ELEMENTI DI TEORIA DEGLI INSIEMI

Diamo per note le nozioni fondamentali di teoria degli insiemi, come:

- la nozione di appartenenza di un elemento a un insieme ($x \in A$),
- la nozione di *insieme vuoto* (indicato con $\emptyset$) e la sua unicità,
- la nozione di inclusione di un insieme in un altro ($A \subset B$, $A \subseteq B$),
- le operazioni di unione ($A \cup B$) e intersezione ($A \cap B$), le proprietà commutativa e associativa di ciascuna di esse, la proprietà distributiva dell'una rispetto all'altra,
- la nozione di complementare di un insieme rispetto a un insieme ambiente dato (${}^cA$),
- le nozioni di differenza insiemistica ($A \setminus B$, $B \setminus A$) e di differenza simmetrica ($A \triangle B$) di due insiemi,
- le formule di de Morgan:

$$ {}^c(A \cup B) = {}^cA \cap {}^cB \ , \qquad {}^c(A \cap B) = {}^cA \cup {}^cB \ . $$

1. Prodotto cartesiano di due insiemi

Siano a, b due elementi, non necessariamente distinti tra loro. Quando si parla di *coppia ordinata* (a, b) si vuole specificare la posizione dei due termini nella coppia, e cioè che essa consiste di un *primo termine* a e di un *secondo termine* b. Per questo motivo, la coppia (a, b) è un entità del tutto diversa dall'insieme $\{a, b\}$.

Due coppie (a, b) e (a', b') sono uguali se e solo se sono uguali a due a due i termini corrispondenti. In formule:

$$ (a, b) = (a', b') \iff a = a' \text{ e } b = b' \ . $$

In particolare, $(a, b) \neq (b, a)$ se $a \neq b$.

Per poter accogliere una simile definizione nella teoria, una coppia va definita come un insieme. La definizione più comunemente adottata è la seguente:

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

E' un semplice esercizio verificare che effettivamente

$$ \big\{\{a, b\}, \{a\}\big\} = \big\{\{a', b'\}, \{a'\}\big\} \iff a = a' \text{ e } b = b' \ . $$

Siano ora A e B due insiemi. Si chiama *prodotto cartesiano* di A e B l'insieme $A \times B$ delle coppie ordinate (a, b), al variare di a in A e di b in B:

$$ A \times B = \big\{(a, b) : a \in A \ , \ b \in B\big\} \ . $$

Si osservi che, se $A \neq B$,

$$ A \times B \neq B \times A \ . $$

Il prodotto cartesiano $A \times A$ di un insieme A con se stesso si indica anche con A^2. Si chiama *diagonale* di A^2 l'insieme

$$\mathrm{diag}\,(A^2) = \big\{(a,a) : a \in A\big\}\ .$$

2. Relazioni

Si chiama *relazione* tra elementi di un insieme A ed elementi di un insieme B un qualunque sottoinsieme $\mathcal{R}$ del prodotto cartesiano $A \times B$.

Se la coppia $(a,b) \in A \times B$ appartiene a $\mathcal{R}$, si dice che a *è in relazione con* b; si usa la notazione[1] $a\mathcal{R}b$.

Esempi.

(1) Con $A = \{1, 2, \ldots, 100\}$ e $B = \{1, 2, \ldots, 200\}$ (l'insieme dei numeri naturali), poniamo la relazione

$$a\mathcal{R}b \iff M.C.D.(a,b) > 1\ .$$

Una scrittura equivalente è

$$\mathcal{R} = \big\{(a,b) \in A \times B : M.C.D.(a,b) > 1\big\}\ .$$

(2) Con $A = B = \mathbb{N}$ (l'insieme dei numeri naturali), l'insieme

$$\big\{(m,n) \in \mathbb{N}^2 : m \le n\big\}$$

fornisce la relazione $\le$.

3. Relazioni di equivalenza

Una relazione $\mathcal{R}$ tra elementi di uno stesso insieme A si dice una *relazione di equivalenza su* A se soddisfa le seguenti proprietà:

- *riflessiva*: $\forall\, a \in A\ ,\ a\mathcal{R}a$;
- *simmetrica*: $a\mathcal{R}b \Rightarrow b\mathcal{R}a$;
- *transitiva*: $a\mathcal{R}b$ e $b\mathcal{R}c \Rightarrow a\mathcal{R}c$.

Simboli comunemente usati per relazioni di equivalenza sono: $\sim$, $\simeq$, $\approx$, e simili.

Sia dunque $\sim$ una relazione di equivalenza. Fissato $a \in A$, si chiama *classe di equivalenza di* a *modulo* $\sim$ l'insieme

$$C_a = \{b \in A : b \sim a\}\ .$$

Lemma 3.1. *Se $a \sim a'$, allora $C_a = C_{a'}$. Se $a \not\sim a'$, allora $C_a \cap C_{a'} = \emptyset$.*

Dimostrazione. Supponiamo $a \sim a'$ e $b \in C_a$. Allora $b \sim a$ e per la proprietà transitiva $b \sim a'$. Dunque $b \in C_{a'}$. Questo prova che $C_a \subseteq C_{a'}$. Allo stesso modo si dimostra che $C_{a'} \subseteq C_a$. Dalla doppia inclusione segue che $C_a = C_{a'}$.

Dimostriamo ora che

$$C_a \cap C_{a'} \neq \emptyset \Longrightarrow a \sim a'\ . \tag{3.1}$$

[1] Invece di lettere, come $\mathcal{R}$, è comune usare simboli come $\sim$, $\le$, ecc., secondo i casi (v. seguito).

Infatti, sia $b \in C_a \cap C_{a'}$. Allora $b \sim a$ e $b \sim a'$. Per le proprietà simmetrica e transitiva, $a \sim a'$.

Vale allora la contronominale della (3.1), cioè

$$a \not\sim a' \Longrightarrow C_a \cap C_{a'} = \emptyset \ . \qquad \square$$

Si chiama *partizione* di A una famiglia di sottoinsiemi non vuoti di A che siano a due a due disgiunti e la cui unione sia tutto A.

