Elementi di Teoria degli Insiemi, 2010-11

Alessandro Berarducci

Versione del 20 Maggio 2011. Ancora in corso d'opera

Queste note sono imperfette ed ancora in corso d'opera. Possono essere lette come complemento al testo di K. Hrbackek e T. Jech, Introduction to Set Theory, Macell Dekker, Inc. 1999. Il contenuto del corso corrisponde grosso modo ai primi 10 capitoli dello Hrbacek-Jech più i capitoli 14 e 15. Per la forma normale di Cantor degli ordinali e per le somme infinite di cardinali si veda lo Hrbacek-Jech.

Indice

1 I numeri naturali

1.1 Il principio di induzione

Le proprietà fondamentali dell'insieme $\mathbb{N}$ dei numeri naturali sono le seguenti.

1.1 Definizione (Assiomi di Peano)**.** $\mathbb{N}$ è dotato di un elemento $0 \in \mathbb{N}$ (zero) e di una funzione $S\colon \mathbb{N} \to \mathbb{N}$ (successore) tali che:

1. Due numeri diversi non possono avere lo stesso successore. In altre parole la funzione successore $S\colon \mathbb{N} \to \mathbb{N}$ è iniettiva. Questo può essere espresso in simboli nel modo seguente:
$$\forall x, y(S(x) = S(y) \to x = y),$$
dove x, y variano su elementi di $\mathbb{N}$.
2. 0 non è il successore di alcun numero. In simboli:
$$\forall x(S(x) \neq 0);$$
3. Vale il seguente principio di induzione. Sia P è una proprietà sui numeri naturali. Supponiamo che valga $P(0)$ (base dell'induzione), e supponiamo che per ogni $x \in \mathbb{N}$ se vale $P(x)$ vale anche $P(S(x))$ (passo induttivo). Allora P vale per tutti i numeri naturali.

Dato $x \in \mathbb{N}$, il suo successore $S(x)$ viene anche indicato $x + 1$.

In base al principio di induzione per dimostrare che una proprietà P vale per tutti i numeri naturali, basta quindi dimostrare che P vale per 0 (caso base) e "passa al successore" (passo induttivo) nel senso che se vale per un certo numero naturale x (ipotesi induttiva) allora vale anche per $S(x)$.

Il seguente esercizio mostra che ogni numero naturale diverso da zero ha un predecessore.

1.2 Esercizio. Per ogni $x \in \mathbb{N}$ con $x \neq 0$ esiste y con $S(y) = x$. Tale y è unico e viene chiamato un predecessore di x.

Dimostrazione. Sia $P(x)$ il predicato "x o è zero o esiste un predecessore di x". Dimostriamo per induzione che ogni numero naturale x verifica P. Chiaramente vale $P(0)$ (base). Il passo induttivo $P(u) \to P(S(u))$ è immediato in quanto un predecessore di $S(u)$ è u stesso (non abbiamo neppure bisogno di sfruttare l'ipotesi induttiva). Quindi per induzione vale $P(x)$ per ogni x. □

Oltre ad uno zero e un successore, i numeri naturali hanno anche una struttura d'ordine. L'idea è che $x < y$ se y si può ottenere da x applicando "un certo numero di volte" la funzione successore. Diamo la definizione precisa:

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

ordine

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

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

Dimostrazione. Esercizio. □

successore

1.5 Lemma. *Per ogni $x \in \mathbb{N}$ abbiamo:*

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

Dimostrazione. Esercizio. □

principio-del-minimo

1.6 Lemma. *Vale il* **principio del minimo***: ogni insieme non vuoto di numeri naturali ha un minimo elemento (rispetto all'ordine $\leq$ sopra definito).*

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

1.2 Definizioni ricorsive

Assumerò nel seguito il seguente principio.

1.7. Definizioni per induzione. È possibile definire una funzione f sui numeri naturali dando il valore di $f(0)$ e dando una regola H che permette di determinare $f(n+1)$ conoscendo n ed $f(n)$. Più formalmente, data una funzione $H\colon \mathbb{N}\times A \to A$ ed un elemento $a \in A$, esiste una ed una sola funzione $f\colon \mathbb{N} \to A$ tale che $f(0) = a$ ed $f(n+1) = H(n, f(n))$. Più in generale si può ammettere che $f(n+1)$ dipenda dall'intera successione $(f(i) : i \leq n)$ dei valori precedenti. In questo caso la definizione prende la forma $f(n) = H(n, (f(i) : i < n))$ dove H è una funzione data (in questo caso il secondo argomento di H è una successione di elementi di A).

La giustificazione (e generalizzazione) di questo principio nel quadro della teoria di Zermelo-Fraenkel è dato dal teorema di ricursione (Teorema 4.37) che si applica non solo ai numeri naturali ma a qualsiasi insieme "bene ordinato", ossia un insieme per cui valga il "principio del minimo".

1.8 Esempio. Possiamo definire per induzione sul secondo argomento la somma di numeri naturali nel modo seguente $x+0 = x$, $x+S(y) = S(x+y)$. Avendo definito la somma possiamo definire il prodotto per induzione sul secondo argomento nel modo seguente $x \cdot 0 = 0, x \cdot S(y) = x \cdot y + x$. Analogamente avendo il prodotto possiamo definire per induzione l'esponenziale: $x^0 = 1, x^{n+1} = x^n \cdot x$.

1.9 Esempio. La funzione fattoriale è definita per ricursione da $!0 = 1, !(n+1) = (n+1)!n$.

1.10 Esercizio. La successione di Fibonacci è definita da $F(0) = F(1) = 1$, $F(n+2) = F(n+1)+F(n)$. Si mostri che la definizione di F si può far rientrare nello schema $F(n) = H(n, (F(i) : i < n))$ scegliendo opportunamente H.

2 Teoria degli insiemi di Cantor

2.1 Equipotenza tra insiemi

2.1 Definizione. Diciamo che due insiemi X ed Y sono equipotenti se esiste una corrispondenza biunivoca tra di essi.

pari

2.2 Esempio. L'insieme dei numeri naturali $\mathbb{N}$ è equipotente al sottoinsieme dei numeri pari.

Dimostrazione. Una corrispondenza biunivoca è data dalla funzione che ad ogni numero naturale associa il suo doppio. □

Tramite un processo di astrazione associamo ad ogni insieme X un'entità $|X|$ chiamata la cardinalità di X in modo tale che X è equipotente ad Y se e solo se $|X| = |Y|$, ovvero se e solo se X ed Y hanno la stessa cardinalità. Queste entità sono chiamate numeri cardinali. Ad esempio, supponendo che a, b, c siano oggetti distinti, possiamo considerare il numero 3 come la cardinalità dell'insieme $\{a, b, c\}$.

Chi abbia familiarità con le classi di equivalenza può pensare ad $|X|$ come la classe di equivalenza di tutti gli insiemi equipotenti ad X. Un'altra possibilià, dovuta a von Neumann, è quella di definire X come un particolare rappresentante, scelto in modo opportuno, della classe di equivalenza di X. Questa seconda possibilià ha il vantaggio di poter essere sviluppata all'interno della teoria assiomatica degli insiemi di Zermelo Fraenkel. Per il momento non è importante approfondire l'argomento in quanto per i primi risultati parlare di cardinalità sarà solo un modo indiretto di parlare di corrispondenze biunivoche.

2.2 Insiemi numerabili

2.3 Definizione. Un insieme è **numerabile** se può essere messo in corrispondenza biunivoca con l'insieme $\mathbb{N}$ dei numeri naturali. La cardinalità degli insiemi numerabili viene indicata con il simbolo $\aleph_0$ (aleph-zero).

Contrariamente a quanto accade per gli insiemi finiti, un insieme infinito può essere messo in corrispondenza con una parte propria di se stesso. Ad esempio abbiamo:

2.4 Proposizione.
1. *L'insieme* $\mathbb{N}$ *ha la stessa cardinalità di* $\mathbb{N}\setminus\{0\}$.
2. *Se aggiungiamo un elemento* a *ad un insieme numerabile* X *otteniamo ancora un insieme numerabile. In simboli:* $\aleph_0 + 1 = \aleph_0$.

Dimostrazione. (1) Mandiamo n in $n + 1$.

(2) Mettiamo in corrispondenza biunivoca l'insieme numerabile X con $\mathbb{N}\setminus\{0\}$, e al nuovo elemento a associamo il numero 0. □

Questi esempi possono essere illustrati nel modo seguente. L'albergo di Hilbert ha infinite stanze, una per ogni numero naturale. L'albergo è pieno

ma arriva un nuovo cliente. Possiamo trovargli posto? Un modo per farlo è di spostare ogni cliente nella stanza successiva (quello della stanza n nella stanza $n+1$) e mettere il nuovo arrivato nella stanza zero.

2.5 Proposizione. *L'unione di due insiemi numerabili disgiunti A e B è numerabile. In simboli:* $\aleph_0 + \aleph_0 = \aleph_0$.

Dimostrazione. I pari e i dispari sono sottoinsiemi numerabili di $\mathbb{N}$. Possiamo mettere A in corrispondenza con i pari e B con i dispari. In tal modo abbiamo stabilito una corrispondenza biunivoca tra $\mathbb{N}$ e l'unione di A e B. □

2.6 Esempio. L'insieme dei numeri interi $\mathbb{Z}$ è numerabile.

Dimostrazione. $\mathbb{Z}$ è l'unione degli interi negativi e di quelli non negativi, entrambi numerabili. □

2.7 Proposizione. *Il prodotto cartesiano $A \times B$ di due insiemi numerabili è numerabile. In simboli:* $\aleph_0 \cdot \aleph_0 = \aleph_0$.

Dimostrazione. Basta mostrare che $\mathbb{N} \times \mathbb{N}$ è numerabile in quanto se A è equipotente a $\mathbb{N}$ e B è equipotente ad $\mathbb{N}$, allora $A \times B$ è equipotente ad $\mathbb{N} \times \mathbb{N}$.

Dobbiamo quindi mostrare che esiste una funzione biunivoca $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Dato $(x, y) \in \mathbb{N} \times \mathbb{N}$ con $n = x + y$, esistono $n(n+1)/2$ coppie $(u, v) \in \mathbb{N} \times \mathbb{N}$ con $u + v < n$ ed altre x coppie (u, v) con $u + v = n$ ed $u < x$. Ne segue che la funzione f che manda $(x, y) \in \mathbb{N} \times \mathbb{N}$ in $(x+y)(x+y+1)/2 + x$ è biunivoca (esercizio).

Alternativamente si può usare la funzione che manda (x, y) in $2^x(2y+1)-1$. Tale funzione è biunivoca in quanto ogni numero naturale diverso da zero si scrive in modo unico come potenza di due per un numero dispari. Il "-1" nella formula serve per includere lo zero. □

2.8 Definizione. Sia X un insieme ed n un numero naturale. Diciamo che X ha n elementi se X è equipotente all'insieme dei numeri naturali $< n$ (serve il minore stretto perché si parte da zero). Diciamo che X è un insieme **finito** se esiste $n \in \mathbb{N}$ tale che X ha n elementi. Diciamo che X è **infinito** se non è finito.

2.9 Esercizio. Un sottoinsieme di un insieme finito è finito.

2.10 Teorema. *Un qualsiasi sottoinsieme A di $\mathbb{N}$ è finito o è numerabile. Più in generale un sottoinsieme di un insieme numerabile o è finito o è numerabile.*

Dimostrazione. La dimostrazione formale è posposta a quando avremo introdotto le definizioni induttive. L'idea è comunque quella di enumerare gli elementi A in modo crescente $a_0 < a_1 < \ldots < a_n < \ldots$. Se A è infinito è sempre possible proseguire e otteniamo una corrispondenza biunivoca $n \mapsto a_n$ da $\mathbb{N}$ ad A. □

2.11 Teorema. *Sia $f\colon \mathbb{N} \to X$ una funzione surgettiva. Allora X è finito o numerabile.*

Dimostrazione. Dato un elemento x di X, sia $n_x \in \mathbb{N}$ il minimo numero naturale tale che $f(n_x) = x$. La funzione $x \mapsto n_x$ manda iniettivamente X in un sottoinsieme di $\mathbb{N}$. Quindi X è finito o numerabile. □

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

Dimostrazione. (Prima dimostrazione) Dato un razionale $x \in \mathbb{Q}$ scegliamo $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ tale che $x = m/n$. In tale modo abbiamo stabilito una corrispondenza biunivoca tra $\mathbb{Q}$ e un sottoinsieme infinito di $\mathbb{Z} \times \mathbb{Z}$. Ora usiamo il fatto che un sottoinsieme infinito di un insieme numerabile è numerabile.

