Università degli Studi di Pisa

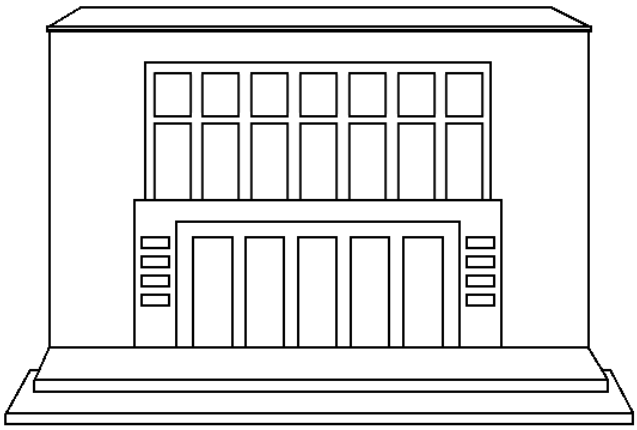
FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea Triennale in Matematica

Dispensa non ufficiale
basata sul corso ETI di M. Di Nasso

Elementi di Teoria degli Insiemi

Aggiornata il 9 Aprile 2020

Luca Tonelli



Anno accademico 2017/2018

Indice

alle mie donne
in Villa Tonelli

1 Introduzione

Non so se questo corso abbia avuto la colpa di farmi assuefare a LaTeX, oppure se questa nuova piacevole dipendenza dal perfezionismo stilistico mi abbia fatto assuefare al corso, ma dalla commistione delle due è emerso questo lavoro.

Questa dispensa nasce infatti da una personale rielaborazione delle lezioni tenute dal Prof. Mauro Di Nasso per il corso di Elementi di Teoria degli Insiemi nell'anno accademico 2017/2018 presso l'Università di Pisa.

Non dovrebbero esserci mancanze dal punto di vista del contenuto, che è stato invece ben riordinato per un approccio più diretto alla teoria di ZFC. Questo tipo di approccio è forse meno funzionale dal punto di vista didattico rispetto a quello trattato a lezione, ma è sicuramente migliore per chi ha già seguito il corso o per chi vuole usare la dispensa come strumento di ripasso per le lezioni del suo anno accademico (sebbene lo si sconsigli, non si esclude la possibilità di affrontare la materia con l'uso esclusivo della presente dispensa). Si è cercato di non aggiungere contenuti non visti a lezione, ma in certi casi, quando alcune osservazioni sono evidenti o molto semplici e al tempo stesso ritenute importanti, lo si fa senza evidenziarlo. Il capitolo 2 dà un panorama storico della nascita e dei primi sviluppi della Teoria degli Insiemi ed è interamente tratto da [2] e [3]. Il capitolo 6 (Numeri interi, razionali e reali) è stato trattato poco a lezione, ma lo si ritiene importante per fini di completezza ed è inoltre necessario in vista della stesura di dispense di altri corsi (per i quali la Teoria degli Insiemi e la Logica Matematica fanno da fondamento). L'ultimo capitolo contiene una serie di esercizi assegnati nelle prove d'esame dei corsi di Elementi di Teoria degli Insiemi tenuti dal Prof. Mauro Di Nasso negli anni passati presso l'Università di Pisa, con le soluzioni (si spera giuste) dell'autore di questa dispensa. Ovviamente il contenuto sviluppato in quel capitolo non rientra nelle conoscenze previste dal corso, e in generale si consiglia di far riferimento al registro delle lezioni per il programma effettivamente svolto.

Si fa solo un accenno alla parte introduttiva sulla Teoria intuitiva degli Insiemi (nel capitolo 2) e si passa subito ad elencare gli assiomi di ZFC. Inoltre, per una scelta personale, non si tratta la Teoria delle classi.

Si danno per scontate le nozioni basilari di logica su connettivi e quantificatori, e allo stesso tempo si prende in modo un po' informale e introduttivo la nozione di indecidibilità, avendo in mente l'idea di un enunciato per il quale esistono modelli di ZFC in cui esso è vero e altri in cui non è vero (tra l'altro anche il concetto di modello è per ora solo un'idea intuitiva). Si rimanda ai corsi di Logica chi volesse una conoscenza più approfondita sull'argomento. La dicitura (AC) all'inizio di un Teorema (Proposizione, Lemma...) sta ad indicare la necessità dell'Assioma di scelta per la dimostrabilità del Teorema in questione.

La presenza di un asterisco (*) all'inizio di un Teorema (Proposizione, Lemma...) significa che questo è stato lasciato per esercizio a lezione e pertanto si consiglia al lettore di provare a dimostrarlo personalmente e di ricorrere alla dispensa solo dopo vari tentativi e altrettanti fallimenti (sarà raro ma non impossibile che accada).

Per la poca forza di volontà dell'autore nel prendere appunti, alcune dimostrazioni non sono presumibilmente quelle svolte a lezione, per cui lo stesso si assume ogni responsabilità per qualsiasi tipo di mancanza o errore e sarà lieto di ricevere eventuali correzioni allo scopo di rendere questa dispensa il più corretta e semplice possibile.

Buon lavoro, sommadidueprimi@gmail.com

2 Cenni storici

Ordinali e cardinali hanno segnato il punto di svolta per una disciplina, la matematica ottocentesca, che rantolava dietro a contraddizioni irrisolte e pochezza formale. Si parla tuttavia di una svolta né rapida né facile da accettare.

Nella seconda metà dell'Ottocento, in cui l'Analisi aveva subito una violenta impennata, si sentiva la necessità di dare una sistemazione formale a diverse questioni rimaste irrisolte e spesso tacitamente trascurate (soprattutto riguardo ai numeri reali e al concetto di infinito).

Dopo un primo tentativo di Bolzano di sistemare la cosa, Georg Cantor (1845-1918) fu il vero artefice del grande cambiamento ed è oggi ritenuto il fondatore della Teoria degli Insiemi, una branca della matematica che riesce a formalizzare al suo interno tutti gli oggetti con cui hanno a che fare ogni giorno gli addetti ai lavori (insiemi numerici, funzioni, strutture algebriche...).

Spesso chi si approccia per la prima volta a questa materia ne è fortemente coinvolto per il ruolo fondazionale, l'alone di mistero e gli svariati teoremi dalle sembianze paradossali (si veda l'esistenza di cardinali k per cui $\aleph_k = k$ o $\beth_k = k$).

Grossa parte di questo coinvolgimento è senza dubbio dovuta all'"Ipotesi del continuo": Cantor aveva dimostrato che i numeri reali sono "di più" dei numeri naturali, ma non riuscì a risolvere il problema di determinare se vi fossero delle "cardinalità" intermedie fra quelle di questi due insiemi. L'Ipotesi del continuo afferma proprio la non esistenza di queste cardinalità intermedie. Lo stesso Hilbert si dedicò alla questione, anch'egli senza successo. Hilbert riteneva l'Ipotesi del continuo talmente degna di nota da metterla prima nella lista dei problemi matematici più importanti presentati al Congresso internazionale dei matematici del 1900.

Inizialmente Cantor e i suoi lavori ricevettero durissime critiche anche da matematici di un certo calibro, come Kronecker e Poincaré, che si riferì al suo lavoro descrivendolo come "una malattia da cui le generazioni che verranno potranno dire di essere guarite". Fortunatamente già allora c'era chi si rendeva conto della portata delle idee cantoriane, per esempio Hilbert, che nel 1926 disse "Nessuno riuscirà mai ad espellerci dal paradiso che Cantor ha creato per noi".

Per quanto riguarda l'Ipotesi del continuo, solo in seguito Gödel e Cohen ne provarono l'indipendenza dagli assiomi di ZFC, ma si preferisce non dilungarsi oltre sulle questioni storiche...

Resta solo da evidenziare un fatto fondamentale per introdurre al meglio il prossimo capitolo e il vero inizio della teoria: il lavoro di Cantor e la sua successiva assiomatizzazione portavano ancora a delle contraddizioni (le vedremo più avanti), tutte derivanti dall'assumere l'esistenza di insiemi "troppo grandi", come l'insieme di tutti gli insiemi.

Infatti questa nuova assiomatizzazione assumeva l'esistenza, per ogni proprietà P esprimibile nel linguaggio della Teoria degli Insiemi, dell'insieme di tutti e soli gli insiemi soddisfacenti P. Da questo assioma (Comprensione) deriva l'esistenza di $\mathcal{R} := \{x \mid x \notin x\}$ (Russell), cioè l'insieme di tutti gli insiemi che non appartengono a se stessi. Ora ci si può chiedere se $\mathcal{R}$ appartenga oppure no a se stesso e in entrambi i casi si arriva a una contraddizione. A tal proposito si provi a cercare "Paradosso di Russell", "Paradosso di Berry" ed "eterologico".

Il problema fu risolto con la successiva assiomatizzazione dovuta a Zermelo e Fraenkel, da cui ZFC ("Zermelo-Fraenkel with Choice", dove "Choice" si riferisce all'Assioma di scelta) e lo si vedrà nel prossimo capitolo.

Chiaramente con "risolto" si intende che è stata eliminata la possibilità di ottenere insiemi alla Russell nel modo in cui venivano ottenuti precedentemente, ma non certo che si è dimostrata la coerenza di ZFC.

3 Assiomi di ZFC

$\mathcal{E}$ssenzialmente tutti gli studenti di un corso universitario di matematica arrivano a chiedersi che cosa sia un insieme, intendendo come lo si possa definire. Si è infatti abituati a definire ogni oggetto con cui si entra in contatto, ma nel caso degli insiemi questo non viene fatto, così come non si definivano punti e rette nella geometria euclidea studiata alla scuola superiore, in cui questi ultimi venivano presi come "enti primitivi".

Dal punto di vista intuitivo sembra del tutto ragionevole che si debba assumere a priori l'esistenza di qualcosa indefinito da cui poi si trarranno le definizioni degli oggetti successivi. Ed è proprio così che funziona una teoria logica, ovvero non definendo i suoi oggetti (nel nostro caso gli insiemi), ma lasciando che gli assiomi posti su di essi ne descrivano le proprietà che intuitivamente gli attribuiamo.

Perciò negli assiomi che seguono e in tutto il resto della dispensa, ogni variabile potrà essere chiamata "insieme", nel senso che per quanto ci riguarda ogni oggetto della nostra teoria è un insieme (in questo caso si dice che non esistono "atomi" e che ZFC è una teoria "pura" degli insiemi). Talvolta si userà il termine "famiglia" come sinonimo di "insieme".

Ecco dunque gli assiomi di ZFC.

Assioma 1 (Estensionalità)**.** *Due insiemi sono uguali se e solo se hanno gli stessi elementi. In formule*

$$\forall x \forall y (x = y \leftrightarrow \forall z (z \in x \leftrightarrow z \in y))$$

Oss. Questo assioma potrebbe essere eliminato e sostituito da un'equivalente definizione di uguaglianza.

Assioma 2 (Vuoto)**.** *Esiste un insieme che non ha elementi.*
In formule

$$\exists x \forall y \neg (y \in x)$$

Oss. Usando l'Assioma di estensionalità è del tutto banale osservare che l'insieme di cui si parla nell'Assioma del vuoto è unico.

Definizione (Insieme vuoto)**.** *Si dice* ***insieme vuoto*** *l'unico insieme senza elementi e lo si denota* $\emptyset$*.*

Oss. Quando si dice che un insieme del tipo $\{z \mid P(z)\}$ (ammesso che esista) viene denotato con un determinato simbolo ξ, come $\emptyset$ per l'insieme vuoto, si intende che da lì in avanti la scrittura $x = \xi$, che non è una formula della Teoria degli Insiemi, sarà solo un'abbreviazione per $\forall z (z \in x \leftrightarrow P(z))$, e allo stesso modo $x \in \xi$ sarà solo un altro modo per dire $P(x)$.

Non ci si dilunga oltre sulla questione delle notazioni e d'ora in avanti se ne farà largo uso in tutta la dispensa, ritenendo il lettore certamente in grado di capire le abbreviazioni usate (per lo più già viste in altri corsi).

Si vuole solo affermare l'importanza di questo passaggio in matematica, poiché senza notazioni si avrebbe una matematica non solo più lunga e noiosa da scrivere, ma anche molto meno intuitiva. Il lettore provi a pensare, per esempio, alla pesantezza di una scrittura dell'Assioma di scelta (più avanti) senza l'uso di alcuna notazione aggiuntiva.

Assioma 3 (Coppia)**.** *Per ogni a e b esiste un insieme che ha per elementi solo a e b. In formule*

$$\forall a \forall b \exists x \forall y (y \in x \leftrightarrow (y = a \vee y = b))$$

Oss. Anche in questo caso, usando l'Assioma di estensionalità, si ottiene l'unicità dell'insieme di cui si parla nell'Assioma di coppia.

Definizione (Coppia)**.** *Per ogni a e b si dice **coppia** di a e b l'insieme i cui elementi sono a e b e lo si denota $\{a, b\}$.*

Oss. Se $a = b$, allora la coppia di a e b ha un unico elemento, cioè a. In questo caso si parla di ***singoletto*** di a e lo si denota $\{a\}$.

Si è già pronti per definire la coppia ordinata. L'idea matematica di coppia ordinata cui si è abituati è quella di un oggetto che ha una prima e una seconda componente ed è univocamente determinato da queste due e dal loro ordine. Si dà dunque la seguente definizione (dovuta a Kuratowski) e si verifica che rispetti la proprietà appena citata.

Definizione (Coppia ordinata)**.** *Per ogni a e b l'insieme $\{\{a\}, \{a, b\}\}$, che esiste per l'Assioma di coppia, è detto **coppia ordinata** con prima componente a e seconda componente b, e si denota (a, b).*

Proposizione 3.1. *(*) Per ogni a_1, a_2, b_1, b_2 vale*

$$((a_1, b_1) = (a_2, b_2)) \leftrightarrow (a_1 = a_2 \wedge b_1 = b_2)$$

Dim. La dimostrazione si basa solo sull'uso ripetuto dell'Assioma di estensionalità:

- $\rightarrow$: sia $(a_1, b_1) = (a_2, b_2)$, cioè $\{\{a_1\}, \{a_1, b_1\}\} = \{\{a_2\}, \{a_2, b_2\}\}$.

  Se $a_1 = b_1$, allora $(a_1, b_1) = \{\{a_1\}\}$ e dunque $\{a_1\} = \{a_2, b_2\}$, da cui segue $b_1 = a_1 = a_2 = b_2$. La stessa cosa vale se $a_2 = b_2$.

  Se $a_1 \neq b_1$ e $a_2 \neq b_2$, allora si prova facilmente che $\{a_1\} \neq \{a_2, b_2\}$ (e allo stesso modo $\{a_2\} \neq \{a_1, b_1\}$). Infatti, se fosse $\{a_1\} = \{a_2, b_2\}$, si avrebbe $a_1 = a_2 = b_2$ (*Assurdo*). Dunque $\{a_1\} = \{a_2\}$, da cui segue $a_1 = a_2$, e $\{a_1, b_1\} = \{a_2, b_2\}$, da cui segue $b_1 = b_2$ (perché $b_1 \neq a_1 = a_2$).

- $\leftarrow$: se $a_1 = a_2$ e $b_1 = b_2$, allora la tesi è ovvia. $\square$

Oss. Questo non è l'unico modo per definire formalmente il concetto di coppia ordinata: si provi a cercarne degli altri.

Perché $\{a, \{b\}\}$ non funziona?

Assioma 4 (Unione)**.** *Per ogni X esiste un insieme che ha per elementi tutti e soli gli elementi degli elementi di X.*

In formule

$$\forall X \exists y \forall z (z \in y \leftrightarrow \exists w (w \in X \wedge z \in w))$$

Oss. Per l'Assioma di estensionalità anche questo insieme è unico.

Intuitivamente fare l'unione di un insieme X è come prendere tante scatole piene (gli elementi di X) e rovesciarle tutte in un unico contenitore (ottenendo l'unione di X).

Dall'Assioma di coppia e dall'Assioma dell'unione segue banalmente l'esistenza dell'unione binaria di due insiemi.

Definizione (Unione)**.** *Dato un insieme X si definisce **unione** di X l'insieme che ha per elementi tutti e soli gli elementi degli elementi di X, e lo si denota $\bigcup X$. Nel caso dell'unione binaria tra due insiemi x e y si scrive $x \cup y$.*

Definizione (Sottoinsieme e contenimento)**.** *Dati due insiemi x e y si dice che x è **sottoinsieme** di y o che x è **contenuto** in y se ogni elemento di x è anche elemento di y. In questo caso si scrive $x \subseteq y$.*

In formule

$$x \subseteq y \leftrightarrow \forall z (z \in x \rightarrow z \in y)$$

Assioma 5 (Potenza)**.** *Per ogni X esiste l'insieme di tutti e soli i suoi sottoinsiemi. In formule*

$$\forall X \exists y \forall z (z \in y \leftrightarrow z \subseteq X)$$

Oss. Anche in questo caso l'Assioma di estensionalità garantisce l'unicità dell'insieme in questione.

Definizione (Insieme delle parti)**.** *Dato un insieme X, l'insieme di tutti e soli i suoi sottoinsiemi è detto **insieme delle parti** o **insieme potenza** di X e denotato $\mathcal{P}(X)$.*

Il prossimo assioma è il punto di rottura con la prima assiomatizzazione successiva al lavoro di Cantor. Infatti, seguendo una sorta di "principio di limitazione della grandezza" e sostituendo l'Assioma di comprensione con quello di separazione, si è riusciti a sistemare le situazioni contraddittorie come quella del "Paradosso di Russell".

Assioma 6 (Separazione)**.** *Per ogni formula $P(x)$ del linguaggio della Teoria degli Insiemi e per ogni insieme A esiste l'insieme degli elementi di A che soddisfano P. In formule*

$$\forall A \exists x \forall y (y \in x \leftrightarrow (y \in A \wedge P(y)))$$

Oss. Il precedente non è un singolo assioma, ma più propriamente uno schema di assiomi, uno per ogni formula $P(x)$ con una sola variabile libera. Si dice dunque che ZFC non è finitamente assiomatizzabile (in realtà questo andrebbe provato formalmente, ma si tratta di questioni di Logica che fuoriescono dagli obiettivi di questo corso).

Anche in questo caso l'Assioma di estensionalità garantisce l'unicità dell'insieme in questione, che sarà denotato $\{x \in A \mid P(x)\}$.

Inoltre, dato un insieme non vuoto X, l'Assioma di separazione implica l'esistenza dell'insieme di tutti e soli gli insiemi che appartengono a tutti gli elementi di X. Infatti se $A \in X$, allora l'insieme appena citato è

$$\{x \in A \mid \forall y (y \in X \to x \in y)\}$$

Definizione (Intersezione)**.** *Se X è un insieme non vuoto e $A \in X$, allora l'insieme $\bigcap X := \{x \in A \mid \forall y (y \in X \to x \in y)\}$ è detto* ***intersezione*** *di X.*

Oss. Se $X = \{A, B\}$, allora $\bigcap X$ si denota $A \cap B$ ed è l'intersezione binaria cui si è sempre stati abituati.

Allo stesso modo dell'intersezione si può provare l'esistenza dell'insieme di tutti e soli gli elementi di A che non appartengono a B, cioè $\{x \in A \mid x \notin B\}$.

Definizione (Differenza)**.** *Dati due insiemi A e B, l'insieme di tutti e soli gli elementi di A che non appartengono a B è detto* ***differenza*** *tra A e B e denotato $A \setminus B$.*

Oss. È banale osservare che

$$A \subseteq B \leftrightarrow A \cup B = B \leftrightarrow A \cap B = A \leftrightarrow A \setminus B = \emptyset$$

Inoltre si potrebbero provare le ben note proprietà delle operazioni insiemistiche, cioè che unione e intersezione sono associative e commutative e che si distribuiscono l'una rispetto all'altra, e le Leggi di De Morgan, ma le dimostrazioni sono piuttosto monotone e prive di idee originali, quindi si preferisce ometterle.

Definizione (Relazione binaria)**.** *Una* ***relazione binaria*** *(o più semplicemente "relazione") è un insieme di coppie ordinate. In formule "$\mathcal{R}$ è una relazione binaria" si scrive "$\forall x (x \in \mathcal{R} \to \exists y \exists z (x = (y, z)))$".*

Definizione (Dominio e Immagine di una relazione)**.** *Data una relazione binaria $\mathcal{R}$ si definiscono rispettivamente* ***dominio*** *e* ***immagine*** *di $\mathcal{R}$ gli insiemi $\mathcal{D}om\,\mathcal{R} := \{x \in \bigcup\bigcup \mathcal{R} \mid \exists y\ (x,y) \in \mathcal{R}\}$ e $\mathcal{I}m\,\mathcal{R} := \{y \in \bigcup\bigcup \mathcal{R} \mid \exists x\ (x,y) \in \mathcal{R}\}$, che esistono per l'Assioma dell'unione e per l'Assioma di separazione.*

Definizione (Funzione)**.** *Una relazione binaria f è detta* ***univoca*** *o meglio* ***funzione*** *se per ogni $x \in \mathcal{D}om\,f$ esiste un unico y tale che $(x,y) \in f$. In formule "f è una funzione" se e solo se ("f è una relazione binaria" $\wedge\, \forall x \forall y \forall z (x \in \mathcal{D}om\,f \to (((x,y) \in f \wedge (x,z) \in f) \to y = z))$).*

Se $x \in \mathcal{D}om\,f$, allora si indica con $f(x)$ l'unico y per cui $(x,y) \in f$.

Definizione (Funzione di scelta)**.** *Dato un insieme X si dice che una funzione f è una* ***funzione di scelta*** *su X se $\mathcal{D}om\,f = X$ e per ogni $x \in X$ non vuoto vale $f(x) \in x$. In formule "f è una funzione di scelta su X" si scrive ("f è una funzione" $\wedge\, (\mathcal{D}om\,f = X) \wedge \forall x((x \in X \wedge x \neq \emptyset) \to f(x) \in x)$).*

Assioma 7 (Scelta)**.** *Per ogni insieme X esiste una funzione di scelta su X. In formule*

$$\forall X \exists f(\text{"}f \text{ è una funzione di scelta su } X\text{"})$$

Oss. In questo caso si vede facilmente che non vale l'unicità della funzione in questione.

Nei capitoli 9 e 12 si proverà l'equivalenza dell'Assioma di scelta con vari altri enunciati.

C'è chi mette in discussione l'Assioma di scelta giudicandolo poco intuitivo. Però non solo alcune sue forme equivalenti sembrano più che accettabili, ma gran parte della matematica non esisterebbe senza assumere la validità di questo assioma così apparentemente innocuo.

Spesso ci si riferisce all'Assioma di scelta con la sigla AC, che sta per l'inglese "Axiom of choice".

Gli assiomi assunti finora non provano l'esistenza di insiemi infiniti (nel senso intuitivo del termine, dato che non si è ancora definito cosa sia un insieme infinito), e l'assioma seguente entra in gioco proprio per questo motivo.

Definizione (Insieme induttivo)**.** *Un insieme X è detto* ***induttivo*** *se $\emptyset \in X$ e per ogni $y \in X$ vale $y \cup \{y\} \in X$. In formule*

$$\text{"}X \text{ è induttivo"} \leftrightarrow (\emptyset \in X \wedge \forall y(y \in X \to y \cup \{y\} \in X))$$

Dato un insieme X, se per ogni $y \in X$ vale $y \cup \{y\} \in X$, allora si dice che X è ***chiuso per successore****.*

Oss. La condizione $\emptyset \in X$ nella definizione sopra fa sì che non esistano insiemi induttivi del tipo $t = \{t\}$, che non sarebbero infiniti.

Assioma 8 (Infinito)**.** *Esiste un insieme induttivo. In formule*

$$\exists x\,(\text{“}x \text{ è induttivo”})$$

Oss. Si vedrà più avanti nella dispensa che in questo caso non vale l'unicità dell'insieme in questione (ogni ordinale limite è un insieme induttivo). Nel capitolo 5 si farà uso dell'Assioma dell'infinito per definire l'insieme dei numeri naturali e derivarne le proprietà principali.

Il prossimo assioma non sarà necessario nello sviluppo della teoria almeno fino a che non ci si sarà davvero addentrati nello studio degli ordinali. In particolare la prima volta che verrà richiamato sarà quando si dimostrerà che ogni buon ordine è isomorfo ad un (unico) ordinale.

Assioma 9 (Rimpiazzamento)**.** *Per ogni formula del linguaggio della Teoria degli Insiemi $P(x, y)$ (P ha due variabili libere) tale che per ogni x esiste un unico y per cui vale $P(x, y)$, per ogni insieme A esiste l'insieme di tutti e soli gli y per i quali esiste $x \in A$ e vale $P(x, y)$. In formule*

$$\forall A \exists B \forall y (y \in B \leftrightarrow \exists x (x \in A \wedge P(x, y)))$$

Oss. Poiché una proprietà $P(x, y)$ del tipo sopra è essenzialmente univoca, vedendola come una specie di “funzione”, si ottiene che l'Assioma di rimpiazzamento afferma nient'altro che l'esistenza dell'insieme immagine di questa “funzione” applicata ad A.

Dall'Assioma di scelta seguirà che l'immagine di una funzione ha cardinalità minore o uguale a quella del dominio e dunque l'Assioma di rimpiazzamento è in accordo col “principio di limitazione della grandezza” di cui si è già parlato.

Inoltre, come l'Assioma di separazione, non si tratta di un singolo assioma, ma di uno schema di assiomi.

Sempre per quanto riguarda il “principio di limitazione della grandezza”, ci sarebbe da chiedersi se gli assiomi dell'unione e della potenza lo rispettino, ma solo una volta che si sarà sviluppata la teoria sui cardinali si potrà provare ad argomentare la questione.

Strettamente legato alla Gerarchia di Von Neumann, uno degli ultimi argomenti del corso, si va ora a presentare l'Assioma di fondazione, che fa parte degli assiomi di ZFC, ma sarà nominato nuovamente solo negli ultimi capitoli della dispensa.

Assioma 10 (Fondazione)**.** *Ogni insieme non vuoto ha un elemento disgiunto da se stesso. In formule*

$$\forall x (x \neq \emptyset \rightarrow (\exists t (t \in x \wedge t \cap x = \emptyset)))$$

Si è ora pronti per i primi sviluppi della teoria, molti dei quali dovrebbero essere argomenti già ben noti al lettore.

4 Relazioni e funzioni

$\mathcal{M}$olte proprietà essenziali su relazioni e funzioni sono raccolte in questo capitolo e saranno usate a dismisura in tutto il seguito della dispensa.

I concetti di relazione e funzione sono già stati definiti nel capitolo precedente.

Un'operazione fondamentale fra due insiemi A e B è il "prodotto cartesiano", cioè l'insieme di tutte e sole le coppie ordinate con prima componente in A e seconda componente in B. Si passa ora a provare l'esistenza di questo insieme (*). È banale osservare che per ogni $a \in A$ e per ogni $b \in B$ $(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B))$, che esiste per l'Assioma dell'unione e l'Assioma delle parti.

Dunque per l'Assioma di separazione esiste l'insieme

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

dove "$\exists a \exists b(a \in A \wedge b \in B \wedge x = (a, b))$" significa "x è una coppia ordinata con prima componente in A e seconda componente in B".

Definizione (Prodotto cartesiano)**.** *Dati due insiemi A e B, l'insieme $A \times B$ definito sopra è detto* ***prodotto cartesiano*** *fra A e B.*

Oss. Il prodotto cartesiano non è né associativo né commutativo, ma si distribuisce rispetto a unioni e intersezioni.

Definizione. *Dato un insieme A, si dice che una relazione binaria $\mathcal{R}$ è* ***su*** *A se $\mathcal{D}om\,\mathcal{R} \cup \mathcal{I}m\,\mathcal{R} \subseteq A$.*

Oss. Una relazione su A è un sottoinsieme di $A \times A$.

Se $\mathcal{R}$ è una relazione binaria, da qui in avanti si scriverà equivalentemente $x\mathcal{R}y$ al posto di $(x, y) \in \mathcal{R}$ (si legge "x è in relazione con y secondo $\mathcal{R}$").

Non considerando le funzioni, i principali tipi di relazione usati in matematica sono le relazioni di equivalenza e le relazioni d'ordine.

Definizione (Relazione di equivalenza)**.** *Una relazione binaria $\mathcal{R}$ su un insieme A è detta* ***relazione di equivalenza*** *se verifica le seguenti tre proprietà:*

- *(riflessiva)* $\forall x \in A\ x\mathcal{R}x$;
- *(simmetrica)* $\forall x, y \in A\ (x\mathcal{R}y \to y\mathcal{R}x)$;
- *(transitiva)* $\forall x, y, z \in A\ (x\mathcal{R}y \wedge y\mathcal{R}z) \to x\mathcal{R}z$.

Definizione (Classe di equivalenza)**.** *Data una relazione di equivalenza $\mathcal{R}$ su A e dato $a \in A$, si dice* ***classe di equivalenza*** *di a l'insieme $[a] := \{x \in A \mid x\mathcal{R}a\}$.*

Definizione (Partizione)**.** *Dati due insiemi X e Y, si dice che Y è una* ***partizione*** *di X se $Y \subseteq \mathcal{P}(X)$, $\bigcup Y = X$ e per ogni $A, B \in Y$ tali che $A \neq B$ vale $A \cap B = \emptyset$.*

Oss. Relazioni di equivalenza e partizioni sono due modi distinti di definire essenzialmente lo stesso concetto.

Formalmente, data una relazione di equivalenza $\mathcal{R}$ su un insieme A, questa induce su A una partizione data dall'insieme delle classi di equivalenza dei suoi elementi. Inoltre, data una partizione Y di A, questa induce una relazione di equivalenza $\mathcal{R}$ su A definita da $x\mathcal{R}y \leftrightarrow \exists B \in A\ (x \in B \wedge y \in B)$. Questi procedimenti sono anche uno l'inverso dell'altro.

Definizione (Relazione d'ordine)**.** *Una relazione binaria $\leq$ è detta* ***relazione d'ordine parziale largo*** *su A se verifica le seguenti tre proprietà:*

- *(riflessiva):* $\forall a \in A\ a \leq a$;
- *(antisimmetrica):* $\forall a, b \in A\ (a \leq b \wedge b \leq a) \rightarrow a = b$;
- *(transitiva):* $\forall a, b, c \in A\ (a \leq b \wedge b \leq c) \rightarrow a \leq c$.

Una relazione binaria $<$ è detta ***relazione d'ordine parziale stretto*** *su A se verifica le seguenti tre proprietà:*

- *(irriflessiva):* $\forall a \in A\ a \not< a$;
- *(asimmetrica):* $\forall a, b \in A\ a < b \rightarrow b \not< a$;
- *(transitiva):* $\forall a, b, c \in A\ (a < b \wedge b < c) \rightarrow a < c$.

Una coppia $(A, \mathcal{R})$, dove $\mathcal{R}$ è una relazione d'ordine parziale su A, è detta ***insieme parzialmente ordinato****.*

Esempio. Il contenimento $\subseteq$ è una relazione d'ordine parziale largo su un qualsiasi insieme.

Oss. La definizione di ordine stretto data sopra è ridondante perché se vale la proprietà transitiva, allora la proprietà irriflessiva e quella asimmetrica sono equivalenti.

Ordini larghi e stretti sono essenzialmente la stessa cosa, nel senso che da un ordine largo $\leq$ si ottiene un ordine stretto ponendo $a < b \leftrightarrow (a \leq b \wedge a \neq b)$, e da un ordine stretto $<$ si ottiene un ordine largo ponendo $a \leq b \leftrightarrow (a < b \vee a = b)$. Inoltre questi due procedimenti sono uno l'inverso dell'altro.

Dunque nel seguito della dispensa si considereranno insiemi ordinati senza specificare se siano ordini stretti o larghi e lasciando che il simbolo di relazione o la situazione chiariscano di quale dei due si tratti. In particolare si indicherà con $\leq$ un ordine largo e con $<$ un ordine stretto. Inoltre quando

si considereranno più insiemi ordinati nello stesso momento, si userà per i loro ordini lo stesso simbolo, ma sarà chiaro dal contesto a quale dei due ci si riferisce di volta in volta (formalmente bisognerebbe sempre scrivere $<_A$ e $<_B$, ma sarebbe pesante e non necessario). In aggiunta si scriverà spesso $a > b$ al posto di $b < a$ e $a \geq b$ al posto di $b \leq a$.

Se $(A, \leq)$ è un insieme parzialmente ordinato e $B \subseteq A$, allora $(\leq \cap (B \times B))$ è un ordine parziale su B, che sarà denotato semplicemente $\leq$ e talvolta chiamato ***ordinamento indotto*** su B.

Definizione. *Dati un insieme parzialmente ordinato $(A, \leq)$ e un sottoinsieme B di A, si dice che $a \in A$ è:*

- ***minorante*** *per B se per ogni $b \in B$ vale $a \leq b$;*
- ***maggiorante*** *per B se per ogni $b \in B$ vale $b \leq a$;*
- ***minimale*** *in B se $a \in B$ e non esistono $b \in B$ tali che $b < a$;*
- ***massimale*** *in B se $a \in B$ e non esistono $b \in B$ tali che $a < b$;*
- ***minimo*** *in B se $a \in B$ e per ogni $b \in B$ vale $a \leq b$;*
- ***massimo*** *in B se $a \in B$ e per ogni $b \in B$ vale $b \leq a$;*
- ***estremo inferiore*** *di B (denotato $\inf B$) se è il massimo dei minoranti per B;*
- ***estremo superiore*** *di B (denotato $\sup B$) se è il minimo dei maggioranti per B.*

Oss. Dato un insieme parzialmente ordinato $(A, \leq)$ e un suo sottoinsieme B, non è garantita l'esistenza di un minorante, maggiorante, elementi minimali...e così via per tutti i tipi di elementi definiti sopra. Per esempio, quando si saranno definiti i numeri interi $\mathbb{Z}$, si vedrà che questo insieme (col suo ordinamento) non ha minimo.

Massimo e minimo, se esistono, sono banalmente unici. Questo non vale per gli elementi massimali e minimali: per esempio in $(\mathbb{Z} \setminus \{1\}, \mid)$ tutti i numeri primi sono elementi minimali.

Valgono inoltre le banali implicazioni:

- "Minimo" $\rightarrow$ "Minorante, Minimale e Inf" e "Massimo" $\rightarrow$ "Maggiorante, Massimale e Sup";
- "Minorante $\in B$" $\rightarrow$ "Minimo" e "Maggiorante $\in B$" $\rightarrow$ "Massimo".

Definizione (Confrontabilità)**.** *Dato un insieme parzialmente ordinato $(A, \leq)$ e dati $a, b \in A$, si dice che a e b sono* ***confrontabili*** *se vale almeno una fra $a \leq b$ e $b \leq a$, o equivalentemente se vale una e una sola fra $a < b$, $a = b$ e $b < a$.*

Definizione (Ordine totale e tricotomia)**.** *Si dice che un insieme parzialmente ordinato $(A, \leq)$ è* ***totalmente ordinato*** *se tutti i suoi elementi sono mutualmente confrontabili.*

In questo caso si dice anche che vale la ***tricotomia*** *di $<$.*

Oss. In un insieme totalmente ordinato i concetti di elemento massimale ed elemento minimale coincidono rispettivamente con massimo e minimo.

Definizione (Catena)**.** *Dato un insieme parzialmente ordinato $(A, \leq)$ si dice che un sottoinsieme B di A è una* ***catena*** *di A se è totalmente ordinato dall'ordinamento indotto.*

Detto altrimenti, una catena di A è un suo sottoinsieme totalmente ordinato.

Definizione (Segmento iniziale)**.** *Dato un insieme parzialmente ordinato $(A, \leq)$ si dice che un sottoinsieme S di A è un* ***segmento iniziale*** *di A se per ogni $x \in S$ e per ogni $y \in A$ vale $(y \in A \wedge y < x) \to y \in S$.*

Esempio. Se $(A, \leq)$ è un insieme parzialmente ordinato, allora per ogni $a \in A$ l'insieme $A_a := \{x \in A \mid x < a\}$ è un segmento iniziale di A, detto ***segmento iniziale generato*** da a.

Inoltre $\emptyset$ è un segmento iniziale di A, e (se A è totalmente ordinato) è generato se e solo se A ha minimo.

Oss. In generale non tutti i segmenti iniziali di un insieme parzialmente ordinato sono generati, per esempio in $(\mathbb{Q}, \leq)$ (che è pure totalmente ordinato) si ha che $S := \{x \in \mathbb{Q} \mid x^2 < 2\} \cup \mathbb{Q}_{\leq 0}$ è un segmento iniziale, ma non è generato.

Inoltre A è sempre un segmento iniziale di se stesso, ma non è mai generato.

Definizione (Buon ordine)**.** *Un insieme totalmente ordinato $(A, \leq)$ è detto* ***bene ordinato*** *o* ***buon ordine*** *se ogni suo sottoinsieme non vuoto ha minimo.*

Esempio. Quando si sarà definito l'insieme dei numeri naturali col suo ordinamento standard, si vedrà che si tratta di un insieme bene ordinato.

Oss. Ogni sottoinsieme di un insieme bene ordinato è bene ordinato dall'ordine indotto.

Si afferma fin da ora l'importanza dei buoni ordini: tutto il corso è sostanzialmente basato sul concetto di insieme bene ordinato.

Definizione (Sottoinsieme denso)**.** *Dato un insieme totalmente ordinato $(A, \leq)$ e un suo sottoinsieme B, si dice che B è* ***denso*** *in A se per ogni $a_1, a_2 \in A$ tali che $a_1 < a_2$ esiste $b \in B$ per cui $a_1 < b < a_2$.*

Esempio. Si vedrà nel capitolo 6 che $\mathbb{Q}$ è denso in $\mathbb{R}$.

Si passa ora allo studio delle funzioni. La prima cosa importante da osservare è il fatto che quello che siamo soliti considerare il "codominio" di una funzione non è una nozione intrinseca della funzione stessa, in quanto per codominio si può scegliere un qualsiasi insieme B che contenga l'immagine della funzione.

D'ora in avanti, con $f\colon A \to B$ si intende che f è una funzione con dominio A e $\mathcal{I}m\, f \subseteq B$. In questo caso si dice che B è il ***codominio*** di f.

(*) Come si è fatto per il prodotto cartesiano, è facile provare l'esistenza dell'insieme di tutte e sole le funzioni da A in B, che si denota $\mathcal{F}un(A, B)$ o talvolta B^A.

Definizione (Iniettività, surgettività, bigettività)**.** *Si dice che una funzione $f\colon A \to B$ è:*

- ***iniettiva*** *se per ogni $x, y \in A$ vale $x \neq y \to f(x) \neq f(y)$, cioè se "manda elementi distinti in elementi distinti";*
- ***surgettiva*** *se $\mathcal{I}m\, f = B$;*
- ***bigettiva*** *se è sia iniettiva che surgettiva.*

Oss. Si noti che l'iniettività è una proprietà intrinseca di una funzione, mentre la surgettività dipende dal codominio scelto.

Spesso per dimostrare l'iniettività di una funzione fa comodo usare la seguente definizione equivalente: $f\colon A \to B$ è iniettiva se e solo se per ogni $x, y \in A$ vale $f(x) = f(y) \to x = y$.

Una funzione bigettiva è anche detta ***bigezione*** e talvolta ***corrispondenza biunivoca***.

Definizione (Funzione composta)**.** *Date due funzioni f e g tali che $\mathcal{I}m\, g \subseteq \mathcal{D}om\, f$ si definisce **funzione composta** di f e g la funzione $f \circ g := \{(x, z) \in \mathcal{D}om\, g \times \mathcal{I}m\, f \mid \exists y (x, y) \in g \wedge (y, z) \in f\}$.*

Oss. È facile provare che la funzione composta è effettivamente una funzione.

Definizione (Funzione identica o identità)**.** *Dato un insieme A si definisce **funzione identica** su A l'insieme $id_A := \{(x, x) \mid x \in A\}$.*

Definizione (Funzione inversa)**.** *Date due funzioni $f\colon A \to B$ e $g\colon B \to A$, si dice che g è la **funzione inversa** di f se $f \circ g = id_B$ e $g \circ f = id_A$. In tal caso si dice che f è **invertibile**.*

*In particolare g è detta **inversa destra** se $f \circ g = id_B$ e **inversa sinistra** se $g \circ f = id_A$.*

Oss. La funzione inversa, se esiste, è unica.

È facile provare che una funzione ha un'inversa sinistra se e solo se è iniettiva.

Se una funzione ha inversa destra allora è surgettiva e nel capitolo 9 si proverà l'equivalenza fra l'Assioma di scelta e l'esistenza di una inversa destra per una funzione surgettiva.

È altrettanto semplice dimostrare che un'inversa destra è iniettiva e un'inversa sinistra è surgettiva e che una funzione è invertibile se e solo se è bigettiva.

Definizione (Restrizione di una funzione)**.** *Data una funzione $f\colon A \to B$ e un sottoinsieme A' di A, si dice* ***restrizione*** *di f ad A' la funzione $f_{|A'} := \{(x,y) \in f \mid x \in A'\}$ e si scrive $f(A')$ al posto di $\mathcal{I}m\, f_{|A'}$.*

Solitamente in matematica, quando si definisce una nuova struttura, si dà un nome alle funzioni che conservano quella determinata struttura, e così si fa anche per gli insiemi ordinati, ottenendo una cosa molto familiare, cioè le funzioni crescenti.

Definizione (Funzione crescente)**.** *Dati due insiemi parzialmente ordinati $(A,\leq)$ e $(B,\leq)$, si dice che una funzione $f\colon A \to B$ è* ***debolmente crescente*** *se per ogni $a,b \in A$ vale $a < b \to f(a) \leq f(b)$. Si dice che f è* ***strettamente crescente*** *se per ogni $a,b \in A$ vale $a < b \to f(a) < f(b)$.*

Oss. È banale osservare che "strettamente crescente" $\to$ "debolmente crescente e iniettiva".

Definizione (Isomorfismo d'ordine)**.** *Dati due insiemi parzialmente ordinati $(A,\leq)$ e $(B,\leq)$, si dice che una funzione strettamente crescente $f\colon A \to B$ è un* ***isomorfismo d'ordine*** *(o più semplicemente "isomorfismo") se è surgettiva (e quindi bigettiva). In questo caso A e B sono detti* ***isomorfi****.*

Se $A = B$ si dice che f è un ***automorfismo*** *di A.*

Oss. Come in ogni isomorfismo, due insiemi ordinati isomorfi differiscono soltanto per il nome dei loro elementi, ma identificano esattamente la stessa struttura di insieme ordinato.

Definizione (Funzioni compatibili)**.** *Due funzioni f e g si dicono* ***compatibili*** *se per ogni $x \in \mathcal{D}om\, f \cap \mathcal{D}om\, g$ vale $f(x) = g(x)$.*

Proposizione 4.1. *"Unione di funzioni compatibili è una funzione".*

Formalmente, se X è una famiglia di funzioni mutualmente compatibili, allora $F := \bigcup X$ è una funzione e $\mathcal{D}om\, F = \bigcup\{\mathcal{D}om\, f \mid f \in X\}$.

Dim. Si deve provare che $\bigcup X$ è una funzione, cioè una relazione binaria univoca. Il fatto che $\bigcup X$ è una relazione binaria è banale perché ogni suo elemento, appartenendo ad una certa funzione di X, deve essere una coppia ordinata.

L'univocità è una diretta conseguenza della mutua compatibilità delle funzioni in X.

Per provare $\mathcal{D}om\, F = \bigcup\{\mathcal{D}om\, f \mid f \in X\}$ si deve solo provare l'esistenza di quest'ultimo, perché l'uguaglianza è del tutto scontata, e questo deriva dal fatto che per ogni $f \in X$ vale $\mathcal{D}om\, f \in \mathcal{P}(\bigcup\bigcup\bigcup X)$ □

Definizione (Operazione)**.** *Dato un insieme A, si dice* ***operazione*** *su A ogni funzione di dominio $A \times A$ e codominio A.*

5 Naturali di Von Neumann

Indotti dall'idea che un numero naturale debba essere un rappresentante per tutti gli insiemi che hanno proprio quell'esatto numero di elementi, si usa il concetto di insieme induttivo per arrivare ad avere $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$,..., $n+1 = n \cup \{n\}$, in modo che ciascuno abbia un numero di elementi pari alla quantità desiderata.

L'Assioma dell'infinito garantisce l'esistenza di un insieme induttivo X: dunque per separazione esiste il più piccolo insieme induttivo, cioè

$$\omega := \{n \in X \mid \forall Y(\text{“}Y \text{ è induttivo”} \ \to n \in Y)\}$$

È banale provare che ω è un insieme induttivo e che è il più piccolo (per contenimento).