Teorema 3.2. *Le classi di equivalenza distinte modulo $\sim$ costituiscono una partizione di A. Viceversa, data una partizione di A, esiste un'unica relazione di equivalenza le cui classi di equivalenza siano gli elementi della partizione stessa.*

Dimostrazione. Il Lemma 3.1 dimostra che le classi di equivalenza distinte modulo $\sim$ sono disgiunte. Inoltre, ogni $a \in A$ appartiene alla classe C_a per la proprietà riflessiva. Quindi l'unione delle classi distinte è tutto A.

Per il viceversa, sia $\{A_i : i \in I\}$ una partizione di A, cioè con $\bigcup_{i\in I} A_i = A$, $A_i \neq \emptyset$ per ogni $i \in I$, e $A_i \cap A_{i'} = \emptyset$ se $i \neq i'$. Si verifica facilmente che la relazione

$$x\mathcal{R}y \iff \exists\, i \in I \text{ tale che } x, y \in A_i$$

è di equivalenza e che le sue classi di equivalenza sono gli A_i. $\square$

L'insieme delle classi di equivalenza,

$$A/\!\sim \ = \{C_a : a \in A\}$$

si chiama l'*insieme quoziente* di A modulo $\sim$.

4. Relazioni d'ordine

Una relazione $\mathcal{R}$ tra elementi di uno stesso insieme A si chiama una *relazione d'ordine*, o un *ordinamento*, su A se valgono le seguenti proprietà:

- *riflessiva*: $\forall\, a \in A\ ,\ a\mathcal{R}a$;
- *antisimmetrica*: $a\mathcal{R}b$ e $b\mathcal{R}a \Rightarrow a = b$;
- *transitiva*: $a\mathcal{R}b$ e $b\mathcal{R}c \Rightarrow a\mathcal{R}c$.

Simboli comunemente usati per relazioni di equivalenza sono: $\leq$, $\preceq$, e simili. I corrispondenti simboli $<$, $\prec$, ecc. si usano allora per indicare che

$$a\mathcal{R}b \ \text{ e } \ a \neq b \ .$$

Un ordinamento si dice *totale* se inoltre vale la proprietà:

- *tricotomia*: $\forall\, a, b \in A\ ,\ a\mathcal{R}b$ o $b\mathcal{R}a$.

Altrimenti si dice che l'ordinamento è parziale.

Esempi.

(1) La relazione $\leq$ su $\mathbb{R}$ è un ordinamento totale.
(2) La relazione $\subseteq$ su $\mathcal{P}(X)$ (l'insieme dei sottoinsiemi di un insieme X) è un ordinamento, solo parziale se X ha almeno due elementi.

(3) La relazione $\mathcal{R}$ su $\mathbb{N}$ data da

$$m\mathcal{R}n \iff m|n$$

è un ordinamento parziale.

(4) Se $\mathcal{R}$ è un ordinamento su A, la *relazione inversa*

$$\mathcal{R}^{-1} = \big\{(a,b) : (b,a) \in \mathcal{R}\big\}$$

è pure un ordinamento.

(5) Se $\mathcal{R}$ è un ordinamento su A e $B \subseteq A$, la *restrizione* di $\mathcal{R}$ a B,

$$\mathcal{R}_{|_B} = \mathcal{R} \cap B^2$$

è un ordinamento su B. Se $\mathcal{R}_{|_B}$ è un ordinamento totale su B, B si dice una *catena* di A.

Uno stesso insieme può ammettere più ordinamenti. E' perciò corretto dire che un *insieme ordinato* è una coppia $(A, \leq)$, dove A è un insieme e $\leq$ un ordinamento su di esso.

5. Funzioni

Una relazione $\mathcal{R} \subseteq A \times B$ si dice una *funzione* (o anche *applicazione*, o *mappa*, o *trasformazione*) *di A in B* se vale la seguente proprietà:

- $\forall\, a \in A$, esiste un unico $b \in B$ tale che $a\mathcal{R}b$.

Si scrive abitualmente $\mathcal{R}(a) = b$ invece di $(a,b) \in \mathcal{R}$. Una funzione $\mathcal{R}$ di A in B si indica nella forma

$$\mathcal{R} : A \longrightarrow B\ .$$

Le seguenti definizioni e notazioni sono standard:

- A si chiama il *dominio* di $\mathcal{R}$ e B il suo *codominio*;
- dato $A' \subset A$, la *restrizione* di $\mathcal{R}$ ad A' è definita da $\mathcal{R}_{|_{A'}} = \mathcal{R} \cap (A' \times B)$;
- l'insieme
$$\operatorname{im}\mathcal{R} = \big\{b \in B : \exists\, a \in A \text{ tale che } \mathcal{R}(a) = b\big\} \subseteq B$$
si chiama l'*insieme immagine*, o anche solo *immagine*, di $\mathcal{R}$;
- dato $A' \subseteq A$, si chiama *immagine di A' secondo $\mathcal{R}$* l'insieme
$$\mathcal{R}(A') = \big\{b \in B : \exists\, a \in A' \text{ tale che } \mathcal{R}(a) = b\big\} = \operatorname{im}\mathcal{R}_{|_{A'}}\ .$$
- dato $B' \subseteq B$, si chiama *controimmagine di B' secondo $\mathcal{R}$* l'insieme
$$\mathcal{R}^{-1}(B') = \big\{a \in A : \mathcal{R}(a) \in B'\big\}\ .$$
- $\mathcal{R}$ si dice *suriettiva* se $\operatorname{im}\mathcal{R} = B$;
- $\mathcal{R}$ si dice *iniettiva* se
$$a, a' \in A \text{ e } a \neq a' \Longrightarrow \mathcal{R}(a) \neq \mathcal{R}(a')\ ;$$
- $\mathcal{R}$ si dice *biiettiva* o *biunivoca*, o anche *corrispondenza biunivoca*, se è iniettiva e suriettiva;
- se $\mathcal{R}$ è biiettiva, $\mathcal{R}^{-1} \subseteq B \times A$ è pure una funzione, detta *funzione inversa* di $\mathcal{R}$;

- se $\mathcal{R} : A \longrightarrow B$ e $\mathcal{S} : B \longrightarrow C$, la *funzione composta* $\mathcal{S} \circ \mathcal{R} : A \longrightarrow C$ è definita da
$$\mathcal{S} \circ \mathcal{R}(a) = \mathcal{S}\big(\mathcal{R}(a)\big) \ , \quad \forall\, a \in A \ ;$$
- la diagonale di A^2 è una funzione, detta *funzione identica* di un insieme A, e indicata con $\iota_A : A \longrightarrow A$.