(Seconda dimostrazione) Sappiamo che $\mathbb{Z} \times \mathbb{Z}$ è numerabile. Ora basta considerare la funzione surgettiva $g\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}$ che manda (n, m) in n/m se $m \neq 0$ e manda (n, m) in un arbitrario elemento di $\mathbb{Q}$ se $m = 0$. □

2.3 Non numerabilità dei reali.

Indichiamo con $\mathbb{R}$ l'insieme dei numeri reali. Per il seguente risultato presupponiamo la conoscenza del fatto che ogni numero reale si può scrivere in notazione decimale usando infinite cifre dopo la virgola.

2.13 Teorema. $\mathbb{R}$ *non è numerabile.*

Dimostrazione. Sia $(a_n : n \in \mathbb{N})$ una successione numerabile di numeri reali $a_n \in \mathbb{R}$. Basta far vedere che, comunque si sia scelta la successione, l'insieme degli a_n non può esaurire tutto $\mathbb{R}$, ovvero che esiste almeno un numero reale $b \in \mathbb{R}$ che non compare tra gli a_n. A tal fine basta scegliere un b tale che, per ogni n, la n-esima cifra decimale di b differisce da quella di a_n (ad esempio scelgo un b nell'intervallo $(0, 1)$ tale che la n-esima cifra di b è 4 se quella di a_n è diversa da 4, ed è 5 se quella di a_n è 4). Tale b differisce da ciascun a_n per almeno una cifra, e quindi non compare nella successione. □

2.4 Relazione d'ordine tra cardinali

2.14 Definizione. Definiamo $|X| \leq |Y|$ se X è equipotente ad un sottoinsieme di Y, o equivalentemente se esiste una funzione iniettiva da X ad Y. Definiamo $|X| < |Y|$ se sono verificate simultaneamente due condizioni: innanzitutto X è equipotente ad un sottoinsieme di Y, e in secondo luogo X non è equipotente ad Y.

Dunque sapendo solamente che X è in corrispondenza biunivoca con un sottoinsieme di Y, anche se il sottoinsieme fosse proprio potremmo solo concluderne che vale la disuguaglianza debole $|X| \leq |Y|$ (ad esempio i numeri pari sono un sottoinsieme proprio dei numeri naturali ma hanno la stessa cardinalità. Per ottenere la disuguaglianza stretta $|X| < |Y|$ abbiamo bisogno dell'ulteriore informazione che, anche cambiando la corrispondenza, non potremmo in ogni caso ottenerne una biunivoca.

2.15 Proposizione. $|\,\mathbb{N}\,| < |\,\mathbb{R}\,|$.

Dimostrazione. Ovviamente $|\mathbb{N}| \leq |\mathbb{R}|$ in quanto $\mathbb{N}$ è incluso in $\mathbb{R}$, e avendo dimostrato che $\mathbb{R}$ non è numerabile deve valere la disuguaglianza stretta. □

2.16 Definizione. Indichiamo con **c** la cardinalità di $\mathbb{R}$. Diciamo che un insieme X ha la cardinalità del **continuo** se $|X| = \mathbf{c}$, ovvero se esiste una corrispondenza biunivoca tra X e $\mathbb{R}$.

2.5 Somma di numeri cardinali

2.17 Osservazione. Dati due insiemi A e B, esistono due insiemi disgiunti A', B' tali che $|A'| = |A|$ e $|B'| = |B|$.

Dimostrazione. Basta prendere $A' = A \times \{0\}$ (l'insieme delle coppie ordinate della forma $(a, 0)$ al variare di a in A) e $B' = B \times \{1\}$ (l'insieme delle coppie $(b, 1)$ con b in B). □

2.18 Definizione. Dati due numeri cardinali κ e λ, definiamo il cardinale $\kappa+\lambda$ nel modo seguente. Prendiamo un insieme A di cardinalià κ e un insieme B di cardinalità λ e disgiunto da A. Allora per definizione $\kappa + \lambda = |A \cup B|$.

Si può dimostrare che la definizione è ben posta, ovvero che il risultato $\kappa + \lambda$ non dipende da come si scelgono gli insiemi disgiunti A, B. Lasciamo la facile verifica al lettore e facciamo invece vedere che non è in generale possibile definire la sottrazione tra cardinali. Supponendo $\kappa \geq \lambda$, come potremmo definire $\kappa - \lambda$? Saremmo tentati di dire: prendiamo un insieme X di cardinalità κ, e un sottoisieme $Y \subseteq X$ di cardinalità λ, e definiamo $\kappa - \lambda$ come la cardinalità della differenza insiemistica $X \setminus Y$ (l'insieme degli elementi di X che non stanno in Y). Però se tentiamo di calcolare $\aleph_0 - \aleph_0$ otteniamo il risultato 0 se prendiamo $X = Y = \mathbb{N}$, e il risultato $\aleph_0$ se prendiamo $X = \mathbb{N}$ e $Y =$ l'insieme dei numeri pari. Quindi la sottrazione non è in generale ben definita (sebbene, come vedremo, questi problemi non sorgono se vale la disuguaglianza stretta $\kappa > \lambda$).

2.19 Osservazione. $\kappa \leq \lambda$ se e solo per qualche cardinale μ, $\lambda = \kappa + \mu$.

2.20 Teorema. *Indichiamo con* 0 *la cardinalità dell'insieme vuoto, e con* 1 *la cardinalità di un insieme con un solo elemento. Per numeri cardinali valgono le seguenti leggi.*

1. $\kappa + \lambda = \lambda + \kappa$.
2. $\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$.
3. $\kappa + 0 = \kappa$.
4. *Se* $\kappa \neq 0$, *allora per qualche* λ, $\kappa = \lambda + 1$.
5. *Se* $\kappa + 1 = \lambda + 1$, *allora* $\kappa = \lambda$.

2.6 Prodotto di numeri cardinali

Ricordiamo che il prodotto cartesiano $A \times B$ di due insiemi A, B è l'insieme di tutte le coppie ordinate (a, b) con $a \in A$ e $b \in B$.

2.21 Definizione. Siano $\alpha = |A|$ e $\beta = |B|$. Definiamo $\alpha \cdot \beta = |A \times B|$. (Scriveremo anche $\alpha\beta$ invece di $\alpha \cdot \beta$.)

2.22 Teorema. *Per il prodotto di numeri cardinali valgono le seguenti leggi (la cui dimostrazione è lasciata al lettore).*

1. $\kappa\lambda = \lambda\kappa$.
2. $\kappa(\lambda\mu) = \kappa\lambda + \kappa\mu$.
3. $\kappa(\lambda + \mu) = \kappa\lambda + \kappa\mu$.
4. $\kappa \cdot 0 = 0$
5. $\kappa \cdot 1 = \kappa$.
6. $\kappa \cdot 2 = \kappa + \kappa$ (2 *indica la cardinalità di un insieme con due elementi).*

2.7 L'insieme delle parti

2.23 Definizione. Sia X un insieme e sia $\mathcal{P}(X)$ l'insieme delle parti (sottoinsiemi) di X.

2.24 Esercizio. Se X è un insieme finito di n elementi, allora $\mathcal{P}(X)$ ha 2^n elementi.

cantor

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

Dimostrazione. Supponiamo di avere associato ad ogni elemento $x \in X$ un sottoinsieme A_x di X. Basta mostrare che la famiglia degli A_x non esaurisce tutte le parti di X. Consideriamo l'insieme $D = \{x \in X : x \notin A_x\}$. Se D appartenesse alla famiglia $\{A_x : x \in X\}$ ci sarebbe un $u \in X$ tale che $D = A_u$. Ma $u \in D$ se e solo se $u \notin A_u$. Assurdo. □

2.8 Esponenziazione di cardinali

2.26 Definizione. Siano $\alpha = |A|$ e $\beta = |B|$. Definiamo $\alpha^\beta = |A^B|$, dove $A^B = \{f \mid f\colon B \to A\}$.

2.27 Teorema.
1. $(\kappa^\lambda)^\mu = \kappa^{\lambda\mu}$.
2. $\kappa^{\lambda+\mu} = \kappa^\lambda \kappa^\mu$.
3. $(\kappa\lambda)^\mu = \kappa^\mu \lambda^\mu$.

2.28 Teorema. *Se $|A| = \kappa$, allora $|\mathcal{P}(A)| = 2^\kappa$.*

Dimostrazione. Per definizione 2^κ è la cardinalità dell'insieme delle funzioni f da A a $\{0,1\}$. Tale insieme è in corrispondenza biunivoca con $\mathcal{P}(A)$. Basta associare ad ogni f il sottoinsieme degli x in A tali che $f(x) = 1$. □

2.29 Teorema. *Per qualsiasi cardinale κ si ha $\kappa < 2^\kappa$.*

Dimostrazione. $\kappa < |P(\kappa)| = 2^\kappa$. □

In particolare non esiste un cardinale più grande di tutti.

2.9 Il teorema di Cantor - Bernstein

Il seguente esempio presuppone la conoscenza di $\mathbb{R}$.

2.30 Esempio. Dati due numeri reali $a < b$, esiste una corrispondenza biunivoca tra l'intervallo aperto (a, b) e l'intervallo chiuso $[a, b]$.

Dimostrazione. Supponiamo per semplicità $a = -1, b = 1$. Ovviamente esiste una funzione iniettiva da $(-1, 1)$ verso $[-1, 1]$ (l'inclusione) e una funzione iniettiva nel verso opposto, ad esempio quella che manda x in $x/2$. Per trovare una funzione biunivoca $f\colon [-1, 1] \to (-1, 1)$ definiamo $f(x) = x/2$ se x è della forma $\pm 1/2^n$ per qualche $n \in \mathbb{N}$, e $f(x) = x$ altrimenti. □

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

Dimostrazione. Siano $f\colon A \to B$ e $g\colon B \to A$ funzioni iniettive. Vogliamo dimostrare che $|A| = |B|$. Sia $B' \subseteq A$ l'immagine della funzione g. Chiaramente $|B| = |B'|$. Basta quindi dimostrare $|A| = |B'|$. Questo è chiaro se $A = B'$. Nel caso contrario troveremo una corrispondenza biunivoca tra A e B' facendo scorrere certi punti lungo certe successioni. A tal fine sia $h\colon A \to B'$ la composizione $g \circ f$. Consideriamo un punto qualsiasi $x \in A \setminus B'$ e sia $O(x)$ l'orbita di x tramite h, ovvero l'insieme degli elementi della successione $x, h(x), h(h(x)), h(h(h(x))), \ldots$ il cui $n+1$-esimo termine $h^{n+1}(x)$ si ottiene per ricursione applicando h all'n-esimo termine $h^n(x)$. Equivalentemente possiamo definire $O(x)$ come l'intersezione di tutti i sottoinsiemi di A che contengono x e sono chiusi per h. Osserviamo che tutti i punti di $O(x)$ tranne x stesso appartengono ad B'. In base alle definizioni se $z \in O(x)$ anche $h(z) \in O(x)$. Viceversa dall'iniettività di h otteniamo facilmente che se $h(z) \in O(x)$, allora $z \in O(x)$. (Dimostrazione: $h(z)$ non può essere x in quanto $x \in A \setminus B'$ e l'immagine di h è contenuta in B'. Quindi $h(z) = h^{n+1}(x)$ per qualche n e dall'iniettività di h segue che $z = h^n(x)$.) Ne segue che se parto da un altro punto $y \in A \setminus B'$, gli insiemi $O(y)$ e $O(x)$ sono disgiunti. Possiamo allora definire una funzione biunivoca $T\colon A \to B'$ ponendo $T(a) = h(a)$ se $a \in O(x)$ per qualche $x \in A \setminus B'$ (necessariamente unico), e $T(a) = a$ negli altri casi. Tale T è la bigezione richiesta (verificare!). □

Usando il teorema di Cantor-Bernstein si dimostra:

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

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

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

2.34 Esercizio. Qualunque intervallo aperto (a, b) non vuoto di $\mathbb{R}$ ha la stessa cardinalità di $\mathbb{R}$ (proiezione stereografica).

