultato:

TEOREMA 6.9. *Sia κ un cardinale limite, e ν un cardinale infinito. Si ha:*

- (1) $\kappa^\nu = \sup_{\mu < \kappa} \mu^\nu$ se $\nu < \text{cof}(\kappa)$.
- (2) $\kappa^\nu = (\sup_{\mu < \kappa} \mu^\nu)^{\text{cof}(\kappa)}$ se $\nu \geq \text{cof}(\kappa)$.

¹² Vedi Esercizio ??.

DIM. (1). Come già osservato nella dimostrazione del Teorema di Hausdorff, se $\nu < \text{cof}(\kappa)$ allora $\text{Fun}(\nu, \kappa) = \bigcup_{\gamma < \kappa} \text{Fun}(\nu, \gamma)$, visto che ogni funzione $f : \nu \rightarrow \kappa$ è limitata. Si ha allora:

$$\begin{aligned} \kappa^\nu = |\text{Fun}(\nu, \kappa)| &= \left| \bigcup_{\gamma < \kappa} \text{Fun}(\nu, \gamma) \right| \leq \sum_{\gamma < \kappa} |\text{Fun}(\nu, \gamma)| = \\ &= \sum_{\gamma < \kappa} |\gamma|^\nu = \max \left\{ \sup_{\gamma < \kappa} |\gamma|^\nu, \kappa \right\} = \max \left\{ \sup_{\mu < \kappa} \mu^\nu, \kappa \right\} = \sup_{\mu < \kappa} \mu^\nu. \end{aligned}$$

dove abbiamo denotato con $\gamma < \kappa$ gli ordinali minori di κ , e con $\mu < \kappa$ i cardinali minori di κ . Sopra abbiamo usato la disuguaglianza $\kappa \leq \sup_{\mu < \kappa} \mu^\nu$, che vale perchè κ è limite. Infatti, per ogni $\mu < \kappa$ si ha banalmente $\mu \leq \mu^\nu$, e quindi $\kappa = \sup_{\mu < \kappa} \mu \leq \sup_{\mu < \kappa} \mu^\nu$.

(2). Visto che κ è un cardinale limite, possiamo scrivere $\kappa = \sum_{i \in \text{cof}(\kappa)} \kappa_i$ dove $(\kappa_i \mid i \in \text{cof}(\kappa))$ è una sequenza crescente di cardinali $\kappa_i < \kappa$. In particolare $\kappa = \sup_{i \in \text{cof}(\kappa)} \kappa_i$. Notando che $\sup_{i \in \text{cof}(\kappa)} \kappa_i \leq \prod_{i \in \text{cof}(\kappa)} \kappa_i$ e applicando la formula del prodotto infinito, otteniamo:

$$\begin{aligned} \kappa^\nu &= \left(\sup_{i \in \text{cof}(\kappa)} \kappa_i \right)^\nu = \left(\left(\sup_{i \in \text{cof}(\kappa)} \kappa_i \right)^{\text{cof}(\kappa)} \right)^\nu = \left(\prod_{i \in \text{cof}(\kappa)} \kappa_i \right)^\nu = \\ &= \prod_{i \in \text{cof}(\kappa)} \kappa_i^\nu = \left(\sup_{i \in \text{cof}(\kappa)} \kappa_i^\nu \right)^{\text{cof}(\kappa)} = \left(\sup_{\mu < \kappa} \mu^\nu \right)^{\text{cof}(\kappa)}. \end{aligned}$$

Sopra abbiamo potuto applicare la formula sui prodotti infiniti anche alla sequenza $(\kappa_i^\nu \mid i \in \text{cof}(\kappa))$, perchè è non-decrescente. Inoltre, visto che $(\kappa_i \mid i \in \text{cof}(\kappa))$ è illimitata in κ , è chiaro che $\sup_{i \in \text{cof}(\kappa)} \kappa_i^\nu = \sup_{\mu < \kappa} \mu^\nu$. $\square$

ESERCIZIO 6.10. Assumiamo l'ipotesi del continuo. Mostrare che esistono cardinali infiniti κ, ν tali che $\kappa > \sup_{\mu < \kappa} \mu^\nu$.

Come diretta conseguenza del teorema precedente, ricaviamo:

TEOREMA 6.11. *Siano κ e ν cardinali infiniti.*

- (1) *Se $\mu^\nu < \kappa$ per ogni $\mu < \kappa$ e se $\nu < \text{cof}(\kappa)$ allora $\kappa^\nu = \kappa$.*
- (2) *Se $\mu^\nu < \kappa$ per ogni $\mu < \kappa$ e se $\nu \geq \text{cof}(\kappa)$ allora $\kappa^\nu = \kappa^{\text{cof}(\kappa)}$.*

DIM. (1). Se κ è limite, per la (1) del Teorema 6.9 si ha $\kappa^\nu = \sup_{\mu < \kappa} \mu^\nu \leq \kappa \leq \kappa^\nu$. Se $\kappa = \theta^+$ è successore, allora $\sup_{\mu < \kappa} \mu^\nu = \theta^\nu < \theta^+$, e per il teorema di Hausdorff si ha $\kappa^\nu = (\theta^+)^nu = \max\{\theta^\nu, \theta^+\} = \theta^+ = \kappa$.