Osservazioni.

(1) Se una funzione $\mathcal{R}$ non è suriettiva e $B' = \operatorname{im}\mathcal{R}$, allora $\mathcal{R} \subseteq A \times B'$, e dunque $\mathcal{R}$ definisce una funzione suriettiva di A su B'. Tuttavia è bene considerare $\mathcal{R} : A \to B$ e $\mathcal{R} : A \to B'$ come funzioni diverse. Per tener conto di ciò in modo formalmente corretto, bisogna dire più precisamente che una funzione da A a B è *una terna* $(A, B, \mathcal{R})$, con $\mathcal{R}$ soddisfacente la proprietà a inizio paragrafo.

(2) Se A è l'insieme vuoto, la relazione $\mathcal{R} = \emptyset$ è una funzione. Infatti ogni condizione della forma "$\forall\, a \in \emptyset,\ P(a)$" è verificata.

6. Prodotto cartesiano di più insiemi

Dati tre insiemi A, B, C, si possono costruire i prodotti cartesiani $(A \times B) \times C$ e $A \times (B \times C)$, costituiti rispettivamente dagli elementi $\big((a, b), c\big)$ e $\big(a, (b, c)\big)$, al variare di $a \in A$, $b \in B$, $c \in C$. Essi sono dunque insiemi diversi tra loro.

Ci interessa invece definire, più semplicemente, il prodotto cartesiano $A \times B \times C$ come l'insieme delle "terne" (a, b, c), con $a \in A$, $b \in B$, $c \in C$. Ma dobbiamo innanzitutto definire cosa sono le terne.

Avendo a disposizione la nozione di funzione, possiamo dare la seguente definizione:

- *Siano A, B, C tre insiemi. Il prodotto cartesiano $A \times B \times C$ è l'insieme delle funzioni*
$$f : \{1, 2, 3\} \longrightarrow A \cup B \cup C$$
tali che $f(1) \in A$, $f(2) \in B$, $f(3) \in C$.

Una terna è dunque una funzione f con le proprietà suddette.

Questa definizione può essere adattata anche a un numero maggiore di insiemi, finito o infinito[2], nel modo seguente.

Sia I un insieme non vuoto di indici, introdotto per parametrizzare una famiglia di insiemi
$$\mathcal{A} = \{A_i : i \in I\} \ .$$

- *Il prodotto cartesiano $\prod_{i \in I} A_i$ è l'insieme delle funzioni*
$$f : I \longrightarrow \bigcup_{i \in I} A_i$$
tali che $f(i) \in A_i$ per ogni $i \in I$.

[2]Ma non al prodotto di due insiemi. Perché?

E' un fatto ovvio che se uno degli insiemi A_i è vuoto, anche il prodotto cartesiano è vuoto, perché la condizione $f(i) \in A_i$ non può essere realizzata per quel particolare i.

Viceversa, non è per nulla ovvio che se nessun A_i è vuoto, allora $\prod_{i\in I} A_i$ è non vuoto. Questa affermazione è in effetti *indipendente* dagli assiomi della teoria degli insiemi comunemente adottatti (teoria di Zermelo-Fraenkel, o ZF). Pertanto può essere indifferentemente accettata per vera oppure no, dando luogo a due teorie degli insiemi diverse, una più ampia e l'altra più ristretta. Nella matematica moderna essa viene comunemente accettata, come assioma aggiuntivo, detto *Assioma della scelta*.

Le seguenti sono formulazioni equivalenti dell'Assioma della scelta.

- Il prodotto cartesiano di una famiglia non vuota di insiemi non vuoti è non vuoto.
- Data una famiglia $\{A_i : i \in I\}$ di insiemi non vuoti a due a due disgiunti, esiste un sottoinsieme B di $\bigcup_{i\in I} A_i$ tale che, per ogni $i \in I$, $B \cap A_i$ contenga un unico elemento.

La seconda formulazione giustifica il nome di "Assioma della scelta": è possibile "scegliere" simultaneamente un elemento da ciascun A_i.

Se tutti gli A_i sono uguali tra loro (chiamiamo allora A quest'unico insieme), il prodotto cartesiano $\prod_{i\in I} A$ è l'insieme di tutte funzioni $f : I \longrightarrow A$. Esso viene indicato con A^I.

Se I è finito, tipicamente $I = \{1, 2, \dots, n\}$, si usa la notazione A^n anziché $A^{\{1,\dots,n\}}$, e i suoi elementi sono le *n-uple* di elementi di A, indicate abitualmente come $(a_1, a_2, \dots, a_n)$.

Se $I = \mathbb{N}$, gli elementi di $A^{\mathbb{N}}$ si chiamano *successioni* di elementi di A, abitualmente indicate come $(a_0, a_1, \dots, a_n, \dots)$, oppure come $(a_n)_{n\in\mathbb{N}}$.

7. Cardinalità di insiemi

- *Si dice che un insieme A ha la stessa* cardinalità*, o* potenza*, di un insieme B se esiste una funzione biiettiva di A in B.*

Si dice anche che A è *equipotente* a B.

Si vede facilmente che:

- un insieme A è equipotente a se stesso (perché ι_A è biiettiva);
- se A è equipotente a B, B è equipotente ad A (perché se $f : A \to B$ è biiettiva, anche $f^{-1} : B \to A$ lo è);
- se A è equipotente a B e B è equipotente a C, allora A è equipotente a C (perché se $f : A \to B$ e $g : B \to C$ sono biiettive, allora $g \circ f : A \to C$ è biiettiva).