2.10 Il continuo è equipotente alle parti degli interi

2.35 Fatto. *Il campo $\mathbb{R}$ dei numeri reali verifica, oltre agli assiomi dei campi ordinati, le seguenti proprietà.*

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

Dall'assioma di Archimede otteniamo:

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

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

Dall'assioma di continuità otteniamo:

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

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

Mettendo insieme le due disuguaglianze otteniamo:

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

2.39 Osservazione. Assumendo l'esistenza di un campo ordinato $\mathbb{R}$ verificante gli assiomi di continuità e di Archimede, abbiamo visto che la funzione g da $\mathbb{R}$ ad $\mathcal{P}(\mathbb{Q})$ che associa $x \in \mathbb{R}$ a $\{q \in \mathbb{Q} : q < x\}$ è iniettiva. L'immagine di g è costituita dall'insieme dei "tagli di Dedekind" di $\mathbb{Q}$ definiti come segue. Diciamo che un sottoinsieme X di $\mathbb{Q}$ è un taglio di Dedekind se verifica le seguenti proprietà: i) ogniqualvolta X contiene un dato razionale contiene anche tutti quelli minori di lui; (ii) X è limitato superiormente in $\mathbb{Q}$; (iii) X non ha un massimo. Questa osservazione consente di definire $\mathbb{R}$ a partire da $\mathbb{Q}$ nel modo seguente. Visto che vogliamo che $\mathbb{Q}$ sia incluso in $\mathbb{R}$, resta solo da definire l'insieme $\mathbb{R} \setminus \mathbb{Q}$ dei numeri "irrazionali". A tal fine possiamo semplicemente identificare $\mathbb{R} \setminus \mathbb{Q}$ con l'insieme dei tagli di Dedekind di $\mathbb{Q}$ privi di un estremo superiore in $\mathbb{Q}$. Lasciamo al lettore l'esercizio di definire le operazioni di campo e l'ordine di $\mathbb{R}$ in base a questa definizione.

sommaomega

2.40 Lemma. *Sia* $\aleph_0 \leq |X|$. *Allora* $|X| + \aleph_0 = |X|$.

Dimostrazione. Poiché $\aleph_0 \leq |X|$ possiamo scriviamo X come unione disgiunta $A \cup N$ con N numerabile. Chiaramente $|X| = |A| + \aleph_0$. Ne segue che $|X| + \aleph_0 = |A| + \aleph_0 + \aleph_0 = |A| + \aleph_0 = |X|$. □

2.41 Teorema. *L'insieme dei numeri irrazionali ha cardinalià* **c**.

Dimostrazione. Sia $X = \mathbb{R} \setminus \mathbb{Q}$ l'insieme dei numeri irrazionali. Osserviamo che l'insieme numerabile $\{\sqrt{2} + q : q \in \mathbb{Q}\}$ è incluso in X, quindi $\aleph_0 \leq |X|$. Per il Lemma 2.40 $|\mathbb{R}| = |X| + \aleph_0 = |X|$. □

In modo analogo si dimostra:

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

2.11 Paradossi

2.43 Corollario (Paradosso di Cantor)**.** *Non esiste un insieme universale, ovvero un insieme* V *tale che* $x \in V$ *per qualsiasi* x.

Dimostrazione. Supponiamo per assurdo che V esista. Essendo V un insieme universale, ogni parte di V appartiene a V. In altre parole $\mathcal{P}(V)$ è un sottoinsieme di V, e quindi $|\mathcal{P}(V)| \leq |V|$, contraddicendo il teorema di Cantor (Teorema 2.25). □

2.44 Definizione. Data una proprietà P, e un insieme X, scriviamo $X = \{x \mid P(x)\}$ se per ogni u abbiamo $u \in X \leftrightarrow P(u)$, ovvero X è l'insieme degli elementi che verificano P. Diciamo in questo caso che l'insieme X è l'estensione della proprietà P.

Il seguente paradosso mostra che non è possibile assumere che ogni proprietà abbia una estensione.

2.45 Teorema (Paradosso di Russell)**.** *Non esiste un insieme R tale che $R = \{x \mid x \notin x\}$.*

Dimostrazione. Se $R = \{x \mid x \notin x\}$, allora $R \in R$ se e solo se $R \notin R$. Assurdo. □

3 Assiomi di Zermelo-Fraenkel

I paradossi della teoria intuitiva degli insiemi possono essere evitati rifondando la teoria su basi assiomatiche. Nello scrivere gli assiomi useremo i simboli logici $\forall, \exists, \wedge, \vee, \neg, \to, \leftrightarrow, =$, le variabili, e il simbolo di appartenenza $\in$ (l'unico simbolo "non logico" della teoria). Per quanto riguarda il significato e l'uso di questi simboli, assumeremo una certa familiarità con le regole per manipolare i connettivi, l'uguaglianza, e i quantificatori $\forall, \exists$. In particolare diamo per note le tavole di verità dei connettivi booleani $\wedge, \vee, \neg, \to, \leftrightarrow$. Per il simbolo $\in$ va invece fatto un discorso a parte. Il simbolo $\in$ rappresenta una relazione binaria tra oggetti che chiamiamo insiemi. Se vale $x \in y$ diciamo che l'elemento x appartiene all'insieme y. Tutte le variabili variano su "insiemi", e gli elementi di un insieme sono essi stessi insiemi. Non assumiamo alcuna proprieà dell'appartenenza $\in$ se non quelle che verranno esplicitate dagli assiomi. Nello scrivere alcuni degli assiomi (comprensione e rimpiazzamento) faremo uso della nozione semi-formale di "proprietà". Le proprietà che ci interessano sono quelle che possono essere espresse da formule ben formate che usano esclusivamente i simboli $\forall, \exists, \wedge, \vee, \neg, \to, \leftrightarrow, =, \in$ e le variabili. Possiamo quindi sostanzialmente identificare le proprietà con le formule di questo linguaggio.

3.1 Primi assiomi

3.1. Assioma di estensionalità.

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

L'assioma dice che se due insiemi x, y contengono gli stessi elementi allora sono uguali.

3.2 Esempio. L'assioma di estensionalità ci dice in particolare che un numero di telefono non può essere considerato un insieme di cifre. Ad esempio 223 e 323 sono due numeri di telefono distinti sebbene in essi compaiano le stesse cifre.

Le variabili libere presenti negli assiomi vanno considerate implicitamente quantificate universalemente. Formalmente l'assioma di estensionalità dovrebbe quindi essere formulato premettendo davanti alla formula i quantificatori $\forall x \forall y$.

3.3 Definizione. Assumiamo il **principio di Leibniz**: se $x = y$ allora ogni proprietà P verificata da x è anche verificata da y.

Fissando z e prendendo come $P(u)$ la proprietà $z \in u$, dal principio di Leibniz deduciamo che se $x = y$ allora $z \in x \leftrightarrow z \in y$. Poiché z è arbitrario otteniamo

$x = y \to \forall z(z \in x \leftrightarrow z \in y)$. Ne segue che nell'assioma di estensionalità vale in effetti la doppia implicazione

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

3.4 Definizione. Definiamo l'inclusione $x \subseteq y$ tra due insiemi x, y nel modo seguente:

$$x \subseteq y \iff \forall z(z \in x \to z \in y).$$

Se $x \subseteq y$ diremo che x è un sottoinsieme di y. L'assioma di estensionalià equivale a: $x \subseteq y \wedge y \subseteq x \leftrightarrow x = y$.

3.5. Schema di assiomi di separazione Data una formula $\varphi(t)$ abbiamo il seguente assioma:

$$\forall a \exists y \forall t(t \in y \leftrightarrow t \in a \wedge \varphi(t))$$

Lo schema di separazione consiste di infiniti assiomi, uno per ogni scelta della formula $\varphi(t)$. Fissata $\varphi(t)$, l'assioma dice che, dato un insieme A, esiste un insieme y i cui elementi sono gli elementi t di A che verificano la proprietà $\varphi(t)$. Tale y è unico per l'assioma di estensionalità e viene indicato con la notazione

$$y = \{t \in A \mid \varphi(t)\}.$$

.

Osserviamo che lo schema di separazione ci permette di creare solamente sottoinsiemi di un insieme A già dato.

3.6. Assioma dell'insieme vuoto.

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

Se x verifica $\forall y(y \notin x)$ diciamo che x è vuoto. L'assioma dice che esiste un insieme vuoto. Per l'assioma di estensionalità ci può essere un solo insieme vuoto, che denoteremo con $\emptyset$. (Per dimostrare l'unicità osserviamo che se u, v fossero entrambi vuoti, allora per ogni t gli enunciati $t \in u$ e $t \in v$ sarebbero entrambi falsi, e poiché un enunciato falso implica qualsiasi altro enunciato, la doppia implicazione $t \in u \iff t \in v$ sarebbe sempre vera, da cui per l'estensionalità $u = v$.)

1.4

3.7 Teorema. *(Inesistenza dell'insieme di tutti gli insiemi) Non esiste un insieme V tale che $\forall x(x \in V)$.*

Dimostrazione. Dato un insieme A, definiamo $R = \{t \in A \mid t \notin t\}$. In base alle defizioni $R \in R$ se e solo se $R \in A$ e $R \notin R$. Ne segue che $R \notin A$ (altrimenti avremmo l'assurdo $R \in R \leftrightarrow R \notin R$). Quindi A non è un insieme universale. Visto che A era arbitrario ne concludiamo che non esiste un insieme universale. □

3.8 Osservazione. Nello schema di separazione la formula $\varphi(t)$ può contenere variabili libere diverse da t che svolgono il ruolo di parametri e sono da considerarsi implicitamente quantificate universalmente nel corrispondente assioma di separazione. Ad esempio se $\varphi(t,u)$ è una formula con due variabili libere t ed u l'assioma prende la forma $\forall u, x \exists y \forall t(t \in y \leftrightarrow t \in x \wedge \varphi(t,u))$ ed asserisce l'esistenza dell'insieme $y = \{t \in x \mid \varphi(t,u)\}$ (dipendente da x e da u).

3.9. Assioma della coppia.

$$\forall x, y \exists z \forall w(w \in z \leftrightarrow w = x \vee w = y)$$

Fissati x, y, l'assioma asserisce l'esistenza dell'insieme $z = \{w \mid w = x \vee w = y\}$ (unico per l'assioma di estensionalità). Per indicarlo usiamo la notazione

$$z = \{x, y\}.$$

3.10 Esercizio. $\{x, y\} = \{y, x\}$.

3.11 Definizione.

$$\{x\} = \{x, x\}$$

L'insieme $\{x\}$ viene chiamato singoletto di x, e contiene solamente x come elemento.

3.12. Assioma dell'unione.

$$\forall x \exists y \forall z(z \in y \leftrightarrow \exists t(z \in t \wedge t \in x))$$

Fissato x l'assioma asserisce l'esistenza dell'insieme $y = \{z \mid \exists t(z \in t \wedge t \in x)\}$ (unico per l'estensionalità). Per indicarlo usiamo la notazione:

$$y = \bigcup_{t \in x} t$$

che si legge: y è l'unione di tutti gli insiemi t che appartengono ad x. Un'altra notazione talvolta usata per lo stesso insieme è $y = \bigcup x$..

Un caso particolare dell'unione à l'usuale unione binaria:

3.13 Definizione. (Unione binaria)

$$\begin{array}{rcl} A \cup B & = & \bigcup_{t \in \{A,B\}} t \\ & = & \{z \mid z \in A \vee z \in B\} \end{array}$$

3.14 Definizione. (triple, quadruple, etc.) Usando l'assioma della coppia e l'unione binaria possiamo definire

$$\begin{array}{l} \{a,b,c\} = \{a,b\} \cup \{c\}, \\ \{a,b,c,d\} = \{a,b,c\} \cup \{d\} \\ \text{etc.} \end{array}$$

Per l'intersezione non abbiamo bisogno di un assioma apposito: basta l'assioma di separazione.

3.15 Definizione. (Intersezione binaria) Dati due insiemi A, B definiamo la loro intersezione:

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

Il fatto che $\{x \mid x \in A \wedge x \in B\}$ sia un insieme segue dall'assioma di separazione e dal fatto che possiamo riscriverlo nella forma $\{x \in A \mid x \in A \wedge x \in B\}$.

Analogamente possiamo definire l'intersezione di una famiglia non vuota di insiemi:

intersezione

3.16 Definizione. (Intersezione di una famiglia non vuota di insiemi) Dato un insieme non vuoto F (che pensiamo come famiglia di insiemi) la classe $\{t \mid \forall X \in F(t \in X)\}$ è un insieme per l'assioma di separazione (Dimostrazione: preso un qualsiasi $A \in F$ tale classe è inclusa nell'insieme A e pertanto è un insieme). Per indicarla introduciamo la notazione

$$\bigcap_{X \in F} X = \{t \mid \forall X \in F(t \in X)\}$$

Analizzando la dimostrazione si vede facilmente che non c'è bisogno che F sia un insieme, può anche essere una classe (l'intersezione sarà in ogni caso un insieme).

3.17. Assioma dell'insieme potenza.

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

Fissato x l'insieme y di cui si asserisce l'esistenza è unico per l'assioma di estensionalità e viene chiamato l'insieme delle parti di x. Per denotarlo usiamo la notazione

$$y = \mathcal{P}(x) = \{z \mid z \subseteq x\}.$$

3.18. Assioma dell'infinito.

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

Se definiamo $0 = \emptyset$ e definiamo il successore di y come $y \cup \{y\}$ vediamo che l'assioma dell'infinito asserisce l'esistenza di un insieme x che contiene 0 ed è chiuso per successore. x deve dunque contenere gli insiemi definiti come segue:

$$\begin{aligned} &0 = \emptyset \\ &1 = 0 \cup \{0\} = \{0\} \\ &2 = 1 \cup \{1\} = \{0, 1\} \\ &3 = 2 \cup \{2\} = \{0, 1, 2\} \\ &\text{etc.} \end{aligned}$$

Si noti che l'assioma dell'infinito non dice che esistono infiniti insiemi (l'assioma dell'insieme vuoto, della coppia e dell'unione già ci permette di definire ciascuno degli insiemi $0, 1, 2, 3 \ldots$), ma che esiste un singolo insieme x che contiene infiniti elementi.