Definizione (Numero naturale)**.** *L'insieme ω definito sopra è detto* ***insieme dei numeri naturali di Von Neumann*** *e i suoi elementi sono detti* ***numeri naturali****.*

Per ogni $n \in \omega$ il numero naturale $n \cup \{n\}$ è detto ***successore*** *di n e denotato $\hat{n}$.*

La funzione $\hat{}: \omega \to \omega$ è detta ***funzione successore*** *su ω.*

Oss. Nel capitolo 8 si proverà che l'immagine della funzione successore su ω è $\omega \setminus \{\emptyset\}$ e che ogni naturale $n \neq \emptyset$ si ottiene da esso iterando un certo numero di volte la funzione successore.

Inoltre si pone $0 = \emptyset$, $1 = \hat{0} = \{\emptyset\}$, $2 = \hat{1} = \{\emptyset, \{\emptyset\}\}$ e cosi via...

Il Teorema seguente è la caratteristica fondamentale dei numeri naturali, e sicuramente non si potrebbe parlare di matematica senza di esso.

Teorema 5.1 (Induzione al primo ordine)**.** *Per ogni proprietà $P(x)$ del linguaggio della Teoria degli Insiemi, se valgono:*

- $P(0)$*;*
- $\forall n \in \omega \ P(n) \to P(\hat{n})$*;*

allora vale $P(n)$ per ogni naturale n.

Dim. Se $A := \{n \in \omega \mid P(n)\}$, allora basta provare che A è induttivo e questa è proprio l'ipotesi. □

Teorema 5.2 (Induzione al secondo ordine)**.** *Se $A \subseteq \omega$ è tale che $0 \in A$ ed è chiuso per successore, allora $A = \omega$.*

Dim. A è un insieme induttivo per ipotesi, dunque $A = \omega$ perché ω è per definizione il più piccolo fra gli insiemi induttivi. □

Oss. È banale osservare che l'induzione al secondo ordine implica quella del primo ordine.

Ciononostante di qui in avanti con induzione si intenderà l'induzione al primo ordine, mentre quella del secondo sarà sempre precisata prima di essere utilizzata.

Definizione (Insieme transitivo)**.** *Un insieme X è detto* ***transitivo*** *se ogni suo elemento è un suo sottoinsieme, cioè se $X \subseteq \mathcal{P}(X)$ o equivalentemente $\bigcup X \subseteq X$. In formule*

$$\text{“}X \text{ è transitivo”} \leftrightarrow \forall y \forall z (y \in z \in X \to y \in X)$$

Proposizione 5.1. *(*) L'insieme ω è transitivo, cioè per ogni $n \in m \in \omega$ vale $n \in \omega$. Verbalmente “ogni elemento di un numero naturale è un numero naturale”.*

Dim. Per induzione su m:

- se $m = 0$ allora la proprietà è vera a vuoto;
- $\mathrm{P}(m) \to \mathrm{P}(\hat{m})$: sia $n \in \hat{m} \in \omega$, allora $n = m$ o $n \in m$. Se $n = m$ allora $n \in \omega$ perché $m \in \omega$. Se $n \in m$ allora si conclude per ipotesi induttiva.

□

Proposizione 5.2. *(*) La relazione $\in$ in ω è transitiva, cioè per ogni $n, m, k \in \omega$ vale l'implicazione $n \in m \in k \to n \in k$.*

Dim. Per induzione su k:

- se $k = 0$ allora la proprietà è vera a vuoto.
- $\mathrm{P}(k) \to \mathrm{P}(\hat{k})$: sia $n \in m \in \hat{k}$, allora $m \in k \cup \{k\}$. Se $m = k$ allora $n \in k$ perché $n \in m$. Se $m \in k$ allora si conclude per l'ipotesi induttiva.

□

Oss. Questo prova che ogni naturale di Von Neumann è un insieme transitivo, e, quando si sarà dimostrato che $(\omega, \in)$ è un insieme parzialmente ordinato, che $(n, \in)$ è un segmento iniziale di ω.

Proposizione 5.3. *(*) Per ogni $n, m \in \omega$ vale l'implicazione $n \in m \to \hat{n} \in \hat{m}$.*

Dim. Per induzione su m:

- se $m = 0$ allora la proprietà è vera a vuoto.

- P(m)→P($\hat{m}$): se $n \in \hat{m}$ allora $n = m$ o $n \in m$. Se $n = m$ allora $\hat{n} \in \hat{\hat{n}} = \hat{\hat{m}}$. Se $n \in m$ allora $\hat{n} \in \hat{m}$ per ipotesi induttiva. Inoltre è banale osservare che $\hat{m} \in \hat{\hat{m}}$ e dunque $\hat{n} \in \hat{\hat{m}}$ per transitività.

□

Oss. Quando si sarà provato che $\in$ è una relazione d'ordine su ω, la Proposizione 13.7 affermerà la stretta crescenza della funzione successore.

Proposizione 5.4. *(*) La relazione $\in$ in ω è irriflessiva, cioè per ogni $n \in \omega$ vale $n \notin n$.*

Dim. Per induzione su n:

- se $n = 0$ allora $0 \notin 0$ perché $0 = \emptyset$ per definizione.
- P(n)→P($\hat{n}$): se per assurdo $\hat{n} \in \hat{n}$ allora $\hat{n} = n$ o $\hat{n} \in n$. Nel primo caso $n \in n$, che è assurdo per l'ipotesi induttiva. Per transitività anche nel secondo caso si ottiene l'assurdo $n \in n$.

□

Proposizione 5.5. *(*) Per ogni $n, m \in \omega$ vale la doppia implicazione $n \in m \leftrightarrow n \subsetneq m$.*

Dim. $\rightarrow$: la transitività di $\in$ fra numeri naturali prova che se $n \in m$ allora $n \subseteq m$ e l'irriflessività garantisce che il contenimento è stretto.

$\leftarrow$: per induzione su m.

- se $m = 0$ allora la proprietà è vera a vuoto.
- P(m)→P($\hat{m}$): se $n \subsetneq \hat{m}$ e $m \notin n$ allora $n \subsetneq m$ e si conclude per l'ipotesi induttiva. Se $m \in n$ allora $m \subsetneq n$ per quanto provato al punto precedente, da cui segue $\hat{m} \subseteq n$ (*Assurdo*).

□

Proposizione 5.6. *(*) La relazione $\in$ è un ordinamento totale stretto su ω.*

Dim. Le proprietà irriflessiva e transitiva di $\in$ tra numeri naturali sono già state provate nelle proposizioni precedenti. Resta solo da dimostrarne la totalità, per la quale sarà fondamentale la proposizione 5.5.

La dimostrazione procede per induzione su n:

- se $n = 0$ allora sono possibili due casi. Se $m = 0$ allora $n = m$, altrimenti $0 \subsetneq m$ e per la proposizione 5.5 si ottiene $0 \in m$.
- P(n)→P($\hat{n}$): per ipotesi induttiva n e m sono confrontabili. Se $m \in n$ allora $m \in \hat{n}$ per transitività. Se $m = n$ allora $m \in \hat{n}$ perché $n \in \hat{n}$. Se $n \in m$ allora $n \subsetneq m$ e $n \cup \{n\} \subseteq m$, cioè $\hat{n} = m$ o $\hat{n} \in m$.

□

Quando si è dimostrato il principio di induzione, lo si è fatto, sia nel caso al primo ordine sia in quello al secondo ordine, facendo riferimento alle cosiddette "forme deboli".

Però di entrambe esiste anche una "forma forte": per esempio nel caso al primo ordine si ha che "se per ogni $n \in \omega$ vale l'implicazione $\forall k \in n\ P(k) \to P(n)$, allora vale $P(m)$ per ogni naturale m".

Il lettore provi a dimostrarla usando la forma debole dell'induzione al primo ordine e provi a formulare e a dimostrare anche quella al secondo ordine.

Proposizione 5.7. *(*) La coppia $(\omega, \in)$ è un insieme bene ordinato.*

Dim. Si è già provato nelle proposizioni precedenti che $\in$ è un ordinamento totale stretto su ω. Resta solo da dimostrare che si tratta di un buon ordine, cioè che ogni sottoinsieme non vuoto di ω ha minimo.

Sia dunque $A \subseteq \omega$ un sottoinsieme non vuoto. Se per assurdo A non ha minimo, allora $0 \in \omega \setminus A$ perché si è già visto che per ogni $n \in \omega$ vale $0 \in n$. Inoltre se per ogni $n \in m$ si ha $n \in \omega \setminus A$, allora si ottiene $m \in \omega \setminus A$ perché altrimenti m sarebbe minimo in A.

Per induzione forte (al secondo ordine) si ottiene $\omega \setminus A = \omega$, cioè $A = \emptyset$ (*Assurdo*). □

Oss. Per ogni naturale n la coppia $(n, \in)$ è un insieme bene ordinato perché n è un sottoinsieme di ω.

Definizione (Successioni e I-sequenze)**.** *Si dice* ***successione*** *una qualsiasi funzione di dominio ω.*

Più in generale, dato un insieme I, una qualsiasi funzione di dominio I è detta ***I-sequenza****.*

Oss. Talvolta la definizione di successione è adottata anche per funzioni che hanno per dominio $\omega \setminus n$ dove n è un numero naturale, cioè successioni che sono definite "da un certo punto in poi".

Fino a questo momento non si sono mai usate quelle che al lettore dovrebbero essere già note da altri corsi come "successioni definite per ricorrenza". Tuttavia nei capitoli che seguono e in generale in tutta la matematica queste sono uno strumento molto potente ed è dunque una buona notizia il fatto che possano essere formalizzate senza alcun problema all'interno di ZFC.

Il Teorema di ricorsione numerabile serve proprio a questo e nella parte rimanente del capitolo lo si enuncia in due forme diverse (una debole e una forte) e si dimostra solo la prima (l'altra dimostrazione è essenzialmente identica).

Teorema 5.3 (Teorema di ricorsione numerabile (forma debole))**.** *Per ogni insieme A, per ogni $f\colon \omega \times A \to A$ e per ogni $a \in A$ esiste un'unica funzione $g\colon \omega \to A$ tale che $g(0) = a$ e per ogni $n \in \omega$ vale $g(n+1) = f(n+1, g(n))$.*

Dim. La dimostrazione può essere suddivisa in 4 passi.

- PASSO 1: si chiama n-approssimazione finita relativa a f e a una funzione (se esiste) $g^{(n)}\colon n+1 \to A$ tale che $g^n(0) = a$ e per ogni $m+1 \in n+1$ valga $g^n(m+1) = f(m+1, g^n(m))$. Ora si dimostra per induzione su n che per ogni $n \in \omega$ esiste ed è unica l'n-approssimazione finita relativa a f e a:

  - se $n = 0$ allora la coppia $\{(0, a)\}$ è la 0-approssimazione finita cercata. È banalmente unica.
  - P(n)→P($\hat{n}$): se $g^{(n)}$ è l'unica n-approssimazione finita relativa a f e a (per ipotesi induttiva), allora la si estende a una funzione $g^{(n+1)}\colon n+2 \to A$ ponendo $g^{(n+1)}(n+1) = f(n+1, g^{(n)}(n))$. Questa è banalmente una $(n+1)$-approssimazione finita relativa a f e a. L'unicità segue dal fatto che se ne esistesse un'altra, allora per ipotesi induttiva coinciderebbero sui naturali fino a n compreso (perché la restrizione a $n+1$ è l'unica n-approssimazione finita) e quindi anche su $n+1$ per la regola ricorsiva.

- PASSO 2: si dimostra che esiste l'insieme di tutte e sole le approssimazioni finite relative a f e a. Per far ciò è comodo dimostrare prima l'esistenza dell'insieme $\bigcup_{n\in\omega} A^n$, cioè l'insieme di tutte e sole le funzioni di dominio un numero naturale e codominio A.

  Banalmente

  $$\bigcup_{n\in\omega} A^n = \{\varphi \in \mathcal{P}(\omega \times A) \mid \varphi \text{ è una funzione e } \exists n \in \omega\, \mathcal{D}om\, \varphi = n\}$$

  e il secondo insieme esiste per separazione (la proprietà richiesta potrebbe essere formalizzata come formula del linguaggio).

  Ora si pone AF:= $\{\varphi \in \bigcup_{n\in\omega} A^n \mid \varphi \text{ è un'approssimazione finita}\}$, ottenendo l'insieme cercato.

- PASSO 3: si dimostra che $g := \bigcup \mathrm{AF}$ è una funzione con le proprietà richieste nel Teorema. Si dovrebbe dimostrare per induzione (banale) che le approssimazioni finite sono mutualmente compatibili. Poiché l'unione di funzioni compatibili è una funzione (proposizione 4.1), si ottiene che g è una funzione. Per ogni $n+1 \in \omega$ si ha che g coincide con $g^{(n+1)}$ su $n+2$ e dunque $g(n+1) = g^{(n+1)}(n+1) = f(n+1, g^{(n+1)}(n) = f(n+1, g(n))$. Pertanto g ha le proprietà ricercate.

- PASSO 4: si dimostra per induzione su n che due funzioni con le proprietà richieste nel Teorema coincidono su ogni n e dunque sono uguali. Siano g_1 e g_2 due funzioni con le proprietà suddette:
  - se $n = 0$ allora $g_1(0) = g_2(0) = a$.
  - $\mathrm{P}(n) \to \mathrm{P}(\hat{n})$: $g_1(n+1) = f(n+1, g_1(n)) = f(n+1, g_2(n)) = g_2(n+1)$.

□

Oss. Nella forma appena dimostrata il Teorema non è sufficiente per garantire l'esistenza di funzioni ricorsive che richiamano al passo $(n+1)$-esimo qualche cosa in funzione non solo del passo precedente, ma anche degli altri passi. Per esempio non è garantita l'esistenza della successione di Fibonacci. È invece garantita l'esistenza di funzioni come il fattoriale, dove $f\colon \omega \times \omega \to \omega$ è il prodotto fra numeri naturali e $a = 1$.

Per questo motivo esiste anche una forma forte del Teorema.

Teorema 5.4 (Teorema di ricorsione numerabile (forma forte))**.** *Per ogni insieme A, per ogni $f\colon \omega \times \bigcup_{n\in\omega} A^n \to A$ esiste un'unica funzione $g\colon \omega \to A$ tale che $g(0) = a$ e $g(n+1) = f(n+1, g_{|n+1})$.*

Dim. La dimostrazione è essenzialmente la stessa della versione in forma debole, pertanto si rimanda a quella. □

Va aggiunta la falsa induzione (cioè il giochino per cui sembrerebbe di poter dimostrare che "se in un gruppo di persone una è femmina allora sono tutte femmine", e altre robe simili).

6 Numeri interi, razionali e reali

$\mathcal{L}$'idea inizialmente era quella di mostrare come si possono definire all'interno di ZFC gli usuali insiemi numerici $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ con le loro proprietà algebriche e d'ordinamento, ma l'argomento è stato a malapena accennato a lezione e nel caso dei numeri reali si tratta pure di un lavoro non poco impegnativo (almeno dal punto di vista del tempo da spenderci).

Dunque, a causa degli esami imminenti, si preferisce omettere questa parte (che un matematico deve comunque pur fare prima o poi nella sua vita) e si rimanda alle dispense del prof. Mauro Di Nasso chi volesse approfondire la questione.

Proprio per l'importanza dell'argomento (anche se fuoriesce quasi completamente dal programma svolto a lezione) si è deciso di lasciare questo capitolo in questo punto perché lo si ritiene il giusto momento nello studio di questa dispensa per approfondire la questione degli insiemi numerici e si ritiene che, qualora lo si fosse omesso, il lettore sarebbe stato ingiustamente indotto a trascurarlo.

Per questo motivo da qui in avanti si useranno gli insiemi numerici come si è sempre stati abituati a fare, mentre le operazioni aritmetiche sui naturali saranno definite per bene nel capitolo 8. Inoltre si scriverà equivalentemente $\mathbb{N}$ al posto di ω.

7 Cardinalità senza cardinali

"$\mathcal{A}$vere lo stesso numero di elementi" è un concetto che, almeno per gli insiemi finiti (ancora da definire), è piuttosto semplice da spiegare e anche da formalizzare matematicamente. L'idea è quella dell'esistenza di una bigezione fra i due insiemi e l'intuito spinge ad accettare questa definizione anche nel caso di insiemi infiniti (anch'essi sempre da definire), pertanto si dà la seguente

Definizione (Equipotenza)**.** *Si dice che due insiemi A e B sono* ***equipotenti*** *o che* ***hanno la stessa cardinalità*** *se sono in bigezione, cioè se esiste una funzione $f\colon A \to B$ bigettiva. In questo caso si scrive $|A| = |B|$.*

Esempio. È banale osservare che $\mathbb{N}$ e $2\mathbb{N}$ sono equipotenti, pur essendo $2\mathbb{N}$ un sottoinsieme proprio di $\mathbb{N}$.

Oss. "Essere equipotenti" fra insiemi ha le proprietà di relazione di equivalenza (banale), ma non è una vera e propria relazione di equivalenza perché il suo dominio sarebbe l'"insieme di tutti gli insiemi $\mathcal{V}$", che non può esistere (si veda poco più avanti il Paradosso di Cantor).

È per questo motivo che non abbiamo a disposizione (almeno per il momento) dei rappresentanti canonici per l'equipotenza (nemmeno usando l'Assioma di scelta, come potremmo fare per una relazione di equivalenza qualsiasi (capitolo 9)) e gran parte del lavoro che seguirà sarà sviluppato proprio per ottenere questi rappresentanti.

Allo stesso modo dell'equipotenza, l'intuito suggerisce che un sottoinsieme di un certo insieme dato ha al più tanti elementi quanti quelli dell'insieme stesso, dunque si dà la seguente

Definizione (Ordine fra "cardinalità")**.** *Dati due insiemi A e B, si dice che la cardinalità di A è* ***minore o uguale*** *di quella di B (e si scrive $|A| \leq |B|$) se esiste una funzione iniettiva da A in B, o equivalentemente se A è equipotente a un sottoinsieme di B.*

Esempio. È banale osservare che per ogni insieme X vale $|X| \leq |\mathcal{P}(X)|$.

Oss. Questo $\leq$ fra cardinalità gode delle proprietà di ordine parziale largo, in quanto la riflessività e la transitività sono ovvie, mentre l'antisimmetria è data dal Teorema di Cantor-Bernstein, che dimostreremo fra poco. Tuttavia non si tratta di una vera relazione d'ordine perché il suo dominio sarebbe l'insieme di tutti gli insiemi $\mathcal{V}$.

Inoltre si proverà nel Capitolo 12 che l'Assioma di scelta è equivalente alla totalità di questa "relazione" d'ordine, cioè che, dati due insiemi A e B, vale sempre almeno una fra $|A| \leq |B|$ e $|B| \leq |A|$.

Il seguente Lemma è la parte "difficile" del Teorema di Cantor-Bernstein.

Lemma 7.1. *Dati tre insiemi X, Y e Z, se $X \subseteq Y \subseteq Z$ e $|X| = |Z|$, allora $|X| = |Y| = |Z|$.*

Dim. Se $f\colon Z \to X$ è una bigezione, si definisce per ricorsione numerabile la seguente successione:

$$\begin{cases} E_0 = Z \setminus Y \\ E_{n+1} = f(E_n) \end{cases}$$

Posto $E := \bigcup_{n\in\omega} E_n$, si verifica facilmente che la funzione

$$\begin{aligned} \varphi\colon Z &\to Y \\ z &\mapsto \begin{cases} f(z) \text{ se } z \in E \\ z \text{ altrimenti} \end{cases} \end{aligned}$$

è una bigezione, da cui la tesi. □

Teorema 7.1 (Cantor-Bernstein)**.** *Dati due insiemi A e B, se $|A| \leq |B|$ e $|B| \leq |A|$ allora $|A| = |B|$.*

Dim. Siano $f\colon A \to B$ e $g\colon B \to A$ due funzioni iniettive. Ora $g(f(A)) \subseteq g(B) \subseteq A$ e dall'iniettività di f e g si ha anche $|g(f(A))| = |A|$. Per il Lemma 7.1 si ottiene $|g(B)| = |A|$, da cui $|B| = |A|$ per l'iniettività di g. □

Il Teorema seguente mostra che dato un insieme ne esiste sempre uno più grande, dunque non esiste una "cardinalità massima".

Teorema 7.2 (Cantor)**.** *Per ogni insieme X non esistono funzioni surgettive $X \to \mathcal{P}(X)$. In particolare vale $|X| < |\mathcal{P}(X)|$.*

Dim. Se per assurdo esiste $f\colon X \to \mathcal{P}(X)$ surgettiva, allora, posto $A := \{x \in X \mid x \notin f(x)\}$, si ha che esiste $y \in X$ tale che $A = f(y)$. Dunque $y \in f(y) \leftrightarrow y \in A \leftrightarrow y \notin f(y)$ (*Assurdo*). □

Oss (Paradosso di Cantor). Non esiste l'insieme di tutti gli insiemi $\mathcal{V}$, perché altrimenti si avrebbe $|\mathcal{V}| < |\mathcal{P}(\mathcal{V})| \leq |\mathcal{V}|$ (*Assurdo*).

Le seguenti sono alcune semplici proprietà delle cardinalità e sono state quasi tutte lasciate per esercizio a lezione.

Proposizione 7.1. *(*) Siano $|A| = |A'|$ e $|B| = |B'|$, allora:*

1. *se $A \cap B = A' \cap B' = \emptyset$, allora $|A \cup B| = |A' \cup B'|$;*
2. *$|A \times B| = |A' \times B'|$;*
3. *$|B^A| = |B'^{A'}|$.*

Dim. In tutta la dimostrazione siano $f\colon A \to A'$ e $g\colon B \to B'$ due bigezioni.

1. La seguente funzione

$$\varphi\colon A \cup B \to A' \cup B'$$
$$x \mapsto \begin{cases} f(x) & \text{se } x \in A \\ g(x) & \text{se } x \in B \end{cases}$$

è una bigezione.

2. La seguente funzione

$$\varphi\colon A \times B \to A' \times B'$$
$$(a, b) \mapsto (f(a), g(b))$$

è una bigezione.

3. La seguente funzione

$$\varphi\colon B^A \to B'^{A'}$$
$$\psi \mapsto g \circ \psi \circ f^{-1}$$

è una bigezione.

□

Oss. Valgono anche le rispettive disuguaglianze nel caso in cui si abbia $|A| \leq |A'|$ e $|B| \leq |B'|$.

Definizione (Funzione caratteristica)**.** *Dati un insieme A e un suo sottoinsieme Y, si dice* ***funzione caratteristica*** *di Y la funzione*

$$\chi_Y\colon A \to \{0, 1\}$$
$$a \mapsto \begin{cases} 0 \text{ se } a \notin Y \\ 1 \text{ se } a \in Y \end{cases}$$

Proposizione 7.2. *(*) Per ogni insieme A vale $|2^A| = |\mathcal{P}(A)|$, cioè esiste una corrispondenza biunivoca fra le funzioni caratteristiche dei sottoinsiemi di A e le sue parti.*

Dim. Una bigezione fra i due insiemi è banalmente quella che manda un sottoinsieme di A nella funzione caratteristica ad esso associata, cioè

$$f\colon \mathcal{P}(A) \to 2^A$$
$$B \mapsto \chi_B$$

□

Oss. Dalle due proposizioni precedenti segue l'implicazione $|A| = |B| \to |\mathcal{P}(A)| = |\mathcal{P}(B)|$ ed esibire una bigezione è del tutto banale.

Anche in questo caso, se $|A| \leq |B|$, si verifica facilmente la disuguaglianza $|2^A| \leq |2^B|$.

Inoltre, sebbene non rientri nelle possibilità di questo corso, può essere interessante sapere che l'enunciato $|\mathcal{P}(A)| = |\mathcal{P}(B)| \to |A| = |B|$ è indecidibile in ZFC.

Proposizione 7.3. *(*) Se $B \cap C = \emptyset$, allora $|A^B \times A^C| = |A^{B \cup C}|$.*

Dim. La seguente funzione

$$\begin{aligned} \varphi \colon A^B \times A^C &\to A^{B \cup C} \\ (f, g) &\mapsto \varphi_{f,g} \end{aligned}$$

$$\begin{aligned} \varphi_{f,g} \colon B \cup C &\to A \\ x &\mapsto \begin{cases} f(x) & \text{se } x \in B \\ g(x) & \text{se } x \in C \end{cases} \end{aligned}$$

è una bigezione. □

Proposizione 7.4. *(*) Dati tre insiemi A, B e C vale l'uguaglianza $|(A^B)^C| = |A^{B \times C}|$.*

Dim. La seguente funzione

$$\begin{aligned} \varphi \colon (A^B)^C &\to A^{B \times C} \\ f &\mapsto \varphi_f \end{aligned}$$

$$\begin{aligned} \varphi_f \colon B \times C &\to A \\ (b, c) &\mapsto (f(c))(b) \end{aligned}$$

è una bigezione. □

Si introducono finalmente le nozioni di "insieme finito" e "insieme infinito".

Definizione (Insieme finito/infinito)**.** *Un insieme A si dice **finito** se è in bigezione con un naturale di Von Neumann n. In tal caso si scrive $|A| = n$.*

*Si dice che A è **infinito** se non è finito.*

Lemma 7.2. *Se $n \in \omega$ e $m \in \hat{n}$ allora $|\hat{n} \setminus \{m\}| = |n|$.*

Dim. Per induzione su n:

- se $n = 0$ allora $\hat{n} = \{0\}$ e $m = 0$, da cui segue $\hat{n} \setminus \{m\} = 0$, e la proprietà è verificata.

- P(n)→P($\hat{n}$): sia $m \in \hat{\hat{n}}$. Se $m = \hat{n}$ allora $\hat{\hat{n}} \setminus \{m\} = \hat{n}$ e la proprietà è verificata.

  Se $m \neq \hat{n}$ allora $\hat{\hat{n}} \setminus \{\hat{n}, m\} = \hat{n} \setminus \{m\}$ e quest'ultimo è in bigezione con n per ipotesi induttiva. Per concludere basta estenderla a una bigezione $\hat{\hat{n}} \setminus \{m\} \to \hat{n}$ con $\hat{n} \mapsto n$.

□

Proposizione 7.5. *Se $|A| = n$ e $B \subsetneq A$ allora esiste $k \in n$ per cui $|B| = k$, e dunque "sottoinsiemi di insiemi finiti sono finiti".*

Dim. Per induzione su n:

- se $n = 0$ allora la tesi è vera a vuoto;
- P(n)→P($\hat{n}$): poiché $B \subsetneq A$ si ha che esiste $a \in A \setminus B$. Per il Lemma 7.2 vale $|A \setminus \{a\}| = |n|$. Se $B = A \setminus \{a\}$ allora si è concluso. Altrimenti la tesi è immediata conseguenza dell'ipotesi induttiva.

□

Proposizione 7.6. *(*) Per ogni $n, m \in \omega$ vale l'implicazione $|n| = |m| \to n = m$.*

Dim. Per induzione su n:

- se $n = 0$ allora la proprietà è banalmente vera perché l'unico insieme equipotente al vuoto è l'insieme vuoto stesso.
- P(n)→P($\hat{n}$): se $f \colon m \to \hat{n}$ è una bigezione, allora $m \neq 0$ perché altrimenti si avrebbe $\hat{n} = 0$, che è assurdo. Dunque esiste $k \in \omega$ tale che $m = \hat{k}$. Ora $f_{|k} \colon k \to \hat{n} \setminus \{f(k)\}$ è una bigezione e il codominio ha cardinalità n per il lemma 7.2. Dall'ipotesi induttiva segue $k = n$. Dunque $\hat{k} = m = \hat{n}$.

□

Oss. Nella dimostrazione precedente si è usato il fatto che ogni naturale diverso da 0 è un successore (facile induzione).

Corollario 7.1. *Ogni numero naturale non è in bigezione con un sottoinsieme proprio. (Lo stesso vale per ogni insieme finito).*

Oss. Si può già provare in vari modi che ω è un insieme infinito: uno di questi sarà dato dal fatto che la funzione "successore" è una bigezione fra ω e $\omega \setminus \{0\}$.

Inoltre, data una funzione $f \colon X \to X$ dove X è un insieme finito, si ha che f è iniettiva se e solo se è surgettiva se e solo se è bigettiva.

Si è inoltre provato che ogni insieme finito A è in bigezione con un unico naturale n, dunque si scrive $|A| = n$ e il problema di determinare dei rappresentanti per la "relazione" data dall'equipotenza è risolta nel caso finito.

Proposizione 7.7 (Principio dei cassetti)**.** *Se $n > m$ sono due numeri naturali, allora non esistono funzioni iniettive da n in m.*

Dim. L'immersione è un funzione iniettiva da m in n, dunque, se per assurdo esiste una funzione iniettiva da n in m, allora per Cantor-Bernstein si ottiene $|n| = |m|$, da cui segue $n = m$ per la proposizione 7.6 e questo è *Assurdo.* □

Proposizione 7.8. *(*) Se A e B sono insiemi finiti, con $|A| = n$ e $|B| = m$, allora sono finiti anche gli insiemi $A \cup B$, $A \cap B$, $A \setminus B$, $A \times B$, $\mathcal{P}(A)$, $f(A)$ dove f è una funzione di dominio A.*

Dim.

- $A \cup B$: per induzione su n.
  - se $n = 0$ allora $A = \emptyset$. Dunque $A \cup B = B$ è finito.
  - P(n)→P($\hat{n}$): se $f\colon \hat{n} \to A$ è una bigezione allora $f_{|n}\colon n \to A \setminus \{f(n)\}$ è una bigezione. Per ipotesi induttiva $(A \setminus \{f(n)\}) \cup B$ è finito, cioè esistono $k \in \mathbb{N}$ e $\varphi\colon (A \setminus \{f(n)\}) \cup B \to k$ bigezione. Se $f(n) \in B$ allora si è concluso. Altrimenti si considera la funzione $\varphi^*\colon A \cup B \to \hat{k}$ che coincide con φ su $(A \setminus \{f(n)\}) \cup B$ e manda $f(n)$ in k. Questa è una bigezione.
- $A \cap B$ e $A \setminus B$ sono finiti perché sono sottoinsiemi di insiemi finiti.
- $A \times B$: per induzione su n.
  - se $n = 0$ allora $A \times B$ è vuoto e dunque finito.
  - P(n)→P($\hat{n}$): $\hat{n} \times m = (n \times m) \cup (\{n\} \times m)$. Il primo insieme di questa unione è finito per ipotesi induttiva e l'altro perché è banalmente equipotente ad m. Si conclude usando quanto già dimostrato sull'unione di due insiemi finiti.
- $\mathcal{P}(A)$: per induzione su n.
  - se $n = 0$ allora $\mathcal{P}(A) = \{0\} = 1$ è finito.
  - P(n)→P($\hat{n}$): la funzione

$$f\colon \mathcal{P}(\hat{n}) \to \mathcal{P}(n) \times \{0,1\}$$
$$A \mapsto \begin{cases} (A \cap n, 1) \text{ se } n \in A \\ (A \cap n, 0) \text{ altrimenti} \end{cases}$$

    è bigettiva e il suo codominio è finito per l'ipotesi induttiva e per quanto già dimostrato sul prodotto cartesiano di due insiemi finiti.

- $f(A)$: usando la finitezza di A e il buon ordine dei naturali si ottiene facilmente $|f(A)| \leq |A|$ e dunque $f(A)$ è finito perché in bigezione con un sottoinsieme di un insieme finito.

□

Proposizione 7.9. *(*) Se $\langle A_i \mid i \in n \rangle$ è una n-sequenza di insiemi finiti allora $\bigcup_{i \in n} A_i$ è un insieme finito, cioè "unione finita di insiemi finiti è finita".*

Dim. Per induzione su n:

- se $n = 0$ allora l'unione è vuota e dunque finita.
- $\mathrm{P}(n) \to \mathrm{P}(\hat{n})$: basta osservare che

$$\bigcup_{i \in \hat{n}} A_i = (\bigcup_{i \in n} A_i) \cup A_n$$

  e poi concludere usando l'ipotesi induttiva e la proposizione 7.8.

□

Definizione (Cardinalità numerabile)**.** *Un insieme X è detto **numerabile** se è equipotente a ω e si scrive $|X| = \aleph_0$.*

*Un insieme X è detto **più che numerabile** se $|\omega| < |X|$ e in questo caso si scrive $\aleph_0 < |X|$.*

*Un insieme X è detto **al più numerabile** se $|X| \leq |\omega|$ e in questo caso si scrive $|X| \leq \aleph_0$.*

Esempio. L'insieme dei numeri naturali pari è numerabile, mentre $\mathcal{P}(\mathbb{N})$ è più che numerabile per il Teorema di Cantor.

Inoltre per come sono stati definiti nel capitolo 6, gli insiemi $\mathbb{Z}$ e $\mathbb{Q}$ sono anch'essi numerabili, pur essendo $\mathbb{Q}$ un insieme denso in se stesso.

Nella proposizione seguente si denota con $[n, +\infty)_{\mathbb{N}}$ l'insieme dei numeri naturali maggiori o uguali a n, dove n è per l'appunto un certo numero naturale.

Proposizione 7.10. *Per ogni numero naturale n vale l'uguaglianza $|[n, +\infty)_{\mathbb{N}}| = \aleph_0$.*

Dim. Basta osservare che la funzione

$$\begin{aligned} f \colon \omega &\to [n, +\infty)_{\mathbb{N}} \\ m &\mapsto m + n \end{aligned}$$

è una bigezione. □

Proposizione 7.11. *(*) Se $A \subseteq \mathbb{N}$, allora A è finito o numerabile.*

Dim. Se A è finito allora si ha la tesi.

Sia dunque A infinito e siano $A \subseteq \mathbb{N}$, $a \in A$. Si definisce per ricorsione numerabile $a_0 = a$, $a_{n+1} = min(A \setminus \{a_0, a_1, \dots a_n\})$. Allora $\langle a_n \mid n \in \mathbb{N} \rangle$ è ben definita perché A è infinito ed è una funzione iniettiva da $\mathbb{N}$ in A. Si conclude usando Cantor-Bernstein e osservando che l'inclusione $i \colon A \to \mathbb{N}$ è iniettiva. □

Oss. È importante osservare che non è necessario l'Assioma di scelta perché il "minimo" è una funzione di scelta su $\mathcal{P}(\mathbb{N})$.

Si è inoltre dimostrato che un insieme è al più numerabile se e solo se è finito o numerabile.

Proposizione 7.12. *(*) L'unione di due insiemi numerabili è numerabile.*

Dim. Per la proposizione 7.1 si possono considerare l'insieme dei numeri naturali pari e quello dei numeri naturali dispari, che sono disgiunti e numerabili (per la proposizione 7.11, visto che sono banalmente infiniti) e la loro unione è $\mathbb{N}$. □

Oss. Se gli insiemi della proposizione precedente non sono disgiunti, la tesi resta banalmente vera.

Il Teorema seguente ha un'importanza enorme in Teoria degli insiemi e sarà in seguito generalizzato (con l'uso dell'Assioma di scelta) a tutti gli insiemi infiniti. Per la sua importanza se ne danno due dimostrazioni diverse, la prima è quella più nota e fornisce una bigezione vera e propria fra $\mathbb{N} \times \mathbb{N}$ e $\mathbb{N}$, mentre la seconda usa il Teorema fondamentale dell'aritmetica e conclude col Teorema di Cantor-Bernstein.

Teorema 7.3. *Vale l'equipotenza* $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.

Dim. 1. L'idea è quella di considerare $\mathbb{N} \times \mathbb{N}$ come un reticolo e di andare ad enumerarne i punti partendo da $(0,0)$ e seguendo le varie diagonali in una forma a "zig-zag" (cioè $(0,0)$, $(1,0)$, $(0,1)$, $(2,0)$, $(1,1)$, $(0,2) \dots$).

Il lettore provi a fare un disegno per avere ben chiara l'idea di questo procedimento.

Osservando che le coppie che stanno su una stessa diagonale hanno somma costante e che la diagonale in cui sta la coppia (n,m) ha $n + m + 1$ coppie, si ottiene facilmente la seguente bigezione

$$\begin{aligned} f \colon \mathbb{N} \times \mathbb{N} &\longrightarrow \mathbb{N} \\ (n,m) &\mapsto \frac{(n+m) \cdot (n+m+1)}{2} + m + 1 \end{aligned}$$

e dunque la tesi.

2. Si ha banalmente $|\mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}|$, dunque basta provare $|\mathbb{N} \times \mathbb{N}| \leq |\mathbb{N}|$ e concludere con Cantor-Bernstein.

   La funzione
   $$f \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$
   $$(n, m) \mapsto 2^n \cdot 3^m$$
   è iniettiva per il Teorema fondamentale dell'aritmetica, da cui la tesi. □

Oss. Per induzione si ottiene che per ogni $k \in \omega$ vale $|\mathbb{N}^k| = \aleph_0$.

Proposizione 7.13. *(*) Se $f \colon \mathbb{N} \to A$ è surgettiva, allora A è finito o numerabile.*

Dim. Basta provare che f ha un'inversa destra e anche stavolta sarà fondamentale il buon ordinamento dei naturali. Infatti un'inversa destra è in questo caso una funzione iniettiva da A in $\mathbb{N}$ e la tesi segue dalla proposizione 7.11.

Ponendo
$$g \colon A \to \mathbb{N}$$
$$a \mapsto min\,(f^{-1}(\{a\}))$$
si ottiene un'inversa destra di f.

Si noti che g è ben definita perché f è surgettiva. □

Oss. Per poter applicare la proposizione 7.13 basta avere una funzione surgettiva da un insieme numerabile all'insieme in questione.

È probabile che in questo capitolo si faccia uso un paio di volte di qualche forma equivalente dell'Assioma di scelta che sarà dimostrata nel capitolo 9.

Teorema 7.4. *(AC) Se $\langle A_i \mid i \in I \rangle$ è una famiglia di insiemi al più numerabili e $|I| \leq \aleph_0$, allora $\bigcup_{i \in I} A_i$ è al più numerabile, cioè "un'unione al più numerabile di insiemi al più numerabili è al più numerabile".*

Dim. Per l'Assioma di scelta (facile da formalizzare) si prende l'insieme $\mathcal{F} := \{f_i \mid i \in I\}$ dove per ogni i si ha che f_i è una funzione surgettiva da $\mathbb{N}$ in A_i. Inoltre esiste $\psi \colon \mathbb{N} \to I$ surgettiva.

Ora si definisce
$$\varphi \colon \mathbb{N} \times \mathbb{N} \to \bigcup_{i \in I} A_i$$
$$(n, m) \mapsto f_{\psi(n)}(m)$$
e si osserva che è una funzione surgettiva.

Si conclude con il Teorema 7.3 e la proposizione 7.13. □

Si introducono due notazioni utili nel resto della dispensa: da qui in avanti, dato un insieme A, si indica con $\mathcal{F}in\,A$ l'insieme dei sottoinsiemi finiti di A, e con $\mathcal{S}eq\,A$ l'insieme delle n-sequenze di A, dove n varia fra i numeri naturali.

Proposizione 7.14. *(*) Se $|A| = |B|$, allora $|\,\mathcal{F}in\,A| = |\,\mathcal{F}in\,B|$ e $|\,\mathcal{S}eq\,A| = |\,\mathcal{S}eq\,B|$.*

Dim. Se $f\colon A \to B$ è una bigezione, allora la funzione da $\mathcal{F}in\,A$ in $\mathcal{F}in\,B$ che manda X in $f(X)$ è una bigezione, e lo stesso vale per la funzione da $\mathcal{S}eq\,A$ in $\mathcal{S}eq\,B$ che manda la sequenza $(a_0, \dots, a_n)$ in $(f(a_0), \dots, f(a_n))$. □

Proposizione 7.15. *Vale $|\,\mathcal{F}in\,\mathbb{N}| = |\,\mathcal{S}eq\,\mathbb{N}| = \aleph_0$.*

Dim. Banalmente vale $\aleph_0 \leq |\,\mathcal{F}in\,\mathbb{N}|$ perché basta considerare i singoletti.

Inoltre $|\,\mathcal{F}in\,\mathbb{N}| \leq |\,\mathcal{S}eq\,\mathbb{N}|$ perché basta mandare un sottoinsieme finito nella sequenza che ha per coordinate i suoi elementi in ordine crescente.

Infine $|\,\mathcal{S}eq\,\mathbb{N}| = |\bigcup_{n\in\omega} \mathbb{N}^k| \leq \aleph_0$ per il Teorema 7.4.

Si conclude con Cantor-Bernstein. □

Proposizione 7.16. *(*) (AC) Ogni insieme infinito ha un sottoinsieme numerabile, e dunque (anche se per il momento non se ne potrebbe parlare) $\aleph_0$ è il più piccolo cardinale infinito.*

Dim. Siano A un insieme infinito e $f\colon \mathcal{P}(A) \to A$ una funzione di scelta su $\mathcal{P}(A)$.

Si definisce $a_0 = f(A)$, $a_{n+1} = f(A \setminus \{a_0, a_1, \dots a_n\})$ per ricorsione numerabile. Allora $\langle a_n \mid n \in \mathbb{N}\rangle$ è ben definita perché A è infinito ed è una bigezione $\mathbb{N} \to \{a_n\}_{n\in\mathbb{N}}$. □

Definizione (Insieme Dedekind-infinito)**.** *Un insieme A è detto **Dedekind-infinito** se è in bigezione con un suo sottoinsieme proprio.*

Esempio. L'insieme ω è Dedekind-infinito perché la funzione successore è una bigezione da ω in $\omega \setminus \{0\}$ (si vedrà nel Capitolo 8).

Proposizione 7.17. *(*) (AC) Se $B \subseteq A$, A è più che numerabile e $|B| = \aleph_0$, allora $|A \setminus B| = |A|$.*

Dim. Si verifica facilmente, poiché A è più che numerabile, che $A \setminus B$ è infinito e dunque ha un sottoinsieme numerabile C per la proposizione 7.16.

C può essere diviso in due sottoinsiemi entrambi numerabili (facile): siano essi C_1 e C_2.

Allora mandando bigettivamente B in C_1, C in C_2 e lasciando fissi tutti gli altri elementi di A, si ottiene una bigezione da A in $A \setminus B$. □

Proposizione 7.18. *(*) (AC) Un insieme è Dedekind-infinito se e solo se è infinito.*

Dim. $\rightarrow$: un insieme Dedekind-infinito è in bigezione con un suo sottoinsieme proprio. Per il corollario 7.1 si ha che l'insieme in questione non può essere finito, e dunque è finito.

$\leftarrow$: (AC) si è già dimostrato con l'Assioma di scelta che un insieme infinito A ha un sottoinsieme numerabile (proposizione 7.16). Se A è più che numerabile, allora si conclude con la proposizione 7.17. Se $|A| = \aleph_0$, allora è banale.

□

Definizione (Cardinalità del continuo)**.** *Si dice che un insieme X ha la cardinalità del continuo se è in bigezione con $\mathbb{R}$ e si scrive $|X| = \mathfrak{c}$.*

Proposizione 7.19. *Vale $|\mathcal{P}(\mathbb{N})| = \mathfrak{c}$.*

Dim. La funzione

$$\begin{aligned} \varphi\colon 2^{\mathbb{N}} &\to \mathbb{R} \\ \sigma &\mapsto \sum_{n=0}^{\infty} \frac{\sigma(n)}{10^n} \end{aligned}$$

è iniettiva, dunque $|\mathcal{P}(\mathbb{N})| = |2^{\mathbb{N}}| \leq |\mathbb{R}|$.

Inoltre la funzione

$$\begin{aligned} f\colon \mathbb{R} &\to \mathcal{P}(\mathbb{Q}) \\ r &\mapsto \{q \in \mathbb{Q} \mid q \leq r\} \end{aligned}$$

è iniettiva perché $\mathbb{Q}$ è denso in $\mathbb{R}$, e perciò $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})| = |\mathcal{P}(\mathbb{N})|$.

Si conclude con Cantor-Bernstein che vale $|\mathcal{P}(\mathbb{N})| = \mathfrak{c}$. □

Oss. Poiché $|\mathcal{P}(\mathbb{N})| = |2^{\mathbb{N}}| = \mathfrak{c}$, si scrive anche $\mathfrak{c} = 2^{\aleph_0}$ (in seguito sarà più che una semplice notazione).

