ELEMENTI DI TEORIA DEGLI INSIEMI
Dispensa 9

Mauro Di Nasso

Ultimo aggiornamento: December 12, 2024

Formulazioni equivalenti dell'assioma di scelta

Ci sono proprietà in matematica che possono essere equivalentemente riformulati in modi diversi apparentemente molto distanti l'uno dall'altro; quando questo accade, ciò è considerato un segno della rilevanza di tali proprietà.

In questo capitolo ci concentreremo sull'assioma di scelta, e ne dimostreremo cinque diverse formulazioni equivalenti tra le più significative. Naturalmente, nel dimostrare quelle equivalenze, dovremo fare molta attenzione a lavorare sempre all'interno della teoria ZF, senza mai usare né l'assioma di scelta, nè alcuna delle sue conseguenze.

È bene precisare che lo studio delle varie forme di assioma di scelta è stato molto approfondito ed ha permesso di isolare centinaia di formulazioni equivalenti, oltre che di una miriade di principi più deboli, ma comunque non dimostrabili senza l'assioma di scelta.[1]

1. Il Lemma di Zorn, il Teorema di Zermelo, e la confrontabilità

Una formulazione equivalente dell'assioma di scelta è data dal seguente principio, che ha larga applicazione in diverse aree della matematica.

> Lemma di Zorn.
> *Sia $(P, \leq)$ un insieme parzialmente ordinato. Se ogni catena ammette maggioranti allora esistono elementi massimali.*

Ricordiamo che un sottoinsieme $C \subseteq P$ si dice *catena* se la restrizione dell'ordine parziale a C è un ordine totale, cioè se per tutti i $c, c' \in C$ si ha $c \leq c'$ o $c' \leq c$. Un elemento $p \in P$ si dice *maggiorante* dell'insieme $X \subseteq P$ se $p \geq x$ per ogni $x \in X$. Un elemento $p \in P$ si dice *massimale* se non esistono elementi $q \in P$ con $p < q$. Nel caso di un ordine totale, un elemento massimale è necessariamente il massimo di P. Tuttavia, nel caso di ordini parziali P, possono esistere elementi massimali distinti (e quindi inconfrontabili).

TEOREMA 1.1 (ZF). *"Assioma di scelta" $\Rightarrow$ "Lemma di Zorn".*

Diamo di questo risultato due diverse dimostrazioni. La prima è piuttosto elaborata, ma ha il vantaggio di non richiedere conoscenze specifiche di teoria degli insiemi. La seconda, più breve e diretta, si basa sulla ricorsione transfinita.

DIM.1. Sia $(P, \leq)$ un insieme parzialmente ordinato dove ogni catena ammette maggioranti. Vogliamo trovare un elemento massimale. L'idea della dimostrazione è quella di costruire una catena bene ordinata $C \subseteq P$ il "più lunga possibile", in modo che l'unico maggiorante di C sia in realtà il massimo di C ed un elemento massimale per tutto $(P, \leq)$.

[1] Si veda ad esempio il volume *"Consequences of the Axiom of Choice"* di P. Howard e J.E. Rubin (American Mathematical Society, 1998). Il numero di proprietà considerato è talmente grande che era stato preparato un sito web per consultare velocemente l'esistenza di implicazioni tra le varie formulazioni: `http://www.math.purdue.edu/~hrubin/JeanRubin/Papers/conseq.html`. Purtroppo al momento della scrittura di questa dispensa quella pagina non è più funzionante.

Fissiamo una funzione di scelta $f : \mathcal{P}(P) \setminus \{\emptyset\} \to P$. Diciamo che un sottoinsieme non vuoto $A \subseteq P$ è una *f-catena* se:

- $(A, \leq)$ è bene ordinato ;
- Per ogni $a \in A$, si ha $a = f(A^a)$ dove $A^a = \{p \in P \mid p > A_a\}$ è l'insieme dei maggioranti *stretti* del segmento iniziale $A_a = \{a' \in A \mid a' < a\}$.[2]