3.19 Definizione. L'insieme $\mathbb{N}$ dei numeri naturali è definito come l'intersezione della classe di tutti gli insiemi che contengono 0 e sono chiusi per successore:

$$\mathbb{N} = \bigcap_{X \in F} X$$

dove

$$F = \{x \mid \emptyset \in x \wedge \forall y(y \in x \to y \cup \{y\} \in x)\}.$$

La classe F è non vuota per l'assioma dell'infinito, e quindi ha senso farne l'intersezione (vedi Definizione 3.16).

Con questa definizione dei numeri naturali in termini insiemistici è immediato verificare il:

3.20. Principio di induzione: se un insieme x contiene 0 ed è chiuso per successore, allora x contiene tutti i numeri naturali (cioè tutti gli elementi di $\mathbb{N}$).

3.2 Rimpiazzamento

3.21. Schema di assiomi di rimpiazzamento. Data una formula $\phi(x, y)$ abbiamo il seguente assioma: se per ogni x esiste un unico y tale che $\phi(x, y)$, allora, indicando con $F(x)$ tale y, si ha che per ogni insieme A esiste un insieme B i cui elementi sono tutti e soli gli $F(a)$ al variare di a in A. L' insieme B viene indicato con la notazione $\{F(x) \mid x \in A\}$, o equivalentemente con la notazione $\{y \mid \exists x \in A\phi(x, y)\}$, e la proprietà che lo caratterizza è espressa dall'equivalenza

$$x \in \{F(a) \mid a \in A\} \leftrightarrow \exists a \in A(x = F(a))$$

o equivalentemente:

$$x \in B \leftrightarrow (\exists a \in A)\phi(a, x)$$

Analogamente al caso degli assiomi di separazione, anche nello schema di rimpiazzamento la formula ϕ può dipendere da altre variabili che svolgono il ruolo di parametri.

3.3 Prodotto cartesiano, relazioni, funzioni

La proprietà fondamentale delle coppie ordinate è la seguente.

$(x, y) = (z, w)$ se e solo se $x = z$ e $y = w$.

3.22 Teorema. *(Coppia di Kuratowski) Definendo* $(x, y) = \{\{x\}, \{x, y\}\}$ *risulta verificata la proprietà fondamentale delle coppie ordinate. (Sono possibili altre definizioni.)*

Dimostrazione. Esercizio. □

3.23 Teorema. *Dati due insiemi A, B esiste l'insieme $A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$, ovvero l'insieme i cui elementi sono tutte le coppie ordinate (a,b) con $a \in A$ e $b \in B$.*

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

3.24 Esercizio. Si dia una dimostrazione che non usa l'assioma di rimpiazzamento ma usa l'assioma potenza.

Per familiarizzarci con le notazioni osserviamo che $A \times B = \{x \mid (\exists a \in A)(\exists b \in B)(x = (a,b))\}$.

3.25 Definizione. Diciamo che R è una relazione binaria se R è un insieme di coppie ordinate. Diciamo che R è una relazione tra A e B se R è un sottoinsieme di $A \times B$. Scriviamo $R(a,b)$, oppure aRb, se vale $(a,b) \in R$.

3.26 Definizione. Diciamo che f è una funzione se f è un insieme i cui elementi sono coppie ordinate e tale che $(x,y) \in f \wedge (x,z) \in f \to y = z$. Se f è una funzione scriviamo $f(x) = y$ se e solo se $(x,y) \in f$ (diciamo in tal caso che f manda x in y).

3.27 Definizione. Il dominio di una funzione f è definito da

$$\mathrm{dom}(f) = \{a \mid \exists b((a,b) \in f)\}$$

e l'immagine di f è definita da

$$\mathrm{im}(f) = \{b \mid \exists a((a,b) \in f)\}.$$

Un'altra notazione per l'immagine è

$$\mathrm{im}(f) = \{f(a) \mid a \in \mathrm{dom}(f)\}.$$

3.28 Esercizio. Il dominio e l'immagine di una funzione sono insiemi (non occorre l'assioma di rimpiazzamento).

3.29 Definizione. $f\colon A \to B$ significa che f è una funzione il cui dominio è A e la cui immagine $\mathrm{im}(f)$ è inclusa in B. Se $\mathrm{im}(f) = B$ diciamo che $f\colon A \to B$ è surgettiva. Se per ogni $x, y \in A$ si ha $f(x) = f(y) \to x = y$ diciamo che f è iniettiva. Se $f\colon A \to B$ è sia iniettiva che surgettiva diciamo che è biunivoca. In tale caso diciamo anche che f è una corrispondenza biunivoca tra A e B.

3.4 Assioma della scelta

3.30 Definizione. Nella pratica matematica si incontrano le notazioni $\{a_i \mid i \in I\}$ e $(a_i \mid i \in I)$. Con $(a_i \mid i \in I)$ indichiamo la funzione a con dominio I che manda i in $a_i = a(i)$. Con $\{a_i \mid i \in I\}$ indichiamo invece l'immagine di tale funzione. La funzione $(a_i \mid i \in I)$ viene talvolta chiamata famiglia indiciata. Se $A = \{a_i \mid i \in I\}$ dove gli a_i sono insiemi, l'unione $\bigcup_{x \in A} x$ viene scritta più comunemente come $\bigcup_{i \in I} a_i$.

indiciata

3.31 Osservazione. Ogni insieme A può essere scritto nella forma $\{a_i \mid i \in I\}$.

Dimostrazione. $A = \{i \mid i \in A\}$, quindi basta prendere $I = A$ e $a_i = i$. □

3.32. Assioma di scelta. Data una famiglia $F = \{A_i \mid i \in I\}$ di insiemi non vuoti A_i (per $i \in I$), esiste una funzione f, detta funzione di scelta, che associa ad ogni $i \in I$ un elemento $f(i)$ di A_i.

3.33. Assioma di scelta (forma equivalente). Sia F un insieme di insiemi non vuoti. Esiste allora una funzione f con dominio F e tale che $\forall A \in dom(f), f(A) \in A$.

Indichiamo con la sigla AC l'assioma della scelta. L'equivalenza tra le due formulazioni di AC dipende dall'Osservazione 3.31. La forza dell'assioma della scelta sta nel garantire l'esistenza di funzioni che potrebbero non essere definibili tramite una regola esplicita.

3.34 Esempio. In base all'assioma della scelta esiste una funzione f che dato un insieme non vuoto $X \subseteq \mathbb{R}$ di numeri reali restituisce un elemento $f(X)$ dell'insieme X. Sapreste trovare esplicitamente una tale f? (Se pensate di esserci riusciti penso proprio che vi siate sbagliati.) Osserviamo che se invece di sottoinsiemi di $\mathbb{R}$ consideriamo sottoinsiemi di $\mathbb{N}$ l'esistenza di una tale f è dimostrabile senza assioma della scelta: dato $X \subseteq \mathbb{N}$ non vuoto, basta prendere la funzione definita da $f(X) = \min X$.

3.35 Definizione (Prodotto cartesiano infinito)**.** Data una famiglia indiciata $(A_i \mid i \in I)$ di insiemi A_i, definiamo $\Pi_{i\in I} A_i = \{a \colon I \to \bigcup_{i\in I} A_i \mid (\forall i \in I) a(i) \in A_i\}$.

In altre parole l'insieme $\Pi_{i\in I} A_i$ ha come elementi le funzioni $a = (a_i \mid i \in I)$ con $a_i = a(i) \in I$.

3.36 Osservazione. L'assioma della scelta equivale all'affermazione che il prodotto cartesiano $\Pi_{i\in I} A_i$ di una famiglia $(A_i \mid i \in I)$ di insieme non vuoti è non vuoto.

3.37 Osservazione. In base alle regole della logica se nel corso di una dimostrazione assumiamo la verità di una formula della forma $\exists x P(x)$, è lecito continuare la dimostrazione supponendo di poter "scegliere" un a tale che $P(a)$. Questa forma di ragionamento non presuppone l'assioma della scelta, ma fa parte delle regole della logica sottostante.

3.38 Esempio. Supponendo che A e B siano insiemi non vuoti, possiamo dimostrare che $A \times B$ è non vuoto nel modo seguente. Poiché A, B non sono vuoti abbiamo per definizione $\exists x(x \in A)$ e $\exists y(y \in B)$. Scegliamo un a tale che $a \in A$ e un b tale che $b \in B$ (non si richiede l'assioma di scelta!). Allora $(a, b) \in A \times B$. Dunque $A \times B$ è non vuoto.

3.5 Prime conseguenze dell'assioma della scelta

Il seguente teorema richiede l'assioma della scelta (AC), ed è in effetti equivalente ad esso.

surgettiva

3.39 Teorema. *(AC) Se esiste una funzione surgettiva $f\colon B \to A$, allora esiste una iniettiva $g\colon A \to B$.*

Dimostrazione. Per definire g si "sceglie" (usando AC) per ogni $a \in A$ un $b \in B$ tale che $f(b) = a$ (b esiste per la surgettività di f) e si pone $g(a) = b$. □

In base al teorema per dimostrare $|A| \leq |B|$ basta trovare una funzione surgettiva da B ad A.

3.40 Esercizio. Senza AC si dimostri che se esiste una funzione iniettiva $g : A \to B$, allora ne esiste una surgettiva $g : B \to A$.

Nella sua piena generalità il seguente risultato richiede AC.

3.41 Teorema. *L'unione di una famiglia numerabile $\{A_n \mid n \in \mathbb{N}\}$ di insiemi numerabili A_n è numerabile.*

Dimostrazione. Per ipotesi per ogni n esiste una corrispondenza biunivoca g da $\mathbb{N}$ ad A_n. In base ad AC esiste una funzione $(g_n \mid n \in \mathbb{N})$ che sceglie una tale $g = g_n$ in funzione di n. Definiamo $f\colon \mathbb{N} \times \mathbb{N} \to \bigcup_n A_n$ ponendo $f(n, m) = g_n(m)$. Allora f è surgettiva (è biunivoca se gli A_n sono disgiunti). Siccome $|\,\mathbb{N} \times \mathbb{N}\,| = \aleph_0$ ne segue che $\bigcup_n A_n$ è numerabile. □

3.42 Esercizio. Analogamente si dimostra che se $|J| \leq \aleph_0$ e $|A_j| \leq \aleph_0$ per ogni $j \in J$, allora $|\bigcup_{j\in J} A_j| \leq \aleph_0$.

In casi concreti AC non è necessario, come ad esempio nel seguente esercizio:

3.43 Esercizio. L'insieme $\mathbb{Q}[x]$ dei polinomi a coefficienti razionali è numerabile.

Siccome ogni polinomio non zero ha un numero finito di radici, ne segue che l'insieme dei numeri algebrici è numerabile.

scelte-finite

3.44 Esercizio. Se $F = \{A_i \mid i < n\}$ ha un numero finito $n \in \mathbb{N}$ di elementi (dove ammettiamo che gli A_i possano essere infiniti), l'esistenza di una funzione f tale che $f(A_i) \in A_i$ (per ogni $i \in I$) può essere dimostrata senza l'assioma della scelta.

Dimostrazione. Dimostriamo il teorema per induzione su n.

Per $n = 0$ non c'è nulla da dimostrare (F è vuoto, e per f prendiamo la funzione vuota).

Per $n = 1$ la famiglia F ha come unico elemento un insieme non vuoto A. Abbiamo quindi $\exists x(x \in A)$. Sia a un tale x (non è necessario l'assioma di scelta per "scegliere" un tale x). Come f prendiamo allora la funzione che manda A in a.