La "relazione" di equipotenza gode dunque delle proprietà riflessiva, simmetrica e transitiva che caratterizzano le relazioni di equivalenza. Ma su quale insieme è definita la relazione?

Vorremmo poter prendere "l'insieme di tutti gli insiemi", ma così facendo andremmo incontro a seri paradossi. Accontentiamoci dunque di affermare che su una qualunque famiglia di insiemi $\mathcal{A} = \{A_i\}_{i\in I}$ l'equipotenza (che indichiamo con $\sim$) è in effetti una relazione di equivalenza.

Otteniamo dunque un insieme quoziente $\mathcal{A}/\!\sim$. Chiamiamo *cardinalità* i suoi elementi.

L'idea intuitiva dietro queste nozioni è che due insiemi sono equipotenti se "sono ugualmente numerosi". Questa intuizione è corretta per insiemi finiti: un insieme con 37 elementi può essere posto in corrispondenza biunivoca solo con un altro insieme di 37 elementi. Per

insiemi infiniti la questione è molto più delicata, ed è per questo motivo che la trattazione deve essere particolarmente accurata sul piano formale. Trasferire a insiemi infiniti la nostra prima intuizione porta facilmente a errori.

Una volta stabilita la nozione di equipotenza, vogliamo ora dire che certi insiemi sono "meno numerosi di altri". Stabiliamo allora una relazione $\mathcal{R}$ su $\mathcal{A}$ di "minore numerosità" nel modo seguente.

Siano $A, A' \in \mathcal{A}$; diciamo che $A \mathcal{R} A'$ se e solo se esiste $f : A \to A'$ iniettiva.

La nostra intuizione con insiemi finiti ci dice che se A ha n elementi e A' ha n' elementi, esiste una funzione iniettiva di A in A' se e solo se $n \leq n'$. Dunque la validità della relazione $A \mathcal{R} A'$ dipende (per insiemi finiti) solo dalla cardinalità di A e A'. Il seguente lemma afferma che ciò è vero per insiemi generici.

Lemma 7.1. *Supponiamo che $A \mathcal{R} A'$, e siano $B, B' \in \mathcal{A}$ con $B \sim A$, $B' \sim A'$. Allora $B \mathcal{R} B'$.*

Dimostrazione. Per ipotesi, esistono:

(1) $f : A \longrightarrow A'$ iniettiva;
(2) $g : B \longrightarrow A$ biiettiva;
(3) $h : B' \longrightarrow A'$ biiettiva.

Consideriamo allora la composizione $h^{-1} \circ f \circ g : B \longrightarrow B'$,

$$B \xrightarrow{g} A \xrightarrow{f} A' \xrightarrow{h^{-1}} B' \ .$$

Essendo una composizione di funzioni iniettive, essa è iniettiva. □

Possiamo allora "passare la relazione $\mathcal{R}$ al quoziente modulo $\sim$", per definire una relazione sull'insieme quoziente.

Indichiamo con C, C' due classi di equivalenza (cardinalità).

- *Diciamo che $C \preceq C'$ se e solo se, presi $A \in C$ e $A' \in C'$, si ha $A \mathcal{R} A'$.*

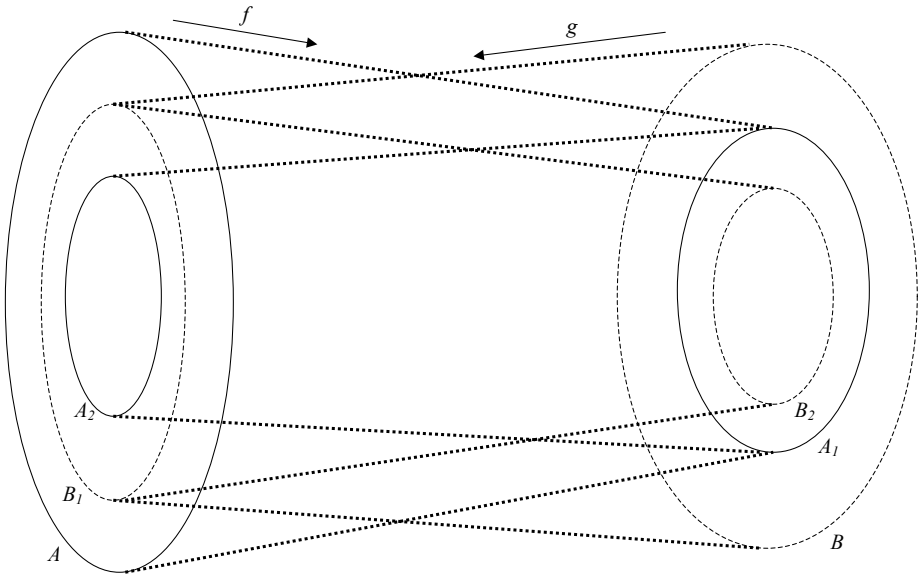
Il Lemma 7.1 ci assicura che questa è una *buona definizione*, ossia che la conclusione $A \mathcal{R} A'$ non dipende dalla scelta di A e A' come rappresentanti di C e C' rispettivamente.

Vogliamo vedere che $\preceq$ è una relazione d'ordine sull'insieme delle cardinalità. Le proprietà riflessiva e transitiva sono facili da verificare. Dimostrare la proprietà antisimmetrica vuol dire dimostrare il seguente teorema.