Teorema 7.5. *Vale $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$.*

Dim. La tesi segue dalla seguente semplice catena di disuguaglianze:

$$|\mathbb{R}| \leq |\mathbb{R} \times \mathbb{R}| = |2^{\mathbb{N}} \times 2^{\mathbb{N}}| = |2^{A \cup B}| = |2^{\mathbb{N}}| = |\mathbb{R}|$$

dove A e B sono due insiemi numerabili disgiunti. □

Oss. Nello stesso modo si prova anche $|\mathbb{R} \times \mathbb{N}| = \mathfrak{c}$.

Si è inoltre provato che l'insieme dei numeri complessi $\mathbb{C}$ ha la cardinalità del continuo.

Proposizione 7.20. *Valgono le due uguaglianze $|\mathbb{R}^{\mathbb{N}}| = \mathfrak{c}$ e $|\mathbb{N}^{\mathbb{N}}| = \mathfrak{c}$*

Dim. Semplicemente $|\mathbb{R}^{\mathbb{N}}| = |(2^{\mathbb{N}})^{\mathbb{N}}| = |2^{\mathbb{N} \times \mathbb{N}}| = |2^{\mathbb{N}}| = \mathfrak{c}$.

La seconda segue dal fatto che $\mathfrak{c} = |(2^{\mathbb{N}})^{\mathbb{N}}| \geq |\mathbb{N}^{\mathbb{N}}| \geq |2^{\mathbb{N}}| = \mathfrak{c}$. □

Nella prossima proposizione si denota con $\mathcal{C}^0(\mathbb{R})$ l'insieme di tutte e sole le funzioni continue da $\mathbb{R}$ in $\mathbb{R}$.

Proposizione 7.21. *Vale* $|\mathcal{C}^0(\mathbb{R})| = \mathfrak{c}$.

Dim. Banalmente vale $\mathfrak{c} \leq |\mathcal{C}^0(\mathbb{R})|$ perché le costanti sono funzioni continue.

Per l'altra disuguaglianza è fondamentale un fatto topologico, ovvero che due funzioni continue che coincidono su un denso sono uguali. In particolare nel caso di $\mathbb{R}$ si ha che $\mathbb{Q}$ è un suo sottospazio denso, dunque le funzioni continue da $\mathbb{R}$ in $\mathbb{R}$ sono al più quante le funzioni da $\mathbb{Q}$ in $\mathbb{R}$, che sono $\mathfrak{c}$ per la proposizione 7.20.

Si conclude con Cantor-Bernstein. □

Nella proposizione seguente si indica con τ la topologia euclidea sun $\mathbb{R}^n$.

Proposizione 7.22. *Vale* $|\tau| = \mathfrak{c}$.

Dim. Banalmente vale $\mathfrak{c} \leq |\tau|$.

Inoltre dalla topologia si sa che $\mathbb{R}^n$ con la topologia euclidea è a base numerabile, dunque gli elementi di τ sono al più quanti i sottoinsiemi di un insieme numerabile, cioè $\mathfrak{c}$.

Si conclude con Cantor-Bernstein. □

Teorema 7.6. *(AC) Se* $\langle A_i \mid i \in I \rangle$ *è una famiglia di insiemi che hanno al più la cardinalità del continuo e* $|I| \leq \mathfrak{c}$*, allora* $\bigcup_{i \in I} A_i$ *ha al più la cardinalità del continuo.*

Dim. È identica a quella già vista per il caso numerabile. □

Proposizione 7.23. *Si ha* $|\mathcal{F}in\,\mathbb{R}| = |\mathcal{S}eq\,\mathbb{R}| = \mathfrak{c}$.

Dim. Banalmente vale $\mathfrak{c} \leq |\mathcal{F}in\,\mathbb{R}|$ perché basta considerare i singoletti.

Inoltre vale $|\mathcal{F}in\,\mathbb{R}| \leq |\mathcal{S}eq\,\mathbb{R}|$ perché basta ordinare gli elementi di ogni insieme finito in ordine crescente.

Infine si ha $|\mathcal{S}eq\,\mathbb{R}| \leq \mathfrak{c}$ perché è unione numerabile di insiemi che hanno la cardinalità del continuo (7.6).

Si conclude con Cantor-Bernstein. □

Dati due insiemi A e B tali che $|B| \leq |A|$ si indica con $[A]^{|B|}$ l'insieme di tutti e soli i sottoinsiemi di A di cardinalità $|B|$. Con $[A]^{\leq |B|}$ si intende l'insieme di tutti e soli i sottoinsiemi di A di cardinalità al più B.

Proposizione 7.24. *(*) Se* $|C| \leq |A| = |B|$*, allora si ha* $|[A]^{|C|}| = |[B]^{|C|}|$.

Dim. Se $f \colon A \to B$ è una bigezione, allora

$$\begin{aligned} \varphi \colon [A]^{|C|} &\to [B]^{|C|} \\ X &\mapsto f(X) \end{aligned}$$

è una bigezione. □

Proposizione 7.25. *(*) Se* $|C| \leq |B| \leq |A|$*, allora si ha* $|[B]^{|C|}| \leq |[A]^{|C|}|$.

Dim. Se $f\colon B \to A$ è una funzione iniettiva, allora

$$\begin{aligned} \varphi\colon [B]^{|C|} &\to [A]^{|C|} \\ X &\mapsto f(X) \end{aligned}$$

è iniettiva, da cui la tesi. □

Nel capitolo 13 verrà fornito un metodo molto semplice per calcolare la cardinalità degli insiemi del tipo $[A]^{|B|}$.

Proposizione 7.26. *Valgono le equipotenze* $|[\mathbb{R}]^{\aleph_0}| = |[\mathbb{R}]^{\leq \aleph_0}| = \mathfrak{c}$ *e* $|[\mathbb{R}]^{\mathfrak{c}}| = 2^{\mathfrak{c}}$.

Dim. Si ha $\mathfrak{c} = |\mathbb{R}^{\mathbb{N}}| \geq |[\mathbb{R}]^{\leq \aleph_0}| \geq |[\mathbb{R}]^{\aleph_0}| = |[\mathbb{R} \times \mathbb{N}]^{\aleph_0}| \geq \mathfrak{c}$ e si conclude con Cantor-Bernstein.

Inoltre vale $|[\mathbb{R}]^{\mathfrak{c}}| \leq |\mathcal{P}(\mathbb{R})| = 2^{\mathfrak{c}}$ e $|[\mathbb{R}]^{\mathfrak{c}}| = |[\mathbb{R} \times \mathbb{R}]^{\mathfrak{c}}| \geq |\mathbb{R}^{\mathbb{R}}| \geq |2^{\mathbb{R}}| = |\mathcal{P}(\mathbb{R})| = 2^{\mathfrak{c}}$. □

Proposizione 7.27. *Se* $\mathbb{K}$ *è un campo o un anello di cardinalità numerabile, allora* $|\mathbb{K}[x]| = \aleph_0$.

Dim. Per ogni $n \in \omega$ si pone $\mathbb{K}[x]_n := \{p(x) \in \mathbb{K}[x] \mid p \text{ ha grado n}\}$ e si ha che $\mathbb{K}[x] = \bigcup_{n \in \omega} \mathbb{K}[x]_n$.

È facile osservare che per ogni n vale $|\mathbb{K}[x]_n| = |\mathbb{K}^n| = \aleph_0$ e dunque $|\mathbb{K}[x]| = \aleph_0$ perché $\mathbb{K}[x]$ è unione numerabile di insiemi di cardinalità numerabile. □

Oss. Si è dunque provato che $|\mathbb{Q}[x]| = \aleph_0$ e perciò i numeri reali algebrici sono numerabili.

Questo prova indirettamente l'esistenza di numeri trascendenti (anzi, prova pure che l'insieme dei numeri reali trascendenti ha la cardinalità del continuo).

Proposizione 7.28. *Per ogni* $a, b \in \mathbb{R}$ *tali che* $a < b$ *si ha* $|(a, b)| = \mathfrak{c}$.

Dim. La funzione arcotangente è una funzione bigettiva da $\mathbb{R}$ in $(-\frac{\pi}{2}, \frac{\pi}{2})$.

Inoltre la funzione

$$\begin{aligned} \sigma\colon (-\frac{\pi}{2}, \frac{\pi}{2}) &\to (a, b) \\ t &\mapsto b\frac{(t + \frac{\pi}{2})}{\pi} + a\frac{(\frac{\pi}{2} - t)}{\pi} \end{aligned}$$

è una bigezione, da cui la tesi. □

Proposizione 7.29. *(*) Se* V *è un* $\mathbb{R}$*-spazio vettoriale e* $\dim V = \aleph_0$*, allora* $|V| = \mathfrak{c}$.

Dim. L'idea della dimostrazione è che vi è una corrispondenza biunivoca tra gli elementi di V e le funzioni da $\mathbb{N}$ in $\mathbb{R}$ che assumono valori diversi da 0 solo in un numero finito di punti.

Sia dunque $\{v_n\}_{n\in\mathbb{N}}$ una base di V (dove $v_i \neq v_j$ se $i \neq j$) e sia $X := \{f \in \mathbb{R}^{\mathbb{N}} \mid f^{-1}(\mathbb{R} \setminus \{0\}) \text{ è finito}\}$. Allora la funzione

$$\begin{aligned} \varphi\colon X &\longrightarrow V \\ f &\mapsto \sum_{n|f(n)\neq 0} f(n)v_n \end{aligned}$$

è una bigezione.

Dunque ora basta calcolare $|X|$. D'altra parte $|X| \leq \mathfrak{c}$ perché $X \subseteq \mathbb{R}^{\mathbb{N}}$ ed è banale osservare che $\mathfrak{c} \leq |X|$. Perciò $|V| = |X| = \mathfrak{c}$ (per Cantor-Bernstein). □

Proposizione 7.30. *(*) Se $A \subseteq \mathbb{R}$ e $|A| \leq \aleph_0$ allora $\mathbb{R} \setminus A$ è denso in $\mathbb{R}$.*

Dim. Si ricorda che un sottoinsieme di $\mathbb{R}$ è denso se e solo se interseca ogni aperto non vuoto. Se per assurdo $\mathbb{R} \setminus A$ non è denso in $\mathbb{R}$, allora A contiene un aperto non vuoto. Poiché ogni aperto non vuoto di $\mathbb{R}$ ha la cardinalità del continuo (contiene un intervallo aperto), si ottiene $|A| = \mathfrak{c}$ (*Assurdo*). □

Lemma 7.3. *(*) Una funzione debolmente monotona $\mathbb{R} \to \mathbb{R}$ ha al più una quantità numerabile di punti di discontinuità.*

Dim. Senza perdita di generalità, sia $f\colon \mathbb{R} \to \mathbb{R}$ una funzione debolmente crescente. Allora (fatto noto da Analisi 1) per ogni $x \in \mathbb{R}$ f ammette limite sinistro $f(x)^-$ e limite destro $f(x)^+$, cioè f ha solo punti di discontinuità "di salto".

Siano $g\colon \mathbb{N} \to \mathbb{Q}$ una bigezione e sia A l'insieme dei punti di discontinuità di f. Allora la seguente funzione

$$\begin{aligned} \varphi\colon A &\to \mathbb{Q} \\ x &\mapsto g(min\{n \in \mathbb{N} \mid f(x)^- \lneq g(n) \lneq f(x)^+\}) \end{aligned}$$

è ben definita perché $\mathbb{Q}$ è denso in $\mathbb{R}$ ed è iniettiva perché se x_1 e x_2 sono due punti di discontinuità per f e $x_1 \lneq x_2$, allora $f(x_1)^+ \leq f(x_2)^-$. □

Lemma 7.4. *(*) Ogni $X \subseteq \mathbb{R}$ denso ha un sottoinsieme denso e numerabile.*

Dim. Sia f una funzione di scelta su $\mathcal{P}(X)$.

L'immagine della funzione

$$\begin{aligned} \varphi\colon \mathbb{Q} \times \mathbb{N} &\to X \\ (q, m) &\mapsto f(X \cap B_{\frac{1}{m}}(q)) \end{aligned}$$

è un sottoinsieme denso e numerabile di X. □

Proposizione 7.31. *(*) Dimostrare l'equipotenza*

$$\mathfrak{c} = |\{f\colon \mathbb{R} \to \mathbb{R} \mid f \text{ è } \textit{debolmente monotona}\}|$$

Dim. SI PUÒ FARE MEGLIO

Si è già provato che una funzione debolmente monotona da $\mathbb{R}$ in $\mathbb{R}$ ha al più una quantità numerabile di punti di discontinuità. Questo ci permetterà di ottenere la tesi.

Si deve fare attenzione al fatto che l'insieme dei punti di discontinuità di una tale funzione potrebbe essere denso in sé (pur essendo numerabile). Dato un punto di discontinuità, questo fatto impedisce di considerarne "il successore". Senza questa considerazione si potrebbero ottenere dimostrazioni un po' più semplici, ma fallaci.

Sia $X := \{f\colon \mathbb{R} \to \mathbb{R} \mid f \text{ è debolmente monotona}\}$: banalmente $\mathfrak{c} \leq |X|$ perché basta considerare le funzioni costanti.

Per ogni $f \in X$ sia X_f l'insieme dei suoi punti di discontinuità. Per provare $|X| \leq \mathfrak{c}$ si consideri la funzione

$$\begin{aligned} \varphi\colon X &\to [\mathbb{R}]^{\leq \aleph_0} \times \bigcup_{A \in [\mathbb{R}]^{\leq \aleph_0}} \mathbb{R}^A \times \bigcup_{A \in [\mathbb{R}]^{\leq \aleph_0}} \{g\colon \mathbb{R} \setminus A \to \mathbb{R} \mid g \text{ è continua}\} \\ f &\mapsto (X_f, f_{|X_f}, f_{\mathbb{R}\setminus X_f}) \end{aligned}$$

φ è iniettiva, dunque basta provare che il suo codominio ha la cardinalità del continuo.

Si è già provato (proposizione 7.26 l'insieme $[\mathbb{R}]^{\leq \aleph_0}$ ha la cardinalità del continuo.

L'insieme $\bigcup_{A \in [\mathbb{R}]^{\leq \aleph_0}} \mathbb{R}^A$ ha la cardinalità del continuo perché è unione indicizzata su un insieme di cardinalità $\mathfrak{c}$ di insiemi di cardinalità $\mathfrak{c}$.

Per ogni $A \in [\mathbb{R}]^{\leq \aleph_0}$ l'insieme $\mathbb{R} \setminus A$ è denso in $\mathbb{R}$ per il lemma 7.4. Per il lemma 7.3 l'insieme $\mathbb{R} \setminus A$ ha un sottoinsieme denso e numerabile B_A. La funzione

$$\begin{aligned} \psi\colon \{g\colon \mathbb{R} \setminus A \to \mathbb{R} \mid g \text{ è continua}\} &\to \{g\colon B_A \to \mathbb{R} \mid g \text{ è continua}\} \\ g &\mapsto g_{|B_A} \end{aligned}$$

è iniettiva perché due funzioni continue che coincidono su un denso sono uguali.

Dunque $|\{g\colon \mathbb{R} \setminus A \to \mathbb{R} \mid g \text{ è continua}\}| = \mathfrak{c}$ e anche il terzo insieme del prodotto cartesiano considerato precedentemente ha la cardinalità del continuo.

Si conclude osservando che il prodotto cartesiano finito di insiemi che hanno la cardinalità del continuo ha la cardinalità del continuo. □

Proposizione 7.32. *(*) (AC) Dati due insiemi A e B si definisce la loro differenza simmetrica $A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$. Si provi che se A e B sono infiniti e $A \Delta B$ è finita, allora $|A| = |B| = |A \cap B| = |A \cup B|$.*

Dim. Per definizione $A \Delta B = (A \setminus B) \cup (B \setminus A)$. Se $A \Delta B$ è finita, allora anche $A \setminus B$ è finito. Ora $A \setminus (A \setminus B) = A \cap B$ e dalla proposizione 7.17 segue $|A| = |A \cap B|$. La stessa cosa vale per B, dunque si ottiene $|A| = |B| = |A \cap B|$. Poiché $(A \cup B) \setminus (A \Delta B) = A \cap B$, sempre dalla proposizione 7.17 si ottiene che $|A \cup B| = |A \cap B|$. □

Proposizione 7.33. *(*) (AC) Se $\mathcal{R}$ è una relazione binaria, allora $|\mathcal{D}om\,\mathcal{R}| \leq |\mathcal{R}|$ e $|\mathcal{I}m\,\mathcal{R}| \leq |\mathcal{R}|$.*

Dim. Le funzioni

$$\begin{aligned} f &\colon \mathcal{R} \to \mathcal{D}om\,\mathcal{R} \\ (x, y) &\mapsto x \end{aligned}$$

$$\begin{aligned} g &\colon \mathcal{R} \to \mathcal{I}m\,\mathcal{R} \\ (x, y) &\mapsto y \end{aligned}$$

sono surgettive.

Per l'Assioma di scelta f e g hanno inverse destre e queste sono iniettive. □

8 Aritmetica di Peano

$\mathcal{U}$n passo importante negli sviluppi di ZFC sarà quello di dimostrare che i numeri naturali che si sono definiti (i naturali di Von Neumann) hanno tutte le proprietà che idealmente si attribuiscono ai numeri naturali e che sono formalizzate nell'Aritmetica di Peano.

Si presenta dunque la teoria logica dell'Aritmetica di Peano e se ne studiano alcune proprietà, poi si passa a provare che ω soddisfa tutti gli assiomi necessari e che è l'unico modello (a meno di isomorfismi) dell'Aritmetica di Peano del secondo ordine.

Definizione (Sistema di numeri naturali)**.** *Una quintupla ordinata* $(\mathcal{N}, 0, \mathcal{S}, +, \cdot)$*, dove* $\mathcal{N}$ *è un insieme,* $0 \in \mathcal{N}$ *è un suo elemento,* $\mathcal{S}\colon \mathcal{N} \to \mathcal{N}$ *è una funzione detta* ***successore****,* $+$ *e* $\cdot$ *sono due operazioni su* $\mathcal{N}$ *dette rispettivamente* ***somma*** *e* ***prodotto****, è detta* ***sistema di numeri naturali*** *se soddisfa i seguenti* ***assiomi di Peano****:*

PA1 : "Tutti e soli i numeri diversi da zero sono successori".

Formalmente $\mathcal{I}m\mathcal{S} = \mathcal{N} \setminus \{0\}$*;*

PA2 : "La funzione successore è iniettiva".

Formalmente

$$\forall n, m \in \mathcal{N}\ n \neq m \to \mathcal{S}(n) \neq \mathcal{S}(m)\ ;$$

PA3 : la somma gode delle seguenti proprietà:

(s1) : per ogni $n \in \mathcal{N}$ *si ha* $n + 0 = n$*;*

(s2) : per ogni $n, m \in \mathcal{N}$ *si ha* $n + \mathcal{S}(m) = \mathcal{S}(n + m)$*;*

PA4 : il prodotto gode delle seguenti proprietà:

(p1) : per ogni $n \in \mathcal{N}$ *si ha* $n \cdot 0 = 0$*;*

(p2) : per ogni $n, m \in \mathcal{N}$ *si ha* $n \cdot \mathcal{S}(m) = n \cdot m + n$*;*

PA5 : "Principio di induzione del secondo ordine", cioè "se $A \subseteq \mathcal{N}$*,* $0 \in A$ *e* A *è chiuso per successore, allora* $A = \mathcal{N}$*".*

Oss. Quella definita sopra è l'Aritmetica di Peano del secondo ordine, ma ne esiste anche una del primo ordine, in cui cambia solo il Principio d'induzione. Il Principio d'induzione del primo ordine è "per ogni proprietà $P(x)$ del linguaggio dell'Aritmetica di Peano, se valgono $P(0)$ e $\forall n(P(n) \to P(\mathcal{S}(n))$, allora per ogni $n \in \mathcal{N}$ vale $P(n)$".

È facile osservare che il Principio d'induzione del secondo ordine implica quello del primo ordine.

Nelle varie proposizioni che seguono si dimostrano alcune proprietà che discendono direttamente dagli assiomi appena visti ed è sottointeso che $(\mathcal{N}, 0, \mathcal{S}, +, \cdot)$ è un modello dell'Aritmetica di Peano del primo ordine.

Proposizione 8.1. *(*) La somma è associativa, cioè per ogni $n, m, k \in \mathcal{N}$ vale $n + (m + k) = (n + m) + k$.*

Dim. Per induzione su k:

- se $k = 0$ allora $n + (m + 0) = n + m = (n + m) + 0$.
- P$(k)\to$P$(\mathcal{S}(k))$: $n + (m + \mathcal{S}(k)) = n + (\mathcal{S}(m + k)) = \mathcal{S}(n + (m + k)) = \mathcal{S}((n + m) + k) = (n + m) + \mathcal{S}(k)$.

□

Lemma 8.1. *Per ogni $n \in \mathcal{N}$ si ha $0 + n = n$.*

Dim. Per induzione su n:

- $0 + 0 = 0$.
- P$(n)\to$P$(\mathcal{S}(n))$: $0 + \mathcal{S}(n) = \mathcal{S}(0 + n) = \mathcal{S}(n)$.

□

Lemma 8.2. *(*) Per ogni $n, m \in \mathcal{N}$ vale $\mathcal{S}(n) + m = n + \mathcal{S}(m)$.*

Dim. Per induzione su m:

- se $m = 0$ allora $\mathcal{S}(n) + 0 = \mathcal{S}(n)$ e $n + \mathcal{S}(0) = \mathcal{S}(n + 0) = \mathcal{S}(n)$.
- P$(m)\to$P$(\mathcal{S}(m))$: $\mathcal{S}(n) + \mathcal{S}(m) = \mathcal{S}(\mathcal{S}(n) + m) = \mathcal{S}(n + \mathcal{S}(m)) = n + \mathcal{S}(\mathcal{S}(m))$.

□

Proposizione 8.2. *(*) La somma è commutativa, cioè per ogni $n, m \in \mathcal{N}$ vale $n + m = m + n$.*

Dim. Per induzione su m:

- se $m = 0$ allora $n + 0 = n$ e $0 + n = n$ (la seconda per il lemma 8.1).
- P$(m)\to$P$(\mathcal{S}(m))$: $n + \mathcal{S}(m) = \mathcal{S}(n + m) = \mathcal{S}(m + n) = m + \mathcal{S}(n) = \mathcal{S}(m) + n$ per il lemma 8.2.

□

Proposizione 8.3. *(*) Il prodotto è distributivo rispetto alla somma, cioè per ogni $n, m, k \in \mathcal{N}$ vale $n(m + k) = nm + nk$.*

Dim. Per induzione su k:

- se $k = 0$ allora $n(m + 0) = nm = nm + 0 = nm + n0$.
- P(k)→P($\mathcal{S}(k)$): $n(m + \mathcal{S}(k)) = n\mathcal{S}(m + k) = n(m + k) + n = (nm + nk) + n = nm + (nk + n) = nm + n\mathcal{S}(k)$.

□

Proposizione 8.4. *(*) Il prodotto è associativo, cioè per ogni $n, m, k \in \mathcal{N}$ vale $n(mk) = (nm)k$.*

Dim. Per induzione su k:

- se $k = 0$ allora $n(m0) = n0 = 0 = (nm)0$.
- P(k)→P($\mathcal{S}(k)$): $n(m\mathcal{S}(k)) = n(mk + m) = n(mk) + nm = (nm)k + nm = (nm)\mathcal{S}(k)$.

□

Dato un sistema di numeri naturali $(\mathcal{N}, 0, \mathcal{S}, +, \cdot)$, per ogni $n, m \in \mathcal{N}$ si pone $n < m$ se e solo se esiste un $k \neq 0$ in $\mathcal{N}$ tale che $m = n + k$.

Nelle due proposizioni seguenti si dimostra che questa relazione è una relazione d'ordine totale stretto su $\mathcal{N}$. Si potrebbe inoltre dimostrare che si tratta di un buon ordinamento.

Proposizione 8.5. *(*) "Non esistono naturali fra un numero e il suo successore" (e per questo ha proprio senso parlare di "successore"), cioè per ogni $n, m \in \mathcal{N}$ vale l'implicazione $n < \mathcal{S}(m) \to (n = m \vee n < m)$.*

Dim. Per induzione su n:

- se $n = 0$ considero due casi. Se $m = 0$ allora $n = m$. Se $m \neq 0$ allora $m = 0 + m$ e dunque $n = 0 < m$.
- P(n)→P($\mathcal{S}(n)$): se $\mathcal{S}(n) < \mathcal{S}(m)$ allora $\mathcal{S}(m) = \mathcal{S}(n) + k$ con $k \in \mathcal{N}$ e $k \neq 0$. Inoltre $\mathcal{S}(n) + k = k + \mathcal{S}(n) = \mathcal{S}(k + n)$. Per l'iniettività di $\mathcal{S}$ si ottiene $m = n + k$, cioè $n < m$.

□

Oss. Non si è scritto, ma è del tutto banale provare che per ogni $n \in \mathcal{N}$ vale $n < \mathcal{S}(n)$, infatti $n + 1 = n + \mathcal{S}(0) = \mathcal{S}(n + 0) = \mathcal{S}(n)$.

Proposizione 8.6. *(*) La relazione $<$ è un ordine totale stretto su $\mathcal{N}$.*

Dim. Si ricorda che un ordine stretto su un insieme è una relazione binaria irriflessiva (o equivalentemente asimmetrica) e transitiva. Per essere totale è necessario che tutti gli elementi siano confrontabili, cioè che per ogni $n, m \in \mathcal{N}$ valga almeno una (in realtà una sola, perché si escludono l'un l'altra) tra $n < m$, $n = m$ e $m < n$.

Seguono le necessarie verifiche:

- prop. irriflessiva: per ogni $n \in \mathcal{N}$ non vale $n < n$. Si dimostra per induzione su n.
  - se $n = 0$ e per assurdo esiste $k \in \mathcal{N}$ tale che $k \neq 0$ e $0 = 0 + k$, allora si ottiene $0 = k$ ($\mathcal{A}ssurdo$).
  - passo induttivo: se per assurdo $\mathcal{S}(n) = \mathcal{S}(n) + k$ e $k \neq 0$ allora $\mathcal{S}(n) = k + \mathcal{S}(n) = \mathcal{S}(k + n)$, da cui si ottiene $n = k + n$ per l'iniettività di $\mathcal{S}$. Ma questo è assurdo per l'ipotesi induttiva.
- prop. transitiva: per ogni $n, m, k \in \mathcal{N}$ vale l'implicazione $(n < m \wedge m < k) \to n < k$. Si dimostra per induzione su k.
  - se $k = 0$ allora la proprietà è banalmente vera a vuoto.
  - passo induttivo: siano $n < m$ e $m < \mathcal{S}(k)$. Per la proposizione 8.5 $m = k$ o $m < k$. Se $m = k$ allora segue banalmente $n < k$. Se $m < k$ allora la proprietà vale per l'ipotesi induttiva.
- totalità: per ogni $n, m \in \mathcal{N}$ vale una e una sola delle seguenti: $n < m$, $m < n$, $n = m$. La dimostrazione segue lo stesso stile delle precedenti e il passo induttivo segue direttamente dalla proposizione 8.5.

□

Si passano ora a definire le operazioni di somma e prodotto fra numeri naturali di Von Neumann e poi a provare che ω con queste operazioni e la sua funzione successore è un modello dell'Aritmetica di Peano del secondo ordine.

Definizione (Somma in ω)**.** *Dati $n, m \in \omega$ si definisce $n + m$ come l'unico numero naturale equipotente ad una unione disgiunta $A \cup B$ dove $|A| = n$ e $|B| = m$.*

Oss. Si è già provato che se $|A| = |A'|$, $|B| = |B'|$ e $A \cap B = A' \cap B' = \emptyset$ allora $|A \cup B| = |A' \cup B'|$, dunque la definizione di somma data sopra non dipende dalla scelta dei due insiemi A e B in questione.

Inoltre una tale unione è finita per la proposizione 7.8 ed è in bigezione con un unico naturale di Von Neumann perché si è dimostrato che numeri naturali distinti non sono in bigezione fra loro.

Resta solo da provare l'esistenza di due tali insiemi A e B. Per far questo si possono considerare $A = n$ e $B = m \times \{\omega\}$, che sono ovviamente disgiunti e delle cardinalità volute.

Proposizione 8.7. *(*) Per ogni $n \in \omega$ vale $n + 1 = \hat{n}$.*

Dim. Gli insiemi n e $\{n\}$ sono disgiunti e rispettivamente in bigezione con n e 1. Per definizione $n + 1$ è l'unico naturale in bigezione con $n \cup \{n\} = \hat{n}$, cioè proprio $\hat{n}$. □

Definizione (Prodotto in ω)**.** *Dati $n, m \in \omega$ si definisce $n \cdot m$ come l'unico naturale equipotente ad un prodotto cartesiano $A \times B$ dove $|A| = n$ e $|B| = m$.*

Oss. Anche la definizione sopra è ben posta per gli stessi motivi precedenti.

Teorema 8.1. *(*) La quintupla $(\omega, \emptyset, \hat{}\,, +, \cdot)$ è un modello dell'Aritmetica di Peano del secondo ordine.*

Dim. Nel capitolo 5 si è già provato che ω gode del Principio di induzione del secondo ordine. Restano perciò da provare le proprietà di $\hat{}$, $+$ e $\cdot$.

- *La funzione $\hat{}\colon \omega \to \omega \setminus 0$ è bigettiva.*

  Prima di tutto si osserva che la funzione è ben definita, nel senso che $0 \notin \mathcal{I}m(\hat{})$ perché per ogni $n \in \omega$ vale $\hat{n} = n \cup \{n\}$ e dunque $\hat{n} \neq \emptyset$.

  L'iniettività segue dal fatto che se $n \neq m$ allora per la totalità di $\in$ si può considerare senza perdita di generalità $n \in m$ e si è già visto che questo implica $\hat{n} \in \hat{m}$, da cui $\hat{n} \neq \hat{m}$.

  Si dimostra la surgettività per induzione su n con la proprietà $\mathrm{P}(n)$="$n \neq 0 \to n \in \mathcal{I}m(\hat{})$":

  - se $n = 0$ allora la proprietà è vera a vuoto.
  - $\mathrm{P}(n) \to \mathrm{P}(\hat{n})$: ovvio.

  È interessante osservare che la surgettività prova che ogni naturale di Von Neumann si ottiene da 0 iterando un certo numero di volte la funzione successore.

- *Proprietà di $+$:*

  - per definizione $n + 0$ è l'unico numero naturale in bigezione con $A \cup B$ dove $|A| = n$, $|B| = 0$ e $A \cap B = \emptyset$. In questo caso si ottiene $B = \emptyset$ e quindi $A \cup B = A$ è in bigezione con n. Perciò $n + 0 = 0$.
  - Per ogni $n, m \in \omega$ si deve provare $n + \hat{m} = \widehat{n + m}$. Per definizione $n + \hat{m}$ è l'unico naturale in bigezione con $A \cup B$ dove $|A| = n$, $|B| = \hat{m}$ e $A \cap B = \emptyset$.

    Dunque basta provare che $\widehat{n + m}$ è in bigezione con $A \cup B$.

    Se $b \in B$, allora esiste una bigezione $f\colon n + m \to A \cup (B \setminus \{b\})$.

La funzione

$$\begin{aligned}\varphi\colon \widehat{n+m} &\to A \cup B\\ x &\mapsto f(x) \text{ se } x \in n+m\\ n+m &\mapsto b\end{aligned}$$

è una bigezione e conclude la dimostrazione.

- *Proprietà di* $\cdot$:
  - per definizione $n \cdot 0$ è l'unico naturale in bigezione con l'insieme $n \times \emptyset = \emptyset$, cioè 0.
  - Per ogni $n, m \in \omega$ si deve dimostrare $n \cdot \hat{m} = n \cdot m + n$. Per definizione $n \cdot \hat{m}$ è l'unico naturale in bigezione con l'insieme $n \times \hat{m}$, e $n \cdot m + n$ è l'unico naturale in bigezione con $(n \times m) \cup (n \times \{m\})$. Poiché $n \times \hat{m} = (n \times m) \cup (n \times \{m\})$, si ottiene proprio $n \cdot \hat{m} = n \cdot m + m$.

□

Teorema 8.2. *(*) Esiste un solo modello dell'Aritmetica di Peano del secondo ordine (a meno di isomorfismi).*

Dim. Dato un modello dell'Aritmetica di Peano del secondo ordine $(\mathcal{N}, 0, \mathcal{S}, +, \cdot)$, si prova che è isomorfo a $(\omega, \emptyset, \hat{}, +, \cdot)$, cioè che esiste una funzione bigettiva $\psi\colon \omega \to \mathcal{N}$ tale che

- $\psi(\emptyset) = 0$;
- per ogni $n \in \omega$ vale $\psi(\hat{n}) = \mathcal{S}(\psi(n))$;
- per ogni $n, m \in \omega$ vale $\psi(n + m) = \psi(n) + \psi(m)$;
- per ogni $n, m \in \omega$ vale $\psi(n \cdot m) = \psi(n) \cdot \psi(m)$.

Per il Teorema di ricorsione numerabile esiste la funzione

$$\begin{aligned}\psi\colon \omega &\to \mathcal{N}\\ \emptyset &\mapsto 0\\ n+1 &\mapsto \mathcal{S}(\psi(n))\end{aligned}$$

Ora basta provare che ψ è bigettiva e che per ogni $n, m \in \omega$ valgono $\psi(n + m) = \psi(n) + \psi(m)$ e $\psi(n \cdot m) = \psi(n) \cdot \psi(m)$.

- ψ è iniettiva: si prova per induzione su m l'enunciato $\forall n \in \omega\ n \neq m \to \psi(n) \neq \psi(m)$. Se $n \neq 0$, allora n è successore in ω e dunque $\psi(n)$ è un successore in $\mathcal{N}$, quindi $\psi(n) \neq 0$. Se $n \neq m + 1$, allora ci sono due possibilità: se $n = 0$ allora $\psi(n) = 0 \neq \psi(m + 1)$ perchè 0 non è un successore; se n è un successore, cioè $n = k + 1$, allora

$k \neq m$ e dunque $\psi(k) \neq \psi(m)$ per ipotesi induttiva, ma allora $\psi(n) = \psi(k+1) = \mathcal{S}(\psi(k)) \neq \mathcal{S}(\psi(m)) = \psi(m+1)$. Si è usata l'iniettività della funzione successore.

- ψ è surgettiva: poiché la funzione successore è surgettiva su $\mathcal{N} \setminus \{0\}$ e $0 \in \mathcal{I}m\,\psi$ per definizione, basta provare per induzione su n l'enunciato $\forall n \in \mathcal{N}\ \mathcal{S}(n) \in \mathcal{I}m\,\psi$. Si ha $\mathcal{S}(0) = \mathcal{S}(\psi(0)) = \psi(1)$. Inoltre $\mathcal{S}(\mathcal{S}(n)) = \mathcal{S}(\psi(k)) = \psi(\hat{k})$.

- $\psi(n+m) = \psi(n) + \psi(m)$: per induzione su m. Si ha $\psi(n+0) = \psi(n) = \psi(n) + 0 = \psi(n) + \psi(0)$. Inoltre $\psi(n+\hat{m}) = \psi(\widehat{n+m}) = \mathcal{S}(\psi(n) + \psi(m)) = \psi(n) + \mathcal{S}(\psi(m)) = \psi(n) + \psi(\hat{m})$.

- $\psi(n \cdot m) = \psi(n) \cdot \psi(m)$: per induzione su m. Si ha $\psi(n \cdot 0) = \psi(0) = 0 = \psi(n) \cdot 0 = \psi(n) \cdot \psi(0)$. Inoltre $\psi(n \cdot \hat{m}) = \psi(n \cdot m + n) = \psi(n \cdot m) + \psi(n) = \psi(n) \cdot \psi(m) + \psi(n) = \psi(n) \cdot (\mathcal{S}(\psi(m)) = \psi(n) \cdot \psi(\hat{m})$.

□

Oss. Nella dimostrazione c'è un'imprecisione: perché non si è usata l'induzione del secondo ordine? Era davvero necessaria?

La risposta è "sì", infatti gli enunciati che vengono dimostrati, contenendo ψ, non sono esprimibili nel linguaggio della Teoria degli insiemi, dunque si sarebbe dovuta usare l'induzione del secondo ordine, ma la dimostrazione resta sostanzialmente la stessa.

9 Forme equivalenti dell'Assioma di scelta (1)

Resta da dimostrare, per concludere la parte "iniziale" del corso, l'equivalenza dell'Assioma di scelta con alcuni altri enunciati.

Nel capitolo 12 si proverà l'equivalenza fra AC, il Lemma di Zorn e alcuni enunciati di grande importanza.

Si riportano invece qui di seguito delle semplici forme equivalenti di AC ("semplici" nel senso che non trattano alcuna struttura matematica particolare, ma solo le poche cose introdotte nella primissima parte del corso).

Si dà prima una

Definizione (Insieme di scelta)**.** *Data una famiglia non vuota di insiemi non vuoti X, si dice che Y è un* ***insieme di scelta*** *per X se per ogni $x \in X$ esiste un y tale che $Y \cap x = \{y\}$.*

Teorema 9.1. *(*) (ZF) Sono fatti equivalenti:*

1. *(AC) se $\langle A_i \mid i \in I\rangle$ è una I-sequenza infinita di insiemi non vuoti, allora*
$$\prod_{i\in I} A_i \neq \emptyset$$
2. *ogni famiglia non vuota di insiemi non vuoti ha una funzione di scelta;*
3. *ogni famiglia non vuota di insiemi non vuoti a due a due disgiunti ha un insieme di scelta;*
4. *se $f\colon A \to B$ è surgettiva (e $B \neq \emptyset$), allora ha un'inversa destra;*
5. *se $\langle A_{i,j} \mid (i,j) \in I \times J\rangle$ è una $(I \times J)$-sequenza, allora*
$$\bigcap_{i\in I}\bigcup_{j\in J} A_{i,j} = \bigcup_{f\in J^I}\bigcap_{i\in I} A_{i,f(i)}$$
$$\bigcup_{i\in I}\bigcap_{j\in J} A_{i,j} = \bigcap_{f\in J^I}\bigcup_{i\in I} A_{i,f(i)}$$

Dim. Lo schema dimostrativo seguito è (1) $\to$ (2) $\to$ (3) $\to$ (4) $\to$ (1), (1) $\leftrightarrow$ (5).

- (1) $\to$ (2): sia $\mathcal{F}$ una famiglia non vuota di insiemi non vuoti.

  Se $\mathcal{F}$ è finita, allora una funzione di scelta si ottiene banalmente per induzione sulla sua cardinalità.

  Se $\mathcal{F}$ è infinita, allora la si può indicizzare con $id_{\mathcal{F}}$ e poi usare l'Assioma di scelta. Infatti $id_{\mathcal{F}}$ è una sequenza non vuota di insiemi non vuoti e dunque per AC esiste $f \in \prod_{A\in\mathcal{F}} A$. Questa f è banalmente una funzione di scelta per $\mathcal{F}$.

- (2) $\to$ (3): sia $\mathcal{F}$ una famiglia non vuota di insiemi non vuoti a due a due disgiunti. Per (2) $\mathcal{F}$ ha una funzione di scelta f e $\mathcal{I}m\, f$ è un insieme di scelta per $\mathcal{F}$.

- (3) $\to$ (4): sia $f\colon A \to B$ surgettiva e sia $X := \{f^{-1}(\{b\}) \mid b \in B\}$. È banale provare l'esistenza di X in ZFC.

  Dalla surgettività di f segue che X è una famiglia non vuota di insiemi non vuoti a due a due disgiunti. Dunque per (3) X ha un insieme di scelta Y.

  Ponendo
  $$\begin{aligned} g\colon B &\to A \\ b &\mapsto a^* \end{aligned}$$
  dove a^* è l'unico elemento che sta sia in $f^{-1}(\{b\})$ sia in Y, cioè $a^* = \bigcup(f^{-1}(\{b\}) \cap Y)$, si ottiene un'inversa destra di f.

  Questa g è iniettiva perché ha un'inversa sinistra.

- (4) $\to$ (1): sia $\langle A_i \mid i \in I\rangle$ una I-sequenza infinita di insiemi non vuoti e per ogni $a \in \bigcup_{i\in I} A_i$ sia $X_a := \{i \in I \mid a \in A_i\}$.

  Si pone $X := \{X_a \times \{a\} \mid a \in \bigcup_{i\in I} A_i\}$ e si osserva che è lecito farlo perché $X_a \times \{a\} \in \mathcal{P}(I \times \bigcup_{i\in I} A_i)$ (si usa l'Assioma di separazione).

  La funzione
  $$\begin{aligned} f\colon \bigcup X &\to I \\ (i, a) &\mapsto i \end{aligned}$$
  è surgettiva e per (4) ha un'inversa destra g.

  Dunque si definisce
  $$\begin{aligned} g^*\colon I &\to \bigcup_{i\in I} A_i \\ i &\mapsto a^* \end{aligned}$$
  dove a^* è la seconda componente di $g(i)$, cioè $a^* = \bigcup((\bigcup g(i)) \setminus \{i\})$.

  È banale osservare che $g^* \in \prod_{i\in I} A_i$.

- (1) $\to$ (5): si dimostra solo la prima uguaglianza perché la seconda segue in modo banale applicando le Leggi di De Morgan.

  $\subseteq$: gli insiemi $A_{i,j}$ possono essere immaginati come elementi di una matrice con i righe e j colonne. Si ha che $a \in \bigcap_{i\in I}\bigcup_{j\in J} A_{i,j}$ se e solo se in ogni riga c'è almeno un insieme a cui appartiene e usando l'Assioma di scelta se ne può prendere uno in particolare.

  Si considera I infinito, perché altrimenti la tesi si dimostra banalmente per induzione sulla sua cardinalità.

Sia $a \in \bigcap_{i\in I}\bigcup_{j\in J} A_{i,j}$ e per ogni $i \in I$ sia $B_i := \{j \in J \mid a \in A_{i,j}\}$. $\langle B_i \mid i \in I\rangle$ è una sequenza infinita di insiemi non vuoti, dunque per AC esiste $f \in \prod_{i\in I} B_i$ ed è banale osservare che $f \in J^I$ e $a \in \bigcap_{i\in I} A_{i,f(i)}$.

$\supseteq$: se $a \in \bigcup_{f\in J^I}\bigcap_{i\in I} A_{i,f(i)}$ allora esiste $f \in J^I$ tale che in ogni riga i si ha $a \in A_{i,f(i)}$. Dunque $a \in \bigcap_{i\in I}\bigcup_{j\in J} A_{i,j}$ per l'osservazione fatta precedentemente.

- (5) $\to$ (1): sia $\langle A_i \mid i \in I\rangle$ una I-sequenza infinita di insiemi non vuoti e sia $J := \bigcup_{i\in I} A_i$.

  Si consideri la $(I \times J)$-sequenza

  $$g\colon I \times J \to \{A_i \mid i \in I\} \cup \{\emptyset\}$$
  $$(i, a) \mapsto \begin{cases} J & \text{se } a \in A_i \\ \emptyset & \text{se } a \notin A_i \end{cases}$$

  Da (5) si ottiene l'uguaglianza

  $$\bigcap_{i\in I}\bigcup_{a\in J} g(i, a) = \bigcup_{f\in J^I}\bigcap_{i\in I} g(i, f(i))$$

  Il primo termine è non vuoto (è proprio J) perché in ogni riga c'è almeno un J dato che gli A_i sono non vuoti. Dunque anche il secondo termine dell'uguaglianza è non vuoto e perciò esiste $f\colon I \to J$ tale che per ogni $i \in I$ vale $g(i, f(i)) \neq \emptyset$, cioè $f(i) \in A_i$.

□

Oss. Sarebbe molto semplice dimostrare l'equivalenza fra l'Assioma di scelta, l'esistenza di una funzione di scelta per $\mathcal{P}(A)$ con A insieme qualsiasi e l'esistenza di un insieme di scelta per una partizione di un insieme qualsiasi (equivalentemente "ogni relazione di equivalenza ha un sistema di rappresentanti").

10 Buoni ordini

$\mathcal{A}$ questo punto si è pronti per entrare nel vivo della teoria.

Tutto quello che è stato fatto finora è servito per costruire gli strumenti necessari allo studio di buoni ordini, ordinali e cardinali.

Lemma 10.1. *(*) Ogni insieme totalmente ordinato finito e non vuoto ha massimo e minimo. In particolare è un buon ordine.*

Dim. Sia $(A, \leq)$ un insieme totalmente ordinato finito con $|A| = n$.