Il passo induttivo da n ad $n+1$ si dimostra come segue. Sia $F = \{A_i \mid i < n+1\}$ e supponiamo per ipotesi induttiva che $\exists f : \forall i < n, f(A_i) \in A_i$. Fissiamo una tale f. Siccome A_{n+1} è non vuoto abbiamo $\exists x(x \in A_{n+1})$. Sia $a \in A$ un tale x. Definiamo f' come la funzione che si comporta come la f su $\{A_i \mid i < n\}$ e manda A_{n+1} in a. Tale f' testimonia $\exists f : \forall i < n+1, f(A_i) \in A_i$. □

3.6 Insiemi e classi proprie

In certe formulazioni della teoria degli insiemi esistono due tipi di entità, gli insiemi, e le classi. Data una proprietà $\phi(x)$, esiste sempre la classe $\{x \mid \phi(x)\}$ (dove x varia tra gli insiemi). Ogni insieme x è una classe (in quanto $x = \{y \mid y \in x\}$) ma solo certe classi sono insiemi. Una classe è un insieme se e solo se è un elemento di un'altra classe. Le classi che non sono insiemi vengono chiamate classi proprie. Ad esempio per il Teorema 3.7 la classe $\{t \mid t = t\}$ non è un insieme (dove t varia tra gli insiemi). Per noi le classi sono solo un modo indiretto di parlare di proprietà (o di formule) secondo le abbreviazioni seguenti:

3.45 Definizione. (Classe definita da una proprietà)

"$y \in \{t \mid \phi(t)\}$" significa "$\phi(y)$"
"$y = \{t \mid \phi(t)\}$" significa "$\forall t(t \in y \leftrightarrow \phi(t))$"
"$\{t \mid \phi_1(t)\} = \{t \mid \phi_2(t)\}$" significa "$\forall t(\phi_1(t) \leftrightarrow \phi_2(t))$"
"$\{t \mid \phi_1(t)\} \subseteq \{t \mid \phi_2(t)\}$" significa "$\forall t(\phi_1(t) \to \phi_2(t))$"
"$\{t \mid \phi(t)\}$ è un insieme" significa "$\exists y(y = \{t \mid \phi(t)\}$"

Usando il linguaggio delle classi lo schema di assiomi di separazione dice che una classe della forma $\{t \mid t \in x \wedge \phi(t)\}$ è sempre un insieme. Detto in altri termini: se una classe $\{t \mid \phi(t)\}$ è inclusa in un insieme x allora è essa stessa un insieme.

Io schema di rimpiazzamento dice che se F è una funzione-classe ed A è un insieme, allora la classe $\{F(x) \mid x \in A\}$ è un insieme. In altre parole l'immagine di una funzione-classe ristretta ad un insieme è un insieme.

4 Buoni ordini

4.1 Relazioni d'ordine

4.1 Definizione. Un ordine parziale è un insieme A dotato di una relazione binaria $\leq$ che gode della proprietà riflessiva $x \leq x$, transitiva $x \leq y \wedge y \leq z \to x \leq z$, e antisimmetrica $x \leq y \wedge y \leq x \to x = y$. Un ordine totale è un ordine parziale tale che per ogni x, y si ha $x \leq y \vee y \leq x$.

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

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

Osserviamo che

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

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

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

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

4.2 Esempio. Un esempio di ordine parziale è l'insieme dei sottoinsiemi di $\mathbb{N}$ ordinato per inclusione. Un esempio di ordine totale è dato dai numeri reali con l'usuale ordinamento.

4.2 Insiemi bene ordinati

4.3 Definizione. Una relazione binaria R su un insieme A si dice ben fondata se ogni sottoinsieme non vuoto X di A ha un elemento $a \in X$ tale che non esiste alcun $x \in A$ con xRa. Tale a si dice un elemento R-minimale di X.

Si noti che in generale può esistere più di un elemento R-minimale di X, ma se R è un ordine totale ne esiste al massimo uno (il minimo di X, se esiste).

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

In altre parole un buon ordine è un ordine totale $(A, \leq)$ tale che la relazione di ordine stretto associata a $\leq$ è ben fondata (in tal caso chiameremo indifferentemente buon ordine sia $(A, \leq)$ che $(A, <)$).

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

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

4.3 Somma e prodotto di buoni ordini

4.6 Definizione. Dati due ordini totali $(A, \leq_A)$ e $(B, \leq_B)$ definiamo un nuovo ordine totale $(A + B, \leq) = (A, \leq_A) + (B, \leq_B)$ come segue. Il dominio $A + B$ è

definito come $A \times \{0\} \cup B \times \{1\}$. L'ordine su $A + B$ è definito stabilendo che $(a, 0) < (b, 1)$ per ogni $a \in A$ e $b \in B$, mentre per coppie con la stessa seconda componente si segue l'ordine delle prime componenti rispetto agli ordini $\leq_A$ e $\leq_B$ (cioè $(a, 0) < (a', 0)$ se $a <_A a'$ e $(b, 1) < (b', 1)$ se $b <_B b'$).

4.7 Lemma. *Se $(A, \leq_A)$ e $(B, \leq_B)$ sono buoni ordini, anche $(A + B, \leq)$ lo è.*

Dimostrazione. Dato un sottoinsieme non vuoto X di $A+B = A\times\{0\}\cup B\times\{1\}$, consideriamo l'insieme $A' = \{a \in A \mid (a, 0) \in X\}$. Nel caso in cui A' è non vuoto, il minimo di X è $(a, 0)$, dove a è il minimo di A' (che esiste dato che $(A, <_A)$ è un buon ordine). Se invece A' è vuoto, allora chiaramente non è vuoto l'insieme $B' = \{b \in B \mid (b, 1) \in X\}$. Il minimo di X è in tal caso $(b, 1)$ dove b è il minimo di B'. □

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

4.9 Esercizio. Si verifica che se $(A, \leq_A)$ e $(B, \leq_B)$ sono buoni ordini, anche $(A \times B, \leq)$ lo è.

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

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

In $(\mathbb{N}, \leq) \times (\mathbb{N}, \leq)$ vi sono infiniti elementi limite.

4.4 Isomorfismi di buoni ordini

I prossimi risultati mostrano che i buoni ordinamenti sono "rigidi", ovvero che vi sono pochi isomorfismi.

4.12 Definizione. Dati due insiemi ordinati $(A, \leq_A)$ e $(B, \leq_B)$ una funzione $f\colon A \to B$ si dice crescente se $x < y$ implica $fx < fy$ per ogni $x, y \in A$. Se f è anche biunivoca diremo che f è un isomorfismo (si verifica in tal caso che l'inversa è anch'essa crescente).

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

crescente

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

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

Il precedente lemma non si estende a ordini totali arbitrari, ad esempio la funzione $f\colon x \mapsto x^2$ è una funzione crescente dall'intervallo reale $[0, 1]$ a se stesso, ma $f(1/2) = 1/4 < 1/2$.

4.15 Corollario. *Il solo isomorfismo di un buon ordine $(W, \leq)$ in se stesso è l'identità.*

Dimostrazione. Per il lemma $f(x) \geq x$ e $f^{-1}(x) \geq x$ per ogni $x \in W$. Quindi $x = f^{-1}fx \geq fx \geq x$, da cui $x = fx$. □

unico-iso

4.16 Corollario. *Se due buoni ordini sono isomorfi, l'isomorfismo tra loro è unico.*

Dimostrazione. Se vi fossero due isomorfismi f, g da un insieme bene ordinato $(A, \leq_A)$ ad un insieme bene ordinato $(B, \leq_B)$, applicando prima f e poi l'inversa di g si otterrebbe un isomorfismo da $(A, \leq_A)$ in se stesso diversa dall'identità. □

rigidita-ord

4.17 Lemma. *Un insieme bene ordinato non è mai isomorfo ad un suo segmento iniziale proprio.*

Dimostrazione. Se f è un tale isomorfismo e $\mathrm{im}(f) = \{x \mid x < u\}$, allora $fu < u$ contraddicendo il fatto che: f crescente $\Rightarrow f(x) \geq x$ per ogni $x \in W$. □

4.18 Osservazione. Un insieme bene ordinato può essere isomorfo ad un suo sottoinsieme proprio con l'ordine indotto: ad esempio $\mathbb{N}$ con l'usuale ordine è isomorfo al sottoinsieme dei numeri pari.

unicita-forte

4.19 Corollario. *Se f è un isomorfismo da un buon ordine $(A, \leq_A)$ a un segmento iniziale di $(B, \leq_B)$, e g è anch'esso un isomorfismo da un buon ordine $(A, \leq_A)$ ad un segmento iniziale di $(B, \leq_B)$ (possibilmente diverso), allora $f = g$.*

Dimostrazione. Osserviamo innanzitutto $\mathrm{im}(f)$ e $\mathrm{im}(g)$ sono due segmenti iniziali di $(B, \leq_B)$ isomorfi (essendo entrambi isomorfi ad $(A, \leq_A)$). Quindi per il Lemma 4.17 $\mathrm{im}(f) = \mathrm{im}(g)$. Quindi f, g sono isomorfismi con lo stesso dominio e la stessa immagine, e per il Corollario 4.16 $f = g$. □

4.5 Confrontabilità dei buoni ordini

4.20 Teorema. *Dati due buoni ordini $(A, \leq_A)$ e $(B, \leq_B)$, uno dei due è isomorfo ad un segmento iniziale dell'altro (non necessariamente proprio).*

Dimostrazione. Dati $a \in A$ e $b \in B$, diciamo che a corrisponde a b se l'insieme bene ordinato degli elementi di A minori o uguali a a (rispetto all'ordine $\leq_A$) è isomorfo all'insieme bene ordinato degli elementi di B minori o uguali a b. Si noti che ciascun $a \in A$ può corrispondere al massimo ad un $b \in B$, ovvero non ci possono essere $b_1 <_B b_2$ entrambi corrispondenti ad a (altrimenti avremmo due segmenti iniziali di B isomorfi l'uno all'altro, il che è impossibile per un buon ordine). Similmente ciascun $b \in B$ può corrispondere al massimo ad un $a \in A$. Inoltre se $a' <_A a$ ed a corrisponde a b, allora ovviamente a' corrisponde a qualche $b' <_B b$ (ottenuto restringendo l'isomorfismo). Scriviamo aRb se a corrisponde a b. Abbiamo così definito una relazione funzionale $R \subset A \times B$ il cui dominio $\mathrm{dom}(R) = \{a \in A : (\exists b \in B)(aRb)\}$ è un segmento iniziale di A e la cui immagine $\mathrm{img}(R) = \{b \in B : (\exists a \in B)(aRb)\}$ è un segmento iniziale di B. Per concludere basta dimostrare che $\mathrm{dom}(R) = A$ oppure $\mathrm{img}(R) = B$. Infatti nel primo caso R definisce un isomorfismo da A ad un segmento iniziale di B e nel secondo caso l'inversa di R definisce un isomorfismo da B ad un segmento iniziale di A. Se il teorema fosse falso, ci sarebbe un $a \in A$ che non corrisponde ad alcun $b \in B$ ed un $b \in B$ che non corrisponde ad alcun $a \in A$. Prendiamo a, b minimi (nei rispettivi ordini) con tale proprietà. Consideriamo ora la funzione $f\colon \{x \in A : x \leq_A a\} \to \{y \in B : y \leq_B b\}$ definita come segue: $f(a) = b$ e per $x <_A a$ poniamo $f(x) = y$ se e solo se x corrisponde ad y. Si noti che un tale y deve esistere per la minimalità di a, e deve essere $<_B b$ (perché se un elemento maggiore di b corrisponde a qualche elemento di a, anche b deve corrispondere a qualche elemento di A). È immediato verificare che f così definita è un isomorfismo tra $\{x \in A : x \leq_A a\}$ e $\{y \in B : y \leq_B b\}$. Ma allora per come abbiamo definito la corrispondenza a dovrebbe corrispondere a b, contraddicendo il modo in cui a, b sono stati scelti. □

confrontabili

4.21 Corollario. *Dati due buoni ordini $(A, \leq_A)$ e $(B, \leq_B)$, vale una ed una sola delle seguenti alternative: (i) $(A, \leq_A)$ è isomorfo ad un segmento iniziale proprio di $(B, \leq_B)$; (ii) $(B, \leq_B)$ è isomorfo ad un segmento iniziale proprio di $(A, \leq_A)$; (iii) $(A, \leq_A)$ è isomorfo a $(B, \leq_B)$.*

4.22 Definizione. Se valessero contemporaneamente due delle alternative, componendo gli isomorfismi violeremmo il teorema che stabilisce che un buon ordine non è mai isomorfo ad un suo segmento iniziale proprio.

4.23 Teorema. *Sia $(A, <)$ un buon ordine e sia X un sottoinsieme di A. Allora X, con l'ordine indotto da $(A, <)$, è isomorfo ad un segmento iniziale di $(A, <)$.*

Dimostrazione. In caso contrario, per la confrontabilità dei buoni ordini, esiste un isomorfimo f da $(A, <)$ ad un segmento iniziale proprio di X, ovvero una funzione crescente $f : A \to A$ la cui immagine è un segmento iniziale proprio di X. In particolare esiste $b \in X$ tale che tutti i valori di f sono $< b$. Quindi in particolare $f(b) < b$, contraddicendo il Lemma 4.14. □

4.6 Tipi d'ordine

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

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

4.25 Definizione. Definiamo la somma e il prodotto di tipi d'ordine nel modo seguente. Se α è il tipo di $(A, \leq_A)$ e β quello di $(B, \leq_B)$, allora definiamo $\alpha + \beta$ come il tipo di $(A, \leq_A) + (B, \leq_B)$ e $\alpha \cdot \beta$ come il tipo di $(A, \leq_A) \times (B, \leq_B)$ secondo le definizioni precedentemente date.