Ragioniamo informalmente per capire meglio l'idea che guida la dimostrazione. Se $p_0 = f(P)$, allora $A = \{p_0\}$ è una una f-catena. Infatti il segmento iniziale A_{p_0} è vuoto, e banalmente l'insieme dei suoi maggioranti stretti $A^{p_0} = P$, quindi $f(A^{p_0}) = p_0$. Se p_0 è elemento massimale, abbiamo finito. Altrimenti $A^{p_0} \neq \emptyset$ e possiamo prendere $p_1 = f(A^{p_0})$. È facile verificare che anche $\{p_0 < p_1\}$ è una f-catena. Di nuovo, se p_1 è un elemento massimale di P, la tesi è raggiunta. Altrimenti possiamo iterare il procedimento e, se non troviamo elementi massimali, arriviamo a definire una f-catena infinita $A = \{p_0 < p_1 < p_2 < \ldots < p_n < p_{n+1} < \ldots\}$.

Adesso, per ipotesi ogni catena ammette maggioranti, dunque possiamo prendere l'elemento $p_\omega = f(\{p \in P \mid p > A\})$ ed aggiungerlo alla f-catena A. Si osservi che anche $A' = A \cup \{p_\omega\}$ è una f-catena, visto che il segmento iniziale $(A')_{p_\omega} = A$, che $(A')^{p_\omega} = \{p \in P \mid p > A\}$, e che quindi $p_\omega = f((A')^{p_\omega})$. Proseguiamo in questo modo, e "allunghiamo" la catena finché ciò è possibile, cioè fin quando esistono maggioranti stretti.

Per rendere rigorosa questa costruzione informale, ci occorre intanto la seguente proprietà.

($\star$) *Se A e B sono due f-catene, allora una è segmento iniziale dell'altra.*

Visto che A e B sono buoni ordini, uno dei due è isomorfo ad un segmento iniziale dell'altro. Ad esempio, supponiamo che $\theta : A \to S$ sia un isomorfismo, dove S è un segmento iniziale (non necessariamente proprio) di B. Vogliamo dimostrare che θ è l'identità. Procediamo per assurdo, e consideriamo $a = \min\{x \in A \mid \theta(x) \neq x\}$. I segmenti iniziali A_a e $B_{\theta(a)}$ coincidono, dunque anche i corrispondenti insiemi di maggioranti stretti $A^a = B^{\theta(a)}$ sono uguali. Ma allora si avrebbe che $a = f(A^a) = f(B^{\theta(a)}) = \theta(a)$, contro l'ipotesi.

Sappiamo che l'unione di un insieme di buoni ordini che sono uno segmento iniziale dell'altro è ancora un buon ordine. Dunque l'unione $(C, \leq)$ di tutte le f-catene è un sottoinsieme bene ordinato di P. Inoltre è facile verificare che C stesso è una f-catena, e quindi C è la f-catena massima. In particolare, non esistono maggioranti stretti di C, altrimenti la catena C potrebbe essere estesa. Da questo segue che un elemento maggiorante della catena C è necessariamente il massimo di C, ed è inoltre un elemento massimale per P. □

Dim.2. Sia $(P, \leq)$ un insieme parzialmente ordinato dove ogni catena ammette maggioranti. Fissiamo una funzione di scelta $f : \mathcal{P}(P) \setminus \{\emptyset\} \to P$, e prendiamo un elemento $\star \notin P$. Per ricorsione transfinita, definiamo $p_0 = f(P)$, e per $\alpha > 0$:

$$p_\alpha = \begin{cases} f(P^\alpha) & \text{se } \star \notin \{p_\beta \mid \beta < \alpha\} \text{ e } P^\alpha = \{p \in P \mid \forall\, \beta < \alpha \;\; p > p_\beta\} \neq \emptyset \\ \star & \text{altrimenti.} \end{cases}$$

Con questa definizione, costruiamo una sequenza strettamente crescente di elementi di P, fino a che ciò è possibile. Notiamo che se arriviamo ad un passo α dove l'insieme P^α dei maggioranti *stretti* di $\{p_\beta \mid \beta < \alpha\}$ è vuoto, allora $p_\alpha = \star$. Inoltre,

[2] Se $X \subseteq P$ è un insieme, scriviamo $p > X$ per intendere $p > x$ per tutti i $x \in X$.

se questo accade, dalla definizione segue immediatamente che allora avremo $p_\beta = \star$ per tutti gli ordinali $\beta > \alpha$.