Si procede per induzione su n:

- se $n = 1$ allora A ha un solo elemento che è sia massimo che minimo per A;
- $\mathrm{P}(n) \to \mathrm{P}(n+1)$: se $a \in A$ allora $|A \setminus \{a\}| = n$ e per l'ipotesi induttiva esistono $M = max(A \setminus \{a\})$ e $m = min(A \setminus \{a\})$.

  Si osserva facilmente che $max(\{M, a\}) = max(A)$ e $min(\{m, a\}) = min(A)$.

□

Proposizione 10.1. *(*) Se $(A, \leq)$ è un insieme totalmente ordinato finito, allora $(A, \leq) \cong (n, \in)$ dove $|A| = n$.*

In particolare gli $(n, \in)$ sono gli unici insiemi bene ordinati finiti a meno di isomorfismo.

Dim. Per induzione su n:

- se $|A| = 0$ allora l'isomorfismo è la funzione vuota;
- $\mathrm{P}(n) \to \mathrm{P}(n+1)$: se $|A| = n + 1$ e $a = max(A)$ (lemma 10.1), allora $|A \setminus \{a\}| = n$ e $A \setminus \{a\}$ è un insieme totalmente ordinato finito.

  Per l'ipotesi induttiva esiste $\varphi \colon A \setminus \{a\} \to n$ isomorfismo d'ordine: ora basta estendere φ a $\varphi_1 \colon A \to n + 1$ ponendo $\varphi_1(a) = n$.

  È banale osservare che φ_1 è un isomorfismo d'ordine. (In realtà si vedrà che è l'unico isomorfismo d'ordine).

□

Oss. I naturali di Von Neumann non sono solo rappresentanti per le cardinalità degli insiemi finiti, ma anche per i buoni ordini finiti.

Definizione (Tipo d'ordine)**.** *Dati due insiemi bene ordinati $(A, \leq)$ e $(B, \leq)$, si dice che A ha **tipo d'ordine minore** di B se è isomorfo ad un segmento iniziale proprio di B e si scrive $ot(A) < ot(B)$*

*Se $A \cong B$ si dice che A e B hanno lo **stesso tipo d'ordine** e si scrive $ot(A) = ot(B)$.*

Oss. $ot(A)$ sta per l'inglese "order type".

Proposizione 10.2. *(*) Ogni insieme bene ordinato finito ha tipo d'ordine minore (strettamente) di* $(\omega, \in)$. *Inoltre* $(\omega, \in)$ *ha il più piccolo tipo d'ordine fra gli insiemi bene ordinati infiniti.*

Dim. Si osserva prima di tutto che per ogni $n \in \omega$ si ha che n ha tipo d'ordine minore di ω perché è un suo segmento iniziale proprio.

Se $(A, \leq)$ è un buon ordine infinito, allora si definisce per ricorsione numerabile la successione

$$\begin{cases} a_0 = min\, A \\ a_{n+1} = min\, A \setminus \{a_0, \ldots, a_n\} \end{cases}$$

Si vede banalmente che $\langle a_n \mid n \in \omega \rangle$ è un isomorfismo d'ordine fra ω e $\{a_n \mid n \in \omega\}$, che è un segmento iniziale di A. □

A questo punto uno potrebbe chiedersi se "cardinalità" e "tipo d'ordine" fra buoni ordini siano la stessa cosa, per esempio una domanda lecita sarebbe: "esistono buoni ordini numerabili non isomorfi fra loro?" La risposta è affermativa e per esempio si può prendere $(\omega \cup \{\omega\}, \in)$. Si passa ora a dimostrare alcune proprietà generali dei buoni ordini.

Proposizione 10.3. *(AC)* $(A, \leq)$ *è un buon ordine se e solo se non esistono catene discendenti* $a_0 > a_1 > \ldots$

Dim. $\rightarrow$: se per assurdo A ha una catena discendente B, allora B è un sottoinsieme non vuoto di A privo di minimo ($\mathcal{A}ssurdo$).

$\leftarrow$: (AC) se per assurdo $(A, \leq)$ non è un buon ordine, allora, usando l'Assioma di scelta, si va a costruire per ricorsione numerabile una catena discendente (strettamente) in A.

Siano dunque $B \subseteq A$ non vuoto e privo di minimo e $\varphi \colon \mathcal{P}(B) \to B$ una funzione di scelta.

Ora si pone

$$\begin{cases} b_0 = \varphi(B) \\ b_{n+1} = \varphi(\{x \in B \mid \forall i \in n+1\ x < b_i\}) \end{cases}$$

Si osserva che $\{b_n \mid n \in \omega\}$ è una catena discendente (strettamente) di A ($\mathcal{A}ssurdo$).

□

Proposizione 10.4. *Dato un insieme totalmente ordinato* $(A, \leq)$, *si ha che* $(A, \leq)$ *è un buon ordine se e solo se ogni suo segmento iniziale proprio è generato.*

Dim. $\rightarrow$ Dato un segmento iniziale proprio S di A si deve provare che è generato. L'idea è che il generatore deve essere il minimo elemento che non sta in S (esiste perché A è un buon ordine).

Da $S \subsetneq A$ segue $A \setminus S \neq \emptyset$ e poiché A è un buon ordine si pone $a = min\, A \setminus S$. Ora si prova che vale $A_a = S$: $A_a \subseteq S$ per la minimalità di a e $S \subseteq A_a$ perché se per assurdo esiste un $s \in S \setminus A_a$, allora $s \geq a$, da cui segue $a \in S$ ($\mathcal{A}ssurdo$).

$\leftarrow$: dato un sottoinsieme non vuoto B di A, l'insieme $\{x \in A \mid \forall b \in B\ x < b\}$ è un segmento iniziale proprio di A, dunque è generato da un certo elemento a.

Ora si prova che $a \in B$ e che è il minimo. Intanto si ha che esiste un $b \in B$ tale che $b \leq a$ e inoltre non può valere la disuguaglianza stretta perché altrimenti sarebbe $b < b$. Dunque $a \in B$ ed è il minimo sempre per lo stesso motivo.

□

Proposizione 10.5. *Se $(A, \leq)$ è un buon ordine e $\varphi \colon A \to A$ è strettamente crescente, allora per ogni $a \in A$ si ha $\varphi(a) \geq a$.*

Dim. Si pone $B := \{a \in A \mid \varphi(a) < a\}$. Se per assurdo $B \neq \emptyset$, allora ha un elemento minimo b.

Ora $\varphi(b) < b$ e dunque $\varphi(\varphi(b)) \geq \varphi(b)$ per la minimalità di b in B.

Dalla stretta crescenza di φ segue inoltre che $\varphi(\varphi(b)) < \varphi(b)$ ($\mathcal{A}ssurdo$).

□

Oss. l'ipotesi di buon ordine è necessaria perché $\psi \colon \mathbb{Z} \to \mathbb{Z}$ che manda k in $k - 1$ è strettamente crescente (anzi è un isomorfismo), ma non ha la proprietà richiesta.

Corollario 10.1. *Seguono facilmente i seguenti fatti:*

1. *ogni buon ordine ha un solo automorfismo, cioè l'identità;*
2. *se $(A, \leq)$ e $(B, \leq)$ sono due insiemi bene ordinati isomorfi, allora l'isomorfismo è unico.*

Dim. La seconda proprietà è una semplice conseguenza della prima.

1. Siano $(A, \leq)$ un insieme bene ordinato e $\varphi \colon A \to A$ un suo automorfismo.

   Allora per ogni $a \in A$ vale $\varphi(a) \geq a$ per la proposizione 10.5.

   Inoltre è banale osservare che φ^{-1} è un automorfismo di A e dunque (sempre per la stessa proposizione) si ha anche $\varphi^{-1}(a) \geq a$. Dunque $a = \varphi(\varphi^{-1}(a)) \geq \varphi(a)$, da cui segue $\varphi(a) = a$, cioè che $\varphi = id_A$.

2. se $\varphi\colon A \to B$ e $\psi\colon A \to B$ sono due isomorfismi, allora $\varphi \circ \psi^{-1}$ è un automorfismo di A, dunque $\varphi \circ \psi^{-1} = id_A$, da cui segue $\varphi = \psi$.

□

Proposizione 10.6. *(*) Se $(A, \leq)$ è un buon ordine, allora*

1. *A non è isomorfo a nessun suo segmento iniziale proprio;*
2. *$A_a \cong A_{a'} \to a = a'$.*

Dim. 1. Se per assurdo esistono $a \in A$ e un isomorfismo $\varphi\colon A \to A_a$, allora φ è strettamente crescente da A in A e dunque $\varphi(a) \geq a$ ($\mathcal{A}ssurdo$).

2. Se per assurdo $a \neq a'$, allora sia *wlog* $a < a'$. Se $\varphi\colon A_{a'} \to A_a$ è l'isomorfismo fra i due, allora $\varphi(a) \geq a$ ($\mathcal{A}ssurdo$).

□

Proposizione 10.7. *(*) Se $(A, \leq)$ e $(B, \leq)$ sono due buoni ordini e $\varphi\colon A \to B$ è un isomorfismo, allora per ogni $a \in A$ si ha che $\varphi_{|A_a}\colon A_a \to B_{\varphi(a)}$ è un isomorfismo.*

Dim. Si deve dimostrare che $\mathcal{I}m(\varphi_{|A_a}) = B_{\varphi(a)}$ e che $\varphi_{|A_a}$ è strettamente crescente. La stretta crescenza è banale, dunque basta provare che $\mathcal{I}m(\varphi_{|A_a}) = B_{\varphi(a)}$.

Per ogni $x \in A_a$ si ha che $x < a$, dunque $\varphi(x) < \varphi(a)$, da cui segue che $\varphi(x) \in B_{\varphi(a)}$. Perciò $\mathcal{I}m(\varphi_{|A_a}) \subseteq B_{\varphi(a)}$.

Per ogni $b \in B_{\varphi(a)}$ vale $b < \varphi(a)$: φ è surgettiva, dunque esiste $a' \in A$ tale che $b = \varphi(a')$. Se fosse $a' \geq a$, allora $\varphi(a') \geq \varphi(a)$, da cui seguirebbe $\varphi(a) > \varphi(a)$ ($\mathcal{A}ssurdo$).

Dunque $a' < a$ e $b \in \mathcal{I}m(\varphi_{|A_a})$. □

Si è ora pronti per enunciare un risultato fondamentale sui buoni ordini, cioè la "Tricotomia dei buoni ordini", che rende l'"ordine" fra buoni ordini un ordine totale.

Teorema 10.1 (Tricotomia dei buoni ordini)**.** *Se $(A, \leq)$ e $(B, \leq)$ sono due buoni ordini, allora vale una e una sola delle seguenti:*

$$ot(A) < ot(B);$$

$$ot(A) = ot(B);$$

$$ot(A) > ot(B).$$

Detto altrimenti, "due buoni ordini o sono isomorfi o uno è isomorfo a un segmento iniziale proprio dell'altro".

Dim. Si considera l'insieme $\varphi := \{(a,b) \in A \times B \mid A_a \cong B_b\}$ e si prova che è un isomorfismo tra A e B o tra uno dei due e un segmento iniziale dell'altro.

- φ è una funzione: una funzione è una relazione binaria univoca e φ è per definizione una relazione binaria. L'univocità segue dalla proposizione 10.6.

- φ è strettamente crescente: se $a < a'$, da $A_a \cong B_{\varphi(a)}$ e $A_{a'} \cong B_{\varphi(a')}$ segue che $B_{\varphi(a)}$ è un segmento iniziale proprio di $B_{\varphi(a')}$. Dunque $\varphi(a) < \varphi(a')$.

  Si è inoltre ottenuto che φ è un isomorfismo fra $\mathcal{D}om\,\varphi$ e $\mathcal{I}m\,\varphi$.

Ora basta provare che $\mathcal{D}om\,\varphi$ e $\mathcal{I}m\,\varphi$ sono segmenti iniziali rispettivamente di A e di B. Infatti, in tal caso, non può succedere che siano entrambi segmenti iniziali propri perché per come è definita φ, se questi segmenti fossero A_a e B_b, allora si otterrebbe $a \in \mathcal{D}om\,\varphi = A_a$ ($\mathcal{A}ssurdo$).

Il fatto che si tratta di segmenti iniziali è una semplice conseguenza della proposizione 10.7. □

Corollario 10.2. *Una famiglia non vuota X di buoni ordini ha un elemento con tipo d'ordine minimo.*

Dim. L'idea è quella di usare un elemento qualsiasi A di X per confrontarci tutti gli altri (lo si può fare per la tricotomia dei buoni ordini) e poi concludere col buon ordinamento di A.

Sia $A \in X$. Se per ogni $B \in X$ vale $ot(A) \leq ot(B)$, allora A ha tipo d'ordine minimo in X.

Altrimenti si considera $a := min\{a \in A \mid \exists B \in X\ B \cong A_a\}$ e si ottiene che il tipo d'ordine minimo in X è quello di A_a. □

Oss. Questo significa che l'"ordine" fra tipi d'ordine di insiemi bene ordinati sarebbe un buon ordine (se solo fosse una vera e propria relazione).

Corollario 10.3. *Se $(A, \leq)$ è un buon ordine e $B \subseteq A$, allora $ot(B) \leq ot(A)$.*

Dim. È banale osservare che $(B, \leq)$ è un buon ordine (è sottoinsieme di un buon ordine).

Se per assurdo fosse $ot(B) \not\leq ot(A)$, allora per la tricotomia dei buoni ordini vale $ot(A) < ot(B)$, cioè esiste un isomorfismo $\varphi\colon A \to B_b$ per un certo $b \in B$.

Ora si ha che $\varphi_{|B}\colon B \to B_b$ è una funzione strettamente crescente e dunque $\varphi(b) \geq b$ ($\mathcal{A}ssurdo$). □

Oss. Può succedere che un buon ordine sia isomorfo a un suo sottoinsieme proprio, per esempio $\mathbb{N}$ è isomorfo a $2\mathbb{N}$.

Teorema 10.2 (Induzione transfinita sui buoni ordini)**.** *Su ogni buon ordine* $(A, \leq)$ *vale il Principio d'induzione transfinita, cioè*

"Per ogni $X \subseteq A$*, se per ogni* $a \in A$ *vale l'implicazione* $A_a \subseteq X \to a \in X$*, allora* $X = A$*".*

Dim. Se per assurdo $X \subsetneq A$, allora sia $x := min\,(A \setminus X)$. Per la minimalità di x, si ottiene $A_x \subseteq X$ e dunque $x \in X$ ($\mathcal{A}ssurdo$). □

Proposizione 10.8. *(*) Un insieme di insiemi totalmente ordinati mutualmente confrontabili ("uno contenuto nell'altro") ha per unione un insieme totalmente ordinato.*

Dim. Sia $\{A_i \mid i \in I\}$ una famiglia di ordini totali come nell'ipotesi e sia $A := \bigcup_{i \in I} A_i$.

È facile vedere che A è un insieme parzialmente ordinato e la sua totalità segue dal fatto che gli A_i sono uno contenuto nell'altro. □

Oss. Lo stesso fatto non vale per gli insiemi bene ordinati. Per esempio $\mathbb{Z}$ è l'unione degli insiemi $[-n, \infty]_{\mathbb{Z}}$, che sono bene ordinati e mutualmente confrontabili, ma non è bene ordinato.

Vale però il seguente fatto.

Proposizione 10.9. *(*) Se* $\langle A_i \mid i \in I \rangle$ *è una I-sequenza di buoni ordini che sono uno segmento iniziale dell'altro, allora* $\bigcup_{i \in I} A_i$ *è un buon ordine.*

Dim. Se $A := \bigcup_{i \in I} A_i$, allora A è un insieme totalmente ordinato per la proposizione 10.8.

Resta da dimostrarne il buon ordinamento. Se $B \subseteq A$ è non vuoto, allora sia A_i un certo insieme della famiglia per cui $A_i \cap B \neq \emptyset$. Posto $b := min\,(A_i \cap B)$, si vuole provare che b è il minimo elemento in B.

Se per assurdo esiste $b' \in B$ tale che $b' < b$, allora esiste $j \in I$ tale che $b' \in A_j$ e dunque A_i è un segmento iniziale di A_j, ma allora $b' \in A_i$ ($\mathcal{A}ssurdo$). □

Manca la parte sulle operazioni fra buoni ordini.

Si aggiungono nel finale di questo capitolo, sebbene non si parli di buoni ordini, alcune importanti proprietà dell'ordinamento standard di $\mathbb{Q}$.

Proposizione 10.10. $(\mathbb{Q}, \leq)$ *è universale tra gli insiemi totalmente ordinati numerabili, cioè per ogni insieme totalmente ordinato numerabile* $(A, \leq)$ *esiste un sottoinsieme di* $\mathbb{Q}$ *ad esso isomorfo.*

Dim. Basta trovare una funzione strettamente crescente da A in $\mathbb{Q}$.

Poiché A è numerabile esiste una funzione $f : \mathbb{N} \to A$ bigettiva.

Ora si definisce per ricorsione numerabile

$$\begin{aligned}\varphi\colon A &\to \mathbb{Q}\\ a_0 &\mapsto 0\\ a_{n+1} &\mapsto \begin{cases} max\{\varphi(a_i) \mid i \leq n\} + 1 \text{ se } a_{n+1} = max\{a_i \mid i \leq n+1\} \\ min\{\varphi(a_i) \mid i \leq n\} - 1 \text{ se } a_{n+1} = min\{a_i \mid i \leq n+1\} \\ \frac{\varphi(a_i)+\varphi(a_j)}{2} \text{ se } a_i \overset{\checkmark}{<} a_{n+1} \overset{\checkmark}{<} a_j \end{cases}\end{aligned}$$

(dove si è indicato con $\overset{\checkmark}{<}$ il predecessore immediato di a_{n+1} in $\{a_0, \dots a_{n+1}\}$) e si osserva che è strettamente crescente. □

Oss. Il lettore più attento potrebbe essersi accorto che nella dimostrazione si sono usati solo due fatti relativi all'ordinamento di $\mathbb{Q}$, cioè la densità e il fatto che è privo di massimo e minimo, dunque si potrebbe generalizzare.

Non solo, vale qualcosa di molto più forte ed è argomento della proposizione seguente.

Proposizione 10.11. *(*) Ogni insieme totalmente ordinato $(A, \leq)$ numerabile, denso e privo di massimo e minimo è isomorfo a $(\mathbb{Q}, \leq)$.*

Dim. DA RIVEDERE
Si procede esattamente come nella proposizione precedente immergendo in $\mathbb{Q}$ prima A e poi $\mathbb{Q}$ stesso. In questo modo si ottengono due isomorfismi fra A e l'immagine del primo e fra $\mathbb{Q}$ e l'immagine del secondo. Se si dimostra che questi isomorfismi hanno la stessa immagine, allora si è concluso. Questa è una semplice conseguenza del fatto che A è denso e privo di massimo e minimo.

Siano infatti $f\colon A \to \mathbb{Q}$ e $g\colon \mathbb{Q} \to \mathbb{Q}$ le due funzioni trovate sopra. Se per assurdo $\mathcal{I}m\, f \neq \mathcal{I}m\, g$, allora sia *wlog* $\mathcal{I}m\, f \nsubseteq \mathcal{I}m\, g$. Sia inoltre $m = min\{n \in \omega \mid f(a_n) \notin \mathcal{I}m\, g\}$. Allora m è necessariamente un successore, cioè $m = k + 1$, perché $0 \in \mathcal{I}m\, g$. Dunque $f(a_m) = f(a_{k+1}) \in \mathcal{I}m\, g$ per la minimalità di m, la densità di $\mathbb{Q}$ e il fatto che non ha né massimo né minimo ($\mathcal{A}ssurdo$).

Se si fosse assunto $\mathcal{I}m\, g \neq \mathcal{I}m\, f$ si sarebbe usata la densità di A e il fatto che è privo di massimo e minimo. □

11 Ordinali

Ricordando la definizione di "insieme transitivo" presente nel capitolo 5 si dà la seguente

Definizione (Ordinale)**.** *Un* ***ordinale*** *è un insieme transitivo bene ordinato rispetto a* $\in$ *(come ordine stretto).*

Solitamente gli ordinali si denotano con lettere greche minuscole.

Esempio. ω e tutti i naturali di Von Neumann sono ordinali.

Proposizione 11.1. *Se* $(\alpha, \in)$ *è un buon ordine, allora* α *è un ordinale se e solo se per ogni* $x \in \alpha$ *vale* $\alpha_x = x$*.*

Dim. $\rightarrow$ Il contenimento $\alpha_x \subseteq x$ è una diretta conseguenza della definizione di α_x. D'altra parte per ogni $y \in x$ si ha $y \in \alpha$ perché α è un ordinale e dunque $y \in \alpha_x$, da cui la tesi.

$\leftarrow$ Basta provare che α è un insieme transitivo: per ogni $y \in x \in \alpha$ da $\alpha_x = x$ segue $y \in \alpha$, cioè la tesi.

□

Lemma 11.1. *Se* α *è un ordinale, allora* $\alpha \notin \alpha$*.*

Dim. Se per assurdo fosse $\alpha \in \alpha$ allora non sarebbe valida la proprietà irriflessiva dell'ordine stretto dato da $\in$ su α. □

Proposizione 11.2. *Se* α *è un ordinale, allora* $\alpha \cup \{\alpha\}$ *è un ordinale.*

Dim.

- $\alpha \cup \{\alpha\}$ è transitivo: se $x \in y \in \alpha \cup \{\alpha\}$, allora $y \in \alpha$ o $y = \alpha$. Nel primo caso si ottiene $x \in \alpha$ perché α è un insieme transitivo. Nel secondo caso si ha già si ottiene $x \in \alpha$ per estensionalità.

- $\alpha \cup \{\alpha\}$ è ben ordinato da $\in$:

  - irriflessività: per ogni $x \in \alpha \cup \{\alpha\}$ o $x \in \alpha$ o $x = \alpha$. Se $x \in \alpha$ allora $x \notin x$ perché $\in$ è un ordine stretto su α. Se $x = \alpha$ allora si conclude col Lemma 11.1;
  - transitività: siano $x, y, z \in \alpha \cup \{\alpha\}$ e $x \in y \in z$. Se $z \in \alpha$ allora anche $x, y \in \alpha$ per transitività e $x \in z$ per la transitività dell'ordine dato da $\in$ su α. Se $z = \alpha$ allora $x \in z$ perché α è un insieme transitivo;
  - totalità: per ogni $x, y \in \alpha \cup \{\alpha\}$ se $x = \alpha$ e $y = \alpha$ allora $x = y$, se $x \in \alpha$ e $y = \alpha$ allora $x \in y$ (e analogamente se $y \in \alpha$ e $x = \alpha$). Invece se $x, y \in \alpha$ allora vale la tricotomia per l'ordine in α.

– buon ordinamento: dato un sottoinsieme A di $\alpha \cup \{\alpha\}$, se $\alpha \notin A$, allora $A \subseteq \alpha$ ha minimo perché α è un buon ordine. Se $\alpha \in A$, allora ci sono due possibilità. Se $A = \{\alpha\}$, allora α è il minimo elemento di A, altrimenti $A \setminus \{\alpha\}$ ha un elemento minimo perché è un sottoinsieme di α che è un buon ordine, e questo elemento è anche il minimo di A perché è ovviamente minore di α.

□

Proposizione 11.3. *(*) Ogni elemento di un ordinale è un ordinale.*

Dim. Siano α un ordinale e $\beta \in \alpha$ un suo elemento.

- β è transitivo: se $x \in y \in \beta$ allora $x, y \in \alpha$ perché α è un insieme transitivo e dunque $x \in \beta$ per la transitività dell'ordinamento dato da $\in$ su α.
- $(\beta, \in)$ è un buon ordine perché è un sottoinsieme di un buon ordine.

□

Teorema 11.1. *Se α e β sono ordinali, allora $\alpha \cong \beta \to \alpha = \beta$. Detto altrimenti, "ordinali isomorfi sono uguali".*

Dim. Sia $\varphi\colon \alpha \to \beta$ un isomorfismo (l'unico) e siano per assurdo $\alpha \neq \beta$ e *wlog* $\alpha \nsubseteq \beta$.

Allora $\alpha \setminus \beta \neq \emptyset$ e dunque esiste $x := min\,(\alpha \setminus \beta)$. Per la proposizione 10.7 $\varphi_{|\alpha_x}\colon \alpha_x \to \beta_{\varphi(x)}$ è un isomorfismo e inoltre si può provare che α_x è un segmento iniziale di β. Infatti $\alpha_x \subseteq \beta$ per la minimalità di x e se $b \in \beta$ e $y \in \alpha_x$ sono tali che $b \in y$ allora valgono anche $b \in \alpha$ e $b \in x$ perché α e x sono ordinali (x è elemento di un ordinale), e dunque $b \in \alpha_x$. Dunque $\alpha_x = \beta_{\varphi(x)}$, cioè $x = \varphi(x)$ per la proposizione 11.1 (*Assurdo* perché $x \notin \beta$). □

Teorema 11.2 (Tricotomia degli ordinali)**.** *Dati due ordinali α e β vale una e una sola delle seguenti:*

$$\alpha \in \beta;$$

$$\alpha = \beta;$$

$$\beta \in \alpha.$$

Dim. Per la Tricotomia dei buoni ordini vale una e una sola fra $\alpha \cong \beta$, $\alpha \cong \beta_b$ per un qualche $b \in \beta$ e $\beta \cong \alpha_a$ per un qualche $a \in \alpha$.

Nel primo caso si ottiene $\alpha = \beta$ perché ordinali isomorfi sono uguali. Gli altri due casi si risolvono esattamente nello stesso modo e per esempio se $\alpha \cong \beta_b = b$ si ottiene $\alpha = b$ perché elementi di ordinali sono ordinali e ordinali isomorfi sono uguali, da cui $\alpha \in \beta$. □

Proposizione 11.4. *(*) Se α e β sono ordinali, allora vale la doppia implicazione $\alpha \in \beta \leftrightarrow \alpha \subsetneq \beta$.*

Dim. $\rightarrow$: se $\alpha \in \beta$, allora $\alpha \subseteq \beta$ perché gli ordinali sono insiemi transitivi. Inoltre non può valere l'uguaglianza perché $\beta \notin \beta$ (lemma 11.1).

$\leftarrow$: per la tricotomia degli ordinali resta solo da escludere il caso $\beta \in \alpha$ e questo non può valere perché altrimenti $\beta \subsetneq \alpha$ per quanto dimostrato al punto precedente.

□

Proposizione 11.5. *(*) Se β è un ordinale, allora $\beta \cup \{\beta\}$ è il minimo degli ordinali maggiori di β (e lo si denota $\beta + 1$).*

Dim. Si ha banalmente $\beta \in \beta \cup \{\beta\}$. Dunque si deve solo provare che $\beta \cup \{\beta\}$ è il minimo ordinale maggiore di β.

Se α è un ordinale maggiore di β, cioè $\beta \in \alpha$, allora $\beta \subsetneq \alpha$ e perciò $\beta \cup \{\beta\} \subseteq \alpha$. Se vale l'uguaglianza allora si è concluso, altrimenti si ha il contenimento stretto e per la proposizione 11.4 si ottiene $\beta \cup \{\beta\} \in \alpha$. □

Oss. Se $\alpha < \beta + 1$, allora $\alpha \leq \beta$.

Definizione (Ordinale successore/limite)**.** *Un ordinale del tipo $\alpha \cup \{\alpha\}$ è detto* ***ordinale successore****, altrimenti è detto* ***ordinale limite****.*

Solitamente si indica un ordinale limite con la lettera greca λ.

Proposizione 11.6. *(*) Un ordinale ha massimo se e solo se è un successore.*

Dim. Se $\alpha = \beta \cup \{\beta\}$, allora β è banalmente il massimo di α.

D'altra parte se un ordinale α ha massimo β, allora si vuole provare l'uguaglianza $\alpha = \beta \cup \{\beta\}$. Il contenimento $\subseteq$ è scontato. Per l'altro contenimento basta provare che vale $\beta \subseteq \alpha$, ma questo segue dal fatto che α è un insieme transitivo. □

Proposizione 11.7. *(*) Se X è un insieme di ordinali, allora $\bigcup X$ è un ordinale e $\bigcup X = \sup X$.*

Dim. Si prova prima che $\bigcup X$ è un insieme transitivo: se $x \in y \in \bigcup X$, allora esiste $\alpha \in X$ tale che $y \in \alpha$ e dunque $x \in \alpha$ perché α è un insieme transitivo. Perciò vale anche $x \in \bigcup X$.

Si è già provato con la proposizione 10.9 che l'unione di un insieme di buoni ordini che sono uno segmento iniziale dell'altro è un buon ordine, e da questo segue direttamente il buon ordinamento di $\bigcup X$.

Poiché $\bigcup X$ contiene tutti gli ordinali di X, si ha $\bigcup X \geq \alpha$ per ogni $\alpha \in X$. Inoltre se un ordinale β ha questa proprietà allora contiene anche $\bigcup X$ e dunque quest'ultimo è il più piccolo dei maggioranti per X. □

Oss. In particolare X ha massimo se e solo se $\bigcup X \in X$.

Se α è un ordinale, allora α è successore se e solo se ha massimo se e solo se $\bigcup \alpha \in \alpha$.

Detto altrimenti, α è limite se e solo se non ha massimo se e solo se $\bigcup \alpha = \alpha$.

Si è inoltre provato che un'unione di insiemi transitivi è un insieme transitivo.

Proposizione 11.8. *(*) Se $X \neq \emptyset$ è un insieme di ordinali, allora $\bigcap X$ è un ordinale e inoltre $\bigcap X = min\, X$.*

Dim. Si è già provato nel corollario 10.2 che un insieme non vuoto di buoni ordini ha un elemento con tipo d'ordine minimo. Nel caso degli ordinali, "avere tipo d'ordine minimo" significa essere segmento iniziale proprio di tutti gli altri, e dunque, detto α questo ordinale con tipo d'ordine minimo in X, si ha $\bigcap X = \alpha = min\, X$. □

Proposizione 11.9. *Un insieme di ordinali è un ordinale se e solo se è transitivo.*

Dim. Basta osservare che un insieme di ordinali è bene ordinato dall'appartenenza e questo è vero perché si è già dimostrato che ogni famiglia di buoni ordini ha un elemento con tipo d'ordine minimo (corollario 10.2). □

Corollario 11.1 (Paradosso di Burali-Forti)**.** *Non esiste l'insieme di tutti gli ordinali.*

Dim. Se esistesse l'insieme di tutti gli ordinali ORD, allora questo sarebbe un insieme transitivo e dunque sarebbe un ordinale e apparterrebbe a se stesso ($\mathcal{A}ssurdo$ per il lemma 11.1). □

Il Teorema seguente è un risultato importantissimo in Teoria degli Insiemi e caratterizza gli ordinali come rappresentanti canonici dei tipi d'ordine degli insiemi bene ordinati.

Teorema 11.3. *Ogni insieme bene ordinato è isomorfo a un unico ordinale.*

Dim. L'unicità, una volta provata l'esistenza, è del tutto banale perché ordinali isomorfi sono uguali.

Dato un insieme bene ordinato $(A, \leq)$, si considerano gli insiemi $X := \{a \in A \mid \exists \beta \text{ ordinale}\,,\ \beta \cong A_a\}$ e $Y := \{\beta \mid \beta \text{ ordinale } \wedge \exists a \in X\ \beta \cong A_a\}$.

Qui è bene osservare che l'esistenza di Y è garantita dall'Assioma di Rimpiazzamento applicato ad X e alla proprietà $P(x, y)$ definita da "$x \in X \wedge y$ è l'unico ordinale isomorfo ad A_a oppure $x \notin X$ e $y = \emptyset$".

Ora si considera la funzione

$$\begin{aligned} f\colon X &\to Y \\ a &\mapsto \beta \text{ dove } \beta \cong A_a \end{aligned}$$

e si va a provare che $X = A$, Y è un ordinale e f è un isomorfismo.

- se per assurdo $X \subsetneq A$, allora $A \setminus X \neq \emptyset$ e si può porre $a := min(A \setminus X)$. Per la minimalità di a, si ha che per ogni $a' \in A_a$ vale $a' \in X$, cioè esiste β ordinale tale che $A_{a'} \cong \beta$.

  Ora si considera l'insieme $Z := \{\beta \mid \exists a' \in A_a \ \beta \cong A_{a'}\}$, che esiste ancora una volta per l'Assioma di Rimpiazzamento. Z è un insieme di ordinali ed è facile provare che è transitivo e dunque un ordinale.

  Inoltre è facile provare che la funzione

  $$\begin{aligned} \varphi \colon A_a &\to Z \\ a' &\mapsto \beta \text{ dove } A_{a'} \cong \beta \end{aligned}$$

  è un isomorfismo e dunque $a \in X$ ($\mathcal{A}ssurdo$).

- Y è un insieme transitivo di ordinali, e dunque è un ordinale (come sopra).

- (Facile, come sopra)

□

Si enuncia ora una fondamentale generalizzazione del Principio d'induzione già visto per i numeri naturali.

Proposizione 11.10 (Principio d'induzione transfinita (forte))**.** *Data una proprietà $P(x)$ del linguaggio della Teoria degli Insiemi, se per ogni ordinale β vale l'implicazione $(\forall \alpha \in \beta \ P(\alpha)) \to P(\beta)$, allora vale $P(\beta)$ per ogni ordinale β.*

Dim. Se per assurdo esiste un ordinale β per cui non vale $P(\beta)$, allora sia $\alpha := min\{\gamma \in \beta \mid \neg P(\gamma)\}$. Per ipotesi, dalla minimalità di α si ottiene che vale $P(\alpha)$ ($\mathcal{A}ssurdo$). □

Proposizione 11.11 (Principio d'induzione transfinita (debole))**.** *Data una proprietà $P(x)$ del linguaggio della Teoria degli Insiemi, se valgono:*

- $P(0)$*;*
- $\forall \alpha (P(\alpha) \to P(\alpha + 1))$*;*
- *se λ è limite vale $(\forall \gamma \in \lambda \ P(\gamma)) \to P(\lambda)$;*

allora vale $P(\alpha)$ per ogni ordinale α.

Dim. Banale conseguenza del Principio d'induzione transfinita (forte). □

Così come esiste un Principio di induzione in "versione ordinale", la stessa cosa vale anche per il Teorema di ricorsione, e si va ora a dimostrarne una forma che permetterà di definire l'aritmetica ordinale e di dimostrare svariate proprietà degli ordinali.

Si danno prima un paio di definizioni.

Definizione (Operazione)**.** *Data una proprietà $P(x, y)$ del linguaggio della Teoria degli Insiemi tale che per ogni x esiste un unico y per cui vale $P(x, y)$, si dice* ***operazione indotta da*** *P valutata in x l'unico y per cui vale $P(x, y)$ e si scrive $O_P(x) = y$.*

Definizione. *Data un'operazione O e un insieme x, l'unica funzione di dominio f tale che per ogni $y \in x$ vale $f(y) = O(y)$ è detta* ***O-approssimazione di lunghezza*** *x (si osservi che tale funzione esiste per l'Assioma di rimpiazzamento) e si scrive $f := O_{|x}$.*

Teorema 11.4 (Teorema di ricorsione transfinita)**.** *Data un'operazione G e la proprietà $P(x, y)$="(x è un ordinale e $y = t(y)$ dove t è una G-approssimazione di lunghezza x) oppure (x non è un ordinale e $y = 0$)", si ha che P induce un'operazione tale che per ogni ordinale α vale $O_P(\alpha) = G(O_{P|\alpha})$.*

Dim. La dimostrazione è una versione lievemente modificata di quella già vista per il caso numerabile, dunque la si omette. □

Ora si definiscono per ricorsione transfinita le operazioni aritmetiche fra ordinali.

Definizione (Somma ordinale)**.** *Dato un ordinale α, si definisce ricorsivamente $\alpha + \beta$ nel modo seguente:*

$$\begin{cases} \alpha + 0 = \alpha \\ \alpha + (\beta + 1) = (\alpha + \beta) + 1 \\ \alpha + \lambda = \bigcup_{\gamma \in \lambda} \alpha + \gamma \quad \textit{se } \lambda \textit{ limite} \end{cases}$$

Oss. Si ottiene $\alpha + 1 = \alpha \cup \{\alpha\}$, come si era già denotato in precedenza.

Il lettore faccia attenzione a non cadere in un facile errore: i "+1" che compaiono nella definizione appena data sono quelli usati per denotare il successore di un ordinale e non la somma ordinale. Dunque non si tratta di una fallace definizione autoreferenziale.

Definizione (Prodotto ordinale)**.** *Dato un ordinale α, si definisce ricorsivamente $\alpha \cdot \beta$ nel modo seguente:*

$$\begin{cases} \alpha \cdot 0 = 0 \\ \alpha \cdot (\beta + 1) = (\alpha \cdot \beta) + \alpha \\ \alpha \cdot \lambda = \bigcup_{\gamma \in \lambda} \alpha \cdot \gamma \quad \textit{se } \lambda \textit{ limite} \end{cases}$$

Definizione (Esponenziazione ordinale)**.** *Dato un ordinale α, si definisce ricorsivamente α^β nel modo seguente:*

$$\begin{cases} \alpha^0 = 1 \\ \alpha^{\beta+1} = \alpha^\beta \cdot \alpha \\ \alpha^\lambda = \bigcup_{\gamma\in\lambda} \alpha^\gamma \qquad \textit{se } \lambda \textit{ limite} \end{cases}$$

Manca la parte sull'isomorfismo fra le operazioni ordinali e quelle fra buoni ordini.

Si provano ora varie proprietà dell'aritmetica ordinale.

Proposizione 11.12. *(*) Per ogni ordinale α vale $0 + \alpha = \alpha$.*

Dim. Per induzione su α:

- $0 + 0 = 0$;
- $0 + (\alpha + 1) = (0 + \alpha) + 1 = \alpha + 1$;
- se λ limite, allora $0 + \lambda = \bigcup_{\gamma\in\lambda} 0 + \gamma = \bigcup_{\gamma\in\lambda} \gamma = \lambda$.

□

Proposizione 11.13. *(*) Se α_1, α_2 e β sono ordinali, allora $\alpha_1 < \alpha_2 \leftrightarrow \beta + \alpha_1 < \beta + \alpha_2$.*

Dim. $\rightarrow$: per induzione su α_2. Se $\alpha_2 = 0$ allora la proprietà è vera a vuoto. Se $\alpha_1 < \gamma + 1$, allora $\alpha_1 \leq \gamma$ e per ipotesi induttiva $\beta + \alpha_1 \leq \beta + \gamma < (\beta + \gamma) + 1 = \beta + (\gamma + 1)$. Se $\alpha_1 < \lambda$ con λ limite, allora $\beta + \lambda = \bigcup_{\gamma\in\lambda} \beta + \gamma > \beta + \alpha$ perché, essendo λ limite, esiste $\gamma \in \lambda$ tale che $\gamma > \alpha_1$ e poi si conclude per ipotesi induttiva.

$\leftarrow$: se per assurdo $\alpha_2 < \alpha_1$, allora per quanto dimostrato al punto precedente si ottiene $\beta + \alpha_2 < \beta + \alpha_1$ (*Assurdo*).

□

Proposizione 11.14. *(*) Se α_1, α_2 e β sono ordinali, allora $\alpha_1 = \alpha_2 \leftrightarrow \beta + \alpha_1 = \beta + \alpha_2$.*

Dim. Banale conseguenza della proposizione precedente. □

Oss. Le due proposizioni precedenti permettono di usare la cancellazione a sinistra le somme sia nelle equazioni che nelle disequazioni fra ordinali.

Non vale invece la cancellazione a destra: per esempio $\omega = 1 + \omega = 2 + \omega$, ma $1 \neq 2$.

Proposizione 11.15. *Se α e β sono ordinali, allora $\alpha < \beta \leftrightarrow (\alpha + 1) < (\beta + 1)$.*

Dim. $\rightarrow$: da $\alpha \in \beta$ segue $(\alpha + 1) \leq \beta < \beta + 1$.

$\leftarrow$: da $\alpha + 1 < \beta + 1$ segue $\alpha + 1 \leq \beta$, cioè $\alpha + 1 \subseteq \beta$. Dunque vale $\alpha \in \beta$.

□

Proposizione 11.16. *(*) Se α, β e γ sono ordinali tali che $\alpha < \beta$, allora $\alpha + \gamma \leq \beta + \gamma$.*

Dim. Per induzione su γ. Prima di tutto i osserva che $\alpha + 0 = \alpha < \beta = \beta + 0$.

Inoltre $\alpha + (\gamma + 1) = (\alpha + \gamma) + 1 \leq (\beta + \gamma) + 1 = \beta + (\gamma + 1)$. Si osservi che oltre all'ipotesi induttiva si è usata la proposizione 11.15.

Infine, se λ è limite, si ha $\alpha + \lambda = \bigcup_{\gamma \in \lambda} \alpha + \gamma \leq \bigcup_{\gamma \in \lambda} \beta + \gamma = \beta + \lambda$. □

Oss. In generale non vale la disuguaglianza stretta: per esempio $\omega = 1 + \omega = 2 + \omega$, ma $1 < 2$.

Proposizione 11.17. *(*) Per ogni ordinale α vale $0 \cdot \alpha = 0$.*

Dim. Per induzione su α.

Se $\alpha = 0$, allora $0 \cdot 0 = 0$ per la definizione di prodotto ordinale.

Inoltre $0 \cdot (\alpha + 1) = 0 \cdot \alpha + 0 = 0 + 0 = 0$ e se λ è limite $0 \cdot \lambda = \bigcup_{\gamma \in \lambda} 0 \cdot \gamma = \bigcup_{\gamma \in \lambda} 0 = 0$. □

Proposizione 11.18. *(*) Se α_1, α_2 e $\beta \neq 0$ sono ordinali, allora $\alpha_1 < \alpha_2 \leftrightarrow \beta \cdot \alpha_1 < \beta \cdot \alpha_2$.*

Dim. $\rightarrow$: Per induzione su α_2. Se $\alpha_2 = 0$, allora la proprietà è vera a vuoto.

Se $\alpha_1 < \gamma + 1$, allora $\alpha_1 \leq \gamma$ e dunque per ipotesi induttiva $\beta \cdot \alpha_1 \leq \beta\gamma < \beta \cdot \gamma + \beta = \beta \cdot (\gamma + 1)$.

Se $\alpha_1 < \lambda$ con λ limite, allora $\beta \cdot \lambda = \bigcup_{\gamma \in \lambda} \beta \cdot \gamma$. Da $\alpha_1 < \lambda$, segue che esiste $\gamma_1 \in \lambda$ tale che $\gamma_1 > \alpha_1$ e dunque, per ipotesi induttiva $\beta \cdot \gamma_1 > \beta \cdot \alpha_1$, da cui $\beta \cdot \lambda > \beta \cdot \alpha_1$.

$\leftarrow$: c'è solo da escludere il caso $\alpha_2 < \alpha_1$ e questo è una banale conseguenza del punto precedente.

□

Proposizione 11.19. *(*) Se α_1, α_2 e $\beta \neq 0$ sono ordinali, allora $\alpha_1 = \alpha_2 \leftrightarrow \beta \cdot \alpha_1 = \beta \cdot \alpha_2$.*

Dim. Banale conseguenza della proposizione precedente. □

Oss. Le due proposizioni precedenti permettono di cancellare a sinistra prodotti sia nelle equazioni che nelle disequazioni fra ordinali.

Non vale invece la cancellazione a destra: per esempio $\omega = 2 \cdot \omega = 3 \cdot \omega$, ma $2 \neq 3$.

Proposizione 11.20. *(*) Se α, β e γ sono ordinali tali che $\alpha < \beta$, allora $\alpha \cdot \gamma \leq \beta \cdot \gamma$.*

Dim. Per induzione su γ. Prima di tutto si osserva che $\alpha \cdot 0 = 0 = \beta \cdot 0$.
Inoltre $\alpha \cdot (\gamma + 1) = \alpha \cdot \gamma + \alpha \leq \beta \cdot \gamma + \alpha < \beta \cdot \gamma + \beta = \beta \cdot (\gamma + 1)$.
Infine, se λ è limite, si ha $\alpha \cdot \lambda = \bigcup_{\gamma \in \lambda} \alpha \cdot \gamma \leq \bigcup_{\gamma \in \lambda} \beta \cdot \gamma = \beta \cdot \lambda$. □

Oss. In generale non vale la disuguaglianza stretta: per esempio $\omega = 2 \cdot \omega = 3 \cdot \omega$, ma $2 < 3$.

Proposizione 11.21. *(*) Se α, β_1 e β_2 sono ordinali con $\alpha > 1$, allora $\beta_1 < \beta_2 \leftrightarrow \alpha^{\beta_1} < \alpha^{\beta_2}$.*

Dim. $\rightarrow$: Per induzione su β_2. Se $\beta_2 = 0$, allora la proprietà è vera a vuoto.