4.26 Definizione. Con riferimento al Corollario 4.21, scrivendo α per il tipo d'ordine di $(A, \leq_A)$ e β per il tipo d'ordine di $(B, \leq_B)$, nel caso (i) diciamo che $\alpha < \beta$, nel caso (ii) che $\alpha = \beta$, e nel caso (iii) che $\beta < \alpha$.

4.7 Unione di buoni ordini

Sia F una famiglia di buoni ordini, ovvero un insieme i cui elementi sono buoni ordini. Ci chiediamo in quali casi esista un buon ordine $(X, \leq)$ tale che tutti i buoni ordini di F siano segmenti iniziali di $(X, \leq)$. Chiaramente una condizione necessaria affinchè ciò avvenga è la seguente:

> (*) Dati due buoni ordini $(A, \leq_A)$ e $(B, \leq_B)$ in F uno dei due è un segmento iniziale dell'altro.

Con ciò intendiamo che o A è un segmento iniziale di $(B, \leq_B)$ e $\leq_A$ è la restrizione di $\leq_B$ ad A, oppure che B è un segmento iniziale di $(B, \leq_B)$ e $\leq_A$ è la restrizione di $\leq_B$ ad A

unione-bo

4.27 Teorema. *Supponiamo che la famiglia F di buoni ordini verifichi la condizione (*). Allora esiste un buon ordine $(X, \leq)$ tale che ogni buon ordine appartenente ad F è un segmento iniziale di $(X, \leq)$.*

Dimostrazione. Definiamo

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

cioè $x \in X$ se e solo se esiste $(A, \leq_A) \in F$ con $x \in A$. Ora definiamo la relazione $\leq$ su X ponendo

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

cioè $x \leq y$ se e solo se esiste $(A, \leq_A) \in F$ tale che $x, y \in A$ e $x \leq_A y$.

Dobbiamo verificare che $(X, \leq)$ è un buon ordine. Cominciamo con il dimostrare che è un ordine totale. Osserviamo che dati $(A, \leq_A)$ e $(B, \leq_B)$ in F, e due punti x, y appartenenti sia ad A che a B, si ha in base alla (*):

$$x \leq_A y \iff x \leq_B y. \tag{3}$$

Questo ci dice che nella definizione dell'ordine $x \leq y$ di X non importa quale $(A, \leq_A)$ si prende per confrontare x, y: se esiste un $(A, \leq_A)$ con $x \leq_A y$, allora ciò avviene in tutti gli $(A, \leq_A)$ che contengono x, y. Quindi in definitiva, preso un qualunque $(A, \leq_A) \in F$ con $x, y \in A$ abbiamo:

$$x \leq_A y \iff x \leq y \tag{4}$$

Cioè $\leq_A$ coincide con la restrizione di $\leq$ ad A.

Per dimostrare la proprietà transitiva $x \leq y \wedge y \leq z \to x \leq z$ osserviamo che, poiché la famiglia costituita dagli insiemi A con $(A, <_A) \in F$ è totalmente ordinata per inclusione, per ogni sottoinsieme finito $\{x_1, \ldots, x_k\}$ di X esiste un $(A, \leq_A) \in F$ con $\{x_1, \ldots, x_k\} \subseteq A$. Ciò si può facilmente verificare per induzione su k, ma a noi serve solo il caso $k \leq 3$ che si ottiene come segue: x_1, x_2, x_3 apparterranno rispettivamente a certi A_1, A_2, A_3, e prendendo il più grande degli A_i (che esiste perché gli A_i sono totalmente ordinati per inclusione) si ottiene l'A desiderato. Ciò stabilito, fissati $x, y, z \in X$ per i quali vogliamo verificare la proprietà transitiva $x \leq y \wedge y \leq z \to x \leq z$, scegliamo $(A, \leq_A) \in F$ tale che $x, y, z \in A$ e concludiamo usando la transitività di $\leq_A$ e la (4).

Similmente si dimostrano le altre altre proprietà nella definizione di ordine totale.

Mostriamo ora che ogni $(A, \leq_A)$ è un segmento iniziale di $(X, \leq)$. Siano dunque $a \in A$, $b \in X$ tali che $b \leq a$. Dobbiamo mostrare che $b \in A$. A priori sappiamo che $b \in B$ per qualche $(B, \leq_B) \in F$. Se $B \subseteq A$ abbiamo finito. Nel caso contrario per la (*) abbiamo che A è un segmento iniziale di $(B, \leq_B)$ ed essendo b un elemento di B minore di $a \in A$ ne concludiamo di nuovo che $b \in A$.

Mostiamo infine che $(X, \leq)$ è un buon ordine. Dato un sottoinsieme non vuoto Y di X dobbiamo mostrare che Y ha un minimo in $(X, \leq)$. Sicuramente esiste $(A, \leq_A) \in F$ tale che $Y \cap A \neq \emptyset$. Sia a il minimo di $Y \cap A$ nel buon ordine $(A, \leq_A)$. Dico che a è il minimo di Y in $(X, \leq)$. Supponiamo per assurdo che esista un $b \in Y$ con $b < a$. Essendo $(A, \leq_A)$ un segmento iniziale di $(X, \leq)$ gli elementi di X minori di a appartengono ad A, quindi in particolare $b \in A$. Ne segue che $b \in Y \cap A$. Ciò è assurdo perché $b < a$ ed a era il minimo di $Y \cap A$. □

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

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

4.8 Lemma di Zorn

Sia $\{A_i \mid i \in I\}$ una famiglia di insiemi. Ricordiamo che per l'assioma della scelta (AC) esiste una funzione f, detta funzione di scelta, che associa ad ogni $i \in I$ un elemento $f(i)$ di A_i.

Diamo il seguente lemma preparatorio al Lemma di Zorn.

LZorn

4.30 Lemma. *(Usando AC) Sia $(A, \leq)$ un ordine parziale. Allora esiste almeno una catena M di $(A, \leq)$ senza maggioranti stretti (ovvero maggioranti che non siano in M).*

Dimostrazione. Sia $\mathcal{F}$ la famiglia delle catene di A che hanno un maggiorante stretto. Usando l'assioma di scelta, esiste una funzione da $\mathcal{F}$ ad A che associa ad ogni catena $X \in \mathcal{F}$ uno dei suoi maggiornanti stretti $a_X \in A$. Possiamo ora definire una funzione f da catene a catene come segue. Se la catena X ha un maggiorante stretto $f(X) = X \cup \{a_X\}$, altrimenti $f(X) = X$.

Diamo ora una definizione. Diciamo che una catena B di $(A, \leq)$ è una f-catena se per ogni segmento iniziale proprio X di B la catena $f(X)$ continua ad essere un segmento iniziale di B. Osserviamo che se B è una f-catena anche $f(B)$ lo è (usando il fatto che i segmenti iniziali di $f(B)$ sono B stesso e i segmenti iniziali di B).

Per dimostrare il lemma prenderemo come M l'unione di tutte le f-catene. Occorrono però alcune verifiche. Dimostriamo innanzitutto che se B e C sono due f-catene, allora una delle due è un segmento iniziale dell'altra. A tal fine consideriamo l'unione D di tutti segmenti iniziali comuni di B e C. Tale D è evidentemente il più grande segmento iniziale comune a B e C. Se D fosse contenuto propriamente sia in B che C, allora da un lato D sarebbe contenuto propriamente in $f(D)$ (in quanto D avrebbe un maggiorante stretto) e dall'altro $f(D)$ sarebbe anch'esso un segmento iniziale sia di B che di C (per le proprietà delle f-catene). Questo contraddice però il fatto che D era il più grande di tali segmenti. Ne seque che D coincide con B o con C, ovvero B è un segmento iniziale di C o viceversa.

Sia ora $M \subseteq A$ l'unione di tutte le f-catene. Facciamo vedere che M è anch'essa una f-catena. Innanzitutto è chiaramente una catena in quanto unione di catene a due a due una contenuta nell'altra. Inoltre visto che le f-catene di cui M è unione sono a due a due una segmento iniziale dell'altra, ne segue (verificate!) che ciascuna di esse è un segmento iniziale di M. Per mostrare che M è una f-catena sia X un segmento iniziale proprio di M e mostriamo che $f(X)$ è un segmento iniziale di M. Consideriamo a tal fine un elemento a di M che non appartiene ad X. Tale a dovrà ovviamente appartenere ad una delle f-catene B di cui M è unione. Indicando con $\subseteq_i$ la relazione di inclusione come segmento iniziale, ne segue che $X \subseteq_i \{x \in M : x < a\} \subseteq_i B$. Poiché B è una f-catena e l'inclusione $X \subseteq_i B$ è stretta (in quanto $a \in B$), ne segue che $f(X) \subseteq_i B$, da cui a maggior ragione $f(X) \subseteq_i M$. Ciò completa la verifica che M è una f-catena.

Ovviamente, esendo l'unione di tutte le f-catene, M le include tutte, e pertanto coincide con $f(M)$. Per definizione di f questo può capitare solo se M non ha maggioranti stretti. □

4.31 Esercizio. Si dimostri che ogni f-catena (definita nella dimostrazione del lemma precedente) è bene ordinata.

4.32 Teorema (Lemma di Zorn)**.** *Sia $(P, \leq)$ un ordine parziale in cui ogni catena ha un maggiorante. Allora esiste in P almeno un elemento massimale.*

Dimostrazione. (AC) Per il Lemma 4.30 esiste una catena X di P senza maggioranti stretti. D'altra parte per ipotesi X ha un maggiorante a, che non potendo essere stretto deve appartenere ad X. Tale a deve evidentemente essere un elemento massimale di P. □

4.9 Teorema di Zermelo

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

Dimostrazione. Usiamo il lemma di Zorn. Vogliamo dimostrare l'esistenza di un buon ordinamento su X. Sia P l'insieme di tutte le coppie della forma $(A, \leq)$ dove A è un sottoinsieme di X e $\leq$ è un buon ordine su A. Chiaramente P è non vuoto in quanto ad esempio ogni sottoinsieme finito di X può essere bene ordinato. Mettiamo su P il seguente ordine parziale $\preceq$: diciamo che $(A, \leq) \preceq (A', \leq')$ se e solo se $(A, \leq)$ è un segmento iniziale di $(A', \leq')$ (cioè A è un segmento iniziale di $(A', \leq')$ e $\leq$ coincide con la restrizione di $\leq'$ ad A). In base al teorema 4.27 ogni catena in $(P, \leq)$ ha un maggiorante, dato dall'unione della catena. Per il lemma di Zorn ne segue che esiste un elemento massimale $(M, \leq)$ in P. Per finire dimostriamo che $M = X$. Nel caso contrario sia $a \in X \setminus M$, e definiamo un buon ordinamento $\leq'$ su $M \cup \{a\}$ mantenendo su M il precedente ordinamento $\leq$ e stabilendo che a è maggiore rispetto ad $\leq'$ di ogni elemento di M. Evidentemente $(M, \leq)$ è un segmento iniziale di $(M \cup \{a\}, \leq')$, contraddicendo la massimalità di $(M, \leq)$ in P. □

4.34 Osservazione. Il teorema di Zermelo implica a sua volta l'assioma della scelta.

Dimostrazione. Data una famiglia di insiemi non vuoti $\{A_i : i \in I\}$, si consideri la funzione f che dato $i \in I$ restituisce il minimo elemento $f(i)$ di A_i in base ad un fissato buon ordinamento di $\bigcup_{i \in I} A_i$. Tale f è una funzione di scelta per la famiglia. □

Un importante corollario del teorema di Zermelo è il seguente:

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

Dimostrazione. Bene ordiniamo X ed Y e usiamo il fatto che due buoni ordini sono l'uno isomorfo ad un segmento iniziale dell'altro. □

4.10 Teorema di ricursione

4.36 Osservazione (Induzione su relazioni ben fondate)**.** Sia R una relazione ben fondata su A. Sia P una proprietà tale che, per ogni $a \in A$, se vale $P(x)$ per ogni x con xRa, allora vale anche $P(a)$. Allora $(\forall x \in A)P(x)$.

Dimostrazione. Altrimenti si consideri un elemento $a \in A$ che sia R-minimale tra quelli che non verificano P. Ma allora per gli x con xRa vale $P(x)$. Per ipotesi deve allora valere anche $P(a)$. □

ricursione

4.37 Teorema (Teorema di ricursione)**.** *Sia R una relazione ben fondata su un insieme A e sia $\varphi(x,y,z)$ una proprietà tale che per ogni x,y esiste un unico z che verifica $\varphi(x,y,z)$. Indichiamo tale z con $H(x,y)$ e scriviamo $z = H(x,y)$ come abbreviazione di $\varphi(x,y,z)$ (H definisce una funzione-classe). Esiste una ed una sola funzione f con dominio A tale che per ogni $a \in A$ si ha*

$$f(a) = H(a, f_{|\{x\in A|xRa\}}).$$

Il teorema afferma che è possibile definire una funzione f dando una regola (la H) per calcolare $f(a)$ a partire da a e dalla conoscenza di f ristretta all'insieme degli $x \in A$ con xRa (se tale insieme è vuoto abbiamo $f(a) = H(a,\emptyset)$).