Teorema 7.2. (Teorema di Cantor-Bernstein). *Siano A, B due insiemi, e supponiamo che esistano due funzioni $f : A \to B$ e $g : B \to A$ iniettive. Allora A e B sono equipotenti.*

Dimostrazione. Sia $A_1 = f(A) \subseteq B$. Allora $f : A \to A_1$ è biiettiva, per cui $A \sim A_1$. Analogamente, $B \sim B_1 = g(B) \subseteq A$. Ricorsivamente, costruiamo

$$A_{2k} = g(A_{2k-1}) \subseteq A \ , \quad A_{2k+1} = f(A_{2k}) \subseteq B \ , \quad B_{2k} = f(B_{2k-1}) \subseteq B \ , \quad B_{2k+1} = g(B_{2k}) \subseteq A \ .$$



Si prova facilmente per induzione che

$$\begin{aligned} &A \supseteq B_1 \supseteq A_2 \supseteq \cdots \supseteq B_{2k-1} \supseteq A_{2k} \supseteq \cdots \\ &B \supseteq A_1 \supseteq B_2 \supseteq \cdots \supseteq A_{2k-1} \supseteq B_{2k} \supseteq \cdots \end{aligned} \tag{7.1}$$

e che

$$A_n \sim A \ , \qquad B_n \sim B \ , \qquad \forall\, n \ .$$

E' dunque sufficiente dimostrare che $A \sim B_1$.

Per la prima catena di inclusioni nella (7.1),

$$\bigcap_{k>0} A_{2k} = \bigcap_{k>0} B_{2k+1} \ .$$

Se indichiamo con C questo sottoinsieme di A, abbiamo

$$A \setminus C = (A \setminus B_1) \cup (B_1 \setminus A_2) \cup \cdots (A_{2k} \setminus B_{2k+1}) \cup (B_{2k+1} \setminus A_{2k+2}) \cup \cdots \ ,$$

ossia (ponendo $A_0 = A$ a secondo membro)

$$A = \Big(\bigcup_{k\geq 0} (A_{2k} \setminus B_{2k+1}) \Big) \cup \Big(\bigcup_{k\geq 0} (B_{2k+1} \setminus A_{2k+2}) \Big) \cup C \ .$$

Allo stesso modo,

$$B_1 = \Big(\bigcup_{k\geq 1} (A_{2k} \setminus B_{2k+1}) \Big) \cup \Big(\bigcup_{k\geq 0} (B_{2k+1} \setminus A_{2k+2}) \Big) \cup C \ .$$

In entrambi i casi, tutti gli insiemi a secondo membro sono disgiunti a due a due.

Per dimostrare che $A \sim B_1$ è dunque sufficiente dimostrare l'esistenza di una applicazione biiettiva

$$h : \bigcup_{k\geq 0}(A_{2k} \setminus B_{2k+1}) \longrightarrow \bigcup_{k\geq 1}(A_{2k} \setminus B_{2k+1}) \ .$$

Infatti, una volta ottenuta una tale funzione h, si può costruire la funzione $H : A \to B_1$ così definita:

$$\begin{cases} H(x) = h(x) & \text{se } x \in \bigcup_{k\geq 0}(A_{2k} \setminus B_{2k+1}) \ , \\ H(x) = x & \text{se } x \in \Big(\bigcup_{k\geq 0}(B_{2k+1} \setminus A_{2k+2})\Big) \cup C \ . \end{cases}$$

E' facile allora dimostrare che H è biiettiva.

Per costruire h, osserviamo che $g \circ f$ applica A_{2k} biiettivamente su A_{2k+2} e B_{2k+1} biiettivamente su B_{2k+3}. Scomponendo

$$A_{2k} = B_{2k+1} \cup (A_{2k} \setminus B_{2k+1})$$
$$A_{2k+2} = B_{2k+3} \cup (A_{2k+2} \setminus B_{2k+3}) \ ,$$

si conclude che $g \circ f$ applica $A_{2k} \setminus B_{2k+1}$ biiettivamente su $A_{2k+2} \setminus B_{2k+3}$. Basta allora definire h come la restrizione di $g \circ f$ a $\bigcup_{k\geq 0}(A_{2k} \setminus B_{2k+1})$. □

Fin qui abbiamo dimostrato che la relazione $\preceq$ tra cardinalità è un ordinamento, ma non che è totale. Come vedremo, si arriva a questa conclusione facendo uso dell'Assioma della scelta.

8. Cardinalità di $\mathcal{P}(A)$

L'insieme $\mathcal{P}(A)$ delle *parti di* A è l'insieme di tutti i sottoinsiemi di A. Dimostriamo due proprietà della sua cardinalità:

Teorema 8.1. *Valgono le seguenti relazioni:*

(i) $\operatorname{card} \mathcal{P}(A) = \operatorname{card} \{0,1\}^A$*;*
(ii) $\operatorname{card} \mathcal{P}(A) \succ \operatorname{card} A$*.*

Dimostrazione. Per dimostrare la (i), costruiamo la funzione $\Phi : \mathcal{P}(A) \to \{0,1\}^A$ così definita: dato $A' \subseteq A$, $\Phi(A') = \chi_{A'}$, la *funzione caratteristica di* A', tale che

$$\chi_{A'}(a) = \begin{cases} 1 & \text{se } a \in A' \\ 0 & \text{se } a \notin A' \ . \end{cases}$$

Si verifica facilmente che Φ è iniettiva. Per la suriettività, basta osservare che ogni funzione f da A in $\{0,1\}$ è la funzione caratteristica di $f^{-1}\big(\{1\}\big)$.

Per dimostrare la (ii) bisogna provare che da A a $\mathcal{P}(A)$ esistono applicazioni iniettive, ma nessuna che sia biiettiva. E' evidente che la funzione $f(a) = \{a\}$ è iniettiva da A in $\mathcal{P}(A)$. Supponiamo per assurdo che $g : A \to \mathcal{P}(A)$ sia suriettiva. Poniamo

$$A' = \{a \in A : a \notin g(a)\} \ .$$

Allora esiste a_0 tale che $A' = g(a_0)$. Ci sono due casi, $a_0 \in A'$ e $a_0 \notin A'$. Se $a_0 \in A'$, allora $a_0 \notin g(a_0) = A'$, il che è assurdo. Se $a_0 \notin A'$, allora $a_0 \in g(a) = A'$, che è ancora assurdo. □

Questo teorema mostra che ci sono insiemi infiniti con cardinalità diverse. Per esempio,

$$\operatorname{card}\mathbb{N} \prec \operatorname{card}\mathcal{P}(\mathbb{N}) \prec \operatorname{card}\mathcal{P}\big(\mathcal{P}(\mathbb{N})\big) \prec \cdots$$

9. Il Lemma di Zorn

Il Lemma di Zorn è un enunciato equivalente all'Assioma della scelta. Di esso viene fatto frequente uso in vari campi della matematica. Per poterlo enunciare, dobbiamo premettere alcune nozioni relative a insiemi ordinati.