Verifichiamo che esistono effettivamente indici α tali che $p_\alpha = \star$. Se così non fosse, ogni $p_\alpha = f(P^\alpha) \in P^\alpha \subseteq P$, e dunque la funzione-classe $\mathbb{F} : \alpha \mapsto p_\alpha$, che è definita sulla classe propria degli ordinali, sarebbe strettamente crescente, quindi iniettiva. Ma allora anche la sua immagine $\{p_\alpha \mid \alpha \in \mathbf{ORD}\}$ sarebbe una classe propria, e questo è impossibile perché si tratta di un sottoinsieme di P.

Sia adesso α il più piccolo indice con $p_\alpha = \star$. Se per assurdo α fosse un ordinale limite, ogni maggiorante della catena crescente $\{p_\beta \mid \beta < \alpha\}$ sarebbe anche un maggiorante stretto, e quindi un elemento di P^α. Ma allora dovrebbe essere $p_\alpha = f(P^\alpha) \in P$, contro l'ipotesi $p_\alpha = \star \notin P$. Concludiamo allora che $\alpha = \beta + 1$ è un successore, e quindi p_β è l'ultimo elemento della sequenza diverso da $\star$. È adesso facile verificare che p_β è un elemento massimale in $(P, \leq)$, perché un eventuale $p > p_\beta$ apparterrebbe a $P^{\beta+1}$, e sarebbe $p_{\beta+1} \neq \star$. □

Teorema 1.2 (ZF). *(Teorema di Zermelo) "Lemma di Zorn" ⇒ "Ogni insieme è bene ordinabile".*

Dim. Dato un insieme X, consideriamo la collezione di tutti i possibili buoni ordini ottenuti con suoi sottoinsiemi:

$$\mathcal{B} = \{(B, \leq_B) \text{ buon ordine} \mid B \subseteq X\}.$$

Il fatto che $\mathcal{B}$ è effettivamente un insieme segue per separazione, notando che ogni elemento di $\mathcal{B}$ appartiene a $\mathcal{P}(X) \times \mathcal{P}(X \times X)$.[3] Su $\mathcal{B}$ definiamo la seguente relazione:

$$(B, \leq_B) \preceq (B', \leq_{B'}) \ \text{ se e solo se } (B, \leq_B) \text{ è un segmento iniziale di } (B', \leq_{B'}).$$

Più precisamente, richiediamo che $B \subseteq B'$, che la relazione d'ordine $\leq_{B'}$ ristretta ad elementi di B coincida con $\leq_B$, ed infine che se $x \leq_{B'} b$ dove $b \in B$, allora anche $x \in B$. È immediato verificare che $\preceq$ è un ordinamento parziale su $\mathcal{B}$. Inoltre, ogni catena C di $\mathcal{B}$ ammette maggiorante (basta considerare l'unione $\bigcup C$ e ricordare che unione di bene ordinati che sono uno segmento iniziale dell'altro è ancora un buon ordine). Possiamo allora applicare il *Lemma di Zorn* e ricavare l'esistenza di un elemento massimale $(B, \leq_B) \in \mathcal{B}$. Per concludere la dimostrazione, resta da verificare che $B = X$. Se così non fosse, potremmo prendere un elemento $\xi \in X \setminus B$, e sull'insieme $B \cup \{\xi\}$ considerare il buon ordinamento $\leq$ dove ξ viene posto "dopo" tutti gli elementi di B, cioè $x \leq y$ se e solo se $x, y \in B$ e $x \leq_B y$, oppure $y = \xi$. Allora $(B \cup \{\xi\}, \leq)$ sarebbe un buon ordine avente B come segmento iniziale generato da ξ, contro la massimalità di $(B, \leq_B)$. □

La proprietà del buon ordinamento di Zermelo implica direttamente l'assioma di scelta.