Dimostrazione. Data una funzione g diciamo che g è buona se

1. $\mathrm{dom}(g) \subseteq A$,
2. Se xRy e $y \in \mathrm{dom}(g)$, anche $x \in \mathrm{dom}(g)$,
3. Per ogni $a \in \mathrm{dom}(g)$, $g(a) = H(a, g_{|\{x\in A|xRa\}})$.

Dobbiamo mostrare che esiste ed è unica una funzione buona f il cui dominio sia tutto A. Mostriamo intanto che date due funzioni buone g ed h, esse coincidono nell'intersezione dei loro domini. Si noti che questo implica che l'unione di una famiglia di funzioni buone è una funzione buona e che se esiste una funzione buona con dominio A essa è unica. Per dimostrare il nostro assunto, supponiamo per assurdo che esista $a \in \mathrm{dom}(g) \cap \mathrm{dom}(h)$ con $g(a) \neq h(a)$. Siccome R è ben fondata possiamo prendere un elemento $a \in A$ che sia R-minimale con questa proprietà. Ma allora $g_{\{x\in A|xRa\}} = h_{\{x\in A|xRa\}}$. In base alla clausola (3) nelle definizione di funzione buona ne segue che $g(a) = h(a)$, contraddicendo la scelta di a.

Dimostriamo ora che per ogni $a \in A$ esiste una funzione buona g con $a \in \mathrm{dom}(g)$. Ragionando per assurdo sia a R-minimale per cui questa proprietà non sia vera. Allora per ogni x con xRa esiste una funzione buona h con $x \in \mathrm{dom}(h)$. Tra queste ve ne sarà una ed una sola, chiamiamola h_x, il cui dominio è il più piccolo possibile (considero l'intersezione di tutte le h buone con $x \in \mathrm{dom}(h)$). Per l'assioma di rimpiazzamento $\{h_x \mid xRa\}$ è un insieme, e per l'assioma dell'unione lo sarà anche la sua unione $G = \bigcup\{h_x \mid xRa\}$. Tale G è ancora una funzione buona, il cui dominio include tutti gli x con xRa ma non comprende a stesso. Possiamo estendere G ad una funzione g con $a \in \mathrm{dom}(g)$ definendo $g(a) = H(a, G_{|\{x\in A|xRa\}})$ e stabilendo che g coincide con G sul dominio di G.

Ne segue che ad ogni $a \in A$ possiamo associare una funzione buona g_a il cui dominio comprende l'elemento a. Per finire, usando di nuovo l'assioma di rimpiazzamento, sia f l'unione di tutte le g_a con $a \in A$. Tale f è una funzione buona il cui dominio coincide con A. □

4.38 Osservazione. Nel teorema precendente se assumiamo che H sia una funzione anziché una funzione-classe, allora nella dimostrazione non abbiamo bisogno dell'assioma di rimpiazzamento.

5 Ordinali

Una possibile definizione dei numeri ordinali è la seguente:

5.1 Definizione (Definizione provvisoria)**.** Un numero ordinale è il tipo d'ordine di un insieme bene ordinato.

Questa definizione va bene per molti scopi ma ha lo svantaggio che i tipi d'ordine, intesi come classi di isomorfismo di insiemi bene ordinati, non sono insiemi ma classi proprie. Conviene allora procedere diversamente e definire gli ordinali come particolari rappresentanti delle classi di isomorfismo dei buoni ordini. Il modo di scegliere i rappresentanti è spiegato nella sezione seguente.

5.1 Ordinali di von Neumann

5.2 Definizione. Un insieme α si dice transitivo se per ogni x, y tali che $x \in y$ e $y \in \alpha$ si ha $x \in \alpha$. Equivalentemente α è transitivo se $x \in \alpha \to x \subseteq \alpha$.

ordinale

5.3 Definizione. Un insieme α è un ordinale se è transitivo e $(\alpha, \in)$ è un buon ordine stretto.

5.4 Esempio. I seguenti insiemi sono ordinali: $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$ etc.

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

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

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

minore-ord

5.6 Lemma. *Siano α e β due ordinali. Sono equivalenti:*

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

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

confrontabilita-ord

5.7 Lemma. *Se α e β sono ordinali, allora $\alpha \subseteq \beta$ oppure $\beta \subseteq \alpha$.*

Dimostrazione. Sia $\gamma = \alpha \cap \beta$. Chiaramente γ è un ordinale, e $\gamma \subseteq \alpha$, $\gamma \subseteq \beta$. Basta mostrare che $\gamma = \alpha$ oppure $\gamma = \beta$. Se così non fosse, γ sarebbe incluso strettamente sia in α che in β e quindi per il lemma precedente apparterrebbe sia ad α che a β: $\gamma \in \alpha$, $\gamma \in \beta$. Ma allora $\gamma \in \alpha \cap \beta = \gamma$, e quindi $\gamma \in \gamma$ contraddicendo la definizione di ordinale (cioè il fatto che $\in$ è un ordine stretto su α e γ è un elemento di α). □

unicita-ordinali

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

Dimostrazione. Se $\alpha \neq \beta$ allora in base ai Lemmi 5.7 e 5.6 α è un segmento iniziale proprio di β o viceversa. Ma questo è assurdo in quanto per il Lemma 4.17 un buon ordine non è mai isomorfo ad un suo segmento iniziale proprio. □

5.9 Definizione. Se α e β sono ordinali scriviamo $\alpha < \beta$ se $\alpha \in \beta$.

Con questa definizione abbiamo:

minoredia

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

5.2 L'ordinale associato ad un buon ordine

5.11 Definizione (Rango di una relazione ben fondata)**.** Sia R una relazione ben fondata su un insieme A. Definiamo per ricursione su R una funzione ρ da A alla classe ON degli ordinali nel modo seguente. Dato $y \in A$,

$$\rho(y) = \sup\{\rho(x) + 1 \mid xRy\}.$$

In altre parole $\rho(y)$ è il minimo ordinale strettamente maggiore di $\rho(x)$ per ogni $x \in A$ con xRy. La ρ è chiamata funzione rango associata ad (A, R). Il rango di (A, R) è definito come il minimo ordinale α strettamente maggiore di $\rho(y)$ per ogni $y \in A$.

5.12 Proposizione. *Il rango β di (A, R) sopra definito coincide con l'immagine della funzione rango $\rho : A \to ON$.*

immaginerho

Dimostrazione. L'immagine di ρ consiste di ordinali strettamente minori di β e pertanto è inclusa in β. Mostriamo l'inclusione opposta. Per assurdo supponiamo che ci sia un ordinale strettamente minore di β che non appartiene all'immagine di ρ e sia α il minimo di tali ordinali. Deve esistere un elemento y di A con rango $\rho(y) = \gamma > \alpha$ altrimenti il sup β non potrebbe essere raggiunto. Scegliendo γ più piccolo possibile possiamo assumere che non ci siano elementi di A di rango strettamente compreso tra α e γ. Per definizione $\rho(y) = \sup\{\rho(x) + 1 \mid xRy\}$. Questo però è assurdo in quanto l'ordinale $\gamma = \rho(y) > \alpha$ non può essere il sup di una famiglia di ordinali $\leq \alpha$. □

5.13 Teorema. *Per ogni buon ordine $(A, <)$ esiste uno ed un solo ordinale α tale che $(A, <)$ è isomorfo a $(\alpha, \in)$. Tale α viene chiamato il tipo d'ordine di $(A, <)$ e coincide con il rango di $(A, <)$ sopra definito.*

Dimostrazione. L'unicità di α segue dal fatto che due ordinali isomorfi sono uguali. Per dimostrare l'esistenza onsideriamo la funzione rango $\rho : A \to ON$ associata ad $(A, <)$. Per $y \in A$ abbiamo per definizione

$$\rho(y) = \sup\{\rho(x) + 1 \mid x < y\}.$$

Ovviamente se $x < y$ allora $\rho(x) < \rho(y)$. Visto che dati due elementi distinti uno dei due è maggiore dell'altro, ne segue che ρ è iniettiva e che deve in effetti valere la doppia implicazione: $x < y \leftrightarrow \rho(x) < \rho(y)$. Poiché tra gli ordinali il $<$ coincide con l'appartenenza $\in$, ne segue che ρ è un isomorfismo da $(A, <_A)$ ad $(\alpha, \in)$. □

5.14 Osservazione. Per la dimostrazione del teorema precedente è necessario lo schema di assiomi di rimpiazzamento (esse viene utilizzato nel teorema di ricursione).

5.3 Induzione e ricursione sugli ordinali

5.15 Teorema. *(Principio del minimo per gli ordinali) Sia $\phi(x)$ una formula. Se esiste un ordinale α che verifica $\phi(\alpha)$, allora esiste un minimo tale α.*

Dimostrazione. Supponiamo che valga $\phi(\alpha)$. Se α non è il minimo con questa proprietà allora $\{\beta < \alpha \mid \phi(\beta)\}$ è un sottoinsieme non vuoto dell'insieme bene ordinato α e pertanto ha un minimo. □

5.16 Corollario. *La classe $Ord = \{x \mid$ x è un ordinale $\}$ non è un insieme.*

Dimostrazione. Se lo fosse sarebbe un insieme transitivo e bene ordinato da $\in$, e pertanto sarebbe un ordinale. Ma visto che X contiene tutti gli ordinali ed è esso stesso un ordinale, $X \in X$. Questo è assurdo perché un ordinale non può appartenere a se stesso (essendo i suoi elementi ordinati strettamente da $\in$). □

Ciò nonostante possiamo fare induzione e ricursione su Ord nel modo seguente.

5.17 Teorema. *Sia X un insieme di ordinali. Allora $\bigcup_{\alpha \in X} \alpha$ è un ordinale, ed è il minimo ordinale maggiore o uguale a tutti gli ordinali di X, cioè $\bigcup_{\alpha \in X} \alpha = \sup X$.*

Dimostrazione. Per il Teorema 4.27 l'unione $\bigcup_{\alpha \in X} \alpha$ è un ordinale. Ora poiché l'ordine tra ordinali coincide con l'inclusione, chiaramente il sup coincide con l'unione. □

5.18 Corollario. *Ogni insieme X di ordinali è limitato superiormente.*

5.19 Teorema. *Se α è un ordinale, $\alpha \cup \{\alpha\}$ è un ordinale ed è il minimo ordinale maggiore di α. Definiamo quindi $\alpha + 1 = \alpha \cup \{\alpha\}$ (da non confondersi con il "+1" tra cardinali).*

Dimostrazione. Esercizio. □

5.20 Teorema. *(Induzione sugli ordinali) Sia $\phi(x)$ una formula. Supponiamo che:*

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

Allora tutti gli ordinali verificano $\phi(x)$.

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

Analogamente si dimostra un teorema di ricursione transfinita per definire "funzioni" definite su tutto Ord. Ad esempio vedremo come si possa definire una funzione-classe somma $+: Ord \times Ord \to Ord$ (da non confondersi con la somam cardinale!) per induzione sul secondo argomento.

5.4 Operazioni sui numeri ordinali

5.21 Definizione. Definiamo la somma di due numero ordinali per induzione sul secondo argomento:

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

La giustificazione di questa definizione è data dal teorema di ricursione. Formalmente non possiamo applicare il teorema di ricursione nella forma precedentemente data perchè gli ordinali formano una classe propria. Tuttavia si può procedere nel modo seguente. Per definire $\alpha + \beta$ fissiamo un ordinale $\gamma \geq \beta$. Gli ordinali $\leq \gamma$ formano un insieme (coincidente con $\gamma + 1$), quindi in base al teorema di ricursione è lecito definire per ricursione la funzione $x \mapsto \alpha + x$ per $x \leq \gamma$ usando le clausole induttive (1),(2),(3). In particolare risulta in questo modo definito $\alpha + \beta$. Lasciamo al lettore la verifica che il risultato di questa operazione non dipende da γ.

5.22 Definizione. Definiamo il prodotto di due numero ordinali per induzione sul secondo argomento:

1. $\alpha \cdot 0 = 0$,
2. $\alpha \cdot S(\beta) = \alpha \cdot \beta + \alpha$,

3. $\alpha \cdot \lambda = \sup_{\beta<\lambda} \alpha \cdot \beta$, se λ è un ordinale limite.

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

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

5.24 Esercizio. Le definizioni di somma e prodotto concordano con le definizioni di somma e prodotto di tipi d'ordine precedentemente date.