Inoltre se $\beta < \delta + 1$, allora $\beta \leq \delta$, da cui $\alpha^{\beta} \leq \alpha^{\delta} < \alpha^{\delta} \cdot \alpha = \alpha^{\delta+1}$.

Se $\beta < \lambda$ con λ limite, allora si conclude come al solito.

$\leftarrow$: banale conseguenza di quanto dimostrato al punto precedente.

□

Proposizione 11.22. *(*) Se α, β_1 e β_2 sono ordinali con $\alpha > 1$, allora $\beta_1 = \beta_2 \leftrightarrow \alpha^{\beta_1} = \alpha^{\beta_2}$.*

Dim. Banale conseguenza della proposizione precedente. □

Ci si potrebbe chiedere come si comportino limiti e successori nelle varie operazioni aritmetiche: per esempio cosa si ottiene se si moltiplicano un limite e un successore? E se li si somma?

Le prossime proposizioni risolvono completamente la questione nel caso di somma e prodotto e in esse α e β sono sempre due ordinali. Il caso dell'esponenziazione sarà trattato in seguito.

Proposizione 11.23. *$\alpha+\beta$ è successore se e solo se lo è β. Detto altrimenti, $\alpha + \beta$ è dello stesso "tipo" di β.*

Dim. Basta osservare che per definizione vale $\alpha + (\delta + 1) = (\alpha + \delta) + 1$. Quindi se β è successore lo è anche $\alpha + \beta$.

Inoltre se $\beta = \lambda$ è limite, allora $\alpha + \lambda$ non ha massimo per la proposizione 11.13 e dunque è anch'esso un ordinale limite. □

Proposizione 11.24. *$\alpha \cdot \beta$ è successore se e solo se α e β sono entrambi successori.*

Dim. Prima di tutto si osserva che se $\beta = \lambda$ è limite, allora $\alpha \cdot \lambda$ non ha massimo per la proposizione 11.18 (se $\alpha = 0$, allora il prodotto fa 0, che è limite).

Inoltre $\alpha \cdot (\delta + 1) = \alpha \cdot \delta + \alpha$ e dunque in questo caso si ottiene un successore se e solo se α è un successore (proposizione 11.23). □

Le operazioni dell'aritmetica ordinale godono solo di alcune delle usuali proprietà dell'aritmetica naturale, per esempio è facile vedere che somma e prodotto non sono commutative.

Proposizione 11.25. *(*) La somma ordinale è associativa, cioè per ogni α, β e γ ordinali vale l'uguaglianza $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.*

Dim. Per induzione transfinita su γ. Prima di tutto si osserva che $(\alpha+\beta)+0 = \alpha+\beta = \alpha+(\beta+0)$.

Inoltre $(\alpha + \beta) + (\gamma + 1) = ((\alpha + \beta) + \gamma) + 1 = (\alpha + (\beta + \gamma)) + 1 = \alpha + ((\beta + \gamma) + 1) = \alpha + (\beta + (\gamma + 1))$.

Infine, se λ è limite, allora $(\alpha+\beta)+\lambda = \bigcup_{\gamma\in\lambda}((\alpha+\beta)+\gamma) = \bigcup_{\gamma\in\lambda}(\alpha+(\beta+\gamma))$.

Ora si ha che $\beta+\lambda$ è limite per la proposizione 11.23 e dunque $\bigcup_{\gamma\in\lambda}(\alpha+(\beta+\gamma)) = \alpha+(\beta+\lambda)$, da cui la tesi. □

Proposizione 11.26. *(*) Il prodotto si distribuisce a destra rispetto alla somma, cioè per ogni α, β_1 e β_2 ordinali, vale l'uguaglianza $\alpha \cdot (\beta_1 + \beta_2) = \alpha \cdot \beta_1 + \alpha \cdot \beta_2$.*

Dim. Per induzione su β_2. Prima di tutto si osserva che $\alpha \cdot (\beta+0) = \alpha \cdot \beta = \alpha \cdot \beta + 0 = \alpha \cdot \beta + \alpha \cdot 0$.

Inoltre $\alpha\cdot(\beta+(\delta+1)) = \alpha\cdot((\beta+\delta)+1) = \alpha\cdot(\beta+\delta)+\alpha = (\alpha\cdot\beta+\alpha\cdot\delta)+\alpha$. Si conclude con la proprietà associativa.

Infine, se λ è limite, allora $\beta + \lambda$ è limite per la proposizione 11.23 e quindi $\alpha\cdot(\beta+\lambda) = \bigcup_{\gamma\in\lambda}\alpha\cdot(\beta+\gamma) = \bigcup_{\gamma\in\lambda}(\alpha\cdot\beta+\alpha\cdot\gamma)$. Dalla proposizione 11.24 anche $\alpha\cdot\lambda$ è limite e dunque $\bigcup_{\gamma\in\lambda}(\alpha\cdot\beta+\alpha\cdot\gamma) = \alpha\cdot\beta+\alpha\cdot\lambda$, da cui la tesi. □

Oss. Non vale invece la proprietà distributiva a sinistra: per esempio si può dimostrare che $(\omega + 1) \cdot \omega = \omega^2$, che è diverso da $\omega^2 + \omega$.

Proposizione 11.27. *(*) Il prodotto ordinale è associativo, cioè per ogni α, β e γ ordinali vale l'uguaglianza $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.*

Dim. Per induzione su γ. Per prima cosa si osserva che $(\alpha \cdot \beta) \cdot 0 = 0 = \alpha \cdot 0 = \alpha \cdot (\beta \cdot 0)$.

Inoltre $(\alpha\cdot\beta)\cdot(\gamma+1) = (\alpha\cdot\beta)\cdot\gamma+\alpha\cdot\beta = \alpha\cdot(\beta\cdot\gamma)+\alpha\cdot\beta = \alpha\cdot(\beta\cdot\gamma+\beta) = \alpha\cdot(\beta\cdot(\gamma+1))$. Si noti che si è usata la proprietà distributiva.

Infine, se λ è limite, allora $(\alpha\cdot\beta)\cdot\lambda = \bigcup_{\gamma\in\lambda}(\alpha\cdot\beta)\cdot\gamma = \bigcup_{\gamma\in\lambda}\alpha\cdot(\beta\cdot\gamma) = \alpha\cdot(\beta\cdot\lambda)$, dove l'ultima uguaglianza segue dalla proposizione 11.24. □

Per l'aritmetica ordinale valgono alcune delle proprietà delle potenze già note sui numeri naturali, ed è quanto mostrano le due proposizioni seguenti.

Proposizione 11.28. *Dati tre ordinali α, β e γ, si ha $\alpha^\beta \cdot \alpha^\gamma = \alpha^{\beta+\gamma}$.*

Dim. Per induzione su γ. Prima di tutto si osserva che $\alpha^\beta \cdot \alpha^0 = \alpha^\beta \cdot 1 = \alpha^\beta = \alpha^{\beta+0}$.

Inoltre $\alpha^\beta \cdot \alpha^{\gamma+1} = \alpha^\beta \cdot (\alpha^\gamma \cdot \alpha) = (\alpha^\beta \cdot \alpha^\gamma) \cdot \alpha = (\alpha^{\beta+\gamma}) \cdot \alpha = \alpha^{(\beta+\gamma)+1} = \alpha^{\beta+(\gamma+1)}$.

Se λ è limite, allora $\alpha^\beta \cdot \alpha^\lambda = \bigcup_{\gamma\in\lambda} \alpha^\beta \cdot \alpha^\gamma = \bigcup_{\gamma\in\lambda} \alpha^{\beta+\gamma} = \alpha^{\beta+\lambda}$. □

Proposizione 11.29. *Dati tre ordinali α, β e γ, si ha $(\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}$.*

Dim. Per induzione su γ. Prima di tutto si osserva che $(\alpha^\beta)^0 = 1 = \alpha^0 = \alpha^{\beta\cdot 0}$.

Inoltre $(\alpha^\beta)^{\gamma+1} = (\alpha^\beta)^\gamma \cdot \alpha^\beta = \alpha^{\beta\cdot\gamma} \cdot \alpha^\beta = \alpha^{\beta\cdot\gamma+\beta} = \alpha^{\beta\cdot(\gamma+1)}$.

Se λ è limite, allora $(\alpha^\beta)^\lambda = \bigcup_{\gamma\in\lambda} (\alpha^\beta)^\gamma = \bigcup_{\gamma\in\lambda} \alpha^{\beta\cdot\gamma} = \alpha^{\beta\cdot\lambda}$. □

Oss. Non vale invece la proprietà $\alpha^\gamma \cdot \beta^\gamma = (\alpha \cdot \beta)^\gamma$, come si può vedere prendendo $\alpha = 2$, $\beta = 3$ e $\gamma = \omega$.

Anche fra ordinali esistono, in una forma particolare, le operazioni di sottrazione e divisione, ed è quanto mostra il seguente

Teorema 11.5. *Valgono i seguenti fatti:*

1. *se α e β sono due ordinali tali che $\alpha \leq \beta$, allora esiste un unico ordinale γ tale che $\beta = \alpha + \gamma$. (**Sottrazione a destra**)*

2. *se α e β sono ordinali e $\beta \neq 0$, allora esistono e sono unici due ordinali δ e ρ tali che $\rho < \beta$ e $\alpha = \beta \cdot \delta + \rho$. (**Divisione euclidea**)*

Dim. 1. Si ha $\alpha + (\beta + 1) \geq \beta + 1 > \beta$ e dunque esistono ordinali γ tali che $\beta < \alpha + \gamma$. Si pone $\delta = min\,(\{\xi \in \beta + 1 \mid \beta < \alpha + \xi\})$.

Ora si prova che δ è un ordinale successore. Se per assurdo δ è un ordinale limite, allora o $\delta = 0$ (*Assurdo* perché $\alpha \leq \beta$) oppure $\beta < \alpha + \delta = \bigcup_{\xi\in\delta} \alpha + \xi$, da cui segue l'esistenza di uno $\xi \in \delta$ per cui $\beta < \alpha + \xi$ (*Assurdo* per la minimalità di δ).

Quindi $\delta = \gamma + 1$ per un certo ordinale γ e $\alpha + \gamma \leq \beta < \alpha + (\gamma + 1) = (\alpha + \gamma) + 1$, e dunque $\beta = \alpha + \gamma$.

L'unicità segue dal fatto che si può cancellare a sinistra.

2. Si procede come sopra, osservando innanzitutto che esistono degli ordinali γ tali che $\alpha < \beta \cdot \gamma$, per esempio $\alpha + 1$.

   Si pone $\gamma = min\,(\{\xi \in \alpha + 1 \mid \alpha < \beta \cdot \xi\})$ e si va a dimostrare che è un ordinale successore. Se per assurdo γ è un ordinale limite, allora o $\gamma = 0$ (*Assurdo* perché $\alpha < \beta \cdot \gamma$), oppure $\alpha < \beta \cdot \gamma = \bigcup_{\xi\in\gamma} \beta \cdot \xi$, da

cui segue l'esistenza di uno $\xi \in \gamma$ per cui $\alpha < \beta \cdot \xi$ (*Assurdo* per la minimalità di γ).

Dunque $\gamma = \delta + 1$ per un certo ordinale δ e $\beta \cdot \delta \leq \alpha$: per la sottrazione a destra esiste un unico ordinale ρ tale che $\alpha = \beta \cdot \delta + \rho$. Banalmente $\rho < \beta$.

L'unicità segue dalla seguente considerazione: se $\beta \cdot \delta_1 + \rho_1 = \beta \cdot \delta_2 + \rho_2$ con $\rho_1, \rho_2 < \beta$ e per assurdo $\delta_1 < \delta_2$, allora $\beta \cdot \delta_1 + \rho_1 < \beta \cdot \delta_1 + \beta = \beta \cdot (\delta_1 + 1) < \beta \cdot \delta_2 + \rho_2$ (*Assurdo*).

□

Oss. La sottrazione a sinistra può non esistere. Per esempio non esistono ordinali γ tali che $\beta = \gamma + \lambda$ se β è successore e λ è limite.

Non solo, qualora abbia soluzioni, queste possono essere infinite. Per esempio $\omega = n + \omega$ per ogni naturale n.

Esempio. Si calcolino quoziente e resto della divisione euclidea

$$(\omega^2 5 + \omega 3 + 12) \div (\omega 3 + 7)$$

Sol. Si cerca il minimo γ tale che $\omega^2 5 \lneq (\omega 3 + 7) \cdot \gamma$, cioè $\omega 5 + 1$ e si prende il predecessore $\omega 5$ (si è usato $(\omega 3 + 7) \cdot \omega = \omega^2$).

Ora si vede banalmente che $(\omega^2 5 + \omega 3 + 12) = (\omega 3 + 7) \cdot (\omega 5 + 1) + 5$. □

Il seguente corollario dimostra un fatto spesso utile nel calcolo ordinale.

Corollario 11.2. *Ogni ordinale α si può scrivere nella forma $\lambda + n$ dove λ è un ordinale limite (eventualmente 0).*

Dim. Basta fare la divisione euclidea fra α e ω e usare la proposizione 11.24.
□

Proposizione 11.30. *Se $\alpha > 1$, allora α^β è successore se e solo se α è successore e β è un naturale.*

Dim. Prima di tutto si osserva che se λ è limite, allora $\alpha^\lambda = \bigcup_{\gamma \in \lambda} \alpha^\gamma$, che non ha massimo per la proposizione 11.21 e dunque è limite.

Inoltre $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$, che è limite se α è limite.

Resta dunque da esaminare solo il caso in cui α e β sono entrambi successori, cioè $(\alpha + 1)^{\beta+1}$. Dal corollario 11.2 si ottiene $\beta + 1 = \lambda + n$ dove λ è un ordinale limite (eventualmente nullo). Se $\lambda \neq 0$ (cioè $\beta \geq \omega$), allora applicando n volte la definizione di esponenziale con esponente successore si arriva ad avere un prodotto in cui uno dei fattori è un ordinale limite perché ha per esponente un ordinale limite, dunque in questo caso si ottiene proprio un limite. Se $\lambda = 0$, cioè $\beta < \omega$, procedendo allo stesso modo sopra si ottiene un ordinale successore. □

Lemma 11.2. *Per ogni coppia di ordinali α e $\beta \geq 2$ vale $\beta^\alpha \geq \alpha$.*

Dim. Per induzione transfinita su α. Per prima cosa si osserva che $\beta^0 = 1 > 0$ e $\beta^1 = \beta > 1$.

Inoltre $\beta^{\alpha+1} = \beta^\alpha \cdot \beta \geq \alpha \cdot \beta > \alpha$ se $\alpha \geq 1$.

Se λ è limite, allora $\beta^\lambda = \bigcup_{\gamma\in\lambda} \beta^\gamma \geq \bigcup_{\gamma\in\lambda} \gamma = \lambda$. □

Teorema 11.6 (Forma normale di Cantor)**.** *Per ogni ordinale α esistono e sono unici un naturale k, una k-successione di ordinali $\alpha_1 > \alpha_2 > \cdots > \alpha_k$ e una k-successione di naturali $n_1, \ldots, n_k$ tali che $\alpha = \omega^{\alpha_1} \cdot n_1 + \cdots + \omega^{\alpha_k} \cdot n_k$.*

Dim. Si dimostra l'enunciato per induzione transfinita forte su α e dunque si suppone che ogni $\beta < \alpha$ abbia un'unica Forma normale di Cantor.

Per il lemma 11.2 vale $\omega^{\alpha+1} \geq \alpha + 1 > \alpha$, quindi l'insieme $A := \{\beta \in \alpha + 2 \mid \omega^\beta > \alpha\}$ è non vuoto.

Sia $\delta = min A$: ora si mostra che δ è un ordinale successore. Se per assurdo δ è limite, allora $\alpha \in \omega^\delta = \bigcup_{\gamma\in\delta} \omega^\gamma$ e dunque esiste $\gamma < \delta$ tale che $\alpha < \omega^\gamma$ ($\mathcal{A}ssurdo$ per la minimalità di δ).

Dunque $\delta = \beta + 1$ è un ordinale successore e inoltre $\omega^\beta \leq \alpha$.

Per divisione euclidea esistono un naturale n e un ordinale $\rho < \omega^\beta \leq \alpha$ tali che $\alpha = \omega^\beta \cdot n + \rho$. Per l'ipotesi induttiva ρ ha una Forma normale di Cantor e dunque anche α ne ha una.

Per l'unicità si procede per induzione transfinita forte su α. Se $\omega^{\alpha_1} \cdot n_1 + \cdots + \omega^{\alpha_k} \cdot n_k$ e $\omega^{\beta_1} \cdot m_1 + \cdots + \omega^{\beta_l} \cdot m_l$ sono due Forme normali di Cantor di α e per assurdo $\beta_1 < \alpha_1$, allora $\omega^{\beta_1} \cdot m_1 + \cdots + \omega^{\beta_l} \cdot m_l \leq \omega^{\beta_1} \cdot (m_1 + \cdots + m_l) < \omega^{\beta_1+1} \leq \omega^{\alpha_1} \leq \alpha$ ($\mathcal{A}ssurdo$).

Dunque $\alpha_1 = \beta_1$ e $\omega^{\alpha_1} \cdot n_1 + \cdots + \omega^{\alpha_k} \cdot n_k = \omega^{\alpha_1} \cdot m_1 + \cdots + \omega^{\beta_l} \cdot m_l$. Ora per l'unicità di quoziente e resto nella divisione euclidea si ottiene $n_1 = m_1$ e $\omega^{\alpha_2} \cdot n_2 + \cdots + \omega^{\alpha_k} \cdot n_k = \omega^{\beta_2} \cdot m_2 + \cdots + \omega^{\beta_l} \cdot m_l$. Adesso si conclude usando l'ipotesi induttiva. □

Oss. Allo stesso modo, dato un naturale $a \neq 0$, si può ottenere la scrittura in base a di un qualsiasi altro numero naturale n.

Definizione (Ordinale additivamente chiuso)**.** *Un ordinale α è detto **additivamente chiuso** se per ogni coppia di ordinali $\beta, \gamma < \alpha$ vale $\beta + \gamma < \alpha$.*

Per quanto riguarda gli ordinali additivamente chiusi, vale la seguente caratterizzazione:

Proposizione 11.31. *Dato un ordinale α, sono fatti equivalenti:*

1. *per ogni $\beta < \alpha$ vale $\beta + \alpha = \alpha$;*
2. *α è additivamente chiuso;*
3. *esiste un ordinale δ tale che $\alpha = \omega^\delta$ oppure $\alpha = 0$.*

Dim. Si dimostrano le varie implicazioni proprio nell'ordine proposto dalla proposizione.

(1) $\to$ (2) : dati due ordinali $\beta, \gamma \in \alpha$, $\beta + \gamma < \beta + \alpha = \alpha$.

(2) $\to$ (3) : procedendo come nella dimostrazione della Forma normale di Cantor, si prende ω^δ la massima potenza di ω minore o uguale ad α, e per divisione euclidea si ottiene $\alpha = \omega^\delta \cdot n + \rho$ dove n è un numero naturale e ρ è un ordinale minore di ω^δ.

Ora si vuole provare che $\rho = 0$ e $n = 0, 1$.

Se $\rho \geq 1$, allora $\omega^\delta \cdot n < \alpha$ e dunque $\omega^\delta \cdot n + \omega^\delta \cdot n < \alpha$, ma questo è *Assurdo* perché $\rho < \omega^\delta$. Dunque $\rho = 0$.

Se $n > 1$, allora $\omega^\delta \cdot (n-1) < \alpha$ e dunque $\omega^\delta \cdot (n-1) + \omega^\delta \cdot (n-1) < \alpha$, ma questo è un altro *Assurdo*.

(3) $\to$ (1) : per ipotesi esiste un ordinale δ tale che $\alpha = \omega^\delta$. Se $\beta < \alpha$, allora la sua Forma normale di Cantor è $\beta = \omega^{\beta_1} \cdot n_1 + \cdots + \omega^{\beta_k} \cdot n_k$ dove $\beta_1 < \delta$.

Per provare la tesi, basta mostrare che se $\gamma < \delta$, allora $\omega^\gamma + \omega^\delta = \omega^\delta$.

Banalmente $\omega^\gamma + \omega^\delta = \bigcup_{\xi \in \omega^\delta} \omega^\gamma + \xi \supseteq \bigcup_{\xi \in \omega^\delta} \xi = \omega^\delta$.

L'altro contenimento segue dal fatto che, essendo ω^δ un ordinale limite e $\omega^\gamma < \omega^\delta$, allora esiste $\xi_1 \in \omega^\delta$ tale che $\xi_1 > \omega^\gamma$ e $\xi_1 > \xi$, da cui segue $\xi_1 + \xi_1 > \omega^\gamma + \xi$.

□

Definizione (Ordinale moltiplicativamente chiuso)**.** *Un ordinale α è detto* ***moltiplicativamente chiuso*** *se per ogni coppia di ordinali $\beta, \gamma < \alpha$ vale $\beta \cdot \gamma < \alpha$.*

Oss. Un ordinale moltiplicativamente chiuso lo è anche additivamente, perché se $\beta, \gamma < \alpha$ e α è moltiplicativamente chiuso, allora, posto *wlog* $\beta \geq \gamma$, si ottiene $\beta + \gamma \leq \beta + \beta = \beta \cdot 2 < \alpha$.

Come per gli ordinali additivamente chiusi, anche in questo caso c'è una importante caratterizzazione, ma prima si dimostra un'utile proprietà dell'aritmetica ordinale.

Proposizione 11.32. *Dato un ordinale $\omega^{\beta_1} \cdot n_1 + \cdots + \omega^{\beta_k} \cdot n_k$ in Forma normale di Cantor, vale $(\omega^{\beta_1} \cdot n_1 + \cdots + \omega^{\beta_k} \cdot n_k) \cdot \omega = \omega^{\beta_1 + 1}$.*

Dim. Si ha

$$(\omega^{\beta_1} \cdot n_1 + \cdots + \omega^{\beta_k} \cdot n_k) \cdot \omega = \bigcup_{n \in \omega} (\omega^{\beta_1} \cdot n_1 + \cdots + \omega^{\beta_k} \cdot n_k) \cdot n$$

e banalmente

$$(\omega^{\beta_1} \cdot n_1 + \cdots + \omega^{\beta_k} \cdot n_k) \cdot n = \omega^{\beta_1} \cdot (n_1 \cdot n) + \omega^{\beta_2} \cdot n_2 + \cdots + \omega^{\beta_k} \cdot n_k$$

Dunque

$$(\omega^{\beta_1} \cdot n_1 + \cdots + \omega^{\beta_k} \cdot n_k) \cdot \omega = \bigcup_{n \in \omega} \omega^{\beta_1} \cdot (n_1 \cdot n) + \omega^{\beta_2} \cdot n_2 + \cdots + \omega^{\beta_k} \cdot n_k = \omega^{\beta_1 + 1}$$

□

Ecco dunque la preannunciata caratterizzazione degli ordinali moltiplicativamente chiusi.

Proposizione 11.33. *Dato un ordinale α, sono fatti equivalenti:*

1. *per ogni $\beta < \alpha$ vale $\beta \cdot \alpha = \alpha$;*
2. *α è moltiplicativamente chiuso;*
3. *esiste un ordinale δ tale che $\alpha = \omega^{\omega^\delta}$ oppure $\alpha = 0$.*

Dim. Si dimostrano le varie implicazioni proprio nell'ordine proposto dalla proposizione.

(1) → (2) : dati $\beta, \gamma < \alpha$, se $\beta = 0$, allora la tesi è banalmente vera, altrimenti $\beta \cdot \gamma < \beta \cdot \alpha = \alpha$.

(2) → (3) : se α è moltiplicativamente chiuso, allora è anche additivamente chiuso, e dunque esiste un ordinale δ tale che $\alpha = \omega^\delta$.

Ora si vuole provare che δ è additivamente chiuso e questo è molto semplice. Infatti se $\beta, \gamma < \delta$, allora $\omega^\beta, \omega^\gamma < \omega^\delta$ e dunque $\omega^{\beta+\gamma} = \omega^\beta \cdot \omega^\gamma < \omega^\delta$, da cui segue $\beta + \gamma < \delta$, cioè la tesi.

(3) → (1) : se esiste un ordinale δ tale che $\alpha = \omega^{\omega^\delta}$, allora ogni $\beta < \alpha$ ha forma normale di Cantor del tipo $\omega^{\beta_1} \cdot n_1 + \cdots + \omega^{\beta_k} \cdot n_k$ con $\beta_1 < \omega^\delta$ e dunque, per la proposizione 11.32, si ottiene

$$\begin{aligned}
\beta \cdot \alpha &= (\omega^{\beta_1} \cdot n_1 + \cdots + \omega^{\beta_k} \cdot n_k) \cdot \omega^{\omega^\delta} = \\
&= (\omega^{\beta_1} \cdot n_1 + \cdots + \omega^{\beta_k} \cdot n_k) \cdot (\omega \cdot \omega^{\omega^\delta}) = \\
&= ((\omega^{\beta_1} \cdot n_1 + \cdots + \omega^{\beta_k} \cdot n_k) \cdot \omega) \cdot \omega^{\omega^\delta} = \\
&= \omega^{\beta_1 + 1} \cdot \omega^{\omega^\delta} = \omega^{(\beta_1+1)+\omega^\delta} = \omega^{\omega^\delta} = \alpha
\end{aligned}$$

□

Prima di concludere il capitolo si mostra una curiosa applicazione degli ordinali in un ambito alquanto inaspettato.

Definizione (Successione di Goodstein)**.** *Dato un numero naturale $a \neq 0$, si dice* ***successione di Goodstein*** *relativa ad a la successione*

$$\begin{cases} a_0 = a \\ a_{n+1} = m \end{cases}$$

dove m è il numero naturale che si ottiene scrivendo a_n in base $n+2$, sostituendo la base con la base $n+3$ e sottraendo 1 (se $a_n = 0$ allora si pone $a_{n+1} = 0$).

Esempio. Scegliendo $a = 19$ si ottiene

$$\begin{aligned} a_0 &= 19 = 2^4 + 2 + 1 \\ a_1 &= 3^4 + 3 + 1 - 1 = 3^4 + 3 = 84 \\ a_2 &= 4^4 + 4 - 1 = 4^4 + 3 = 259 \\ a_3 &= 5^4 + 3 - 1 = 5^4 + 2 = 627 \\ a_4 &= 6^4 + 2 - 1 = 6^4 + 1 = 1297 \\ a_5 &= 7^4 + 1 - 1 = 7^4 = 2401 \\ a_6 &= 8^4 - 1 = 8^3 \cdot 7 + 8^2 \cdot 7 + 8 \cdot 7 + 7 = 4095 \\ a_7 &= 9^3 \cdot 7 + 9^2 \cdot 7 + 9 \cdot 7 + 7 - 1 = 5739 \\ &\dots \end{aligned}$$

Oss. Apparentemente le successioni di Goodstein sembrerebbero crescere e non poco velocemente... invece vale il seguente risultato:

Proposizione 11.34. *Ogni successione di Goodstein è definitivamente nulla.*

Dim. Data la successione di Goodstein relativa ad a, l'n-esimo termine della successione è del tipo $a_n = (n+2)^{b_1} \cdot k_1 + \dots + (n+2)^{b_l} \cdot k_l$.

Ora al termine n-esimo della successione si associa l'ordinale $\alpha_n = (\omega)^{b_1} \cdot k_1 + \dots + (\omega)^{b_l} \cdot k_l$ e poi basta osservare che la succesione degli α_n è strettamente decrescente e dunque finita (in un buon ordine non vi sono catene discendenti).

Dunque per un certo n vale $\alpha_n = 0$, e poiché banalmente $a_n \leq \alpha_n$ si ottiene $a_n = 0$. □

Si conclude il capitolo con un passaggio fondamentale per lo studio delle cardinalità, che sarà il punto decisivo per la ricerca di rappresentanti canonici per l'equipotenza.

Definizione (Hartogs)**.** *Dato un insieme A si definisce il suo* ***insieme di Hartogs*** *come l'insieme $\mathcal{H}(A) := \{\beta \mid \beta \text{ ordinale }, |\beta| \leq |A|\}$.*

Oss. Per ogni insieme A si ha che $\mathcal{H}(A)$ è effettivamente un insieme perché si considera la proprietà $P(x, y)$ definita da "x è un buon ordine e y è l'unico ordinale isomorfo a x oppure $y = \emptyset$", applicata all'insieme di tutti e soli i buoni ordini sui sottoinsiemi di A, cioè $\Lambda := \{(X, \leq) \in \mathcal{P}(A) \times \mathcal{P}(A \times A) \mid (X, <) \text{ è un buon ordine}\}$.

Proposizione 11.35. *Per ogni insieme A si ha che $\mathcal{H}(A)$ è un ordinale.*

Dim. Poiché $\mathcal{H}(A)$ è un insieme di ordinali, per provare che è un ordinale basta dimostrare che è transitivo.

Se $\alpha \in \beta \in \mathcal{H}(A)$, allora $\alpha \subsetneq \beta$ e dunque $|\alpha| \leq |\beta| \leq |A|$. Perciò $\alpha \in \mathcal{H}(A)$, che dunque è transitivo e pure un ordinale. □

Proposizione 11.36. *Per ogni insieme A vale $|\mathcal{H}(A)| \not\leq |A|$.*

Dim. Se per assurdo $|\mathcal{H}(A)| \leq |A|$, allora $\mathcal{H}(A) \in \mathcal{H}(A)$, ma questo p *Assurdo* perché $\mathcal{H}(A)$ è un ordinale. □

Oss. Nel capitolo 12 si proverà l'equivalenza fra l'Assioma di scelta e la totalità dell'ordine fra cardinalità, e dunque seguirà che per ogni insieme A vale $|A| < |\mathcal{H}(A)|$.

12 Forme equivalenti dell'Assioma di scelta (2)

$\mathcal{E}$cco la tanto attesa seconda parte sulle forme equivalenti dell'Assioma di scelta.

Teorema 12.1. *(ZF) Sono fatti equivalenti:*

1. *Assioma di scelta (AC);*
2. *Lemma di Zorn: "ogni insieme non vuoto e parzialmente ordinato in cui ogni catena ha un maggiorante ha un elemento massimale";*
3. *Teorema di Zermelo: "ogni insieme è bene ordinabile";*
4. *Confrontabilità: per ogni coppia di insiemi A e B vale almeno una fra $|A| \leq |B|$ e $|B| \leq |A|$;*
5. *per ogni insieme infinito A vale $|A \times A| = |A|$.*

Lemma 12.1. *Lemma di Zorn $\rightarrow$ "se A è infinito, allora $\aleph_0 \leq |A|$".*

Dim. Se $P := \{f \colon B \to A \mid f$ è iniettiva e B è un seg. iniz. di $\omega\}$, allora P è banalmente non vuoto. Inoltre esso è parzialmente ordinato da $\subseteq$ e ogni catena ha l'unione come maggiorante, dunque per il Lemma di Zorn P ha un elemento massimale φ. È banale osservare che $\mathcal{D}om\,\varphi = \omega$ perché altrimenti φ sarebbe estendibile contro la sua massimalità. □

Lemma 12.2. *Lemma di Zorn $\rightarrow$ "se A e B sono insiemi infiniti e $|A| = |B|$ allora $|A \cup B| = |A| = |B|$".*

Dim. Prima di tutto si osserva che $|A| \leq |A \cup B| \leq |A \times \{0,1\}|$ e dunque basta dimostrare $|A \times \{0,1\}| \leq |A|$ e concludere con Cantor-Bernstein.

L'insieme $P := \{f \colon B \times \{0,1\} \to B \mid B \subseteq A \wedge f$ iniettiva$\}$ è non vuoto perché A ha un sottoinsieme numerabile e $\aleph_0 \cdot 2 = \aleph_0$ ed è parzialmente ordinato rispetto al contenimento. Inoltre ogni catena ha l'unione come maggiorante, dunque per il lemma di Zorn P ha un elemento massimale $\varphi \colon B \times \{0,1\} \to B$.

Se per assurdo $|B| < |A|$, allora φ è banalmente estendibile, contro la sua massimalità. Dunque $|B| = |A|$, da cui segue la tesi. □

Oss. Dal Lemma 12.2 segue in modo del tutto banale l'implicazione Lemma di Zorn $\rightarrow$ "se A è un insieme finito, allora $|A| = |A \times n|$ per ogni naturale n".

Lemma 12.3. *Lemma di Zorn $\rightarrow$ Confrontabilità.*

Dim. L'insieme $\{f\colon A \to B \mid f \text{ iniettiva}, A \subseteq X \wedge B \subseteq Y\}$ è banalmente non vuoto e parzialmente ordinato rispetto al contenimento. Inoltre ogni catena ha l'unione come maggiorante, dunque per il Lemma di Zorn ha un elemento massimale φ. È banale osservare che deve valere almeno una fra $\mathcal{D}om\,\varphi = X$ e $\mathcal{I}m\,\varphi = Y$, altrimenti$\varphi$ sarebbe estendibile, contro la sua massimalità.

Nel primo caso si ottiene $|X| \leq |Y|$ e nel secondo $|Y| \leq |X|$, da cui la tesi. □

Si passa ora alla dimostrazione del Teorema:

Dim.

- (1)→(2): DA RIVEDERE Dato un insieme non vuoto e parzialmente ordinato $(X, \leq)$ in cui ogni catena ha un maggiorante, per l'Assioma di scelta esiste $f\colon \mathcal{P}(X) \to X$ funzione di scelta. Sia inoltre $p \in X$ un elemento qualsiasi.

  Ora si definisce *f-catena* per X ogni catena $C \subseteq X$ bene ordinata e tale che $p \in C$ e per ogni $c \in C$ valga $c = f(\{x \in X \mid \forall c' \in C(c' < c \to x > c')\})$.

  Si prova che due diverse f-catene C e C' per X sono una segmento iniziale dell'altra. Per la tricotomia dei buoni ordini si assume *wlog* l'esistenza di un isomorfismo d'ordine $\varphi\colon C' \to C_c$ (dove $c \in C$) e si procede a dimostrare che φ è l'identità su C'. Se per assurdo non è così, allora si considera $m = min\{x \in C' \mid \varphi(x) \neq x\}$ e si osserva che $C'_m = C_{\varphi(m)}$ quindi hanno gli stessi maggioranti in X e da questo segue $m = \varphi(m)$ ($\mathcal{A}ssurdo$).

  A queso punto si è quasi concluso: basta infatti osservare che per la proposizione... l'unione di tutte le f-catene per X è una f-catena e non ha maggioranti stretti in X (altrimenti si potrebbe estendere a una f-catena più grande). Per ipotesi ha un maggiorante, che dunque è anche massimo della catena e massimale in X.

- (2)→(5): l'insieme $P := \{f\colon B \times B \to B \mid f \text{ iniettiva} \wedge B \subseteq A \wedge B \text{ infinito}\}$ è non vuoto perché per il lemma 12.1 A ha un sottoinsieme numerabile e $\aleph_0 \cdot \aleph_0 = \aleph_0$.

  Inoltre P è parzialmente ordinato rispetto al contenimento e ogni catena ha l'unione come maggiorante, dunque per il Lemma di Zorn P ha un elemento massimale $\varphi\colon B \times B \to B$ e dunque $|B \times B| = |B|$ per Cantor-Bernstein.

  Ora si vuole provare che $|B| = |A|$, infatti in tal caso $|A| = |B| = |B \times B| = |A \times A|$, cioè la tesi.

  Se per assurdo $|B| < |A|$ si dimostra che $|B| < |A \setminus B|$, infatti se fosse $|A \setminus B| \leq |B|$ (una delle due deve valere per la confrontabilità, garantita dal lemma 12.3) allora sarebbe $|A| \leq |B|$ per il lemma 12.2.

Dunque esiste $B' \subseteq A \setminus B$ tale che $|B'| = |B| < |A|$ e per il lemma 12.2 esiste $g\colon B' \times \{0,1,2\} \to B'$ bigettiva.

Ora si estende φ a

$$\varphi^*\colon B \cup B' \times B \cup B' \to B \cup B'$$
$$(x,y) \mapsto \begin{cases} \varphi(x) \text{ se } x,y \in B \\ g(x,0) \text{ se } x \in B' \text{ e } y \in B \\ g(y,1) \text{ se } x \in B \text{ e } y \in B' \\ g(x,2) \text{ se } x,y \in B' \end{cases}$$

e si osserva che φ^* è iniettiva, contro la massimalità di φ.

- (5)→(3): se A è finito la tesi è ovvia. Se A è infinito, allora si pone $B := A \cup \mathcal{H}(A)$ ($wlog\ A \cap \mathcal{H}(A) = \emptyset$). Ora $|B \times B| = |B|$ e dunque esiste $\varphi\colon B \times B \to B$ bigettiva.

  Per ogni $a \in A$ si definisce

  $$\theta_a\colon \mathcal{H}(A) \to B$$
  $$x \mapsto \varphi(a,x)$$

  Per ogni $a \in A$ si ha che θ_a è iniettiva (φ è iniettiva) e $\mathcal{I}m\,\theta_a \nsubseteq A$ perché $|\mathcal{H}(A)| \not\leq |A|$ e dunque $\mathcal{I}m\,\theta_a \cap \mathcal{H}(A) \neq \emptyset$.

  Allora la funzione

  $$\phi\colon A \to \mathcal{H}(A)$$
  $$a \mapsto min\,(\mathcal{I}m\,\theta_a \cap \mathcal{H}(A))$$

  è iniettiva e dunque A è bene ordinabile.

- (3)→(1): Data una famiglia non vuota X di insiemi non vuoti, per il Teorema di Zermelo $\bigcup X$ è bene ordinabile, cioè esiste una relazione binaria $\leq$ su $\bigcup X$ tale che $(\bigcup X,\ \leq)$ è un buon ordine.

  Allora la funzione

  $$f\colon X \to \bigcup X$$
  $$x \mapsto min\,(x)$$

  è una funzione di scelta per X.

- (3)↔(4):

  → : per il Teorema di Zermelo siano $(A,\leq)$ e $(B,\leq)$ buoni ordini. Allora esistono due ordinali α e β tali che $A \cong \alpha$ e $B \cong \beta$. Per la tricotomia degli ordinali o $\alpha = \beta$ e in tal caso $|A| = |B|$, o $\alpha \subsetneq \beta$ e in tal caso $|A| \leq |B|$, o $\beta \subsetneq \alpha$ e in tal caso $|B| \leq |A|$.

$\leftarrow$: dalla teoria si sa che $|\mathcal{H}(A)| \not\leq |A|$, dunque per la confrontabilità si ottiene $|A| \leq |\mathcal{H}(A)|$, cioè che esiste una funzione $f\colon A \to \mathcal{H}(A)$ iniettiva. Ponendo $a_1 < a_2 \leftrightarrow f(a_1) < f(a_2)$, si ha che f è una funzione strettamente crescente da A in un buon ordine e dunque A è isomorfo a un sottoinsieme di un insieme bene ordinato e pertanto è bene ordinato.

□

Oss. Per bene ordinare un insieme basta trovare una funzione iniettiva da esso in un insieme bene ordinato.

13 Cardinali

Avendo studiato a fondo varie forme equivalenti dell'Assioma di scelta, queste saranno un enorme strumento nello studio dei cardinali, che si vanno giusto ora a definire.

Definizione (Cardinale)**.** *Si dice* ***cardinale*** *o* ***ordinale iniziale*** *un ordinale α tale che per ogni $\beta < \alpha$ vale $|\beta| < |\alpha|$.*

Oss. È facile osservare che:

- i naturali sono tutti e soli i cardinali finiti;
- ogni cardinale infinito è un ordinale limite;
- il più piccolo cardinale infinito è ω, che si denota $\aleph_0$;
- per ogni insieme A si ha che $\mathcal{H}(A)$ è un cardinale (per la confrontabilità vale $|A| < |\mathcal{H}(A)|$);
- se $\mathcal{F}$ è una famiglia di cardinali, allora $\bigcup \mathcal{F}$ è un cardinale;
- fra cardinali l'ordinamento dato da $\in$ e quello dato dalla cardinalità sono due concetti equivalenti.

Si è ora pronti per un risultato atteso da tempo e per cui è stata sviluppata tutta la teoria degli ordinali, ovvero i cardinali faranno da "rappresentanti canonici" per l'equipotenza. Vale infatti il seguente

Teorema 13.1. *(AC) ogni insieme A è equipotente a uno e un solo cardinale k. In questo caso si scrive $|A| = k$.*

Dim. Si dimostra prima l'esistenza di un tale cardinale e poi l'unicità.

Per il Teorema di Zermelo esiste una relazione $\leq$ su A tale che $(A, \leq)$ è un buon ordine. Come buon ordine $(A, \leq)$ è isomorfo a un unico ordinale α e dunque ad esso equipotente. Se α è un cardinale allora si è concluso. Altrimenti si considera $\beta = min\{\gamma \in \alpha \mid |\gamma| = |\alpha|\}$ ed è banale osservare che β è un cardinale.

L'unicità deriva immediatamente dalla definizione di cardinale. □

Il concetto che si sta per introdurre è un punto cruciale per lo studio dei cardinali.

Definizione. *Si definisce per ricorsione transfinita la "sequenza" degli* ***aleph****:*

$$\begin{cases} \aleph_0 = \omega \\ \aleph_{\alpha+1} = H(\aleph_\alpha) \\ \aleph_\lambda = \bigcup_{\gamma \in \lambda} \aleph_\gamma \qquad \textit{se } \lambda \textit{ limite} \end{cases}$$

Oss. Si verifica facilmente che:

- ogni $\aleph_\alpha$ è un cardinale infinito;
- la "sequenza" degli $\aleph_\alpha$ è strettamente crescente;
- $\aleph_{\alpha+1}$ è il più piccolo cardinale maggiore di $\aleph_\alpha$.

Inoltre si denota equivalentemente $\aleph_\alpha$ con ω_α quando si vuole fare riferimento alle sue proprietà come ordinale (per esempio nelle operazioni ordinali).

Proposizione 13.1. *(*) Per ogni ordinale α vale $\alpha \leq \aleph_\alpha$.*

Dim. Per induzione transfinita:

- $\aleph_0 = \omega$ e $0 \in \omega$;
- $\mathrm{P}(\alpha) \to \mathrm{P}(\alpha{+}1)$: per ipotesi induttiva $\alpha \leq \aleph_\alpha$, dunque $\alpha{+}1 \leq \aleph_\alpha{+}1 < \aleph_{\alpha+1}$, dove l'ultima disuguaglianza è data dal fatto che $\aleph_\alpha + 1$ ha la stessa cardinalità di $\aleph_\alpha$;
- λ limite: si deve provare $\lambda \leq \aleph_\lambda$, cioè $\lambda \subseteq \bigcup_{\alpha<\lambda} \aleph_\alpha$. Per ipotesi induttiva, per ogni $\alpha < \lambda$ si ha $\alpha \leq \aleph_\alpha$. Ci sono due possibilità. Se $\alpha = \aleph_\alpha$, allora $\alpha \in \aleph_{\alpha+1}$ e dunque $\alpha \in \aleph_\lambda$. Se $\alpha \in \aleph_\alpha$ allora $\alpha \in \aleph_\lambda$.

□

Oss. A questo punto una domanda lecita sarebbe "esistono cardinali k tali che $k = \aleph_k$? Per quanto possa sembrare paradossale, la risposta è affermativa. Infatti, se si definisce per ricorsione numerabile con rimpiazzamento la seguente successione

$$\begin{cases} k_0 = \aleph_0 \\ k_{n+1} = \aleph_{k_n} \end{cases}$$

e si pone $k = \bigcup k_n$ si ottiene un cardinale con la proprietà cercata.

Infatti k è un cardinale perché è unione di cardinali, e dunque è anche un ordinale limite. Perciò $\aleph_k = \bigcup_{\gamma\in k} \aleph_\gamma$ e banalmente $k \subseteq \aleph_k$. L'altro contenimento deriva dal fatto che i k_n sono illimitati in k (si veda la definizione di "illimitato" poco più avanti nel capitolo).

Si può dire che la "sequenza" degli ordinali "rincorre" quella degli "aleph", e in certi punti le due arrivano a coincidere, poi si riallontanano e ricomincia l'inseguimento...

Si è dimostrato che ogni $\aleph_\alpha$ è un cardinale infinito. Il Teorema seguente prova che vale anche il viceversa, cioè che gli $\aleph_\alpha$ sono tutti e soli i cardinali infiniti e dunque, dato un insieme A, si ha che A è finito oppure A è equipotente ad uno e un solo $\aleph_\alpha$.