Teorema 1.3 (ZF). *"Ogni insieme è bene ordinabile" ⇒ "Assioma di scelta".*

Dim. Sia X un insieme non vuoto fissato. Per ipotesi, esiste un buon ordinamento $\leq$ su X. Una funzione di scelta $f : \mathcal{P}(X) \setminus \{\emptyset\} \to X$ si può allora definire ponendo $f(A) = \min A$ per ogni $A \subseteq X$ non vuoto. □

[3] Ricordiamo che gli insiemi ordinati $(B, \leq_B)$ sono coppie ordinate, dove B è un insieme e la relazione d'ordine $\leq_B$ è uno speciale insieme di coppie ordinate di elementi di B.

Combinando i tre teoremi di questa sezione, otteniamo le seguenti equivalenze:

Teorema 1.4 (ZF). *Le seguenti proprietà sono equivalenti:*
(1) *Assioma di scelta.*
(2) *Lemma di Zorn.*
(3) *Proprietà di Zermelo: "Ogni insieme è bene ordinabile".*

2. Uso della funzione-classe di Hartogs

Il teorema di Hartogs ci permetterà di chiarire il ruolo dell'assioma di scelta riguardo la nozione di cardinalità.

Introduciamo due proprietà relative alla nozione di equipotenza fra insiemi che mostreremo essere equivalenti all'assioma di scelta. La prima riguarda l'ordine fra cardinalità.

- *Confrontabilità delle cardinalità*:
  "Per tutti gli insiemi A, B esiste una funzione iniettiva $f : A \to B$ o esiste una funzione iniettiva $g : B \to A$, cioè si ha $|A| \leq |B|$ o $|B| \leq |A|$".

Abbiamo già dimostrato (senza usare AC) che $|\mathbb{N}\times\mathbb{N}| = |\mathbb{N}|$, e che $|\mathbb{R}\times\mathbb{R}| = |\mathbb{R}|$. Vedremo che l'estensione di questa proprietà a tutti gli insiemi infiniti è una forma equivalente dell'assioma di scelta.

- *Idempotenza delle cardinalità infinite*:
  "Ogni insieme infinito X è equipotente al prodotto cartesiano con sè stesso, cioè $|X \times X| = |X|$".

Grazie allo strumento della funzione-classe di Hartogs, possiamo mostrare l'equivalenza con AC delle proprietà relative alla cardinalità introdotte sopra.

Teorema 2.1 (ZF). *Le seguenti proprietà sono equivalenti:*[4]
(1) *Proprietà di Zermelo: "ogni insieme è bene ordinabile".*
(2) *Confrontabilità delle cardinalità.*
(3) *Idempotenza delle cardinalità infinite.*

Dim. (1) $\Rightarrow$ (2). Per la proprietà di Zermelo, esiste un buone ordine $<_A$ su A ed esiste un buon ordine $<_B$ su B. Per il teorema di tricotomia dei buoni ordini, $(A, <_A)$ è isomorfo ad un segmento iniziale di $(B, <_B)$ o viceversa. Visto che isomorfismi di ordine sono in particolare bigezioni, concludiamo che A è equipotente ad un sottoinsieme di B o viceversa, e quindi $|A| \leq |B|$ o $|B| \leq |A|$.

(2) $\Rightarrow$ (1). Dal Teorema di Hartogs sappiamo che $|\mathbb{H}(A)| \not\leq |A|$. Allora, per la confrontabilità delle cardinalità, deve essere $|A| \leq |\mathbb{H}(A)|$, cioè esiste una funzione iniettiva $f : A \to \mathbb{H}(A)$. Ma $\mathbb{H}(A)$ è un cardinale, dunque bene ordinato, e perciò A "eredita" mediante f un buon ordinamento. Precisamente, se si pone $a < a' \Leftrightarrow f(a) <_A f(a')$ per tutti gli $a, a' \in A$, allora dall'iniettività di f segue che $(A, <_A) \cong (\mathrm{imm}(f), <)$, e quindi $(A, <_A)$ è bene ordinato in quanto isomorfo ad un sottoinsieme ordinato di $\mathbb{H}(A)$.