Sia $(A, \leq)$ un insieme ordinato. Un elemento $m \in A$ si dice *massimo di* A se, per ogni $a \in A$, $a \leq m$.

In modo analogo si definisce il *minimo* di un insieme ordinato.

Lemma 9.1. *Se un insieme ordinato ha un massimo (risp. minimo), esso è unico.*

Dimostrazione. Siano m e m' due massimi. Allora $m' \leq m$ e $m \leq m'$, e, per la proprietà antisimemtrica, $m = m'$. Analogamente per i minimi. □

Le nozioni di massimo e di minimo si applicano ovviamente anche a sottoinsiemi di un insieme ordinato.

Un elemento $m \in A$ si dice *massimale* se non esiste nessun elemento $a \in A$ tale che $m < a$. In modo analogo si definisce un elemento *minimale* di A.

Per un insieme A totalmente ordinato, le nozioni di elemento massimo ed elemento massimale (risp. elemento minimo ed elemento minimale) coincidono. Se l'ordinamento non è totale, il massimo è un elemento massimale, ma non viceversa. Un insieme parzialmente ordinato può possedere più elementi massimali (risp. minimali).

Sia ora A' un sottoinsieme di A. Un elemento $a \in A$ si dice un *maggiorante* di A' se, per ogni $a' \in A'$, $a' \leq a$. In modo analogo di definisce un *minorante* di A'.

Se l'insieme dei maggioranti di A' ha un minimo, questo si chiama l'*estremo superiore di* A'. L'*estremo inferiore* di A' si definisce come il massimo dei minoranti. Per il Lemma 9.1, l'estremo superiore (risp. inferiore), se c'è, è unico.

I simboli max, min, sup, inf indicano rispettivamente massimo, minimo, estremo superiore ed estremo inferiore di un sottoinsieme di un insieme ordinato.

Si noti che

- un maggiorante a di A' in A appartiene ad A' se e solo se $a = \max A'$;
- se $A' \subseteq A$ ha massimo, allora $\max A' = \sup A'$;
- un elemento $a \in A$ è massimale se e solo se $A' = \{a\}$ non ha maggioranti all'infuori di a stesso.

Esempi.

(1) Si consideri $\mathbb{N}$ ordinato dalla relazione $m \preceq n$ se $m \big| n$. Allora $\min \mathbb{N} = 1$ e $\max \mathbb{N} = 0$. Se prendiamo invece $A = \mathbb{N} \setminus \{0, 1\}$ con l'ordinamento indotto, A non ammette né minimo né massimo, i numeri primi sono gli elementi minimali, e non ci sono elementi massimali.

(2) Nell'insieme $\mathbb{Q}$ dei numeri razionali, dotato dell'ordinamento (totale) abituale, si consideri l'insieme $A' = \{m/n : (m/n)^2 < 2\}$. Si dimostri che l'insieme dei maggioranti di A' è $\{p/q > 0 : (p/q)^2 > 2\}$ e che tale insieme non ha minimo. Dunque A' ha dei maggioranti in $\mathbb{Q}$, ma non l'estremo superiore.

Il Lemma di Zorn riguarda una classe speciale di insiemi ordinati, detti induttivi, così definiti:

- Un insieme ordinato $(A, \leq)$ si dice *induttivo* se ogni catena (cioè ogni sottoinsieme totalmente ordinato) di A possiede maggioranti.

Si noti che la definizione stessa implica che un insieme induttivo non è vuoto. Infatti la catena vuota deve avere un maggiorante in A.

Teorema 9.2. (Lemma di Zorn). *Sia $(A, \leq)$ un insieme ordinato induttivo. Per ogni $a \in A$ esiste un elemento massimale $m \geq a$.*

Mostriamo ora alcune applicazioni del Lemma di Zorn, rinviandone la dimostrazione al paragrafo successivo. La prima applicazione riguarda l'ordinamento tra cardinalità.

Teorema 9.3. *Dati due insiemi A e B, esiste sempre una funzione iniettiva di A in B o di B in A. Quindi l'ordinamento tra cardinalità è totale.*

Dimostrazione. La conclusione è ovvia se A o B è vuoto (si prenda la funzione vuota). Supponiamo dunque che A e B siano non vuoti.

Indichiamo con X l'insieme delle funzioni biiettive $f : A' \to B'$, dove $A' \subseteq A$, $B' \subseteq B$. Chiaramente X non è vuoto, perché, fissati $a \in A$ e $b \in B$, la funzione $f : \{a\} \to \{b\}$ tale che $f(a) = b$ è biiettiva.

Per dimostrare la tesi, occorre dimostrare l'esistenza di una funzione $f \in X$ che abbia come dominio tutto A, oppure come immagine tutto B. Nel primo caso, allargando il codominio di f da B' a B, otteniamo una funzione iniettiva da A in B; nel secondo caso, facciamo la stessa operazione su $f^{-1} : B \to A'$, ottenendo una funzione iniettiva di B in A.

Su X definiamo il seguente ordinamento:

$$(f : A' \to B') \preceq (g : A'' \to B'') \iff A' \subseteq A'', B' \subseteq B'' \text{ e } f = g_{|_{A'}} ,$$

(in termini puramente insiemistici, $f \subseteq A' \times B'$, $g \subseteq A'' \times B''$; allora $f \preceq g$ se e solo se $f \subseteq g$).

Si verifica facilmente che $\preceq$ è una relazione d'ordine (parziale a meno che A e B non contengano un unico elemento). Mostriamo che $(X, \preceq)$ è induttivo.