Teorema 13.2. *Ogni cardinale infinito è un $\aleph_\alpha$.*

Dim. Se k è un cardinale infinito, vale $k \leq \aleph_k < \aleph_{k+1}$ e dunque esiste $\alpha := min\{\beta \in k+2 \mid k < \aleph_\beta\}$. È banale osservare che α è un ordinale successore, cioè $\alpha = \gamma + 1$ per un certo ordinale γ ed è altrettanto banale che $k = \aleph_\gamma$. □

Definizione (Somma di due cardinali)**.** *Se k e μ sono cardinali si definisce la loro somma $k + \mu$ come l'unico cardinale in bigezione con $A \cup B$ dove A e B sono due insiemi qualsiasi tali che $|A| = k$, $|B| = \mu$ e $A \cap B = \emptyset$.*

Definizione (Prodotto di due cardinali)**.** *Se k e μ sono cardinali si definisce il loro prodotto $k \cdot \mu$ come l'unico cardinale in bigezione con $A \times B$ dove A e B sono due insiemi qualsiasi tali che $|A| = k$ e $|B| = \mu$.*

Definizione (Esponenziazione)**.** *Se k e μ sono cardinali si definisce la loro esponenziazione k^μ come l'unico cardinale in bigezione con A^B dove A e B sono due insiemi qualsiasi tali che $|A| = k$ e $|B| = \mu$.*

Oss. Le tre definizioni sopra sono ben poste per quanto già dimostrato nel capitolo 7.

Per lo stesso motivo sull'esponenziazione valgono le solite proprietà delle potenze, cioè se k, μ, ν sono cardinali, allora:

- $k^\mu \cdot k^\nu = k^{\mu+\nu}$;
- $(k^\mu)^\nu = k^{\mu \cdot \nu}$.

Inoltre si potrebbe dimostrare che somma e prodotto sono associative e commutative, e che valgono le due proprietà distributive del prodotto rispetto alla somma, ma si evita di farlo perché nel caso finito questo è già stato dimostrato (anche se bisognerebbe provare che queste nuove definizioni rispettano quelle vecchie) e per il caso infinito l'aritmetica cardinale diventa banale, come mostra il seguente

Teorema 13.3. *Per ogni naturale n e per ogni ordinale α vale*

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

Per ogni coppia di ordinali α e β vale

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

Dim.

- Vale la seguente catena di disuguaglianze:

$$\aleph_\alpha \leq \aleph_\alpha + n \leq \aleph_\alpha + \aleph_\alpha = \aleph_\alpha \cdot 2 \leq \aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$$

dove l'ultima uguaglianza segue dall'Assioma di scelta.

Si conclude con Cantor-Bernstein.

- Vale la seguente catena di disuguaglianze:

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

  dove l'ultima uguaglianza segue dall'Assioma di scelta.

  Si conclude come sopra con Cantor-Bernstein.

□

A differenza di somma e prodotto, l'esponenziazione è molto più complessa.

L'ipotesi del continuo (CH, "continuum hypothesis"), cioè $2^{\aleph_0} = \aleph_1$, così come l'ipotesi del continuo generalizzata (GCH, "generalized continuum hypothesis"), cioè $2^{\aleph_\alpha} = \aleph_{\alpha+1}$, sono indecidibili in ZFC.

Inoltre si dimostra (sempre fuori da questo corso) che, per esempio, si potrebbe assumere come ulteriore assioma $2^{\aleph_0} = \aleph_4$, oppure $2^{\aleph_0} = \aleph_{17}$, ma non $2^{\aleph_0} = \aleph_\omega$ (quest'ultimo fatto sarà provato più avanti nella dispensa).

Definizione. *Dato un cardinale infinito $k = \aleph_\alpha$ si definisce il suo* ***cardinale successore*** $k^+ := \aleph_{\alpha+1}$. *Un cardinale infinito che non è successore, cioè $\aleph_\lambda$ con λ ordinale limite, è detto* ***cardinale limite****.*

Oss. Per ogni cardinale successore k^+ vale $k^+ \leq 2^k$ perché k^+ è il più piccolo cardinale maggiore di k e $k \lneq 2^k$ per il Teorema di Cantor.

Il seguente è un primo risultato sull'esponenziazione:

Proposizione 13.2. *Se k e μ sono cardinali tali che $2 \leq k \leq \mu^+$ e μ è infinito, allora $k^\mu = 2^\mu$.*

Dim.

$$2^\mu \leq k^\mu \leq (\mu^+)^\mu \leq (2^\mu)^\mu = 2^{\mu \cdot \mu} = 2^\mu$$

□

Oss. La Proposizione precedente dimostra in particolare che per ogni ordinale α vale $\aleph_{\alpha+1}^{\aleph_\alpha} = \aleph_\alpha^{\aleph_\alpha} = \aleph_1^{\aleph_\alpha} = \aleph_0^{\aleph_\alpha} = 35^{\aleph_\alpha} = 2^{\aleph_\alpha}$.

Per esempio $\aleph_1^{\aleph_0} = 2^{\aleph_0} = \mathfrak{c}$ e $\aleph_0^{\aleph_1} = 2^{\aleph_1}$, anche se $\omega^{\omega_1} = \omega_1$.

Si vuole dunque notare il fatto che l'esponenziazione ordinale e l'esponenziazione cardinale sono due concetti ben distinti! Ed è anche per questo che si usano simboli diversi per indicare gli stessi insiemi, come $\aleph_0$ al posto di ω.

Riguardo alla cardinalità di un'esponenziazione ordinale, vale il seguente risultato

Proposizione 13.3. *(*) Se α e β sono ordinali infiniti, allora*

$$|\alpha + \beta| = |\alpha \cdot \beta| = |\alpha^\beta| = max\{|\alpha|, |\beta|\}$$

Dim. Si dimostra in ordine che $|\alpha+\beta| = max\{|\alpha|, |\beta|\}$, $|\alpha\cdot\beta| = max\{|\alpha|, |\beta|\}$ e $|\alpha^\beta| = max\{|\alpha|, |\beta|\}$.

1. Per la proposizione .. si ha che $\alpha + \beta$ è equipotente ad un'unione disgiunta di due insiemi di cardinalità rispettivamente $|\alpha|$ e $|\beta|$, da cui la tesi.

2. Si prova $|\alpha \cdot \beta| = max\{|\alpha|, |\beta|\}$ per induzione transfinita su β:

   - se $\beta = 0$, allora la tesi è vera a vuoto;
   - P(β)→P($\beta+1$): se β è finito allora l'implicazione è vera a vuoto. Altrimenti, per definizione $\alpha \cdot (\beta + 1) = \alpha \cdot \beta + \alpha$ e da (1) si ottiene $|\alpha \cdot (\beta + 1)| = max\{|\alpha \cdot \beta|, |\alpha|\}$. Per l'ipotesi induttiva $|\alpha \cdot \beta| = max\{|\alpha|, |\beta|\}$, dunque $|\alpha \cdot (\beta + 1)| = max\{|\alpha|, |\beta|\} = max\{|\alpha|, |\beta + 1|\}$ dove l'ultima uguaglianza segue dal fatto che $|\beta| = |\beta + 1|$ perché β è infinito.
   - λ limite: $|\alpha \cdot \lambda| = |\bigcup_{\gamma\in\lambda} \alpha \cdot \gamma| \leq max\{|\lambda|, sup\{max\{|\alpha|, |\gamma|\}\}\} = max\{|\alpha|, |\lambda|\}$ (si è usato un Teorema sulle somme infinite di cardinali che sarà visto più avanti).

     L'altra disuguaglianza è banale.

3. Per induzione transfinita su β:

   - Se $\beta = 0$, allora la tesi è vera a vuoto.
   - P(β)→P($\beta+1$): per definizione $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$, dunque $|\alpha^{\beta+1}| = |\alpha^\beta \cdot \alpha| = max\{|\alpha^\beta|, |\alpha|\} = max\{max\{|\alpha|, |\beta|\}, |\alpha|\} = max\{|\alpha|, |\beta|\}$.
   - Se λ è limite, allora $|\alpha^\lambda| = |\bigcup_{\gamma\in\lambda} \alpha^\gamma| \leq max\{|\lambda|, sup\{max\{|\alpha|, |\gamma|\}\}\} = max\{|\alpha|, |\lambda|\}$ (si è usato un Teorema sulle somme infinite di cardinali che sarà visto più avanti).

     L'altra disuguaglianza è banale.

□

Oss. L'unica operazione interessante dal punto di vista della cardinalità è l'esponenziazione cardinale, in quanto anche l'esponenziazione ordinale ha cardinalità data dal massimo delle cardinalità fra i due operandi.

Nel capitolo 7 si sono già visti degli esempi di cardinalità degli insiemi del tipo $[A]^{|B|}$, cioè l'insieme dei sottoinsiemi di A equipotenti a B.

A tal proposito, vale la seguente

Proposizione 13.4. *Per ogni coppia di cardinali μ e k tali che k è infinito e $\mu \leq k$ vale $|[k]^\mu| = k^\mu$.*

Dim. La funzione

$$\begin{aligned}\varphi\colon \mathcal{F}un(\mu,k) &\to [k]^{\leq\mu}\\ f &\mapsto \mathcal{I}m(f)\end{aligned}$$

è ben definita e surgettiva, dunque si ottiene (usando l'Assioma di scelta)

$$|[k]^{\mu}| \leq |[k]^{\leq\mu}| \leq |\,\mathcal{F}un(\mu,k)| = k^{\mu}$$

Inoltre, poiché k è infinito e $\mu \leq k$, si ottiene $k = \mu \cdot k$, e per la proposizione 7.24 vale $|[k]^{\mu}| = |[\mu \cdot k]^{\mu}| \geq |\,\mathcal{F}un(\mu,k)| = k^{\mu}$, dove l'ultima disuguaglianza segue dal fatto che ogni funzione da μ in k è un sottoinsieme di $\mu \cdot k$ di cardinalità μ.

Si conclude con Cantor-Bernstein. □

Esempio. Si ha $|[\omega_1]^{\aleph_0}| = \aleph_1^{\aleph_0} = 2^{\aleph_0}$.

Si vanno ora a introdurre i concetti di somma e prodotto infinito di cardinali, e successivamente quello di cofinalità di un ordinale. Questi concetti sono interessanti già come sviluppo in sé della teoria, ma sono strumenti molto potenti per lo studio dell'esponenziazione cardinale.

Lemma 13.1. *(*) (AC) Se $\{A_i\}_{i\in I}$ e $\{B_i\}_{i\in I}$ sono due famiglie di insiemi disgiunti indicizzate sullo stesso insieme I e per ogni $i \in I$ vale $|A_i| = |B_i|$, allora $|\bigcup_{i\in I} A_i| = |\bigcup_{i\in I} B_i|$.*

Dim. Per l'Assioma di scelta esiste un insieme di bigezioni $\{f_i\colon A_i \to B_i\}_{i\in I}$.

Ora si definisce

$$\begin{aligned}\varphi\colon \bigcup_{i\in I} A_i &\to \bigcup_{i\in I} B_i\\ a &\mapsto f_i(a) \text{ se } a \in A_i\end{aligned}$$

e si osserva che è una bigezione. □

Definizione (Somma infinita di cardinali)**.** *Data una successione $\langle k_i \mid i \in I\rangle$ di cardinali, si definisce la sua **somma** come l'unico cardinale equipotente ad una unione disgiunta $\bigcup_{i\in I} A_i$ dove per ogni $i \in I$ vale $|A_i| = k_i$.*

Oss. Per provare che la somma infinita di cardinali è ben definita, basta dimostrare l'esistenza di una successione di insiemi disgiunti $\{A_i\}_{i\in I}$ con $|A_i| = k_i$ per ogni $i \in I$, visto che poi vale il lemma 13.1.

Questo si può fare in vari modi: uno di questi è quello di prendere i vari k_i e considerare i loro elementi α come coppie ordinate (α, i) (facilmente formalizzabile).

Inoltre, se gli A_i non sono disgiunti, allora vale banalmente $|\bigcup_{i\in I} A_i| \leq \sum_{i\in I} k_i$, cioè "la cardinalità di un'unione è minore o uguale della somma delle cardinalità".

Lemma 13.2. *(*) (AC) Se $\{A_i\}_{i\in I}$ e $\{B_i\}_{i\in I}$ sono due famiglie di insiemi non vuoti indicizzate sullo stesso insieme I e per ogni $i \in I$ vale $|A_i| = |B_i|$, allora $|\prod_{i\in I} A_i| = |\prod_{i\in I} B_i|$.*

Dim. Per l'Assioma di scelta esiste un insieme di bigezioni $\{f_i \colon A_i \to B_i\}_{i\in I}$.

Ora si definisce

$$\begin{aligned}\varphi \colon \prod_{i\in I} A_i &\to \prod_{i\in I} B_i \\ \psi &\mapsto \psi^* \colon i \mapsto f_i(\psi(i))\end{aligned}$$

e si osserva che è ben definita e bigettiva. □

Definizione (Prodotto infinito di cardinali)**.** *Data una successione $\langle k_i \mid i \in I\rangle$ di cardinali, si definisce il suo **prodotto** come l'unico cardinale equipotente ad un prodotto cartesiano (infinito se I è infinito) $\prod_{i\in I} A_i$ dove per ogni $i \in I$ vale $|A_i| = k_i$.*

Oss. La precedente definizione è ben posta per il lemma 13.2.

Le definizioni di somma infinita e prodotto infinito di cardinali sono generalizzazioni del caso finito.

I seguenti Teoremi sono di fondamentale importanza in quanto mostrano come calcolare una qualsiasi somma infinita o prodotto infinito di cardinali.

Lemma 13.3. *(*) Se k è un cardinale e I è un insieme qualsiasi, allora valgono i seguenti fatti:*

1. $\sum_{i\in I} k = k \cdot |I|$;
2. $\prod_{i\in I} k = k^{|I|}$.

Dim. 1. Sia $\langle A_i \mid i \in I\rangle$ una I-sequenza di insiemi disgiunti tale che per ogni $i \in I$ vale $|A_i| = k$, allora per l'Assioma di scelta esiste un insieme di bigezioni $\{f_i \colon A_i \to k \mid i \in I\}$ e si osserva che la funzione

$$\begin{aligned}\varphi \colon \bigcup_{i\in I} A_i &\to k \times I \\ a &\mapsto (f_i(a), i) \text{ se } a \in A_i\end{aligned}$$

è una bigezione, da cui la tesi.

2. Diretta conseguenza delle definizioni di prodotto cartesiano infinito ed esponenziazione cardinale.

□

Lemma 13.4. *(*) Se $\langle k_i \mid i \in I\rangle$ e $\langle \nu_i \mid i \in I\rangle$ sono due successioni di cardinali indicizzate sullo stesso insieme I, e per ogni $i \in I$ vale $k_i \leq \nu_i$, allora si ha $\sum_{i\in I} k_i \leq \sum_{i\in I} \nu_i$.*

Dim. Date due famiglie $\langle A_i \mid i \in I\rangle$ e $\langle B_i \mid i \in I\rangle$ di insiemi disgiunti tali che per ogni $i \in I$ vale $|A_i| = k_i$ e $|B_i| = \nu_i$, per l'Assioma di scelta esiste un insieme di funzioni iniettive $\{f_i \colon A_i \to B_i \mid i \in I\}$.

Ora si definisce

$$\varphi \colon \bigcup_{i\in I} A_i \to \bigcup_{i\in I} B_i$$
$$a \mapsto f_i(a) \text{ se } a \in A_i$$

e si osserva che è iniettiva. □

Oss. Se fosse $k_i < \mu_i$, si avrebbe comunque $\sum_{i\in I} k_i \leq \sum_{i\in I} \nu_i$: per esempio si vedrà che

$$\sum_{n\in\omega} n = \sum_{n\in\omega} n + 1 = \aleph_0$$

Brutalmente si può dire che "le disuguaglianze strette non passano alle somme infinite".

Lemma 13.5. *Date due successioni di cardinali $\langle k_i \mid i \in I\rangle$ e $\langle \mu_i \mid i \in I\rangle$ tali che per ogni $i \in I$ vale $k_i < \mu_i$, allora:*

$$\sum_{i\in I} k_i \leq \prod_{i\in I} k_i$$
$$\prod_{i\in I} k_i \leq \prod_{i\in I} \mu_i$$

ma in generale non valgono le disuguaglianze strette.

Dim. Si lascia per esercizio. □

Teorema 13.4 (Somma infinita di cardinali)**.** *Data una successione infinita $\langle k_i \mid i \in I\rangle$ di cardinali, si ha*

$$\sum_{i\in I} k_i = max\{|I|,\ sup\, k_i\}$$

Dim. Per ogni i si ha banalmente $\sum_{i\in I} k_i \geq k_i$ e dunque $\sum_{i\in I} k_i \geq sup\, k_i$. Inoltre si ha anche $\sum_{i\in I} k_i \geq \sum_{i\in I} 1 = |I|$. Dunque $\sum_{i\in I} k_i \geq max\{|I|,\ sup\, k_i\}$.

Si pone $k = sup\, k_i$ e per i lemmi 13.4 e 13.3 si ha $\sum_{i\in I} k_i \leq \sum_{i\in I} k = |I| \cdot k = max\{|I|, k\}$. □

Esempio. Si ottengono facilmente le due uguaglianze

$$\sum_{n\in\omega} n = \aleph_0$$
$$\sum_{n\in\omega} \aleph_n = \aleph_\omega$$

Nel capitolo 7 si è già dimostrato che una unione numerabile di insiemi numerabili è numerabile e che la stessa cosa vale per gli insiemi che hanno la cardinalità del continuo. Il seguente Teorema generalizza questa proprietà a tutti i cardinali infiniti.

Teorema 13.5. *Se k è un cardinale infinito, allora un'unione di k insiemi di cardinalità k ha cardinalità k.*

Dim. Data una famiglia $\{A_i \mid i \in k\}$ tale che per ogni $i \in k$ vale $|A_i| = k$, allora $|\bigcup_{i\in k} A_i| \leq \sum_{i\in k} k = k$ e poiché l'altra disuguaglianza è del tutto ovvia si ottiene la tesi. □

Definizione. *Dati un ordinale α e un suo sottoinsieme A, si dice che A è **illimitato** in α se per ogni $\beta \in \alpha$ esiste $a \in A$ tale che $a \geq \beta$, cioè se non ha maggioranti stretti in α.*

Oss. Se k è un cardinale e $A \subseteq k$ è tale che $|A| = k$, allora A è illimitato in k.

Lemma 13.6. *Se ν è un cardinale e $A \subseteq \nu$ ha cardinalità ν, allora A è illimitato in ν.*

Dim. Se per assurdo A è limitato in ν, allora esiste $\alpha \in \nu$ tale che per ogni $a \in A$ vale $a < \alpha$ e dunque $A \subseteq \alpha$, da cui segue $|A| \leq |\alpha| < \nu$ dove la disuguaglianza stretta è ottenuta dalla definizione di cardinale. □

mancano la proprietà associativa generalizzata di somma e prodotto e la scomponibilità di un cardinale k in k sottoinsiemi tutti di cardinalità k

Teorema 13.6 (Prodotto infinito di cardinali)**.** *Data una successione debolmente crescente $\langle k_i \mid i \in \nu\rangle$ di cardinali infiniti, dove ν è un cardinale infinito, si ha*

$$\prod_{i\in\nu} k_i = (sup\, k_i)^\nu$$

Dim. Si pone $k := sup\, k_i$ e dal lemma 13.5 si ottiene $\prod_{i\in\nu} k_i \leq \prod_{i\in\nu} k = k^\nu$.

Per la proposizione ... , esiste una partizione di ν in ν insiemi A_i di cardinalità ν, e per il lemma (associativa) si ottiene

$$\prod_{i\in\nu} k_i = \prod_{i\in\nu}\prod_{s\in A_i} k_s \geq \prod_{i\in\nu} sup_{\,s\in A_i} k_s$$

Ora per il lemma 13.6 gli A_i sono illimitati in ν e dunque, dalla debole crescenza dei k_i, si ottiene $sup_{\,s\in A_i} k_s = k$, da cui la tesi. □

Esempio. Si ottiene facilmente:

$$\prod_{1<n<\omega} n = 2^{\aleph_0}$$

$$\prod_{n\in\omega} \aleph_n = \aleph_\omega^{\aleph_0}$$

Si vedrà più avanti che $\aleph_\omega^{\aleph_0} > \aleph_\omega$.

Oss. Se ν è finito il teorema resta vero ed è pure banale (e poco utile).

(*) L'ipotesi ν cardinale è necessaria. (esercizio)

(*) L'ipotesi di debole crescenza è necessaria. (esercizio)

Un altro strumento fondamentale nello studio dell'esponenziazione cardinale è la cofinalità.

Definizione (Cofinalità (parte 1))**.** *Dato un insieme totalmente ordinato $(X, \leq)$, si dice **cofinalità** di X la minima cardinalità dei suoi sottoinsiemi illimitati superiormente e la si denota $cof X$.*

Esempio. Si osserva facilmente che:

- ogni insieme che ha massimo ha cofinalità 1;
- $cof\omega = cof\mathbb{R} = \aleph_0$;
- $cof\aleph_\omega = \aleph_0$.

  Si vedrà in seguito che $cof(\omega_1) = \aleph_1$.

Oss. La cofinalità (cioè la "raggiungibilità") di un cardinale non ha niente a che fare con la sua grandezza e di sicuro non è crescente nei cardinali.

È banale osservare che se α è un ordinale, allora vale $cof\alpha \leq \alpha$ e dunque se k è un cardinale vale $k^{cofk} \leq 2^k$.

Si danno ora altre due definizioni equivalenti di cofinalità:

Definizione (Cofinalità (parte 2))**.** *Dato un insieme totalmente ordinato $(X, \leq)$, si dice $\boldsymbol{cof_1}$ di X il minimo ordinale α per cui esiste una funzione illimitata da α in X e $\boldsymbol{cof_2}$ il minimo ordinale β per cui esiste una funzione strettamente crescente e illimitata da β in X e le si denota rispettivamente $cof_1 X$ e $cof_2 X$.*

Oss. Le definizioni date sopra sono ben poste.

Le notazioni cof_1 e cof_2 sono create per la dispensa, ma non hanno alcun riscontro al di fuori di essa.

Proposizione 13.5. *Per ogni insieme totalmente ordinato $(X, \leq)$ si ha $cof X = cof_1 X = cof_2 X$.*

Dim. Banalmente $cofX \leq cof_1 X \leq cof_2 X$, dunque resta solo da dimostrare $cof_2 X \leq cofX$.

Sia $A \subseteq X$ illimitato con $|A| = k_0$. Si cerca una funzione strettamente crescente e illimitata $g\colon k_0 \to X$ e in tal caso si avrebbe la tesi.

Dato $x \in X$ e una bigezione $f\colon k_0 \to A$ si definisce per ricorsione transfinita

$$g\colon k_0 \to X$$
$$\beta \mapsto \begin{cases} x \text{ se } \beta = 0 \\ f(\xi) \text{ se } \beta > 0 \end{cases}$$

dove $\xi := min\{\gamma \in k_0 \mid \forall \beta' \in \beta\ f(\gamma) > g(\beta') \wedge f(\gamma) \geq f(\beta)\}$.

Per definizione g è strettamente crescente e illimitata. □

Definizione (Cardinali regolari e singolari)**.** *Un cardinale infinito k è detto* ***regolare*** *se $cofk = k$, altrimenti è detto* ***singolare****.*

Esempio. Si ha che $\aleph_0$ è un cardinale regolare, mentre $\aleph_\omega$ è un cardinale singolare (con la prossima proposizione si proverà che è il più piccolo cardinale singolare).

Proposizione 13.6. *(*) Per ogni insieme totalmente ordinato $(X, \leq)$ si ha che $cofX$ è un cardinale regolare, cioè $cof(cofX) = cofX$.*

Dim. Poiché per definizione $cofX$ è un cardinale, basta provarne la regolarità.

Se $A \subseteq cofX$ è illimitato e $f\colon cofX \to X$ è strettamente crescente e illimitata, allora $f_{|A}\colon A \to X$ è illimitata e dunque $|A| \geq cofX$, da cui la tesi. □

Proposizione 13.7. *Ogni cardinale successore è un cardinale regolare.*

Dim. Dato un cardinale successore k^+, se per assurdo esiste $A \subseteq k^+$ illimitato in k^+ e con $|A| \leq k$, allora $\bigcup A = k^+$ per l'illimitatezza, ma $|\bigcup A| \leq \sum_{\alpha \in A} |\alpha| \leq \sum_{\alpha \in A} k = k$ ($\mathcal{A}ssurdo$). □

Il seguente Teorema è uno dei principali risultati a nostra disposizione sulle operazioni cardinali.

Teorema 13.7 (König)**.** *Date due successioni di cardinali $\langle k_i \mid i \in I\rangle$ e $\langle \mu_i \mid i \in I\rangle$ tali che per ogni $i \in I$ vale $k_i < \mu_i$, allora*

$$\sum_{i \in I} k_i < \prod_{i \in I} \mu_i$$

Dim. Per il lemma 13.5 vale $\sum_{i \in I} k_i \leq \prod_{i \in I} \mu_i$, dunque bisogna provare solo che non può valere l'uguaglianza.

Per far questo si prendono due famiglie $\{A_i \mid i \in I\}$ e $\{B_i \mid i \in I\}$ tali che per ogni i valgono $|A_i| = k_i$, $|B_i| = \mu_i$ e gli A_i sono mutualmente disgiunti.

Ora per definizione $\sum_{i\in I} k_i = |\bigcup_{i\in I} A_i|$ e $\prod_{i\in I} \mu_i = |\prod_{i\in I} B_i|$ e si mostra che non può esistere una funzione surgettiva $\varphi\colon \bigcup_{i\in I} A_i \to \prod_{i\in I} B_i$. Per assurdo si assume l'esistenza di una tale φ.

Per ogni $i_0 \in I$ si pone $\theta_{i_0} := \prod_{i_0} \circ \varphi_{|A_{i_0}}$ dove $\prod_{i_0}\colon \prod_{i\in I} B_i \to B_{i_0}$ è la proiezione canonica.

Per ipotesi $|A_{i_0}| = k_{i_0} < \mu_{i_0} = |B_{i_0}|$ e inoltre la funzione θ_{i_0} non è surgettiva, dunque si può scegliere $\xi_{i_0} \in B_{i_0} \setminus \mathcal{I}m\,\theta_{i_0}$ (si usa la scelta).

Ora $\xi := \langle \xi_i \mid i \in I\rangle \in \prod_{i\in I} B_i$. Si prova che $\xi \notin \mathcal{I}m\,\varphi$. Infatti se esiste $a \in \bigcup_{i\in I} A_i$ tale che $\varphi(a) = \xi$, allora si prende i_0 tale che $a \in A_{i_0}$ e si ottiene $\theta_{i_0}(a) = \xi_{i_0}$, cioè $\xi_{i_0} \in \mathcal{I}m\,\theta_{i_0}$ (*Assurdo*). □

Oss. Parte dell'importanza di questo teorema risiede nel fatto che al momento è l'unico strumento a nostra disposizione per avere disuguaglianze strette.

Il Teorema di Cantor è un caso particolare del Teorema di König, e infatti questa dimostrazione assomiglia (almeno come idea) a quella del procedimento diagonale usato per dimostrare Cantor.

Si raccolgono ora alcune importanti proprietà della cofinalità di un cardinale.

Proposizione 13.8. *Se λ è un ordinale limite, allora $cof\aleph_\lambda = cof\lambda$.*

Dim. Se $f\colon cof\lambda \to \lambda$ è illimitata, allora $g\colon cof\lambda \to \aleph_\lambda$, dove $g(\alpha) = \aleph_{f(\alpha)}$, è illimitata e dunque $cof\lambda \geq cof\aleph_\lambda$.

Se $\varphi\colon cof\aleph_\lambda \to \aleph_\lambda$ è illimitata, allora $\psi\colon cof\aleph_\lambda \to \lambda$, dove $\psi(\alpha) = min\{\beta \in \lambda \mid \aleph_\beta > \varphi(\alpha)\}$, è illimitata e dunque $cof\lambda \leq cof\aleph_\lambda$, da cui la tesi. □

Esempio. Vale $cof\aleph_{\omega+\omega} = cof\omega + \omega = \aleph_0$.

Oss. Per quanto riguarda la cofinalità dei cardinali, se k è un cardinale successore allora $cofk = k$ perché k è regolare (proposizione 13.7), mentre se $k = \aleph_\lambda$ è un cardinale limite allora $cof\aleph_\lambda = cof\lambda$ e dunque il calcolo della cofinalità di un cardinale si riconduce al massimo a quella del calcolo della cofinalità di un ordinale limite.

La seguente proposizione è un'ulteriore e molto utile definizione equivalente di cofinalità (per cardinali).

Proposizione 13.9. *Se $k > \aleph_0$ è un cardinale, allora $cofk$ è il più piccolo cardinale ν per cui esiste una successione di cardinali $\langle k_i \mid i \in \nu\rangle$ tale che per ogni $i \in \nu$ vale $k_i < k$ e $k = \sum_{i\in\nu} k_i$.*

Dim. Si prova prima la minimalità di $cofk$ e poi l'esistenza di una tale successione per $cofk$.

Se per assurdo $\nu < cofk$ è un cardinale e $\langle k_i \mid i \in \nu \rangle$ è una successione di cardinali tale che per ogni $i \in \nu$ vale $k_i < k$ e $\sum_{i \in \nu} k_i = k$, allora $sup_{i \in \nu} k_i = k$ e $\nu \geq cofk$ ($\mathcal{A}ssurdo$).

Per l'esistenza si trattano separatamente i casi in cui k è regolare e k è singolare.

Se k è un cardinale regolare, allora $\sum_{i \in k} 1 = k$.

Se k è un cardinale singolare, allora è un cardinale limite, cioè esiste un ordinale limite λ per cui $k = \aleph_\lambda$. Per la proposizione 13.8 si ottiene $cof\aleph_\lambda = cof\lambda$. Ora si prende $f\colon\ cofk \to \lambda$ illimitata e si ha

$$\sum_{\alpha \in cofk} \aleph_{f(\alpha)} = max\{sup_{\alpha \in cofk} \aleph_{f(\alpha)},\ cofk\} = \aleph_\lambda = k$$

□

Oss. In generale si sarebbe potuta prendere f crescente e dunque ogni cardinale k è il sup di una $cofk$-successione crescente di cardinali minori di k, cioè $k = sup_{i \in cofk} k_i$, dove i k_i crescono (debolmente) e per ogni $i \in cofk$ vale $k_i < k$.

Corollario 13.1. *Per ogni cardinale k vale $k^{cofk} > k$.*

Dim. Se $k = \sum_{i \in cofk} k_i$ dove per ogni $i \in cofk$ vale $k_i < k$ (questa scrittura esiste per la proposizione 13.9), allora per König si ottiene

$$k = \sum_{i \in cofk} k_i < \prod_{i \in cofk} k = k^{cofk}$$

□

Oss. k^{cofk} è la "funzione" gimel valutata in k, si scrive $\beth(k) := k^{cofk}$. Questa "funzione" viene usata per studiare l'ipotesi del continuo e l'esponenziazione cardinale, ma non è stata oggetto del corso.

Vale dunque $k < k^{cofk} \leq 2^k$.

Il caso k regolare è banale.

Esempio. Si può verificare facilmente che $\aleph_\omega^{\aleph_0} > \aleph_\omega$ e $\aleph_{(\omega+\omega)}^{\aleph_0} > \aleph_{(\omega+\omega)}$.

Corollario 13.2. *Per ogni cardinale k vale $cof2^k > k$.*

Dim. Banalmente $2^k < (2^k)^{cof2^k} = 2^{k \cdot cof2^k} = 2^{max\{k,\ cof2^k\}}$, da cui la tesi. □

Oss. Allo stesso modo si può dimostrare che se k e μ sono due cardinali qualsiasi (k infinito), allora $cof(\mu^k) > k$.

Il corollario precedente fornisce uno strumento per avere cardinali di cofinalità sempre più grande.

Come conseguenza si ottiene $cof\mathfrak{c} = cof 2^{\aleph_0} > \aleph_0$, per cui non può essere $2^{\aleph_0} = \aleph_\omega$.

Più in generale per ogni cardinale k vale $2^{cof k} \neq k$.

Teorema 13.8 (Hausdorff)**.** *Per ogni cardinale successore $\aleph_{\alpha+1}$ e per ogni ordinale β vale l'uguaglianza $\aleph_{\alpha+1}^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} \cdot \aleph_{\alpha+1}$*

Dim. Se $\beta \geq (\alpha+1)$, allora $\aleph_{\alpha+1}^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta} > \aleph_\beta \geq \aleph_{\alpha+1}$, da cui la tesi.

Se $\beta < (\alpha+1)$, allora ogni funzione $f\colon \aleph_\beta \to \aleph_{\alpha+1}$ è limitata per la regolarità di $\aleph_{\alpha+1}$, dunque $\mathcal{F}un(\aleph_\beta,\ \aleph_{\alpha+1}) = \bigcup_{\gamma\in(\alpha+1)} \mathcal{F}un(\aleph_\beta,\ \gamma)$. Perciò

$$\aleph_{\alpha+1}^{\aleph_\beta} = |\,\mathcal{F}un(\aleph_\beta,\ \aleph_{\alpha+1})| = |\bigcup_{\gamma\in(\alpha+1)} \mathcal{F}un(\aleph_\beta,\ \gamma)| \leq \sum_{\gamma\in\aleph_{\alpha+1}} |\,\mathcal{F}un(\aleph_\beta,\ \gamma)| =$$

$$= max\{sup_{\gamma\in\aleph_{\alpha+1}}|\gamma|^{\aleph_\beta},\ \aleph_{\alpha+1}\} = max\{\aleph_\alpha^{\aleph_\beta},\ \aleph_{\alpha+1}\} = \aleph_\alpha^{\aleph_\beta} \cdot \aleph_{\alpha+1}$$

L'altra disuguaglianza è banale. □

Oss. L'uguaglianza $\aleph_{\alpha+1}^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} \cdot \aleph_{\alpha+1}$ è detta "Formula di Hausdorff".

In generale vale $\aleph_n^{\aleph_0} = max\{\mathfrak{c},\ \aleph_n\}$, e, poiché ogni ordinale α può essere scritto (in modo unico) come $\alpha = \lambda + n$ dove λ è un ordinale limite, allora per ogni cardinale ν vale $\aleph_{\lambda+n}^{\nu} = max\{\aleph_\lambda^{\nu},\ \aleph_{\lambda+n}\}$, cioè il Teorema di Hausdorff riconduce l'esponenziazione cardinale ad un esponenziazione con base un cardinale limite.

Si nota inoltre che GCH risolve completamente l'esponenziazione con base un cardinale successore e fornisce sempre il risultato più piccolo possibile. Infatti, dati due cardinali infiniti ν, μ, se $\nu \leq \mu$, allora $(\nu^+)^\mu = 2^\mu = \mu^+$ per la proposizione 13.2. Se $\nu > \mu$, allora $(\nu^+)^\mu = (2^\nu)^\mu = 2^\nu = \nu^+$.

Si va dunque ora ad esaminare nel dettaglio l'esponenziazione cardinale con base un cardinale limite, studiando solo il caso in cui la base è maggiore dell'esponente perché l'altro caso è già stato risolto con la proposizione 13.2.

Proposizione 13.10. *(*) Se k è un cardinale limite e $\nu < cof k$ è un altro cardinale, allora $k^\nu = sup_{\mu\in k}\mu^\nu$.*

Dim. Banalmente $k^\nu \geq sup_{\mu\in k}\mu^\nu$, dunque si deve provare solo l'altra disuguaglianza.

Posto $\eta := sup_{\mu\in k}\mu^\nu$, poiché $\nu < cof k$, si ha che ogni funzione $f\colon \nu \to k$ è limitata e dunque $\mathcal{F}un(\nu,\ k) = \bigcup_{\gamma\in k} \mathcal{F}un(\nu,\ \gamma)$.

Perciò

$$k^\nu = |\bigcup_{\gamma\in k} \mathcal{F}un(\nu,\ \gamma)| \leq \sum_{\gamma\in k} |\gamma|^\nu \leq \sum_{\gamma\in k} \eta = k \cdot \eta = \eta$$

da cui la tesi. □

Esempio. Si ottiene $\aleph_{\omega_1}^{\aleph_0} = sup_{\alpha\in\omega_1}\aleph_\alpha^{\aleph_0}$.

Oss. Assumendo GCH, nelle stesse ipotesi della proposizione precedente, si ottiene $k^\nu = k$. Infatti per la proposizione vale $k^\nu = sup_{\mu\in k}\mu^\nu = sup_{\mu\in k}(\mu^+)^\nu = sup_{\mu\in k}\mu^+ = sup_{\mu\in k}\mu = k$.

Si osservi che si è usato quanto già dimostrato per i cardinali successori assumendo GCH.

Per esempio, assumendo GCH, si ottiene $\aleph_{\omega_1}^{\aleph_0} = \aleph_{\omega_1}$.

Proposizione 13.11. *Se k è un cardinale limite e $\nu \geq cofk$ è un altro cardinale, allora $k^\nu = (sup_{\mu\in k}\mu^\nu)^{cofk}$.*

Dim. Si considera $k = sup_{i\in cofk}k_i$ sove i k_i sono crescenti (debolmente) e per ogni $i \in cofk$ vale $k_i < k$.

Allora

$$(sup_{\mu\in k}\mu^\nu)^{cofk} = (sup_{i\in cofk}k_i^\nu)^{cofk} = \prod_{i\in cofk} k_i^\nu =$$
$$= (\prod_{i\in cofk} k_i)^\nu = ((sup_{i\in cofk}k_i)^{cofk})^\nu = k^\nu$$

Si osservi che è stata usata la debole crescenza dei k_i per applicare la formula del prodotto infinito. □

Esempio. Vale l'uguaglianza $\aleph_\omega^{\aleph_1} = (sup_{n\in\omega}\aleph_n^{\aleph_1})^{\aleph_0}$. Inoltre assumendo GCH si prova facilmente $\aleph_\omega^{\aleph_1} = \aleph_\omega^{\aleph_0}$ e si può anche dire $\aleph_\omega^{\aleph_0} = \aleph_{\omega+1}$, come mostra l'osservazione seguente.

Oss. Assumendo GCH, nelle stesse ipotesi della proposizione precedente, si ottiene che:

- Se k è un cardinale regolare, allora $k^\nu = \nu^+$ perché $\nu \geq cofk = k$;
- Se k è un cardinale singolare e $\nu < k$ (altrimenti è banale), allora $k^\nu = (sup_{\mu\in k}\mu^\nu)^{cofk} = (sup_{\mu\in k}(\mu^+)^\nu)^{cofk} = (sup_{\mu\in k}\mu^+)^{cofk} = k^{cofk} > k$. Inoltre si è già visto che $k^{cofk} \leq 2^k = k^+$ dunque $k^\nu = k^+$.

Se si assume GCH, si è provato che l'esponenziazione cardinale è completamente risolta.

Definizione (Cardinale limite forte)**.** *Un cardinale k è detto **limite forte** se per ogni coppia di cardinali $\nu, \mu \in k$ vale $\nu^\mu < k$.*

Oss. Un cardinale limite forte è un cardinale limite. Infatti se k è un cardinale limite forte e per assurdo esiste α ordinale tale che $k = \aleph_{\alpha+1}$, allora $\aleph_\alpha^{\aleph_\alpha} = 2^{\aleph_\alpha} \geq \aleph_{\alpha+1}$.

Assumendo GCH, si è provata in precedenza l'uguaglianza $\aleph_\omega^{\aleph_1} = \aleph_\omega^{\aleph_0}$. In realtà non è necessario assumere GCH, ma basta un'ipotesi più debole, cioè che $\aleph_\omega$ sia un limite forte. Infatti con questa ipotesi più debole si prova facilmente che $\aleph_\omega^{\aleph_n} = \aleph_\omega^{\aleph_0}$ per ogni naturale n. La verifica è ovvia, come ovvio è provare che GCH dimostra che $\aleph_\omega$ è un limite forte.

Non rientra nelle possibilità di questo corso, ma l'esistenza di cardinali limite che non sono limite forte è indipendente da ZFC. Però assumendo GCH si può provare l'equivalenza fra cardinale limite e limite forte. Infatti in tal caso, dato un cardinale limite $\aleph_\lambda$, per ogni $\alpha < \lambda$ vale

$$2^{\aleph_\alpha} = \aleph_{\alpha+1} < \aleph_\lambda$$

Esempio. $\aleph_0$ è un limite forte.

A questo punto ci si potrebbe chiedere se esistano limiti forti più che numerabili e si vedrà che la risposta è affermativa.

Proposizione 13.12. *Dato un cardinale k, allora k è limite forte se e solo se per ogni cardinale $\nu < k$ vale $2^\nu < k$.*

Dim. Una implicazione segue direttamente dalla definizione di limite forte.

Per l'altra implicazione, se $\mu, \nu \in k$ sono due cardinali e $\eta = max\{\nu, \mu\}$, allora $\mu^\nu \leq \eta^\eta = 2^\eta < k$. □

Definizione (Beth)**.** *Si definisce per ricorsione transfinita la "sequenza" dei beth*

$$\begin{cases} \beth_0 = \aleph_0 \\ \beth_{\alpha+1} = 2^{\beth_\alpha} \\ \beth_\lambda = \bigcup_{\alpha\in\lambda} \beth_\alpha \text{ se } \lambda \text{ limite} \end{cases}$$

Oss. Ogni $\beth_\alpha$ è un cardinale. è crescente??

Proposizione 13.13. *(*) Valgono i seguenti fatti:*

1. *se λ è un ordinale limite, allora $cof\beth_\lambda = cof\lambda$;*
2. *k è un limite forte se e solo se esiste λ ordinale limite per cui $k = \beth_\lambda$;*
3. *esistono cardinali k per cui $\beth_k = k$ (punti fissi).*

Dim. 1. analoga a quella già vista per la "sequenza" degli aleph.

2. Si dimostra prima di tutto che se λ è un ordinale limite, allora $\beth_\lambda$ è un limite forte. Per ogni coppia di cardinali $\nu, \mu < \beth_\lambda$ sia $\alpha \in \lambda$ il minimo ordinale per cui vale $\nu, \mu \in \beth_\alpha$ e sia η il maggiore fra ν e μ. Allora $\nu^\mu \leq \eta^\eta = 2^\eta \leq 2^{\beth_\alpha} = \beth_{\alpha+1} < \beth_\lambda$.

   Ora si prova che ogni $\beth_{\alpha+1}$ non è un limite forte: infatti $\beth_\alpha^{\beth_\alpha} = 2^{\beth_\alpha} = \beth_{\alpha+1}$. Questo risultato sarà utile alla fine della dimostrazione.

Se k è un limite forte allora si pone $\alpha = min\{\beta \mid k < \beth_\beta\}$ e si prova che α è un ordinale successore. Se per assurdo α è un ordinale limite, allora da $k \in \beth_\alpha$ segue che esiste $\beta < \alpha$ per cui $k \in \beth_\beta$ (*Assurdo* per la minimalità di α).

Dunque $\alpha = \gamma + 1$ per un certo ordinale γ e adesso si prova $k = \beth_\gamma$. Per la minimalità di α si ottiene $\beth_\gamma \leq k$. Se per assurdo $\beth_\gamma < k$, allora dal fatto che k è limite forte segue $\beth_{\gamma+1} = 2^{\beth_\gamma} = \beth_\gamma^{\beth_\gamma} < k < \beth_{\gamma+1}$ (*Assurdo*).

Inoltre, poiché $k = \beth_\gamma$ è un limite forte, si ottiene che γ è un ordinale limite per quanto dimostrato poco sopra.

3. Si definisce per ricorsione numerabile la successione

$$\begin{cases} k_0 = \beth_0 \\ k_{n+1} = \beth_{k_n} \end{cases}$$

e si osserva facilmente che $k := \bigcup_{n\in\omega} k_n$ è tale che $k = \beth_k$ (i k_n sono illimitati in k).

□

Oss. A questo punto la risposta alla domanda "esistono limiti forti più che numerabili?" è del tutto scontata.

Definizione (Funzione continua tra ordinali)**.** *Dati due ordinali α e β, e una funzione $f\colon \alpha \to \beta$, si dice che f è continua se per ogni $\lambda \in \alpha$ limite vale*

$$f(\lambda) = \bigcup_{\gamma<\lambda} f(\gamma)$$

Oss. Se la "sequenza" degli aleph fosse una funzione, allora sarebbe continua per definizione, e nella prossima dimostrazione si usa lo stesso metodo già visto quando si è provato che la "sequenza" degli aleph ha dei punti fissi.