(1) $\Rightarrow$ (3). Come abbiamo visto nel capitolo sui cardinali (vedi Teorema **??**), ogni insieme infinito bene ordinabile è equipotente ad un aleph. Quindi, per la

[4] L'equivalenza tra AC e la confrontabilità delle cardinalità è attribuita ad Hartogs, 1915. L'equivalenza tra AC e l'idempotenza delle cardinalità infinite è attribuita a Tarski, 1924.

proprietà di Zermelo, ogni insieme infinito X è equipotente ad un $\aleph_\alpha$. La tesi segue allora dalla proprietà $|\aleph_\alpha \times \aleph_\alpha| = |\aleph_\alpha|$ (vedi Teorema **??**).

(3) $\Rightarrow$ (1). Visto che ogni insieme finito è banalmente bene ordinabile, possiamo assumere che A sia infinito. Inoltre, a meno di rimpiazzare A con $A' = A \times \{0\}$, possiamo supporre che A non contenga ordinali, e quindi che $A \cap \mathbb{H}(A) = \emptyset$. Per l'ipotesi $A \cup \mathbb{H}(A)$ è equipotente al prodotto cartesiano $(A \cup \mathbb{H}(A)) \times (A \cup \mathbb{H}(A))$. Visto che quest'ultimo è un soprainsieme di $A \times \mathbb{H}(A)$, esiste allora una funzione iniettiva $\varphi : A \times \mathbb{H}(A) \to A \cup \mathbb{H}(A)$. Per ogni $a \in A$, la restrizione $\varphi_a : \mathbb{H}(A) \to A \cup \mathbb{H}(A)$ dove $\alpha \mapsto \varphi(a, \alpha)$ è anch'essa iniettiva. Ma allora $\mathrm{imm}(\varphi_a) \not\subseteq A$, altrimenti avremmo che $|\mathbb{H}(A)| \leq |A|$, contro il Teorema di Hartogs. Dunque $\mathbb{H}(A) \cap \mathrm{imm}(\varphi_a) \neq \emptyset$ e possiamo prendere $\theta(a) = \min \mathbb{H}(A) \cap \mathrm{imm}(\varphi_a)$. In questo modo resta definita una funzione $\theta : A \to \mathbb{H}(A)$. Visto che φ è iniettiva, è immediato verificare che anche θ è iniettiva, e quindi A "eredita" un buon ordine da $\mathbb{H}(A)$ ponendo $a < a' \Leftrightarrow f(a) < f(a')$ per tutti gli $a, a' \in A$. $\square$

Ci sono molte altre proprietà relative alle cardinalità che sono equivalenti all'assioma di scelta. Ad esempio:

Teorema 2.2 (ZF). *(Tarski 1924). Le seguenti proprietà sono equivalenti:*

(1) *Proprietà di Zermelo.*
(2) $|A \times B| = |A \cup B|$ *per tutti gli insiemi infiniti* A, B *tali che* $A \cap B = \emptyset$.
(3) $|A \times A| = |B \times B| \Rightarrow |A| = |B|$ *per tutti gli insiemi infiniti* A, B.
(4) *Per ogni insieme infinito* A *esiste un insieme* B *tale che* $|A| = |B \times B|$ *(cioè ogni cardinalità infinita ha una radice quadrata).*

Dim. Per esercizio. $\square$

3. Uso del Lemma di Zorn

In questa sezione mostriamo come si possano dimostrare direttamente a partire dal Lemma di Zorn sia la confrontabilità delle cardinalità, sia l'idempotenza dei cardinali infiniti. Anche se si tratta di proprietà già dimostrate con l'uso della funzione-classe di Hartogs, e il percorso in questo caso diventa più tortuoso, si tratta però di esempi significativi di uso del Lemma di Zorn, che può essere istruttivo vedere.