Sia $C = \{f_i : A_i \to B_i : i \in I\}$ una catena di X. Poniamo $\bar{A} = \bigcup_{i \in I} A_i$, $\bar{B} = \bigcup_{i \in I} B_i$, e sia $\bar{f} : \bar{A} \to \bar{B}$ la funzione il cui grafico è l'unione dei grafici delle f_i. E' evidente che $f_i \preceq \bar{f}$ per ogni $i \in I$, e dunque $\bar{f}$ è un maggiorante di C in X.

Essendo dunque X induttivo, per il Lemma di Zorn, esso ammette un elemento massimale $f_0 : A' \to B'$. Se A' e B' fossero entrambi sottoinsiemi propri di A e B rispettivamente, potremmo scegliere $\bar{a} \in A \setminus A'$ e $\bar{b} \in B \setminus B'$ e definire $f_1 : A' \cup \{\bar{a}\} \to B' \cup \{\bar{b}\}$ ponendo

$$f_1(a) = \begin{cases} f_0(a) & \text{se } a \in A' \\ \bar{b} & \text{se } a = \bar{a} \ . \end{cases}$$

Avremmo allora $f_1 \in X$ e $f_0 \prec f_1$, in contrasto con l'ipotesi di massimalità di f_0. □

Teorema 9.4. *Ogni insieme ammette un ordinamento totale.*

Dimostrazione. Sia A un insieme, che supponiamo non vuoto[3]. Chiamiamo X l'insieme delle coppie $(A', \leq)$, dove $A' \subseteq A$ e $\leq$ è un ordinamento totale su A'. Su X definiamo la relazione

$$(A', \leq) \preceq (A'', \sqsubseteq) \iff A' \subseteq A'' \text{ e } \sqsubseteq_{|A'} = \leq \ .$$

X non è vuoto perché i sottoinsiemi di A contenenti un unico elemento ammettono un ovvio ordinamento totale. In modo analogo al teorema precedente, si dimostra che $(X, \preceq)$ è induttivo. Per il lemma di Zorn, esiste un elemento massimale $(A', \leq)$. Se fosse $A' \neq A$, potremmo prendere $\bar{a} \in A \setminus A'$ e definire un ordinamento totale su $A' \cup \{\bar{a}\}$ che estenda $\leq$, stabilendo, per es., che $\bar{a}$ sia l'elemento massimo. Questo contrasterebbe con l'ipotesi di massimalità. □

Come abbiamo anticipato, il Lemma di Zorn è equivalente all'Assioma della scelta. La dimostrazione nel prossimo paragrafo mostrerà che, assumendo vero l'Assioma della scelta, si dimostra il Lemma di Zorn. Mostriamo qui che, viceversa, assumendo vero il Lemma di Zorn, si dimostra l'Assioma della scelta.

Teorema 9.5. *Il Lemma di Zorn implica l'Assioma della scelta.*

Dimostrazione. Sia $\{A_i : i \in I\}$ una famiglia non vuota di insiemi non vuoti. Poniamo

$$X = \left\{ B \subset \bigcup_{i \in I} A_i : \forall\, i \in I\,,\, B \cap A_i \text{ contiene al più un elemento} \right\} .$$

Chiaramente X è non vuoto ($\emptyset \in X$). Ordinando X per inclusione, mostriamo che $(X, \subseteq)$ è induttivo. Se $C = \{B_j : j \in J\}$ è una catena, prendiamo $\bar{B} = \bigcup_{j \in J} B_j$. Dobbiamo mostrare che $\bar{B} \in X$. Supponiamo per assurdo che esista $i \in I$ tale che $\bar{B} \cap A_i$ contenga due elementi distinti b_1, b_2. Esisteranno allora j_1, j_2 tali che $b_1 \in B_{j_1}$ e $b_2 \in B_{j_2}$. Siccome C è totalmente ordinato, uno dei due è contenuto nell'altro. Supponiamo che $B_2 \subseteq B_1$, per cui $b_1, b_2 \in B_{j_1}$. Ma allora $b_1, b_2 \in B_{j_1} \cap A_i$. Ma poiché $B_{j_1} \in X$, deve essere $b_1 = b_2$, da cui l'assurdo.

Per il Lemma di Zorn, X ammette un elemento massimale B_0. Mostriamo che per ogni $i \in I$, $B_0 \cap A_i$ contiene un elemento. Se, per assurdo, esistesse i_0 tale che $B_0 \cap A_{i_0} = \emptyset$, scegliendo un elemento $b \in A_{i_0}$, avremmo l'insieme $B_1 = B_0 \cup \{b\} \in X$, strettamente maggiore di B_0, contrariamente all'ipotesi di massimalità. □

10. Dimostrazione del Lemma di Zorn

Scomponiamo la dimostrazione in più passi. Il primo passo consiste nel ridursi a insiemi ordinati induttivi di tipo particolare.

Diciamo che un insieme ordinato non vuoto $(A, \leq)$ è *strettamente induttivo* se ogni catena di A possiede estremo superiore[4].

[3] Se $A = \emptyset$, la relazione $\emptyset$ è un ordinamento totale.

[4] Gli insiemi induttivi introdotti nel paragrafo precedente sono tutti strettamente induttivi.

Lemma 10.1. *Se il Lemma di Zorn vale per insiemi strettamente induttivi, esso vale per insiemi induttivi.*

Dimostrazione. Sia $(A, \leq)$ induttivo. Chiamiamo $\mathcal{C}$ l'insieme delle catene di A, ordinate per inclusione. Allora $(\mathcal{C}, \subseteq)$ è strettamente induttivo. Sia infatti S una catena di $\mathcal{C}$, cioè una famiglia $\{C_i : i \in I\}$ di catene di A totalmente ordinate per inclusione. Allora $\bar{C} = \bigcup_{i\in I} C_i$ è pure una catena di A ed è la minima catena contenente ciascun C_i. Dunque $\bar{C} = \sup S$.