(2). Con le nostre ipotesi abbiamo che $\text{cof}(\kappa) \leq \nu < 2^\nu < \kappa$, dunque κ è singolare ed è quindi un cardinale limite. Possiamo allora applicare la (2) del Teorema 6.9 ed ottenere:

$$\kappa^\nu = \left(\sup_{\mu < \kappa} \mu^\nu \right)^{\text{cof}(\kappa)} \leq \kappa^{\text{cof}(\kappa)} \leq \kappa^\nu.$$

$\square$

ESERCIZIO 6.12. Dimostrare che $(\aleph_\omega)^{\aleph_1} = 2^{\aleph_1} \cdot (\aleph_\omega)^{\aleph_0}$.

7. Cardinali inaccessibili

Abbiamo visto che ogni cardinale successore è regolare. La validità dell'implicazione inversa è un problema molto delicato; faremo qualche riflessione a proposito alla fine di questa sezione.

DEFINIZIONE 7.1. Un cardinale κ si dice *debolmente inaccessibile* se è un cardinale limite regolare. Un cardinale κ si dice *fortemente inaccessibile* (o semplicemente *inaccessibile*) se è un cardinale limite forte regolare.

Visto che ogni cardinale limite forte è un cardinale limite, banalmente ogni cardinale fortemente inaccessibile è debolmente inaccessibile.

Ricordiamo che se vale l'ipotesi generalizzata del continuo GCH le nozioni di limite e di limite forte coincidono, e quindi in quel caso anche le nozioni di debolmente e di fortemente inaccessibile coincidono.

ESEMPIO 7.2. $\aleph_0$ è fortemente inaccessibile.

L'aggettivo “inaccessibile” è dovuto alla proprietà che non è “raggiungibile” dal basso mediante esponenziazioni, somme o prodotti anche infiniti.

ESERCIZIO 7.3. Un cardinale κ è fortemente inaccessibile se e solo se soddisfa le seguenti tre proprietà:

- (1) Se $\mu, \nu < \kappa$ allora $\mu^\nu < \kappa$.
- (2) Se $(\kappa_i \mid i \in I)$ è una sequenza infinita di cardinali dove $|I| < \kappa$ e $\kappa_i < \kappa$ per ogni $i \in I$, allora $\sum_{i \in I} \kappa_i < \kappa$.
- (3) Se $(\kappa_i \mid i \in I)$ è una sequenza infinita di cardinali dove $|I| < \kappa$ e $\kappa_i < \kappa$ per ogni $i \in I$, allora $\prod_{i \in I} \kappa_i < \kappa$.

TEOREMA 7.4. Sia $\kappa > \aleph_0$ un cardinale regolare. Allora:

- (1) κ è debolmente inaccessibile se e solo se è un punto fisso della funzione-classe aleph: $\kappa = \aleph_\kappa$.
- (2) κ è fortemente inaccessibile se e solo se è un punto fisso della funzione-classe beth: $\kappa = \beth_\kappa$.

DIM. (1). Se κ è inaccessibile, allora $\kappa = \aleph_\lambda$ dove λ è limite perché è un cardinale limite, ed inoltre $\text{cof}(\aleph_\lambda) = \aleph_\lambda$ perché è regolare. Abbiamo la seguente catena di disuguaglianze:

$$\aleph_\lambda = \text{cof}(\aleph_\lambda) = \text{cof}(\lambda) \leq |\lambda| \leq \lambda \leq \aleph_\lambda.$$

Quindi $\kappa = \aleph_\lambda = \lambda$, e dunque $\kappa = \aleph_\kappa$. Viceversa, se $\kappa = \aleph_\kappa$ è un punto fisso regolare della funzione-classe aleph, allora κ è un cardinale limite perché è un aleph con indice un ordinale limite, cioè κ .

(2). Procediamo in modo del tutto analogo a quanto fatto per la dimostrazione del punto (1). Se κ è fortemente inaccessibile, allora $\kappa = \beth_\lambda$ con λ limite perché è un limite forte, ed inoltre $\text{cof}(\beth_\lambda) = \beth_\lambda$ perché è regolare. Abbiamo allora la seguente catena di disuguaglianze:

$$\beth_\lambda = \text{cof}(\beth_\lambda) = \text{cof}(\lambda) \leq |\lambda| \leq \lambda \leq \beth_\lambda.$$

Quindi $\kappa = \beth_\lambda = \lambda$, e dunque $\kappa = \beth_\kappa$. Viceversa, se $\kappa = \beth_\kappa$ è un punto fisso regolare della funzione-classe beth, allora κ è un limite forte perché è un punto limite della funzione beth. $\square$