Teorema 3.1 (ZF). *"Lemma di Zorn" $\Rightarrow$ "Confrontabilità delle cardinalità".*

Dim. Consideriamo l'insieme parzialmente ordinato $(\mathcal{F}, \preceq)$ dove

$$\mathcal{F} = \{f : X \to B \mid X \subseteq A,\ f \text{ iniettiva}\}$$

e dove $f \preceq g$ se e solo se $f \subseteq g$, cioè se g è una estensione di f. È facile verificare che ogni catena $\mathcal{C} \subseteq \mathcal{F}$ ammette maggiorante; infatti, per la proprietà di catena, $\mathcal{C}$ contiene funzioni che sono una estensione dell'altra e quindi l'unione $\varphi = \bigcup \mathcal{C}$ è una funzione iniettiva $\varphi : \widetilde{X} \to B$ dove $\widetilde{X} = \bigcup \{\mathrm{dom}(f) \mid f \in \mathcal{C}\} \subseteq A$ che estende ogni $f \in \mathcal{C}$. Per l'ipotesi, possiamo prendere allora un elemento massimale $F : X \to B$. Se $X = A$ abbiamo $|A| \leq |B|$. Se F è suriettiva, abbiamo una bigezione tra il sottoinsieme $X \subseteq A$ e B, e quindi $|B| \leq |A|$.

Per completare la dimostrazione, mostriamo che la terza eventualità, cioè che $X \neq A$ e $\mathrm{imm}(F) \neq B$, non può accadere. In questo caso infatti potremmo prendere un elemento $a \in A \setminus X$, un elemento $b \in B \setminus \mathrm{imm}(F)$, e considerare la funzione $G : X \cup \{a\} \to B$ che estende F ponendo $G(a) = b$. Chiaramente G è iniettiva e $G \succ F$, contro la massimalità di F. $\square$

Vediamo una prima conseguenza della confrontabilità delle cardinalità.

Proposizione 3.2 (ZF). *Se vale la confrontabilità: "Per tutti gli insiemi A, B si ha $|A| \leq |B|$ o $|B| \leq |A|$", allora per ogni X infinito si ha $|\mathbb{N}| \leq |X|$.*[5]

Dim. Vista l'ipotesi, basta verificare che $|X| < |\mathbb{N}|$ è impossibile. Supponiamo per assurdo che esista $f : X \to \mathbb{N}$ iniettiva; chiaramente $|X| = |\mathrm{imm}(f)|$. Se $\mathrm{imm}(f) \subseteq \mathbb{N}$ fosse infinito allora avremmo che $|\mathrm{imm}(f)| = |\mathbb{N}|$, contro l'assunzione $|\mathbb{N}| \neq |X|$.[6] Allora $\mathrm{imm}(f)$ deve essere finito, ma anche questo non è possibile perché un insieme finito non può essere equipotente a $\mathbb{N}$.[7] $\square$

Esercizio 3.3. Senza usare né l'assioma di scelta, né la confrontabilità, mostrare direttamente che: "Lemma di Zorn" $\Rightarrow$ "per ogni X infinito si ha $|\mathbb{N}| \leq |X|$".

Proposizione 3.4 (ZF). *Sia X un insieme infinito e supponiamo che $|X \times X| = |X|$. Se $|A_1| = \ldots = |A_k| = |X|$ allora anche $|A_1 \cup \ldots \cup A_k| = |X|$.*

Proof. Per ogni $i = 1, \ldots, k$, fissiamo una bigezione $f_i : A_i \to X$, e definiamo la funzione $F : A_1 \cup \ldots \cup A_k \to X \times \{1, \ldots, k\}$ ponendo $F(a) = (f_s(a), s)$ dove $s = \min\{i \mid x \in A_i\}$. Chiaramente F è iniettiva. Inoltre banalmente $|\{1, \ldots, k\}| \leq |X|$ perché X è infinito. La tesi si ottiene applicando il Teorema di Cantor-Bernstein a partire dalle seguenti disuguaglianze:

$$|X| = |A_1| \leq |A_1 \cup \ldots \cup A_k| \leq |X \times \{1, \ldots, k\}| \leq |X \times X| = |X|.$$

$\square$

Teorema 3.5 (ZF). *Lemma di Zorn $\Rightarrow$ $|A \times A|$ per ogni insieme infinito A.*