Proposizione 13.14. *Se k è un cardinale con $cof k > \aleph_0$ e $f\colon k \to k$ è una funzione strettamente crescente e continua, allora $|\mathcal{F}ix\, f| \geq cof k$.*

Dim. Basta far vedere che $\mathcal{F}ix\, f$ è illimitato in k, cioè che per ogni $\alpha \in k$ esiste un ordinale $\beta \in k$ con $\alpha < \beta$ e $f(\beta) = \beta$.

Dato $\alpha \in k$ si definisce per ricorsione numerabile la seguente successione

$$\begin{cases} \beta_0 = \alpha + 1 \\ \beta_{n+1} = f(\beta_n) \end{cases}$$

Ora se esiste $n \in \omega$ per cui $f(\beta_n) = \beta_n$ allora abbiamo trovato il punto fisso cercato. Altrimenti la successione è strettamente crescente (perché una funzione strettamente crescente da un buon ordine in sé ha la proprietà

$f(a) \geq a$ per ogni a) e ponendo $\beta = \bigcup \beta_n$ si ottiene il punto fisso cercato. Infatti β è un ordinale limite per la stretta crescenza della successione dei β_n e, se vale $\beta \in k$, allora si conclude per la continuità di f.

Dunque c'è solo da dimostrare $\beta \in k$ e questa è una semplice conseguenza del fatto che $cof k > \aleph_0$, infatti se per assurdo fosse $k = \beta$, allora i β_n sarebbero illimitati in k, e dunque $cof k = \aleph_0$ ($\mathcal{A}ssurdo$). □

Esempio. Ogni funzione $f\colon \aleph_{\omega_1} \to \aleph_{\omega_1}$ strettamente crescente e continua ha almeno $\aleph_1$ punti fissi.

Oss. L'ipotesi $cof k > \aleph_0$ è necessaria perché si può trovare una funzione continua e strettamente crescente da $\aleph_\omega$ in $\aleph_\omega$ priva di punti fissi.

Per esempio

$$\begin{aligned} f\colon \aleph_\omega &\to \aleph_\omega \\ n &\mapsto \omega + n \\ \omega &\mapsto \omega + \omega \\ \omega_n + \beta &\mapsto \omega_{n+1} + \beta \text{ se } 0 < \beta \leq \omega_{n+1} \end{aligned}$$

ha le proprietà suddette.

Corollario 13.3. *Se k è un cardinale regolare maggiore di $\aleph_0$ e $f\colon k \to k$ è una funzione strettamente crescente e continua, allora $|\mathcal{F}ix(f)| = k$.*

Esempio. Ogni funzione $f\colon \omega_1 \to \omega_1$ strettamente crescente e continua ha $\aleph_1$ punti fissi.

14 Boreliani e Lebesgue-misurabili

$\mathcal{L}$a prima parte di questo capitolo è un ripasso di argomenti già visti in altri corsi.

Si andrà infatti a dimostrare per cardinalità il contenimento stretto $\mathcal{B}(\mathbb{R}^n) \subsetneq \mathcal{L}(\mathbb{R}^n)$, dove $\mathcal{B}(\mathbb{R}^n)$ sono i boreliani di $\mathbb{R}^n$ e $\mathcal{L}(\mathbb{R}^n)$ sono i Lesbegue-misurabili.

Definizione (σ-algebra)**.** *Dato un insieme X e una famiglia $Y \subseteq \mathcal{P}(X)$, si dice che Y è una **σ-algebra** su X se valgono le seguenti tre proprietà:*

- $\emptyset,\ X \in Y$*;*
- Y *è chiusa per unione numerabile;*
- Y *è chiusa per complemento.*

Oss. Per le leggi di De Morgan si ha che ogni σ-algebra è chiusa per intersezione numerabile.

Esempio. Le famiglie $\mathcal{P}(X)$ e $\{\emptyset,\ X\}$ sono due σ-algebre su un qualsiasi insieme X.

Definizione (σ-algebra generata)**.** *Dato un insieme X e una famiglia $Y \subseteq \mathcal{P}(X)$, si definisce **$\sigma$-algebra generata** da Y la più piccola σ-algebra di X contenente Y.*

Oss. Quela appena data è una buona definizione perché $\mathcal{P}(X)$ è una σ-algebra su X che contiene Y.

Definizione (Boreliani)**.** *Dato uno spazio topologico (X, τ), si definisce la famiglia dei **boreliani** su X come la σ-algebra generata da τ, e la si indica con $\mathcal{B}(X)$ laddove è chiara la topologia a cui si fa riferimento.*

Oss. Quando si parla di boreliani di $\mathbb{R}^n$ solitamente si fa riferimento alla topologia euclidea.

Per quanto riguarda i Lebesgue-misurabili non si danno definizioni, perché argomento di altri corsi e a quelli si rimanda per una conoscenza più approfondita. Si assume dunque $|\mathcal{L}(\mathbb{R}^n)| = 2^{\mathfrak{c}}$. (Se uno avesse più nozioni sulla misura di Lebesgue non sarebbe difficile dimostrarlo, infatti basterebbe passare per l'insieme di Cantor, dimostrando che ha la cardinalità del continuo).

Per provare il contenimento stretto $\mathcal{B}(\mathbb{R}^n) \subsetneq \mathcal{L}(\mathbb{R}^n)$ basta allora dimostrare che $|\mathcal{B}(\mathbb{R}^n)| < 2^{\mathfrak{c}}$ e lo si fa provando in particolare che vale $|\mathcal{B}(\mathbb{R}^n)| = \mathfrak{c}$.

Proposizione 14.1. *Vale l'uguaglianza $|\mathcal{B}(\mathbb{R}^n)| = \mathfrak{c}$.*

Dim. Se τ è la topologia euclidea su $\mathbb{R}^n$, si definisce per ricorsione transfinita la "successione"

$$\begin{cases} B_0 = \tau \\ B_{\alpha+1} = B_\alpha \cup \{X^c \mid X \in B_\alpha\} \cup \{\bigcup_{n\in\omega} X_n \mid X_n \in B_\alpha\} \cup \{\bigcap_{n\in\omega} X_n \mid X_n \in B_\alpha\} \\ B_\lambda = \bigcup_{\alpha<\lambda} B_\alpha \quad \text{se } \lambda \text{ limite} \end{cases}$$

Ora si prova che B_{ω_1} è la σ-algebra dei boreliani di $\mathbb{R}^n$ e per farlo si dimostra prima che vale il contenimento $B_{\omega_1} \subseteq \mathcal{B}(\mathbb{R}^n)$ (per induzione transfinita), e poi che B_{ω_1} è una σ-algebra, da cui segue la tesi per la minimalità di $\mathcal{B}(\mathbb{R}^n)$.

Si prova dunque che per ogni $\alpha \in \omega_1$ vale "$X \in B_\alpha \to X$ è boreliano":

- se $X \in B_0$, allora X è un aperto di $\mathbb{R}^n$ e dunque è un boreliano;
- P(α)→P($\alpha+1$): se $X \in B_{\alpha+1}$, allora o $X \in B_\alpha$ (da cui segue la borelianità di X per ipotesi induttiva), oppure X si ottiene da elementi di B_α (che sono boreliani) con operazioni che conservano la borelianità (i boreliani sono una σ-algebra), dunque X è boreliano;
- λ limite: se $X \in B_\lambda$, allora esiste $\alpha \in \lambda$ tale che $X \in B_\alpha$, dunque X è boreliano per ipotesi induttiva.

Ora si prova che B_{ω_1} è una σ-algebra. L'unico fatto non banale da dimostrare è la stabilità per unioni numerabili, cioè che se $\{X_n \mid n \in \omega\}$ è un sottoinsieme di B_{ω_1}, allora $\bigcup_{n\in\omega} X_n \in B_{\omega_1}$.

Sia $f\colon \omega \to \omega_1$ tale che $f(n) = min\{\alpha \mid X_n \in B_\alpha\}$, allora $\mathcal{I}m\, f$ è al più numerabile e dunque limitata in ω_1 (che è un cardinale regolare) e perciò $\beta := sup\{f(n) \mid n \in \omega\} < \omega_1$.

Poiché la sequenza dei B_α è banalmente crescente (per contenimento), si ha che $\{X_n \mid n \in \omega\} \subseteq B_\beta$ e dunque $\bigcup_{n\in\omega} X_n \in B_{\beta+1} \subseteq B_{\omega_1}$.

Dunque si è ottenuta l'uguaglianza $\mathcal{B}(\mathbb{R}^n) = B_{\omega_1}$.

Ora si conclude dimostrando che vale $|B_{\omega_1}| = \mathfrak{c}$.

Prima di tutto si osserva che $|B_{\omega_1}| \geq \mathfrak{c}$ perché contiene gli aperti di $\mathbb{R}^n$. Inoltre $|B_{\omega_1}| \leq \sum_{\alpha\in\omega_1} |B_\alpha| = max\{\aleph_1,\ sup_{\alpha\in\omega_1} |B_\alpha|\}$.

Per cui basta provare che per ogni $\alpha \in \omega_1$ vale $|B_\alpha| = \mathfrak{c}$ e lo si fa per induzione transfinita:

- $|B_0| = \mathfrak{c}$ perché si è già visto nel capitolo 7;
- P(α)→P($\alpha+1$): basta provare che gli insiemi $A_1 := \{X^c \mid X \in B_\alpha\}$, $A_2 := \{\bigcup_{n\in\omega} X_n \mid X_n \in B_\alpha\}$ e $A_3 := \{\bigcap_{n\in\omega} X_n \mid X_n \in B_\alpha\}$ hanno la cardinalità del continuo. Il primo è banalmente in bigezione con B_α, mentre gli elementi degli altri due sono al più quanti i sottoinsiemi numerabili di B_α, che sono $\mathfrak{c}^{\aleph_0} = \mathfrak{c}$ per quanto già visto sulla cardinalità dei sottoinsiemi con cardinalità fissata di un certo insieme. Inoltre A_2 e A_3 hanno cardinalità almeno $\mathfrak{c}$ perché basta prendere le successioni costanti;

- λ limite: $B_\lambda = \bigcup_{\alpha<\lambda} B_\alpha$ è un'unione al più numerabile di insiemi che hanno la cardinalità del continuo e dunque ha la cardinalità del continuo.

Si può finalmente concludere che vale l'uguaglianza $|\mathcal{B}(\mathbb{R}^n)| = \mathfrak{c}$. □

Oss. La costruzione della σ-algebra vista nella dimostrazione precedente si può facilmente generalizzare a una qualsiasi σ-algebra generata da una famiglia di parti di un insieme, però non è detto che sia semplice stimarne la cardinalità.

15 Cardinali inaccessibili e misure su cardinali

$\mathcal{F}$orse il lettore più attento avrà notato che tutti i cardinali limite (diversi da $\aleph_0$)con cui ha avuto a che fare nello studio di questa materia sono cardinali singolari (per esempio $\aleph_\omega, \aleph_{\omega+\omega}$ o anche $\aleph_{\omega_1}$).

Non si tratta di un caso ed è proprio l'argomento iniziale di questo capitolo.

Definizione (Cardinale inaccessibile)**.** *Un cardinale $k > \aleph_0$ è detto* ***debolmente inaccessibile*** *se è regolare e limite ed è detto* ***fortemente inaccessibile*** *se è regolare e limite forte.*

Oss. Non rientra nelle possibilità di questo corso, ma si preannuncia già in questo momento che l'esistenza di cardinali debolmente inaccessibili è indecidibile in ZFC e, proprio per questo motivo, fino ad ora si sono trovati solo cardinali limite singolari.

L'argomento che si va a sviluppare è alla base di una branca della Teoria degli Insiemi che studia i cosiddetti "grandi cardinali", argomento fuori dalla portata di questo corso.

Tuttavia i risultati che si presentano sono di grande interesse già a questo punto dello sviluppo della teoria, anche perché si collegano con argomenti che dovrebbero essere stati affrontati in altri corsi.

Definizione (Misura di probabilità)**.** *Dato un insieme non vuoto X e una σ-algebra $\mathcal{F}$ su X, si dice* ***misura di probabilità*** *su X una funzione $\mu\colon \mathcal{F} \to [0,1]$ tale che*

- *$\mu(\emptyset) = 0$ e $\mu(X) = 1$;*
- *per ogni $\{x\} \in \mathcal{F}$ vale $\mu(\{x\}) = 0$;*
- *μ è* ***σ-additiva****, cioè per ogni sottofamiglia numerabile $\{A_n \mid n \in \omega\}$ di $\mathcal{F}$ tale che per ogni $i \neq j$ si ha $A_i \cap A_j = \emptyset$, vale*

$$\mu(\bigcup_{n\in\omega} A_n) = \sum_{n=0}^{\infty} \mu(A_n)$$

Il risultato che si dimostrerà entro la fine del capitolo è che l'esistenza di una misura di probabilità $\mu\colon \mathcal{P}(\mathbb{R}) \to [0,1]$ implicherebbe $\mathfrak{c} \geq k$ dove k è un cardinale debolmente inaccessibile, dunque non solo proverebbe l'esistenza di un cardinale inaccessibile, ma negherebbe anche l'ipotesi del continuo.

Lemma 15.1. *Se k è un cardinale infinito, $\mu\colon \mathcal{P}(k) \to [0,1]$ è una misura di probabilità e $\mathcal{F}$ è una famiglia di insiemi di misura positiva mutualmente disgiunti, allora $|\mathcal{F}| \leq \aleph_0$.*

Dim. Per ogni $n \in \mathbb{N}$ si pone $\mathcal{F}_n := \{A \in \mathcal{F} \mid \mu(A) \geq \frac{1}{n}\}$ e si osserva che $|\mathcal{F}_n| \leq n$. Dunque $\mathcal{F}$ è al più numerabile perché è contenuta in un'unione numerabile di insiemi finiti. □

Oss. Si può generalizzare a una qualsiasi misura positiva finita...

Definizione (Matrice di Ulam)**.** *Dati due cardinali infiniti k e ν si dice* ***matrice di Ulam*** *una $k \times \nu$-sequenza $\langle B_{\alpha,\gamma} \mid \alpha < k, \gamma < \nu\rangle$ di sottoinsiemi di k tale che:*

- *per ogni $\gamma < \nu$ e per ogni $\alpha, \beta < k$ vale $B_{\alpha,\gamma} \cap B_{\beta,\gamma} = \emptyset$, cioè i $B_{\alpha,\gamma}$ sulle stesse colonne sono disgiunti;*
- *per ogni $\alpha < k$ vale $|k \setminus \bigcup_{\gamma\in\nu} B_{\alpha,\gamma}| < k$, cioè l'unione degli insiemi che stanno su una stessa riga "esauriscono quasi tutto k".*

Lemma 15.2. *Se $k = \nu^+$, allora esiste una $k \times \nu$ matrice di Ulam.*

Dim. Per ogni $\xi < k$ si sceglie una funzione surgettiva $f_\xi \colon \nu \to \xi$ e per ogni $\alpha < k$ e $\gamma < \nu$ si pone $B_{\alpha,\gamma} := \{\xi \in k \mid f_\xi(\gamma) = \alpha\}$.

Ora banalmente gli insiemi che stanno su una stessa colonna sono mutualmente disgiunti.

Inoltre, per ogni α, se $\xi \in k \setminus \bigcup_{\gamma\in\nu} B_{\alpha,\gamma}$, allora $\alpha \notin f_\xi$ e dunque $\xi \leq \alpha$.

Perciò $k \setminus \bigcup_{\gamma\in\nu} B_{\alpha,\gamma} \subseteq \alpha \cup \{\alpha\}$ e $|k \setminus \bigcup_{\gamma\in\nu} B_{\alpha,\gamma}| \leq |\alpha \cup \{\alpha\}| < k$ □

Lemma 15.3 (Principio dei cassetti infinito)**.** *Se $k > \nu$ sono cardinali, k è regolare e $f \colon k \to \nu$ è una funzione, allora esiste $\gamma \in \nu$ tale che $|f^{-1}(\gamma)| = k$.*

Dim. Se per assurdo ogni elemento dell'immagine di f avesse fibra di cardinalità minore di k, allora k sarebbe unione di una famiglia di insiemi di cardinalità minore di k indicizzata su un insieme di cardinalità minore di $cof k = k$, e questo è *Assurdo*. □

Definizione (Misura k-additiva)**.** *Dato un cardinale infinito k, si dice che una misura $\mu \colon \mathcal{P}(k) \to [0,1]$ è* ***k-additiva*** *se per ogni famiglia $\mathcal{F}$ di sottoinsiemi di k di misura nulla tale che $|\mathcal{F}| < k$, si ha $\mu(\bigcup \mathcal{F}) = 0$.*

Oss. Se $\mu \colon \mathcal{P}(k) \to [0,1]$ è una misura k-additiva, $A \subseteq k$ e $|A| < k$, allora $\mu(A) = 0$.

Teorema 15.1. *Dato un cardinale infinito k, se esiste una misura di probabilità k-additiva $\mu \colon \mathcal{P}(k) \to [0,1]$, allora k è un cardinale debolmente inaccessibile.*

Dim. Per provare che k è debolmente inaccessibile si deve provare che è regolare e limite.

Per prima cosa si dimostra che k è un cardinale regolare. Se per assurdo k è singolare, allora esiste una successione $\langle k_i \mid i \in cof k\rangle$ dove per ogni

$i \in cof k$ vale $k_i < k$ e inoltre $k = \bigcup_{i \in cof k} k_i$. Ma dalla k-additività di μ si ottiene che tutti i k_i hanno misura nulla e dunque anche $\mu(\bigcup_{i \in cof k} k_i) = 0$ ($\mathcal{A}ssurdo$).

Ora si prova che k è un cardinale limite. Se per assurdo $k = \nu^+$ è un cardinale successore, allora si prende una $k \times \nu$ matrice di Ulam $\langle B_{\alpha,\gamma} \mid \alpha < k, \gamma < \nu \rangle$, che esiste per il lemma 15.2. Dalle proprietà delle matrici di Ulam e delle misure k-additive si ottiene che per ogni $\alpha < k$ vale $\mu(k \setminus \bigcup_{\gamma<\nu} B_{\alpha,\gamma}) = 0$ e dunque $\mu(\bigcup_{\gamma<\nu} B_{\alpha,\gamma}) = 1$.

Poiché $\nu < k$, si ottiene che per ogni α esiste $\gamma_\alpha < \nu$ tale che $\mu(B_{\alpha,\gamma_\alpha}) > 0$.

Ora per il "Principio dei cassetti infinito" esiste $\gamma < \nu$ tale che l'insieme $\Lambda := \{\alpha < k \mid \gamma_\alpha = \gamma\}$ ha cardinalità k.

Posto $\mathcal{F} := \{B_{\alpha,\gamma} \mid \alpha \in \Lambda\}$, poiché i suoi elementi sono a due a due disgiunti e di misura positiva, dal lemma 15.1 si ottiene $\aleph_0 \geq |\mathcal{F}| = |\Lambda| = k = \nu^+$ ($\mathcal{A}ssurdo$). □

Oss. Se $|X| = |Y|$ ed esiste una misura di probabilità $\mu\colon \mathcal{P}(X) \to [0,1]$, allora esiste una misura di probabilità $\sigma\colon \mathcal{P}(Y) \to [0,1]$.

Teorema 15.2. *Se esiste una misura di probabilità $\mu\colon \mathcal{P}(X) \to [0,1]$, allora $|X| \geq k$ dove k è un cardinale debolmente inaccessibile.*

Dim. Per il Teorema 15.1 basta provare che esistono un cardinale $k \leq |X|$ e una misura di probabilità k-additiva $\sigma\colon \mathcal{P}(k) \to [0,1]$.

Sia dunque $k := min Y$ dove

$$Y := \{\nu \text{ cardinale} \mid \exists \{A_i\}_{i<\nu}\ \forall i \in \nu\ \mu(A_i) = 0 \wedge \mu(\bigcup_{i \in \nu} A_i) > 0 \wedge A_i \cap A_j = \emptyset\}$$

Si osservi che k esiste perché Y è non vuoto, dato che $|X| \in Y$, e inoltre $\aleph_0 < k \leq |X|$.

Ora si prende $\{A_i\}_{i \in k}$ tale che per ogni i vale $\mu(A_i) = 0$, $\mu(\bigcup_{i \in k} A_i) > 0$ e gli A_i sono mutualmente disgiunti, e si definisce

$$\begin{aligned} \sigma\colon \mathcal{P}(k) &\to [0,1] \\ B &\mapsto \frac{\mu(\bigcup_{i \in B} A_i)}{\mu(\bigcup_{i \in k} A_i)} \end{aligned}$$

Adesso si dimostra che σ è una misura di probabilità k-additiva.

Per dimostrare che si tratta di una misura di probabilità bastano un po' di conti poco interessanti, per cui si tralascia questa parte.

La cosa a prima vista non banale è quella di provare la k-additività, che è conseguenza della minimalità di k. Infatti, presa una famiglia $\mathcal{F}$ di sottoinsiemi di k di misura nulla e tale che $|\mathcal{F}| < k$, allora

$$\sigma(\bigcup \mathcal{F}) = \frac{\mu(\bigcup_{B_j \in \mathcal{F}} \bigcup_{i \in B_j} A_i)}{\mu(\bigcup_{i \in k} A_i)} = 0$$

perché $|\mathcal{F}| < k$ e per ogni $B_j \in \mathcal{F}$ vale $\mu(\bigcup_{i \in B_j} A_i) = 0$. □

Corollario 15.1. *Se esiste una misura di probabilità $\mu \colon \mathcal{P}(\mathbb{R}) \to [0,1]$, allora $\mathfrak{c} \geq k$ dove k è un cardinale debolmente inaccessibile.*

Si conclude il capitolo con una caratterizzazione dei cardinali fortemente inaccessibili che sarà fondamentale nel capitolo 17.

Proposizione 15.1. *Un cardinale k è fortemente inaccessibile se e solo se è regolare e $k = \beth_k$.*

Dim. $\rightarrow$: Prima di tutto si osserva che k è regolare per definizione di cardinale fortemente inaccessibile.

Dunque c'è solo da dimostrare che k è un punto fisso della "funzione" beth. Per ipotesi k è un limite forte e dunque per la proposizione 13.13 esiste un ordinale limite λ per cui $k = \beth_\lambda$.

Dalla regolarità di k si ottiene

$$k = cof k = cof \beth_\lambda = cof \lambda \leq \lambda \leq \beth_\lambda = k$$

da cui segue $k = \beth_k$.

$\leftarrow$: k è regolare per ipotesi ed è limite forte per la proposizione 13.13. Dunque k è fortemente inaccessibile.

□

16 Gerarchia di Von Neumann e Assioma di fondazione

$\mathcal{L}$a Gerarchia di Von Neumann si definisce per ricorsione transfinita nel seguente modo:

$$\begin{cases} V_0 = \emptyset \\ V_{\alpha+1} = \mathcal{P}(V_\alpha) \\ V_\lambda = \bigcup_{\alpha\in\lambda} V_\alpha \quad \text{se } \lambda \text{ è limite} \end{cases}$$

I V_α saranno talvolta chiamati "livelli" della gerarchia.

Proposizione 16.1. *Valgono le seguenti proprietà:*

1. *ogni V_α è un insieme transitivo;*
2. *la Gerarchia di Von Neumann è strettamente crescente, cioè per ogni coppia di ordinali α, β vale l'implicazione $\alpha < \beta \to V_\alpha \subsetneq V_\beta$;*
3. *Ogni elemento di V_α è contenuto in qualche livello inferiore, cioè*

$$\forall x(x \in V_\alpha \to (\exists \beta < \alpha(x \subseteq V_\beta)))$$

4. *(*) per ogni ordinale α vale $\alpha \in V_{\alpha+1}$ (cioè $\alpha \subseteq V_\alpha$) ma $\alpha \notin V_\alpha$.*

Dim. 1. Per induzione transfinita:

- la transitività di V_0 è vera a vuoto;
- P(α)→P($\alpha+1$): se $x \in y \in V_{\alpha+1}$ allora $y \subseteq V_\alpha$ e quindi $x \in V_\alpha$. Dalla transitività di V_α (ipotesi induttiva) si ottiene $x \subseteq V_\alpha$, cioè $x \in V_{\alpha+1}$;
- λ limite: se $x \in y \in V_\lambda$ allora esiste $\alpha \in \lambda$ per cui $y \in V_\alpha$ e per l'ipotesi induttiva si ha che V_α è transitivo e dunque vale $x \in V_\alpha$, da cui $x \in V_\lambda$.

2. La transitività dei V_α prova banalmente che per ogni ordinale α vale $V_\alpha \subsetneq V_{\alpha+1}$ (Lemma). Usando questo fatto si prova l'enunciato della proposizione per induzione transfinita su β:

- il caso $\beta = 0$ è vero a vuoto;
- P(β)→P($\beta+1$): se $\alpha < \beta + 1$ allora $\alpha \leq \beta$. Se $\alpha = \beta$ allora la tesi è vera per il Lemma. Se $\alpha < \beta$ allora $V_\alpha \subsetneq V_\beta$ per l'ipotesi induttiva e, sempre per il Lemma, $V_\beta \subsetneq V_{\beta+1}$, da cui $V_\alpha \subsetneq V_{\beta+1}$;
- λ limite: se $\alpha < \lambda$ allora $V_\alpha \subseteq V_\lambda$ per definizione di V_λ e il contenimento è stretto per il Lemma sopra.

3. Se $x \in V_\alpha$ allora ci sono due possibilità: se $\alpha = \beta + 1$ è un ordinale successore, allora $x \subseteq V_\beta$; se α è un ordinale limite (il caso $\alpha = 0$ è banale) allora esiste $\beta < \alpha$ per cui $x \in V_\beta$, da cui $x \subseteq V_\beta$ perché questo è un insieme transitivo.

4. Per induzione transfinita:

   - il caso $\alpha = 0$ è banalmente vero;
   - $\mathrm{P}(\alpha) \to \mathrm{P}(\alpha+1)$: per ogni $x \in \alpha+1$ si ha $x \leq \alpha$. Se $x = \alpha$, $x \subseteq V_\alpha$ per ipotesi induttiva, cioè $x \in V_{\alpha+1}$. Se $x \in \alpha$ allora $x \in V_{\alpha+1}$ perché $V_{\alpha+1}$ è transitivo.
     Inoltre, se per assurdo $(\alpha+1) \in V_{\alpha+1}$, cioè $(\alpha+1) \subseteq V_\alpha$, si ottiene $\alpha \in V_\alpha$ ($\mathcal{A}ssurdo$ per ipotesi induttiva).
   - λ limite: per ogni $x \in \lambda$ vale $x \in V_{x+1}$ per ipotesi induttiva e quindi $x \in V_\lambda$.
     Inoltre, se per assurdo $\lambda \in V_\lambda$, allora esiste un ordinale $\beta < \lambda$ per cui $\lambda \in V_\beta$, e da questo si ottiene $\beta \in V_\beta$ perché V_β è transitivo ($\mathcal{A}ssurdo$ per ipotesi induttiva).

□

Oss. Elementi di elementi di un V_α appartengono a qualche livello inferiore e nel caso degli ordinali successori $\alpha + 1$, si ha che elementi di elementi di $V_{\alpha+1}$ appartengono a V_α.

Brutalmente, "scavando" negli elementi si va all'indietro, mentre "facendo i sottoinsiemi" si va in avanti.

Definizione. *Se esiste un ordinale α tale che $x \in V_\alpha$, allora si dice* ***rango*** *di x il minimo ordinale $\rho(x)$ per cui $x \subseteq V_{\rho(x)}$.*

Proposizione 16.2. *(*) Il rango ha le seguenti proprietà:*

1. *per ogni ordinale α vale $\rho(\alpha) = \alpha$;*

2. *per ogni insieme x su cui sia ben definito il rango vale*

$$\rho(x) = sup\,\{\rho(y) + 1 \mid y \in x\}$$

   In particolare il rango è strettamente crescente, nel senso che per ogni x, y vale l'implicazione $x \in y \to \rho(x) < \rho(y)$.

Dim. 1. La tesi è una banale conseguenza di quanto dimostrato al punto (4) della Proposizione 16.1.

2. Sia $\beta := sup\,\{\rho(y) + 1 \mid y \in x\}$. Prima si prova che $x \subseteq V_\beta$: per ogni $z \in x$ vale $z \in V_{\rho(z)+1}$, dunque $z \in V_\beta$ per la crescenza dei V_α.

Ora si prova la minimalità di β. Se per assurdo esiste un ordinale $\alpha < \beta$ per cui $x \subseteq V_\alpha$, allora esiste $y \in x$ tale che $\alpha < \rho(y) + 1$, cioè $\alpha \leq \rho(y)$.

Da $x \subseteq V_\alpha$ si ottiene $y \in V_\alpha$ e per il punto (3) della Proposizione 16.1 esiste $\gamma < \alpha$ per cui $y \subseteq V_\gamma$, contro la minimalità di $\rho(y)$.

□

Ci si potrebbe chiedere quanto valga $|V_\alpha|$ al variare di α, e la seguente proposizione risolve completamente la questione.

Proposizione 16.3. *(*) Valgono i seguenti fatti:*

- *Per ogni naturale $n \geq 1$ vale $\aleph_0 > |V_n| \geq 2^{n-1}$.*
- *$|V_\omega| = \aleph_0$.*
- *Per ogni ordinale α si ha $|V_{\omega+\alpha}| = \beth_\alpha$.*

  In particolare $|V_\beta| = \beth_\beta$ se e solo se $\beta \geq \omega^2$.

Dim. Il caso con n naturale è una banale induzione.

Per il secondo caso si osserva che $|V_\omega| = |\bigcup_{n\in\omega} V_n|$ e quindi per ogni $n \in \omega$ vale $|V_\omega| \geq 2^{n-1}$. Poiché i 2^{n-1} sono illimitati in ω, si ottiene $|V_\omega| \geq \aleph_0$.

Inoltre

$$|V_\omega| = |\bigcup_{n\in\omega} V_n| \leq \sum_{n\in\omega} |V_n| = max\{\aleph_0, \aleph_0\} = \aleph_0$$

Perciò $|V_\omega| = \aleph_0$.

Il terzo si caso si dimostra per induzione transfinita su α. Il passo base $\alpha = 0$ segue da quanto si è appena dimostrato su V_ω.

Inoltre $|V_{\omega+(\alpha+1)}| = |V_{(\omega+\alpha)+1}| = |\mathcal{P}(V_{\omega+\alpha})| = 2^{|V_{\omega+\alpha}|} = 2^{\beth_\alpha} = \beth_{\alpha+1}$.

Se λ è limite, allora

$$|V_{\omega+\lambda}| = |\bigcup_{\gamma\in\lambda} V_{\omega+\gamma}| \leq \sum_{\gamma\in\lambda} \beth_\gamma = max\{|\lambda|, \beth_\lambda\} = \beth_\lambda$$

Inoltre per ogni $\gamma \in \lambda$ vale $|V_{\omega+\lambda}| \geq |V_{\omega+\gamma}| = \beth_\gamma$ e quindi $|V_{\omega+\lambda}| \geq \beth_\lambda$.

Perciò $|V_{\omega+\lambda}| = \beth_\lambda$. □

Si introduce ora un concetto molto importante nel resto del capitolo, cioè quello di "chiusura transitiva".

Definizione (Chiusura transitiva)**.** *Dato un insieme A si dice che X è la **chiusura transitiva** di A se è il più piccolo insieme transitivo che contiene A. In questo caso si scrive $TC(A) = X$ (TC sta per "transitive closure").*

Oss. Per provare che ogni insieme A ha la chiusura transitiva (l'unicità è banale) basta provare che esiste un insieme transitivo X che lo contiene e poi porre $TC(A) := \{x \in X \mid \forall y(\text{“}y \text{ è transitivo e contiene } A\text{”} \to x \in y)\}$.

Bisogna poi provarne la transitività, ma è del tutto banale.

Proposizione 16.4. *Per ogni insieme A esiste la sua chiusura transitiva.*

Dim. Per il Teorema di ricorsione con rimpiazzamento si definisce la successione

$$\begin{cases} A_0 = A \\ A_{n+1} = \bigcup A_n \end{cases}$$

Ora basta provare che $X := \bigcup_{n\in\omega} A_n$ è un insieme transitivo (e in particolare vale $X = TC(A)$).

Se $x \in y \in X$, allora esiste $n \in \omega$ tale che $y \in A_n$, da cui $x \in A_{n+1}$ e quindi $x \in X$.

Per provare $X = TC(A)$, si deve dimostrare la minimalità di X. Se Y è un insieme transitivo che contiene A, allora si deve provare $X \subseteq Y$, cioè $\forall n \in \omega(A_n \subseteq Y)$ e lo si fa per induzione su n. Il passo base $n = 0$ è vero per ipotesi. Se vale $P(n)$, allora $A_n \subseteq Y$ e per la transitività di Y si ottiene $\bigcup A_n \subseteq Y$, cioè $A_{n+1} \subseteq Y$. □

Proposizione 16.5. *(*) Per ogni insieme A e per ogni x vale*

$$x \in TC(A) \leftrightarrow \textit{esiste una sequenza finita } x \in x_1 \in x_2 \in \ldots \in x_n = A$$

Dim. $\to$: se $x \in TC(A)$ allora, considerando la successione definita nella proposizione 16.4, si ha che esiste $n \in \omega$ per cui $x \in A_n$. Pertanto si dimostra l'enunciato per induzione su n.

Il passo base $n = 0$ è banale.

Se vale $P(n)$ e $x \in A_{n+1}$ allora esiste $y \in A_n$ tale che $x \in y$. Per ipotesi induttiva esiste una sequenza finita $y \in x_1 \in x_2 \in \ldots x_n = A$ e dunque vale $x \in y \in x_1 \in \ldots \in x_n = A$.

$\leftarrow$: banale perché $TC(A)$ è un insieme transitivo.

□

Oss. Brutalmente, gli elementi della chiusura transitiva si ottengono “scavando” dentro gli elementi di A.

Alla fine del capitolo 3 si era parlato dell'Assioma di fondazione, e finora non lo si è mai nominato in tutti gli sviluppi della teoria: esso è strettamente legato alla Gerarchia di Von Neumann, per cui se ne prova prima un'utile forma equivalente e poi si passa a dimostrare un Teorema fondamentale su questi argomenti, che afferma l'equivalenza fra l'Assioma di fondazione e il fatto che ogni insieme appartenga a un qualche V_α.

Proposizione 16.6. *Sono fatti equivalenti:*

1. *Assioma di fondazione.*

2. *Non esistono catene $\in$-discendenti.*

Dim. Si dimostrano entrambe le implicazioni per assurdo.

(1)$\to$(2) : se per assurdo esiste una catena $\in$-discendente $x_0 \ni x_1 \ni x_2 \ldots$, allora l'insieme $A := \{x_n \mid n \in \omega\}$ è non vuoto e per ogni $a \in A$ vale banalmente $a \cap A \neq \emptyset$.

(2)$\to$(1) : se per assurdo esiste $x \neq \emptyset$ tale che per ogni $t \in x$ vale $t \cap x \neq \emptyset$, allora si considerano una funzione di scelta f su $\mathcal{P}(x)$ e un $a \in x$ e si definisce per ricorsione numerabile la seguente successione

$$\begin{cases} x_0 = a \\ x_{n+1} = f(x_n \cap x) \end{cases}$$

Si è così ottenuta una catena $\in$-discendente.

□

Oss. Se vale l'Assioma di fondazione, allora non esistono insiemi x per cui valga $x \in x$, altrimenti $x \ni x \ni \ldots$ sarebbe una catena $\in$-discendente.

Si potrebbe osservare la stessa cosa applicando direttamente l'Assioma di fondazione all'insieme $\{x\}$.

Lemma 16.1. *Per ogni insieme x, se ogni suo elemento appartiene a qualche V_α, allora anche x appartiene a un certo V_α. Formalmente, per ogni x vale l'implicazione*

$$(\forall t(t \in x \to (\exists \alpha(t \in V_\alpha)))) \to (\exists \beta(x \in V_\beta))$$

Dim. Per ogni $t \in x$ si pone $\beta_t := min\{\beta \mid \beta \text{ è un ordinale} \wedge t \in V_\beta\}$.

Per l'Assioma di rimpiazzamento esiste l'insieme $B := \{\beta_t \mid t \in x\}$: ora si pone $\beta^* = \bigcup B$ e si ottiene $x \subseteq V_{\beta^*}$, quindi $x \in V_{\beta^*+1}$. □

Teorema 16.1. *Sono fatti equivalenti:*

1. *Assioma di fondazione;*

2. *per ogni insieme x esiste un ordinale α per cui $x \in V_\alpha$.*

Dim. Si dimostrano entrambe le implicazioni per assurdo.

(1)→(2) : se per assurdo non esiste α tale che $x \in V_\alpha$, allora dal lemma 16.1 segue che esiste $y \in x$ con la stessa proprietà, e iterando il procedimento si otterrà una catena $\in$-discendente.

Formalmente, si considera una funzione di scelta su $\mathcal{P}(TC(A))$ e si definisce per ricorsione numerabile

$$\begin{cases} x_0 = x \\ x_{n+1} = f(\{y \in x_n \mid \forall \alpha \text{ ordinale } y \notin V_\alpha\}) \end{cases}$$

(2)→(1) : se per assurdo esiste un insieme $x \neq \emptyset$ tale che per ogni $y \in x$ vale $y \cap x \neq \emptyset$, allora si considera il minimo livello della gerarchia a cui appertiene almeno un elemento di x, ponendo $\beta_t := min\{\beta \mid \beta \text{ ordinale} \wedge \exists t \in V_\beta \cap x\}$ con $t \in V_{\beta_t} \cap x$. Dunque $t \cap x \neq \emptyset$ e se $s \in t \cap x$ si ha $s \in V_\gamma \cap x$ con $\gamma < \beta_t$ ($\mathcal{A}ssurdo$ per la minimalita di β_t).

□

Oss. L'Assioma di fondazione può essere riformulato come "ogni insieme non vuoto ha un elemento $\in$-minimale".

17 Modelli della Teoria degli Insiemi

$\mathcal{O}$ra

MANCANO UN PO' DI COSE

Proposizione 17.1. *Se k è un cardinale fortemente inaccessibile, allora $V_k \vDash$ 'Rimpiazzamento'.*

Dim. Data una funzione $f\colon V_k \to V_k$ e un certo $A \in V_k$, si deve provare che vale $f(A) \in V_k$.

Per ogni $x \in A$ sia $\alpha_x = min\{\alpha \in k \mid f(x) \in V_\alpha\}$. Posto $\beta := sup\, B$, dove $B := \{\alpha_x \mid x \in A\}$, valgono banalmente $|B| \leq |A| \leq |V_\gamma| \leq \beth_\gamma$ per un certo $\gamma \in k$, e $f(A) \subseteq V_\beta$.

Se $\beta < k$, allora si è concluso perché in questo caso si ottiene $f(A) \subseteq V_\beta$, da cui $f(a) \in V_{\beta+1} \subseteq V_k$.

Si sa che k è un cardinale fortemente inaccessibile se e solo se regolare e punto fisso della 'funzione' beth. Dunque $k = \beth_k$.

Se per assurdo fosse $\beta = k$, allora B sarebbe un sottoinsieme illimitato in k di cardinalità al più $\beth_\gamma < \beth_k$, mentre la cofinalità di k è proprio $\beth_k$ ($\mathcal{A}ssurdo$).

□

Oss. La condizione sopra non è necessaria affinché..., per esempio

18 Elenco di esercizi utili

*W*ow, you did it!

Si presenta una serie di esercizi assegnati negli anni passati nelle prove d'esame del Prof. Mauro Di Nasso, alcuni facili (per motivare il lettore), altri meno, ma tuttavia ritenuti interessanti o utili per la comprensione del corso.

Alcuni esercizi (contrassegnati con un (*)) sono invece stati lasciati a lezione, ma non sembravano utili ai fini degli sviluppi della teoria e per questo sono stati inseriti in questo capitolo.

I problemi sono suddivisi per argomento, ma è probabile che nella loro risoluzione si usino fatti studiati in capitoli successivi, per cui non si assicura che siano risolvibili subito dopo aver studiato il capitolo corrispondente.

Inoltre all'inizio di ciascuno di essi se ne dà un'indicazione sulla difficoltà risolutiva, ovviamente secondo la personale opinione dell'autore, suddividendoli in tre categorie, cioè "facile", "normale" e "difficile". La difficoltà di un esercizio è fortemente condizionata da quelli che lo precedono, perché talvolta sono banali applicazioni di esercizi visti in precedenza o comunque hanno grosse somiglianze con altri esercizi.

Si consiglia infine di svolgere gli esercizi nell'ordine in cui sono proposti, almeno all'interno di uno stesso capitolo, perché spesso vi sono importanti richiami fra un esercizio e uno precedente.

Cardinalità di vari insiemi

1. (Normale) Calcolare la cardinalità dell'insieme

$$A := \{f\colon \mathbb{N} \to \mathbb{N} \mid f \text{ è crescente}\}$$

Sol. Per prima cosa si osserva che $A \subseteq \mathbb{N}^{\mathbb{N}}$, dunque $|A| \leq |\mathbb{N}^{\mathbb{N}}| = 2^{\aleph_0}$.
Inoltre si sa dalla teoria che $|[\mathbb{N}]^{\aleph_0}| = 2^{\aleph_0}$.
Ora si definisce

$$\begin{aligned} \varphi\colon [\mathbb{N}]^{\aleph_0} &\to A \\ X &\mapsto f_X \end{aligned}$$

dove f_X è l'unico isomorfismo fra $\mathbb{N}$ e X, e si osserva che è iniettiva, dunque $2^{\aleph_0} \leq |A|$ e si conclude con Cantor-Bernstein che vale $|A| = 2^{\aleph_0}$. □

2. (Normale) Calcolare la cardinalità dell'insieme

$$A := \{f\colon \mathbb{N} \to \mathbb{N} \mid \forall n\ f(n) \neq n\}$$

Sol.

- Soluzione 1: per prima cosa si osserva che $A \subseteq \mathbb{N}^{\mathbb{N}}$, dunque $|A| \leq |\mathbb{N}^{\mathbb{N}}| = 2^{\aleph_0}$.
  Inoltre, posti $P := \{n \in \mathbb{N} \mid n \text{ è pari}\}$ e $D := \{n \in \mathbb{N} \mid n \text{ è dispari}\}$, si considera la seguente funzione

$$\begin{aligned} \varphi\colon D^P \times P^D &\to A \\ (f, g) &\mapsto \varphi(f, g) \end{aligned}$$

  dove $\varphi(f,g)(2n) = f(2n)$ e $\varphi(f,g)(2n+1) = g(2n+1)$, e si osserva che oltre ad essere ben definita, è pure iniettiva.
  Perciò $|A| \geq |D^P \times P^D| = \aleph_0^{\aleph_0} \cdot \aleph_0^{\aleph_0} = 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$.
  Si conclude con Cantor-Bernstein che vale $|A| = 2^{\aleph_0}$.

- Soluzione 2 (Lorenzo Cecchi): si pone

$$A' := \{f\colon \mathbb{N} \to \mathbb{N} \mid \forall n \in \mathbb{N} \;\; f(n) > n\}$$

  e si osserva che A' e $\mathcal{F}un(\mathbb{N}, \mathbb{N}^+)$ sono in bigezione, data per esempio da

$$\begin{aligned} \varphi\colon A' &\to \mathcal{F}un(\mathbb{N}, \mathbb{N}^+) \\ f &\mapsto g \end{aligned}$$

  dove per ogni $n \in \mathbb{N}$ vale $g(n) = f(n) - n$.
  Dunque $|A| \geq |A'|$ perché $A' \subseteq A$ e $|A'| = 2^{\aleph_0}$, da cui la tesi.

□

3. (Normale) Calcolare la cardinalità dell'insieme

$$A := \{f\colon \mathbb{N} \to \mathbb{N} \mid f \text{ è bigettiva}\}$$

Sol. Per prima cosa si osserva che $A \subseteq \mathbb{N}^{\mathbb{N}}$, dunque $|A| \leq |\mathbb{N}^{\mathbb{N}}| = 2^{\aleph_0}$.

Inoltre, posti $P := \{n \in \mathbb{N} \mid n \text{ è pari}\}$, $D := \{n \in \mathbb{N} \mid n \text{ è dispari}\}$ e $X := \{B \subseteq \mathbb{N} \mid |B| = |\mathbb{N} \setminus B| = \aleph_0\}$, si considera la seguente funzione

$$\begin{aligned} \varphi\colon X &\to A \\ B &\mapsto \varphi_B \end{aligned}$$

dove $\varphi_B(2n) = f_B(2n)$ e $\varphi_B(2n+1) = g_B(2n+1)$, dove $f_B\colon P \to B$ e $g_B\colon D \to \mathbb{N} \setminus B$ sono bigezioni (si usa l'Assioma di scelta).