Sia ora $a \in A$, e ci consideri la catena $C_a = \{a\} \in \mathcal{C}$. Per ipotesi, esiste in $\mathcal{C}$ un elemento massimale C_0 con $\{a\} \subseteq C_0$. Siccome A è induttivo, C_0 ammette un maggiorante $\bar{a}$. Poiché C_0 è massimale, deve essere $\bar{a} \in C_0$, altrimenti $C_0 \cup \{\bar{a}\}$ sarebbe un'altra catena contenente propriamente C_0. Dunque $\bar{a} = \max C_0$ ed è un elemento massimale di A. Inoltre $a \leq \bar{a}$. □

Supponiamo allora che $(A, \leq)$ sia un insieme ordinato strettamente induttivo. Il secondo passo della dimostrazione consiste nell'analizzare le funzioni $f : A \to A$ tali che

$$\forall\, a \in A, \quad a \leq f(a)\ . \tag{10.1}$$

Lemma 10.2. *Sia $(A, \leq)$ strettamente induttivo e sia f una funzione di A in sé che soddisfi la proprietà* (10.1)*. Dato $a \in A$, esiste una catena C di A tale che*

(i) $a = \min C$*;*
(ii) C *ha massimo;*
(iii) $f(C) \subseteq C$.

Dimostrazione. Chiamiamo $\mathcal{S}$ l'insieme dei sottoinsiemi $S \subseteq A$ tali che

(1) $a = \min S$;
(2) $f(S) \subseteq S$;
(3) se C è una catena di S, $\sup C \in S$.

Ovviamente $S = \{x \in A : a \leq x\} \in \mathcal{S}$, per cui $\mathcal{S}$ non è vuoto. Sia

$$M = \bigcap_{S\in\mathcal{S}} S\ .$$

Si verifica facilmente che $M \in \mathcal{S}$. Se dimostriamo che M è totalmente ordinato, la tesi è dimostrata con $C = M$.

Diciamo che un elemento $b \in M$ è una *barriera* se

$$b' \in M\ ,\ b' < b \implies f(b') \leq b\ .$$

Vale la proprietà seguente:

(*) *Se b è una barriera, ogni elemento di M è $\leq b$ oppure $\geq f(b)$.*

Per dimostrarla, facciamo vedere che

$$M_b = \{x \in M : x \leq b\} \cup \{x \in M : x \geq f(b)\} = M'_b \cup M''_b$$

è un elemento di $\mathcal{S}$.

Sicuramente $a \in M_b$. Per vedere che $f(M_b) \subseteq M_b$, consideriamo tre casi per $x \in M_b$. Se $x < b$, allora $f(x) \in M'_b$ perché b è una barriera e perché $M \in \mathcal{S}$. Se $x \in M''_b$, allora $f(x) \geq x \geq f(b)$ ed è in M''_b. Il terzo caso, $x = b$, è ovvio.

Sia ora C una catena di M_b. Se $C \subseteq M_b'$, b è un maggiorante di C, e dunque $\sup C \in M_b'$. Se C contiene elementi di M_b'', allora $\sup C \geq f(b)$, è in M, dunque $\sup C \in M_b''$.

Visto dunque che $M_b \in \mathcal{S}$, ne segue che $M \subseteq M_b$, per definizione di M. Ma l'inclusione opposta, $M_b \subseteq M$ è ovvia, per cui $M_b = M$. Questo dimostra (*).

Dimostriamo ora:

(**) *Ogni elemento di M è una barriera.*

Chiamiamo B l'insieme degli elementi barriera di M. Se mostriamo che $B \in \mathcal{S}$, la (**) è dimostrata.

L'elemento a è una barriera, per il semplice fatto che non ci sono elementi di M minori strettamente di a. Se $x \in B$, mostriamo che $f(x) \in B$. Se $y \in M$ e $y < f(x)$, per la (*) si ha $y \leq x$. Ma allora $f(y) \leq x$ se $y < x$, e $f(y) = f(x)$ se $y = x$. In ogni caso, $f(y) \leq f(x)$.

Sia poi C una catena di B, e sia $s = \sup C$. Vogliamo dimostrare che $s \in B$. Se $s = \max C$ non c'è nulla da dimostrare, perché $s \in C$. Supponiamo dunque che C non abbia massimo.

Siccome $B \subseteq M \in \mathcal{S}$, si ha $s \in M$. Prendiamo $x \in M$, $x < s$. Siccome s è il minimo maggiorante di C, x non può essere un maggiorante di C, e dunque neanche di $f(C)$. Esiste dunque $y \in C$ tale che $x \not\geq f(y)$. Siccome y è una barriera, ciò implica, per la (*), che $x \leq y$.

Se $x < y$, allora $f(x) \leq y < s$. Se $x = y$, siccome stiamo supponendo che C non ha massimo, esiste $y' \in C$ con $y < y'$. Ma allora, essendo y' una barriera, $f(x) \leq y' < s$. Abbiamo così dimostrato la (**).

Siano infine $x, y \in M$. Essendo x una barriera, si hanno due casi: o $y \leq x$, oppure $y \geq f(x) \geq x$. In ogni caso essi sono confrontabili. □

Corollario 10.3. *Sia $(A, \leq)$ un insieme ordinato strettamente induttivo e sia $f : A \to A$ tale che $f(a) \geq a$ per ogni $a \in A$. Per ogni $a \in A$ esiste allora un elemento $m \geq a$ tale che $f(m) = m$.*

Dimostrazione. Dato a, sia C la catena costruita nel Lemma 10.2, e sia m il suo massimo. Poiché $f(C) \subseteq C$, $f(m) \in C$, ma essendo $f(m) \geq m$, deve necessariamente essere $f(m) = m$. □

Conclusione della dimostrazione del Lemma di Zorn.

Per ogni $b \in A$, poniamo

$$X_b = \begin{cases} \{b\} & \text{se } b \text{ è massimale} \\ \{x \in A : x > b\} & \text{altrimenti.} \end{cases}$$

Ciascun X_b è non vuoto, e per l'assioma della scelta esiste una funzione $f : A \to \bigcup_{b \in A} X_b$ tale che $f(b) \in X_b$ per ogni $b \in A$. Per il Corollario 10.3, dato $a \in A$, esiste $m \geq a$ tale che $f(m) = m$. Ma ciò equivale a dire che m è massimale.