5.25 Esercizio. Se α e β sono ordinali numerabili, anche α^β lo è.

Attenzione: nonostante si usino le stesse notazioni, le operazioni sugli ordinali sono diverse dalle omologhe operazioni sui cardinali. Ad esempio se β è un cardinale infinito, 2^β (esponenziazione cardinale) non è numerabile: l'esponenziazione tra cardinali fa uscire dal numerabile.

5.26 Esercizio. Abbiamo:

1. (Sottrazione) Se α e β sono ordinali, ed $\alpha \leq \beta$, allora esiste un unico ordinale γ con $\alpha + \gamma = \beta$.
2. (Divisione con resto) Se α e β sono ordinali, con $\beta \neq 0$, allora esiste una unica coppia di ordinali ξ e ρ tale che $\alpha = \beta\xi + \rho$, con $\rho < \beta$.
3. (Rappresentazione in base γ) Dato un ordinale $\gamma \neq 0$ possiamo rappresentare ogni ordinale $\alpha \neq 0$ in modo unico nella forma $\alpha = \gamma^{\alpha_1} t_1 + \ldots + \gamma^{\alpha_k} t_k$ con $k \in \omega$, $t_1, \ldots, t_k < \gamma$, $\alpha_1 > \ldots > \alpha_k$.
4. (Forma normale di Cantor) In particolare se α è un ordinale diverso da zero, allora esiste un'unica scrittura della forma $\alpha = \omega^{\alpha_1} n_1 + \ldots + \omega^{\alpha_k} n_k$ con $k \in \omega$, $n_1, \ldots, n_k < \omega$, $\alpha_1 > \ldots > \alpha_k$.

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

5.28 Esercizio. Si dimostri che esistono ordinali α arbitrariamente grandi tali che $\alpha = \omega^\alpha$. Sia ε_0 il minimo ordinale tale che $\varepsilon_0 = \omega^{\varepsilon_0}$. Si dimostri che ε_0 è numerabile.

5.5 Cardinali come ordinali iniziali

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

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

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

5.32 Teorema. *Per ogni insieme X esiste uno ed un solo ordinale iniziale α della stessa cardinalità di X.*

Dimostrazione. Bene ordiniamo X e sia β il tipo d'ordine di X con il dato buon ordine. Ora sia α il minimo ordinale della stessa cardinalià di β. □

Ricordiamo che non abbiamo ancora definito $|X|$ (abbiamo solo definito le notazioni $|X| = |Y|$, $|X| \leq |Y|$ e $|X| < |Y|$). Possiamo ora definire:

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

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

5.34 Corollario. *(Principio del minimo per cardinali) Se una formula $\phi(x)$ è verificata da qualche cardinale, allora esiste un minimo cardinale che la verifica.*

Aver identificato i cardinali con gli ordinali iniziali non significa però che il la somma che abbiamo definito sui cardinali coincida con la somma definita sugli ordinali. Ad esempio $\aleph_0 + 1 = \aleph_0$ (aggiungere un elemento ad un insieme numerabile non cambia la cardinalità), mentre $\omega + 1 \neq \omega$ (aggiungere un elemento in fondo ad un buon ordine ne cambia il tipo d'ordine). Questo può causare un po' di confusione in quanto $\aleph_0 = \omega$ (se pensiamo ai cardinali come ordinali iniziali), e quindi ci si aspetterebbe che $\aleph_0 + 1 = \omega + 1$. Il punto però è che nei due casi il + ha un significato diverso. Quando usiamo la notazione $\aleph_0$ usiamo le operazioni cardinali, quando usiamo la notazione ω usiamo le operazioni ordinali. Conviene tenere sempre a mente che, a prescindere dalle identificazioni fatte, ω rappresenta il tipo d'ordine di $(\mathbb{N}, \leq)$, mentre $\aleph_0$ rappresenta la cardinalità di $\mathbb{N}$.

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

5.6 La funzione aleph

5.36 Lemma. *Per ogni cardinale α esiste un cardinale α^+ più grande di α tale che non cè nessun cardinale tra α e α^+.*

Dimostrazione. Sicuramente esiste un cardinale più grande di α (ad esempio 2^α). Quindi esiste un minimo cardinale più grande di α. □

Possiamo quindi definire $\aleph_1 = \aleph_0{}^+$, $\aleph_2 = \aleph_1{}^+$ e così via. Si noti che $\aleph_0 < \aleph_1 \leq 2^{\aleph_0}$. Non si può determinare nella teoria di Zermelo-Fraenkel se valga l'uguaglianza $\aleph_1 = 2^{\aleph_0}$.

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

Dimostrazione. Se $\sup X$ non è iniziale esiste un ordinale iniziale $\kappa < \sup X$ della stessa cardinalità di $\sup X$. Per definizione di sup, esiste $\beta \in X$ con $\kappa < \beta \leq \sup X$. Visto che la relazione $\leq$ tra ordinali coincide con l'inclusione $\subseteq$, e visto che κ e $\sup X$ hanno la stessa cardinalità, ne segue che anche β essendo compreso tra i due ha la stessa cardinalità. Questo è assurdo in quanto β è iniziale, e non può pertanto avere la stessa cardinalità di un ordinale più piccolo. □

5.38 Definizione. Definiamo per ricursione transfinita:

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

La funzione-classe che manda α in $\aleph_\alpha$ è una biiezione da ON verso la classe dei cardinali infiniti che preserva l'ordine.

5.7 $\aleph_\alpha \cdot \aleph_\beta = \max\{\aleph_\alpha, \aleph_\beta\}$

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

Dimostrazione. Sia X un insieme di cardinalità $\aleph_\theta$. Dobbiamo trovare una corrispondenza biunivoca tra $X \times X$ ed X. Possiamo supporre per ipotesi induttiva che la tesi $|Y \times Y| = |Y|$ valga per insiemi infiniti Y di cardinalità strettamente inferiore a quella di X. (Se no ci si riduca a questo caso considerando il minimo cardinale per cui non valga il teorema.) Fissiamo su X un buon ordine $<$ iniziale (ovvero di tipo d'ordine $\aleph_\theta$), in modo che i segmenti iniziali propri di X abbiamo cardinalità strettamente minore a quella di X. L'idea ore è quella di cercare di definire un buon ordine $\prec$ su $X \times X$ in modo che la corrispondenza biunivoca cercata sia un isomorfismo d'ordine. Ordiniamo le coppie $(\alpha, \beta) \in X \times X$ nel modo seguente: $(\alpha, \beta) \prec (\gamma, \delta)$ se e solo se $\max(\alpha, \beta) < \max(\gamma, \delta)$ oppure a parità di massimi $\alpha < \gamma$, oppure a parità di massimi e prime componenti $\beta < \delta$ (i massimi sono presi rispetto all'ordine $<$). Chiaramente $\prec$ è un buon ordine, e per il teorema di confrontabilità dei buoni ordini abbiamo che o $(X \times X, \prec)$ e $(X, <)$ sono isomorfi oppure uno dei due è un segmento iniziale proprio dell'altro. Poichè certamente $|X \times X| \geq |X|$, e i segmenti iniziali propri di X hanno cardinalità minore di $|X|$, una delle tre alternative si esclude subito: $X \times X$ non può essere isomorfo ad un segmento iniziale di X. Resta quindi da escludere

che X sia isomorfo ad un segmento proprio J di $X \times X$, e a tal fine è sufficiente dimostrare che ogni tale J ha cardinalità $< |X|$. Per verificare quest'ultima affermazione notiamo che se $(u, v) \in (X \setminus J)$, allora ogni elemento $(a, b) \in J$ è più piccolo di (u, v) nell'ordine $\prec$, e quindi $\max(a, b) \leq \max(u, v)$. Questo significa che $J \subseteq Y \times Y$, dove $Y = \{x \in X \mid x \leq \max(u, v)\}$, e quindi $|J| \leq |Y \times Y|$. Ma Y è un segmento iniziale proprio di X (non può essere uguale ad X in quanto un buon ordine iniziale infinito non può avere un massimo elemento), e pertanto per le nostre ipotesi $|Y \times Y| = |Y| < |X|$, da cui la tesi. □

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

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

5.8 Teorema di König

5.41 Definizione. Per $i \in I$, sia α_i un cardinale. Definiamo la somma F $\Sigma_{i \in I} \alpha_i$ come la cardinalità di $\bigcup_{i \in I} A_i$ dove gli A_i sono insiemi disgiunti con $|A_i| = \alpha_i$.

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

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

Dimostrazione. Per ogni $i \in I$ fissiamo degli insiemi $A_i \subset B_i$ con $|A_i| = \alpha_i$ e $|B_i| = \beta_i$, e definiamo $A'_i := A_i \times \{i\}$. Osservando che gli A'_i sono a due a due disgiunti, abbiamo $\Sigma_{i \in I} \alpha_i = |\bigcup_{i \in I} A'_i|$ e $\Pi_{i \in I} \beta_i = |\times_{i \in I} B_i|$. Dobbiamo mostrare che esiste una funzione iniettiva $f : \bigcup_{i \in I} A'_i \to \times_{i \in I} B_i$ ma non ne esiste una biunivoca. Cominciamo con il mostrare che esiste una f iniettiva come richiesto. Fissiamo a tal fine una I-upla $(b_i \mid i \in I) \in \times_{i \in I} B_i$ dove i b_i sono stati scelti in modo che $b_i \in B_i \setminus A_i$. Dato un elemento x di $\bigcup_{i \in I} A'_i$, esiste un unico $j \in I$ con $x \in A'_j = A_j \times \{j\}$, e possiamo scrivere x nella forma (a, j) per qualche $a \in A_j$. Associamo a tale $x = (a, j)$ l'elemento $f(x) = (c_i \mid i \in I) \in \times_{j \in I} B_j$ tale che $c_i = b_i$ per $i \neq j$ e $c_j = a$. La f così definita è iniettiva (verificate!).

Per completare la dimostrazione basta mostrare che non esistono funzioni surgettive g da $\bigcup_{i \in I} A'_i$ a $\times_{i \in I} B_i$ (quindi in particolare non esistono funzioni biunivoche). Data $g \colon \bigcup_{i \in I} A'_i \to \times_{i \in I} B_i$, occorre dunque trovare un elemento $(c_i \mid i \in I)$ di $\times_{i \in I} B_i$ che non è nell'immagine di g. Per $j \in I$, consideriamo la funzione $g_j \colon A_j \to B_j$ ottenuta come composizione delle funzioni $A_j \xrightarrow{\iota_j} \bigcup_{i \in I} A'_i \xrightarrow{g} \times_{i \in I} B_i \xrightarrow{\pi_j} B_j$, dove $\iota_j(a) = (a, j)$ e $\pi_j((c_i \mid i \in I)) = c_j$. Poiché $|A_j| < |B_j|$, la g_j non è surgettiva. Possiamo dunque scegliere $(c_i \mid i \in I) \in \times_{i \in I} B_i$ in modo che per ogni $j \in I$ $c_j \notin \mathrm{im}(g_j)$. Se per assurdo $(c_i \mid i \in I) = g(x)$ per qualche $x \in \bigcup_{i \in I} A'_i$, sia $j \in I$ tale che $x \in A'_j$, e scriviamo x nella forma (a, j) con $a \in A_j$. Per definizione di g_j dobbiamo avere $g_j(a) = c_j$, ma questo è assurdo in quanto c_j era stato scelto fuori dall'immagine di g_j. □

Come corollario otteniamo una seconda dimostrazione del teorema di Cantor:

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

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

5.9 Cofinalità

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

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

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

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

5.49 Esercizio.

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

5.50 Definizione. Un ordinale β si dice regolare se $cf(\beta) = \beta$.

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

5.52 Esercizio. Abbiamo:

1. Ogni ordinale regolare è un cardinale (ovvero un ordinale iniziale).
2. Ogni cardinale successore è regolare. In particolare $\aleph_1$ è regolare.
3. Esiste un cardinale non regolare.
4. Un cardinale κ è regolare se e solo se per ogni famiglia $(A_i \mid i \in I)$ di insiemi A_i tali che $|A_i| < \kappa$ e $|I| < \kappa$, si ha $|\bigcup_{i\in I} A_i| < \kappa$.

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

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

5.54 Corollario. *La cofinalità di $2^{\aleph_0}$ è diversa da ω. Quindi in particolare $2^{\aleph_0} \neq \omega$ (ma non si può stabilire, in base agli assiomi, se sia più grande o più piccolo).*

5.10 Gerarchia di von Neumann

5.55 Definizione. La gerarchia di von Neumann è definita per induzione transfinita nel modo seguente:

$V_0 = \emptyset$
$V_{\alpha+1} = P(V_\alpha)$
$V_\lambda = \bigcup_{\alpha<\lambda} V_\alpha$ per λ ordinale limite.

Un insieme è ben fondato se appartiene a V_α per qualche α. Indichiamo con WF la classe $\bigcup_{\alpha\in ON} V_\alpha$.

5.56 Esercizio. L'assioma di fondazione equivale all'affermazione che ogni insieme è ben fondato.