Ora φ è ben definita e iniettiva, quindi $|X| \leq |A|$, ed è facile provare $|X| = 2^{\aleph_0}$ perché $|[\mathbb{N}]^{\aleph_0}| = 2^{\aleph_0}$ e quelli con complementare finito sono tanti quanti i sottoinsiemi finiti di $\mathbb{N}$, cioè $\aleph_0$.

Si conclude con Cantor-Bernstein che vale $A = 2^{\aleph_0}$. □

4. (Normale) Calcolare la cardinalità dell'insieme

$$A := \{f\colon \mathbb{N} \to \mathbb{N} \mid f \text{ è illimitata}\}$$

Sol. Per prima cosa si osserva che $A \subseteq \mathbb{N}^{\mathbb{N}}$, dunque $|A| \leq |\mathbb{N}^{\mathbb{N}}| = 2^{\aleph_0}$.

Inoltre si nota che se una funzione da $\mathbb{N}$ in $\mathbb{N}$ ha immagine numerabile allora è banalmente illimitata, dunque basterà considerare le funzioni da con immagine numerabile, visto che i sottoinsiemi numerabili di $\mathbb{N}$ sono $2^{\aleph_0}$.

Si pone dunque

$$\begin{aligned} \varphi\colon [\mathbb{N}]^{\aleph_0} &\to A \\ B &\mapsto f_B \end{aligned}$$

dove $f_B\colon \mathbb{N} \to B$ è una bigezione (si usa l'Assioma di scelta), e si osserva che φ è iniettiva, da cui $|A| \geq |[\mathbb{N}]^{\aleph_0}| = 2^{\aleph_0}$.

Si conclude con Cantor-Bernstein che vale $|A| = 2^{\aleph_0}$. □

5. (Facile) Calcolare la cardinalità dell'insieme $A := \bigcup_{\gamma\in\omega_1} A_\gamma$, dove $\{A_\gamma \mid \gamma \in \omega_1\}$ èuna famiglia di aperti non vuoti di $\mathbb{R}$.

Sol. Si è già visto che ogni aperto non vuoto di $\mathbb{R}$ ha la cardinalità del continuo (perché contiene un intervallo). Dunque $|A| \geq 2^{\aleph_0}$.

Inoltre vale $|A| \leq \sum_{\gamma\in\omega_1} |A_\gamma| = max\{sup\,|A_\gamma|, \aleph_1\} = 2^{\aleph_0}$.

Si conclude con Cantor-Bernstein che vale $|A| = 2^{\aleph_0}$. □

6. (Facile) Determinare la cardinalità degli insiemi

$$A := \{X \subseteq \omega_1 \mid X \text{ è superiormente limitato}\}$$

$$B := \{X \subseteq \omega_1 \mid X \text{ è illimitato}\}$$

Sol. I sottoinsiemi di ω_1 hanno cardinalità minore o uguale a $\aleph_1$. Quelli che hanno cardinalità $\aleph_1$ sono illimitati (segue direttamente dalla definizione di cardinale), dunque quelli superiormente limitati hanno cardinalità al più numerabile. Inoltre quelli di cardinalità al più numerabile sono superiormente limitati perché ω_1 è un cardinale regolare in quanto cardinale successore.

Dalla teoria si sa che $|[\omega_1]^{\aleph_0}| = \aleph_1^{\aleph_0} = 2^{\aleph_0}$. Inoltre per ogni $n \in \omega$ vale $|[\omega_1]^n| = \aleph_1^n = \aleph_1$, quindi i sottoinsiemi finiti di ω_1 sono al più $\sum_{n\in\omega} \aleph_1 = \aleph_1$.

Si è ottenuto che $|A| = 2^{\aleph_0} + \aleph_1 = 2^{\aleph_0}$.

Per il secondo insieme basta osservare che un sottoinsieme illimitato di ω_1 ha necessariamente cardinalità $\aleph_1$ per la regolarità di ω_1, e dunque $|B| = |[\omega_1]^{\aleph_1}| = \aleph_1^{\aleph_1} = 2^{\aleph_1}$. □

Ordinali

1. (Facile) Determinare quoziente e resto della divisione euclidea tra gli ordinali $\omega^2 \cdot 2 + \omega \cdot 4 + 5$ e $\omega \cdot 2 + 3$.

   Sol. Si prova prima di tutto che $(\omega \cdot 2 + 3) \cdot \omega = \omega^2$.

   Si ha $(\omega \cdot 2 + 3) \cdot \omega = \bigcup_{n \in \omega} (\omega \cdot 2 + 3) \cdot n$ e banalmente (induzione) per ogni n vale $(\omega \cdot 2 + 3) \cdot n = \omega \cdot (2 \cdot n) + 3$, dunque si ottiene $(\omega \cdot 2 + 3) \cdot \omega = \bigcup_{n \in \omega} \omega \cdot (2 \cdot n) + 3 = \bigcup_{n \in \omega} \omega \cdot n = \omega^2$.

   Perciò $(\omega \cdot 2 + 3) \cdot \omega \cdot 2 = \omega^2 \cdot 2$ e banalmente $\omega^2 \cdot 2 + \omega \cdot 4 + 5 = (\omega \cdot 2 + 3) \cdot (\omega \cdot 2 + 2) + 2$.

   Si conclude che il quoziente e il resto cercati sono rispettivamente $\omega \cdot 2 + 2$ e 2. □

2. (Facile) Determinare l'insieme degli ordinali α per cui vale $\alpha + \omega^3 = \omega^3 + \alpha$.

   Sol. Poiché ω^3 e ω^4 sono ordinali additivamente chiusi, oltre ad $\alpha = 0$ non esitono altre soluzioni che siano $< \omega^3$ o $\geq \omega^4$. Se invece $\omega^3 \leq \alpha < \omega^4$, per la Forma normale di Cantor si ottiene $\alpha = \omega^3 \cdot n_1 + \omega^2 \cdot n_2 + \omega \cdot n_3 + n_4$, da cui $\alpha + \omega^3 = \omega^3 \cdot (n_1 + 1)$ e $\omega^3 + \alpha = \omega^3 \cdot (n_1 + 1) + \omega^2 \cdot n_2 + \omega \cdot n_3 + n_4$ e vale l'uguaglianza se e solo se $n_2 = n_3 = n_4 = 0$. Dunque le uniche soluzioni diverse da 0 sono gli $\omega^3 \cdot n$ con $n \geq 1$ naturale. □

3. (Normale) Se ξ è un ordinale, allora vale l'uguaglianza $\xi + \omega = \omega \cdot \xi$ se e solo se esiste un ordinale ζ tale che $\xi = \omega^\omega \cdot \zeta + 1$.

   Dim. $\rightarrow$: per la divisione euclidea esistono ζ e $\rho < \omega^\omega$ ordinali tali che $\xi = \omega^\omega \cdot \zeta + \rho$. Se si dimostra $\rho = 1$ si è concluso. Per ipotesi $\omega^\omega \cdot \zeta + \rho + \omega = \omega \cdot (\omega^\omega \cdot \zeta + \rho) = \omega^\omega \cdot \zeta + \omega \cdot \rho$.

   Prima di tutto si osserva che $\rho = 0$ non funziona. Poi se $\rho = n \in \omega$ è diverso da 1, allora si ottiene $\omega^\omega \cdot \zeta + \omega = \omega^\omega \cdot \zeta + \omega n$, che è *Assurdo* per la forma normale di Cantor. Anche nel caso $\rho \geq \omega$ si ottiene un *Assurdo* per la forma normale di Cantor. Dunque si è concluso.

   $\leftarrow$: $\xi + \omega = \omega^\omega \cdot \zeta + 1 + \omega = \omega^\omega \cdot \zeta + \omega = \omega \cdot (\omega^\omega \cdot \zeta + 1)$.

   □

4. (Normale) Determinare tutti e soli gli ordinali α per cui $\omega \cdot \alpha = \omega^2 \cdot \alpha$.

Sol. Gli α cercati sono tutti e soli i multipli di ω^ω.

Infatti per divisione euclidea si ottiene $\alpha = \omega^\omega \cdot \delta + \rho$ dove $\rho < \omega^\omega$, e dunque $\omega \cdot \alpha = \omega^\omega \cdot \delta + \omega \cdot \rho$ e $\omega^2 \cdot \alpha = \omega^\omega \cdot \delta + \omega^2 \cdot \rho$ perché ω^ω è moltiplicativamente chiuso.

Per cancellazione a sinistra questi due ordinali sono uguali se e solo se $\omega \cdot \rho = \omega^2 \cdot \rho$ e ci si ritrova nella richiesta iniziale, solo che stavolta vale $\rho < \omega^\omega$.

Usando la Forma normale di Cantor è banale provare che l'uguaglianza sopra è verificata se e solo se $\rho = 0$, da cui la tesi. □

5. (Facile) Sia $\epsilon_0 = \bigcup_{n\in\omega} \alpha_n$, dove si pone induttivamente $\alpha_0 = \omega$, $\alpha_{n+1} = \omega^{\alpha_n}$.

   (a) Dimostrare che $\omega^{\epsilon_0} = \epsilon_0$.

   (b) Dimostrare che ϵ_0 è il più piccolo ordinale α tale che $\omega^\alpha = \alpha$.

   Dim. (a) Per una banale induzione si ottiene che la successione degli α_n è strettamente crescente, dunque ϵ_0 è un ordinale limite e $\omega^{\epsilon_0} = \bigcup_{\gamma\in\epsilon_0} \omega^\gamma = \bigcup_{n\in\omega} \alpha_n = \epsilon_0$.

   (b) Dato α tale che $\alpha = \omega^\alpha$, basta provare che per ogni $n \in \omega$ vale $\alpha_n \in \alpha$ e lo si fa per induzione su n. Il caso $\alpha = 0$ è banale. Se $\alpha_n \in \alpha$, allora, visto che α è limite, si ottiene $\alpha_{n+1} = \omega^{\alpha_n} \subseteq \bigcup_{\gamma\in\alpha} \omega^\gamma = \omega^\alpha$.
   Resta da escludere il caso $\omega^{\alpha_n} = \alpha$, ma in questo caso si otterrebbe $\omega^{\alpha_n} = \omega^\alpha$, da cui $\alpha_n = \alpha$ (*Assurdo*).

   □

6. (Facile) Determinare tutti e soli gli ordinali α tali che per ogni ordinale γ vale $\alpha^\gamma + \alpha^{\gamma+1} = \alpha^{\gamma+1}$.

   Sol. Gli α cercati sono tutti e soli quelli maggiori o uguali a ω (oltre ad $\alpha = 0$).

   Infatti basta osservare che $\alpha^\gamma + \alpha^{\gamma+1} = \alpha^{\gamma+1} \leftrightarrow \alpha^\gamma(1 + \alpha) = \alpha^\gamma \cdot \alpha \leftrightarrow 1 + \alpha = \alpha$. □

7. (Normale) Trovare dei sottoinsiemi di $\mathbb{Q}$ isomorfi rispettivamente agli ordinali ω^2 e ω^ω.

8. (Facile) Trovare:

   (a) esempi di ordinali α tali che $n^\alpha = \alpha$ per ogni naturale $n > 1$;

   (b) esempi di ordinali α tali che $\omega_1^\alpha = \alpha$.

Sol. Per il primo caso si può prendere ω, mentre per il secondo si pone $\alpha = \bigcup_{n\in\omega} \alpha_n$, dove $\alpha_0 = \omega_1$ e $\alpha_{n+1} = \omega_1^{\alpha_n}$, e si conclude come nell'esercizio 5. □

9. (Facile) Calcolare la massima cardinalità di una famiglia di buoni ordini numerabili non isomorfi fra loro.

   Sol. Dalla teoria si sa che ogni buon ordine è isomorfo a un unico ordinale, dunque ogni famiglia di buoni ordini numerabili non isomorfi fra loro ha cardinalità minore o uguale a quella degli ordinali numerabili, cioè $\aleph_1$.

   In particolare, se si prende $\omega_1 \setminus \omega$ si ottiene proprio una famiglia di buoni ordini numerabili di cardinalità $\aleph_1$. □

10. (Difficile) Calcolare la massima cardinalità di una famiglia di ordini totali numerabili non isomorfi fra loro.

Assioma di scelta

1. (Normale) (*) Dimostrare direttamente l'implicazione "Lemma di Zorn $\to$ Assioma di scelta".

   Dim. Dato un insieme X, usando il Lemma di Zorn si va a dimostrare l'esistenza di una funzione di scelta per $\mathcal{P}(X)$.

   L'insieme $\{f\colon Y \to \bigcup X \mid Y \subseteq \mathcal{P}(X) \wedge \forall A \in Y (A \neq \emptyset \to f(A) \in A)\}$ è banalmente non vuoto e parzialmente ordinato rispetto al contenimento e ogni catena ha l'unione come maggiorante, dunque per il Lemma di Zorn ha un elemento massimale φ.

   Si prova che $\mathcal{D}om\,\varphi = \mathcal{P}(X)$ e dunque che φ è una funzione di scelta per $\mathcal{P}(X)$. Infatti se esiste $A \in \mathcal{P}(X) \setminus \mathcal{D}om\,\varphi$, allora si definisce $\varphi^*\colon \mathcal{D}om\,\varphi \cup \{A\} \to \bigcup X$ estendendo φ e ponendo $\varphi^*(A) = a$ dove a è un qualsiasi elemento di A (oppure un qualsiasi elemento di X se $A = \emptyset$). Si ha $\varphi^* \supsetneq \varphi$, contro la massimalità di φ. □

2. (Normale) (*) Dimostrare direttamente l'implicazione "Lemma di Zorn $\to$ Teorema di Zermelo".

   Dim. Dato un insieme A, si prova usando il Lemma di Zorn che A è in bigezione con un sottoinsieme di un insieme bene ordinato, e dunque bene ordinabile (infatti se $f\colon A \to X$ è questa bigezione, allora basta porre $a_1 < a_2 \leftrightarrow f(a_1) < f(a_2)$).

   L'insieme $\{f\colon Y \to \mathcal{H}(A) \mid Y \subseteq A \wedge f \text{ è iniettiva}\}$ è banalmente non vuoto e parzialmente ordinato rispetto al contenimento. Inoltre ogni

catena ha l'unione come maggiorante, dunque per il Lemma di Zorn ha un elemento massimale φ. Se $\mathcal{I}m\,\varphi = \mathcal{H}(A)$, allora $|\mathcal{H}(A)| \leq |A|$ (*Assurdo*), dunque $\mathcal{I}m\,\varphi \subsetneq \mathcal{H}(A)$ e dunque esiste $b \in \mathcal{H}(A) \setminus \mathcal{I}m\,\varphi$.

Ora si prova che vale $\mathcal{D}om\,\varphi = A$: se per assurdo esiste $a \in A \setminus \mathcal{D}om\,\varphi$, allora si definisce φ^* estendendo φ e ponendo $\varphi^*(a) = b$. Si ha $\varphi^* \supsetneq \varphi$, contro la massimalità di φ. □

Cardinali

1. (Facile) Supponendo $\mathfrak{c} = \aleph_{14}$, si mettano in ordine i seguenti cardinali:

$$\aleph_{15}^{\aleph_0} \qquad \aleph_{13}^{\aleph_{13}} \qquad \aleph_0^{\aleph_{13}} \qquad \mathfrak{c} \qquad \aleph_{13}^{\aleph_0}$$

Sol. Si studiano i cardinali proposti caso per caso usando quasi solamente la Formula di Hausdorff:

- $\aleph_{15}^{\aleph_0} = \aleph_{15} \cdot \mathfrak{c} = max\{\aleph_{15},\ \aleph_{14}\} = \aleph_{15}$;
- $\aleph_{13}^{\aleph_{13}} = 2^{\aleph_{13}} \geq \aleph_{14}$;
- $\aleph_0^{\aleph_{13}} = 2^{\aleph_{13}} \geq \aleph_{14}$;
- $\mathfrak{c} = \aleph_{14}$;
- $\aleph_{13}^{\aleph_0} = \aleph_{13} \cdot \mathfrak{c} = max\{\aleph_{13},\ \aleph_{14}\} = \aleph_{14}$.

Per concludere, si è ottenuto che $\mathfrak{c} = \aleph_{13}^{\aleph_0}$ è il cardinale più piccolo della lista, poi vengono $\aleph_{13}^{\aleph_{13}} = \aleph_0^{\aleph_{13}} = 2^{\aleph_{13}}$ e $\aleph_{15}^{\aleph_0} = \aleph_{15}$, il cui ordine non è decidibile. □

2. (Facile) Per ogni cardinale $\omega_\alpha > \omega$, vale l'uguaglianza $\omega^{\omega_\alpha} = \omega_\alpha$ (dove l'esponenziazione è intesa in senso ordinale).

Dim. Poiché $|\omega^{\omega_\alpha}| = \aleph_\alpha$, vale $\omega^{\omega_\alpha} \geq \omega_\alpha$.

Inoltre non può valere la disuguaglianza stretta perché $\omega^{\omega_\alpha} = \bigcup_{\gamma \in \omega_\alpha} \omega^\gamma$ e ogni ω^γ ha cardinalità minore di $\aleph_\alpha$. □

Oss. Questa proprietà è utile quando si vuole scrivere la Forma normale di Cantor di un ordinale maggiore di ω_α.

Inoltre si è provato (anche se sarebbe banale farlo direttamente) che tutti i cardinali infiniti sono esponenzialmente chiusi (e quindi anche moltiplicativamente e additivamente chiusi).

3. (Facile) Vale l'uguaglianza $\aleph_\omega^{\aleph_1} = max\{\aleph_\omega^{\aleph_0},\ 2^{\aleph_1}\}$.

Dim. Dalla teoria

$$\aleph_\omega^{\aleph_1} = (sup_{\,\alpha\in\omega}\aleph_\alpha^{\aleph_1})^{\aleph_0} = (sup_{\,\alpha\in\omega}\aleph_{\alpha+1}^{\aleph_1})^{\aleph_0} = (sup_{\,\alpha\in\omega} max\{\aleph_{\alpha+1},\, 2^{\aleph_1}\})^{\aleph_0}$$

Per cui, se $2^{\aleph_1} < \aleph_\omega$, allora $\aleph_\omega^{\aleph_1} = \aleph_\omega^{\aleph_0}$, altrimenti $\aleph_\omega^{\aleph_1} = 2^{\aleph_1}$. □

4. (Normale) Se k è un cardinale infinito, allora $2^k = (sup_{\,\nu\in k} 2^\nu)^{cof k}$.

   Dim. Banalmente $2^k \geq sup_{\,\nu\in k} 2^\nu$ e dunque, poiché $cof k \leq k$, si ottiene $2^k \geq (sup_{\,\nu\in k} 2^\nu)^{cof k}$. Per l'altra disuguaglianza si trattano separatamente i casi in cui k è regolare o singolare.

   Se k è un cardinale regolare, cioè $cof k = k$, allora $2^k \leq (sup_{\,\nu\in k} 2^\nu)^k = (sup_{\,\nu\in k} 2^\nu)^{cof k}$.

   Se k è un cardinale singolare, allora si prende $k = \sum_{i\in cof k} k_i$ dove i k_i sono debolmente crescenti e per ogni $i \in cof k$ vale $k_i < k$ e si nota facilmente che dalla singolarità di k segue che i k_i sono illimitati in k. Allora $(sup_{\,\nu\in k} 2^\nu)^{cof k} = (sup_{\,i\in cof k} 2^{k_i})^{cof k} = \prod_{i\in cof k} 2^{k_i}$.

   Dunque si pone

   $$\varphi\colon \mathcal{F}un(k,\, 2) \to \prod_{i\in cof k} \mathcal{F}un(k_i,\, 2)$$
   $$f \mapsto f^*$$

   dove $f^*\colon cof k \to \bigcup_{i\in cof k} \mathcal{F}un(k_i,\, 2)$ manda i in $f_{|k_i}$ e si osserva che φ è iniettiva, da cui la tesi. □

   Oss. Questa proprietà si rivela molto utile nella pratica.

5. (Facile) Se per ogni $n \in \omega$ vale $2^{\aleph_n} = \mathfrak{c}$, allora $2^{\aleph_\omega} = \mathfrak{c}$.

   Dim. Immediata conseguenza dell'esercizio 4. Infatti

   $$2^{\aleph_\omega} = (sup_{\,n\in\omega} 2^{\aleph_n})^{cof\aleph_\omega} = (sup_{\,n\in\omega} 2^{\aleph_0})^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0} = \mathfrak{c}$$

   □

6. (Normale) Se k è un cardinale singolare e la successione $\langle 2^\nu \mid \nu \in k\rangle$ ha massimo 2^μ (con $\mu \in k$), allora $2^k = 2^\mu$.

   Dim. Per l'esercizio 4 si ha $2^k = (sup_{\,\nu\in k} 2^\nu)^{cof k} = 2^{\mu\cdot cof k}$.

   Se $\mu \geq cof k$, allora $2^k = 2^\mu$, altrimenti $2^k = 2^{cof k} = 2^\mu$, dove l'ultima uguaglianza segue dal fatto che $cof k < k$ (k è singolare) e dalla massimalità di 2^μ. □

7. (Facile) Se per ogni $n \in \omega$ vale $2^{\aleph_{\omega+n}} = 2^{\aleph_\omega}$, allora si ha $2^{\aleph_{\omega+\omega}} = 2^{\aleph_\omega}$.

Dim. Si possono fare i conti (facili), oppure applicare direttamente l'esercizio 6. □

8. (Normale) Dati due ordinali α e β, si calcoli $\beth_\alpha^{\beth_\beta}$.

   Sol. Se $\beta \geq \alpha$, allora $\beth_\alpha^{\beth_\beta} = 2^{\beth_\beta} = \beth_{\beta+1}$.

   Se $\beta < \alpha$ si studiano separatamente i casi in cui α è un ordinale successore o limite.

   Dunque se $\beta < \gamma + 1$, allora $\beth_{\gamma+1}^{\beth_\beta} = (2^{\beth_\gamma})^{\beth_\beta} = 2^{\beth_\gamma} = \beth_{\gamma+1}$.

   Se $\beta < \lambda$ e λ è un ordinale limite, allora $\beth_\lambda$ è un cardinale limite (forte) e $cof\beth_\lambda = cof\lambda$. Si trattano separatamente i casi in cui $\beth_\beta < cof\lambda$ e $\beth_\beta \geq cof\lambda$.

   Se $\beth_\beta < cof\lambda$, allora

   $$\beth_\lambda^{\beth_\beta} = sup_{\,\alpha<\lambda}\beth_\alpha^{\beth_\beta} = sup_{\,\alpha<\lambda}\beth_{\alpha+1}^{\beth_\beta} = sup_{\,\alpha<\lambda}\beth_{\alpha+1} = \beth_\lambda$$

   Se $\beth_\beta \geq cof\lambda$, allora

   $$\beth_\lambda^{\beth_\beta} = (sup_{\,\alpha<\lambda}\beth_\alpha^{\beth_\beta})^{cof\lambda} = (sup_{\,\alpha<\lambda}\beth_{\alpha+1}^{\beth_\beta})^{cof\lambda} = (sup_{\,\alpha<\lambda}\beth_{\alpha+1})^{cof\lambda} = \beth_\lambda^{cof\lambda} > \beth_\lambda$$

   Riassumendo, si è ottenuto

   $$\beth_\alpha^{\beth_\beta} = \begin{cases} \beth_{\beta+1} \text{ se } \beta \geq \alpha \\ \beth_\alpha \text{ se } \beta < \alpha \text{ e } \alpha \text{ successore} \\ \beth_\alpha \text{ se } \beta < \alpha,\ \alpha \text{ limite e } \beth_\beta < cof\alpha \\ \beth_\alpha^{cof\alpha} \text{ se } \beta < \alpha,\ \alpha \text{ limite e } \beth_\beta \geq cof\alpha \end{cases}$$

   □

9. (Normale) $\aleph_\omega$ è un limite forte se e solo se $\aleph_\omega = \beth_\omega$.

   Dim. $\rightarrow$: si è già provato che $\aleph_\omega \leq \beth_\omega$.

   Per provare l'altra disuguaglianza bsta dimostrare che per ogni $n \in \omega$ esiste $k \in \omega$ tale che $\beth_n = \aleph_k$ e lo si fa per induzione su n.

   - Per definizione vale $\beth_0 = \aleph_0$;
   - P(n)$\rightarrow$P($n+1$): $\beth_{n+1} = 2^{\beth_n} = 2^{\aleph_k} < \aleph_\omega$, dove la disuguaglianza segue dal fatto che $\aleph_\omega$ è un limite forte.

   $\leftarrow$: ovvio perché $\beth_\omega$ è un limite forte dato che ω è un ordinale limite.

   □

10. (Normale) L'"Ipotesi dei cardinali singolari" (SCH, "Singular Cardinals Hypothesis") afferma che per ogni cardinale infinito k vale l'uguaglianza $k^{cof k} = k^+ \cdot 2^{cof k}$ ed è indipendente da ZFC.

    Il Teorema di Silver (fuori dalla portata di questo corso) prova che se SCH non vale, allora il più piccolo controesempio ha cofinalità numerabile.

    Si provi, usando il Teorema di Silver, che se per ogni cardinale regolare $k > 2^{\aleph_0}$ vale $k^{\aleph_0} = k$, allora vale SCH.

    Dim. Si nota prima di tutto che un qualsiasi controesempio k per SCH è un cardinale singolare. Infatti se k fosse regolare, allora $k = cof k$, da cui segue $2^k = k^k = k^{cof k} \neq k^+ \cdot 2^{cof k} = k^+ \cdot 2^k = 2^k$ ($\mathcal{A}ssurdo$).

    Un altro fatto semplice da osservare è che per ogni cardinale ν vale $\nu^{cof \nu} \geq \nu^+ \cdot 2^{cof \nu}$, infatti $\nu^{cof \nu} > \nu$ e perciò $\nu^{cof \nu} \geq \nu^+$ e banalmente $\nu^{cof \nu} \geq 2^{cof \nu}$.

    Dunque l'Ipotesi dei cardinali singolari potrebbe essere riformulata nel modo seguente: "non esistono cardinali singolari k tali che $k^{cof k} > k^+ \cdot 2^{cof k}$".

    Ora si procede con la dimostrazione dell'enunciato richiesto e lo si fa provando che l'ipotesi garantisce la non esistenza di controesempi per SCH con cofinalità numerabile (e si conclude con il Teorema di Silver).

    Dato per assurdo un controesempio k per SCH con $cof k = \aleph_0$, allora si ha che k è un cardinale singolare per quanto già osservato precedentemente, dunque $k > cof k = \aleph_0$. Ci sono due casi possibili.

    Se $2^{\aleph_0} \geq k^+$, allora $2^{\aleph_0} \leq k^{\aleph_0} \leq (k^+)^{\aleph_0} \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0}$, da cui segue $k^{\aleph_0} = 2^{\aleph_0}$ ($\mathcal{A}ssurdo$ perché k è un controesempio per SCH).

    Se $k^+ > 2^{\aleph_0}$, allora, poiché k^+ è regolare in quanto cardinale successore, per ipotesi si ha $(k^+)^{\aleph_0} = k^+$. Per la Formula di Hausdorff $k^+ = (k^+)^{\aleph_0} = max\{k^+, k^{\aleph_0}\}$, quindi $k^+ \geq k^{\aleph_0}$. Ma $k^{cof k} = k^{\aleph_0} > k^+$ perché k è un controesempio per SCH, da cui l'$\mathcal{A}ssurdo$. □

11. (Normale) SCH vale se e solo se per ogni cardinale singolare $k > 2^{cof k}$ vale $k^{cof k} = k^+$.

    Dim. L'implicazione $\rightarrow$ è banalmente vera.

    Per l'altra implicazione si osserva prima di tutto che i cardinali regolari soddisfano sempre SCH.

    Invece se k è singolare, ci sono due possibilità, o $k > 2^{cof k}$ o $k < 2^{cof k}$.

    Se $k > 2^{cof k}$, allora $k^+ > 2^{cof k}$ e $k^{cof k} = k^+ = k^+ \cdot 2^{cof k}$.

    Se $k < 2^{cof k}$, allora $k^+ \leq 2^{cof k}$ e si vede facilente che $k^{cof k} = 2^{cof k} = k^+ \cdot 2^{cof k}$. □

12. (Normale) GCH implica SCH.

    Dim. Intanto si osserva che se vale GCH allora per ogni cardinale singolare k vale $k > cofk$, dunque $k \geq (cofk)^+ = 2^{cofk}$. Inoltre si è già visto che per ogni cardinale k vale $k \neq 2^{cofk}$.

    Ora si usa l'esercizio 11 e si deve provare che se vale GCH allora per ogni cardinale singolare vale $k^{cofk} = k^+$ (in realtà vale pure se k è regolare, cioè se vale GCH, allora la "funzione" gimel fornisce come risultato il cardinale successore).

    Dalla teoria $k^+ = 2^k \geq k^{cofk}$. Inoltre $k^{cofk} > k$, da cui segue $k^{cofk} \geq k^+$. □

13. (Facile) Dato un cardinale k infinito, si determinino tutti gli ordinali α tali che $\alpha + k = k$.

    Sol. Si è già dimostrato che ogni cardinale infinito è additivamente chiuso. Dunque se $\alpha < k$, allora $\alpha + k = k$.

    Se invece $\alpha \geq k$, allora $\alpha + k \geq k + k > k$.

    In conclusione gli α cercati sono tutti e soli quelli minori di k. □

14. (Normale) Se k è un cardinale debolmente inaccessibile, allora $\aleph_k = k$.

    Dim. Dalla definizione di cardinale debolmente inaccessibile segue che k è limite e regolare. Dunque esiste un ordinale limite λ tale che $k = \aleph_\lambda$.

    La disuguaglianza $k \leq \aleph_k$ è un fatto già noto. Perciò c'è solo da dimostrare $\aleph_k \leq k$.

    Si ha $\aleph_k = \aleph_{\aleph_\lambda} = \bigcup_{\alpha<\lambda} \aleph_{\aleph_\alpha}$ e perciò $\lambda \geq cof\aleph_k = cof_k = k$ perché k è regolare. Dunque $k = \aleph_\lambda \geq \aleph_k$, da cui la tesi. □

15. (Difficile) Sia k un cardinale infinito e sia $\mathcal{F}$ una famiglia di funzioni $f\colon k^+ \to k^+$ strettamente crescenti e continue. Supponiamo che $|\mathcal{F}| \leq k$. Dimostrare che l'insieme dei punti fissi comuni $\mathcal{F}ix\mathcal{F} := \{\alpha \in k^+ \mid \forall f \in \mathcal{F}\ f(\alpha) = \alpha\}$ ha cardinalità k^+.

    Dim. Poiché k^+ è un cardinale regolare (in quanto successore), basta dimostrare che $\mathcal{F}ix\mathcal{F}$ è illimitato in k^+.

    L'osservazione che si sta per fare è la chiave della soluzione dell'esercizio: poiché $|\mathcal{F}| \leq k$, per ogni ordinale $\alpha \in k^+$ l'insieme $\{f_i(\alpha) \mid f_i \in \mathcal{F}\}$ ha cardinalità al più k e dunque è limitato in k^+ (sempre per un fatto di regolarità).

Con questo in mente, dato $\alpha \in k^+$, si definisce per ricorsione numerabile la successione

$$\begin{cases} a_0 = \alpha \\ a_{n+1} = min\{\beta \in k^+ \mid \forall f_i \in \mathcal{F}\ \beta > f_i(a_n)\} \end{cases}$$

Ora si pone $\lambda = \bigcup_{n\in\omega} a_n$ e si osserva che la successione degli a_n è strettamente crescente perché una funzione strettamente crescente f da un buon ordine in se stesso ha la proprietà $f(a) \geq a$ per ogni a. Dunque λ è un ordinale limite, in quanto unione di una famiglia di ordinali priva di massimo e perciò per ogni $f_i \in \mathcal{F}$ si ha $f_i(\lambda) = \bigcup_{n\in\omega} f_i(a_n)$.

Per come è definita la successione degli a_n è ora banale osservare che per ogni $f_i, f_j \in \mathcal{F}$ vale $f_i(\lambda) = f_j(\lambda)$, cioè che λ è un punto fisso comune per le f_i. Infatti vale banalmente $f_j(a_{n+2}) > f_i(a_{n+1}) > f_j(a_n)$. □

16. (Difficile) (*) Esiste una funzione strettamente crescente e continua $f\colon \aleph_{\omega_1} \to \aleph_{\omega_1}$ con esattamente $\aleph_1$ punti fissi?

17. (Normale) Dato un cardinale infinito k, si dimostri che l'insieme

$$\{A \subseteq k \mid |A| = k \wedge |k \setminus A| = k\}$$

ha cardinalità 2^k.

Dim. (Ludovico Battista) Si considera la funzione

$$\begin{aligned} \varphi\colon \mathcal{P}(k) &\to \mathcal{P}(k \times 3) \\ A &\mapsto (A \times \{0\}) \cup (k \times \{3\}) \end{aligned}$$

e si osserva che è banalmente iniettiva.

L'immagine di φ è contenuta nell'insieme dei sottoinsiemi di $k \times 3$ di cardinalità k e con complementare di cardinalità k. Dunque questo insieme ha cardinalità 2^k e da ciò segue la tesi. □

18. Questo esercizio e il successivo non sono stati tratti dalle prove d'esame degli anni passati, ma riguardano un fatto (facile da dimostrare) che mi è venuto in mente nella risoluzione di un esercizio durante il corso.

(Facile) Gli ordinali limite sono illimitati nei cardinali $k > \aleph_0$.

Dim. Se per assurdo esiste un cardinale k tale che gli ordinali limite sono limitati in k, allora si prende $\delta + 1$ il minimo dei maggioranti stretti per l'insieme degli ordinali limite in k ed è banale osservare che δ è un ordinale limite e in particolare il massimo ordinale limite in k. Ma allora $\delta + \omega$ è un ordinale limite in k (è l'ordinale limite successivo a δ) perché $|\delta + \omega| = |\delta| < |k|$ e inoltre vale $\delta + \omega > \delta$ (*Assurdo*).

Dunque gli ordinali limite sono illlimitati in k, e banalmente lo sono anche gli ordinali successori. □

Oss. È banale provare che gli ordinali successore sono illimitati in qualsiasi ordinale limite.

L'utilità della proprietà dimostrata sta nel fatto che, ogni volta che si ha un cardinale, la cardinalità degli ordinali limite più piccoli è maggiore o uguale alla sua cofinalità. Per esempio in $\aleph_{44}$ ci sono $\aleph_{44}$ ordinali limite e $\aleph_{44}$ ordinali successori.

Ora, se uno applicasse la proprietà appena dimostrata a un cardinale singolare, otterrebbe in realtà una stima pessima sul numero degli ordinali limite e successori minori di k. Infatti nel prossimo esercizio, che è una diretta conseguenza di quello appena svolto, si proverà che vale un fatto molto più forte, cioè che in ogni cardinale $k > \aleph_0$ ci sono k ordinali limite e k ordinali successori. Invece, applicando l'esercizio precedente a $\aleph_{\omega+\omega}$ si otterrebbe che in esso vi sono almeno $\aleph_0$ ordinali limite e almeno $\aleph_0$ ordinali successori.

19. (Facile) In ogni cardinale $k > \aleph_0$ vi sono k ordinali limite e k ordinali successori.

    Dim. Se k è un cardinale regolare allora la tesi è una banale conseguenza dell'esercizio precedente.

    Se k è un cardinale singolare, allora k è un cardinale limite e dunque esiste un ordinale limite λ tale che $k = \aleph_\lambda$. Dal fatto che gli ordinali successori sono illimitati negli ordinali limite (banale) e che i cardinali successori sono regolari, segue che per ogni $\alpha < \lambda$ in $\aleph_\lambda$ vi sono almeno $\aleph_\alpha$ ordinali limite, dunque ve ne sono almeno tanti quanti il *sup* degli $\aleph_\alpha$, cioè $\aleph_\lambda$, da cui la tesi. □

Gerarchia di Von Neumann e Assioma di fondazione

1. (Facile) Si dimostri che per ogni ordinale α vale $|V_{\omega+\alpha}| \geq \aleph_\alpha$.

   Dim. Dalla teoria si ha che per ogni ordinale α vale $|V_{\omega+\alpha}| = \beth_\alpha$.

   Poiché per ogni α si ha $\beth_\alpha \geq \aleph_\alpha$, la tesi è provata. □

2. Dati un cardinale infinito k e un ordinale α, si provi che sono fatti equivalenti:

   (a) $cof\alpha > k$;

   (b) ogni $X \subseteq V_\alpha$ di cardinalità $|X| \leq k$ appartiene a V_α.

3. Dimostrare che $|V_\alpha| = |\mathcal{P}(\alpha)|$ se e solo $\alpha = 4$ o $\alpha = \omega + 1$ o $\alpha = k + 1$ dove k è un punto fisso della "funzione" beth.

4. (a) Trovare il minimo ordinale β, se esiste, tale che ogni insieme x finito e transitivo appartiene a V_β.

   (b) Trovare il minimo ordinale γ, se esiste, tale che ogni insieme x numerabile e transitivo appartiene a V_γ.

5. Per quali ordinali α vale la proprietà: "per ogni funzione f, se $\mathcal{D}om\, f \in V_\alpha$ è numerabile e $\mathcal{I}m\, f \subseteq V_\alpha$, allora $f \in V_\alpha$"?.

6. Sia f una funzione. Dimostrare che se $f \in V_\alpha$, allora $\mathcal{D}om\, f, \mathcal{I}m\, f \in V_\alpha$. Sotto quali ipotesi su α vale l'implicazione inversa?

7. Assumendo l'Assioma di fondazione:

   - Stabilire se esistono insiemi non vuoti A e B tali che $A \times B \subsetneq B$.
   - Stabilire se esistono insiemi non vuoti A e B tali che $A \times B = B$.

Altri esercizi vari

1. (Facile) Potendo usare soltanto gli assiomi dell'insieme vuoto, della coppia e della potenza, si può costruire un insieme con 5 elementi?

   E potendo usare soltanto gli assiomi dell'insieme vuoto, della potenza e dell'unione?

   Sol. Nel primo caso si possono ottenere solo insiemi con 0, 1, 2 o una potenza di 2 elementi. Infatti l'insieme vuoto ha 0 elementi e con la coppia si ottengono insiemi di 1 elemento (singoletti) o 2 elementi. Applicando l'insieme delle parti a un insieme che ha * elementi, si ottiene un insieme che ha 2^* elementi. Ma 5 non rientra in queste categorie, dunque la risposta è negativa.

   Nel secondo caso la risposta è affermativa, infatti si riesce ad ottenere esattamente il naturale di Von Neumann 5, perché con la coppia e l'unione si ha l'unione binaria, e questo basta per avere il successore di un insieme (il singoletto si ottiene con l'assioma di coppia). □

2. (Facile) Stabilire quali delle seguenti proprietà sono vere:

   $(a)\ \bigcup \mathcal{P}(X) = X$ $\qquad$ $(b)\ X = \mathcal{P}(\mathcal{P}(\bigcup X))$

   $(c)\ X \in \mathcal{P}(\mathcal{P}(\bigcup X))$ $\qquad$ $(d)\ \mathcal{P}(\bigcup X) = \{\mathcal{P}(x) \mid x \in X\}$

Sol. La proprietà (a) è vera perché X è un sottoinsieme di X.

La proprietà (c) è vera perché i suoi elementi sono sottoinsiemi di $\bigcup X$.

La proprietà (b) è falsa perché, per esempio, esistono insiemi X tali che $X = \bigcup X$, come ω, dunque la proprietà fallisce per il Teorema di Cantor.

La proprietà (d) è falsa e anche in questo caso ω è un controesempio perché $\bigcup \omega = \omega$, ma ω ha sottoinsiemi infiniti, mentre l'insieme delle parti di un numero naturale è un insieme finito. □

3. (Facile) (*) Non esiste l'insieme di tutti e soli i singoletti.

   Sol. Se per assurdo esiste l'insieme di tutti e soli i singoletti, lo si denota A e si ottiene che $\bigcup A$ è l'insieme di tutti gli insiemi, che non esiste per il paradosso di Cantor. □

4. (Facile) Per ogni $A \neq \emptyset$ non esiste l'insieme $\{B \mid |B| = |A|\}$.

   Dim. Sia per assurdo $Y := \{B \mid |B| = |A|\}$ e sia $a \in A$ un elemento qualsiasi.

   Allora per ogni insieme $x \notin A$, l'insieme $(A \setminus \{a\}) \cup \{x\}$ ha la stessa cardinalità di A e dunque appartiene a Y. Ma allora $\bigcup Y$ sarebbe l'insieme di tutti gli insiemi, contro il paradosso di Cantor. □

5. Ogni funzione debolmente crescente da $\mathcal{P}(X)$ in $\mathcal{P}(X)$ ammette punti fissi.

6. (Difficile) Una famiglia X si dice *quasi disgiunta* se per ogni $A, A' \in X$ con $A \neq A'$ l'intersezione $A \cap A'$ è finita. Dimostrare che esiste una famiglia quasi disgiunta di sottoinsiemi di $\mathbb{N}$ avente la cardinalità del continuo.

7. (Normale) Ogni sottoinsieme bene ordinato A di $(\mathbb{R}, \leq)$ è al più numerabile.

   Dim. Sia $f : \omega \to \mathbb{Q}$ una bigezione.

   Indicando con a^+ il più piccolo elemento di A maggiore di a (il successore di a), si definisce

   $$\begin{aligned} \varphi : A &\to \mathbb{Q} \\ a &\mapsto f(min\{n \in \omega \mid a^+ > f(n) \geq a\}) \end{aligned}$$

   e si osserva che è iniettiva, da cui la tesi. □

8. (Facile) Calcolare la cardinalità dell'insieme

$$A := \{A \in \mathcal{P}(\mathbb{R}) \mid A \text{ è un buon ordine}\}$$

Sol. Per l'esercizio precedente si sa che ogni sottoinsieme bene ordinato di $\mathbb{R}$ è al più numerabile, dunque i sottoinsiemi di $\mathbb{R}$ bene ordinati sono al più quanti i suoi sottoinsiemi al più numerabili, cioè $2^{\aleph_0}$.

Inoltre l'ordinamento indotto da $\mathbb{R}$ su $\mathbb{N}$ è il solito ordinamento di $\mathbb{N}$ e con questo ordinamento $\mathbb{N}$ è un buon ordine. Dunque tutti i sottoinsiemi di $\mathbb{N}$ sono sottoinsiemi bene ordinati di $\mathbb{R}$ e questi sono proprio $2^{\aleph_0}$. □

9. (Facile) Calcolare la cardinalità dell'insieme

$$A := \{\alpha \text{ ordinale} \mid \alpha \text{ è il tipo d'ordine di un sottoinsieme } A \subseteq \mathbb{R}\}$$

Sol. Dagli esercizi precedenti si sa che un sottoinsieme bene ordinato di $\mathbb{R}$ ha cardinalità al più numerabile, dunque gli elementi di A sono sicuramente ordinali al più numerabili (e dunque A è davvero un insieme).

Inoltre dalla teoria si sa che ogni insieme totalmente ordinato numerabile è isomorfo a un sottoinsieme di $\mathbb{Q}$, e quindi anche di $\mathbb{R}$.

Si conclude che gli elementi di A sono tutti e soli gli ordinali al più numerabili, cioè $A = \omega_1$ e $|A| = \aleph_1$. □

10. (Difficile) Un insieme ordinato infinito $(A, \leq)$ si dice *separabile* se ha un sottoinsieme denso e numerabile. Dimostrare che se A è separabile, allora $|A| \leq \mathfrak{c}$.

11. (Difficile) Siano $A, B \subseteq \mathbb{R}^+$ due sottoinsiemi non vuoti di numeri reali positivi. Dimostrare che se A e B sono bene ordinati (con l'ordinamento indotto da $\mathbb{R}$), allora anche l'insieme somma $A + B := \{a + b \mid a \in A, b \in B\}$ è bene ordinato.

12. (Facile) (*) Se A è un insieme infinito, allora $|\mathcal{F}in\, A| = |\mathcal{S}eq\, A| = |A|$.

Bibliografia

[1] Karel Hrbacek, Thomas Jech (1999), *Introduction to Set Theory*

[2] Morris Kline (1999), *Storia del pensiero matematico II.* Dal Settecento a oggi

[3] https://plato.stanford.edu/entries/continuum-hypothesis/