Dim. Visto che banalmente $|A| \leq |A \times A|$, per il Teorema di Cantor-Bernstein basta mostrare l'esistenza di una funzione iniettiva $f : A \times A \to A$. Consideriamo l'insieme parzialmente ordinato $(\mathcal{F}, \preceq)$ dove

$$\mathcal{F} = \{f : X \times X \to X \mid X \subseteq A \text{ infinito, } f \text{ iniettiva}\}$$

e dove $f \preceq g$ se e solo se $f \subseteq g$, cioè g è una estensione di f. Notiamo anzitutto che $\mathcal{F} \neq \emptyset$. Infatti dalla Proposizione 3.2 sappiamo che esiste una funzione iniettiva $\theta : \mathbb{N} \to A$, e quindi un sottoinsieme $X = \mathrm{imm}(\theta) \subseteq A$ con $|X| = |\mathbb{N}|$. Senza usare AC, abbiamo visto $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$. Allora abbiamo che $|X \times X| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}| = |X|$; più esplicitamente, se $\psi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ è una bigezione, allora la funzione $f : X \times X \to X$ dove $f(\theta(n), \theta(m)) = \theta(\psi(n, m))$ è una bigezione, e quindi appartiene ad $\mathcal{F}$.

Procedendo in modo analogo alla dimostrazione del Teorema 3.1 di sopra, è facile verificare che ogni catena $\mathcal{C} \subseteq \mathcal{F}$ ha come maggiorante l'unione $\bigcup_{f \in \mathcal{C}} f$. Per il Lemma di Zorn esiste allora un elemento massimale $F : X \times X \to X$. Notiamo che per Cantor-Bernstein deve essere $|X \times X| = |X|$.

[5] Ricordiamo che avevamo già dimostrato questa proprietà degli insiemi infiniti usando però l'assioma di scelta (vedi Teorema **??**).

[6] Qui abbiamo usato la Proposizione **??**, che era stata dimostrata senza usare l'assioma di scelta.

[7] Qui abbiamo usato la Proposizione **??**, con la quale abbiamo mostrato, senza usare l'assioma di scelta, che $\mathbb{N}$ non è equipotente ad alcun insieme finito

Visto che $X \subseteq A$, banalmente $|X| \leq |A|$. Se $|X| = |A|$, allora $|A \times A| = |X \times X| = |X| = |A|$, come voluto. Per completare la dimostrazione, resta da vedere che $|X| < |A|$ è impossibile.

Supponiamo allora per assurdo che $|X| < |A|$, e consideriamo il complemento $A \setminus X$. La disuguaglianza $|A \setminus X| \leq |X|$ non può valere, altrimenti si avrebbe

$$|A| = |X \cup (A \setminus X)| \leq |(X \times \{1\}) \cup (X \cup \{2\})| = |X \times \{1, 2\}| \leq |X \times X| = |X| < |A|.$$

Allora, per la confrontabilità (che segue dal Lemma di Zorn, vedi Teorema 3.1) deve valere la disuguaglianza $|X| < |A \setminus X|$. Possiamo allora prendere un sottoinsieme $X' \subseteq A \setminus X$ con $|X'| = |X|$. Il nostro scopo è adesso quello di estendere F ad una funzione iniettiva $G : (X \cup X') \times (X \cup X') \to X \cup X'$, contraddicendo così la massimalità di F.

Notiamo che $(X \cup X') \times (X \cup X')$ è dato dall'unione disgiunta di $(X \times X)$ con $Y = (X \times X') \cup (X' \cup X) \cup (X' \times X')$. Adesso, $|X \times X'| = |X' \times X| = |X' \times X'| = |X \times X| = |X|$ e quindi $|X| \leq |Y| = |X \times \{1, 2, 3\}| \leq |X \times X| = |X|$. Possiamo prendere allora una bigezione $F' : Y \to X'$, e definire $G = F \cup F'$. È immediato verificare che $G : (X \cup X') \times (X \cup X') \to X \cup X'$ è iniettiva, in quanto unione disgiunta di due funzioni iniettive. $\square$