Lezione 12

Alessandro Ardizzoni

Cardinalità di un insieme

Finora, abbiamo intuitivamente definito un insieme finito come un insieme con un numero finito di elementi. Vogliamo ora rendere più precisa questa idea. Partiamo con la seguente definizione.

Diremo che due insiemi X e Y hanno la stessa cardinalità, e scriveremo $|X| = |Y|$, se esiste una biiezione $X \to Y$.
Il simbolo $|X|$ è detto il numero cardinale dell'insieme X. Lo si indica anche col simbolo $\#X$.

E' facile verificare le seguenti proprietà dove X, Y e Z sono insiemi:

- $|X| = |X|$;
- $|X| = |Y| \Rightarrow |Y| = |X|$;
- $|X| = |Y| \wedge |Y| = |Z| \Rightarrow |X| = |Z|$.

Definiamo ora, per ogni $n \in \mathbb{N}$, l'insieme $I_n := \{1, \ldots, n\}$ assumendo, per convenzione, $I_0 := \{\ \} = \emptyset$.

Vogliamo dimostrare che $|I_m| = |I_n| \Rightarrow m = n$.

Prima servono un paio di risultati.

Lemma

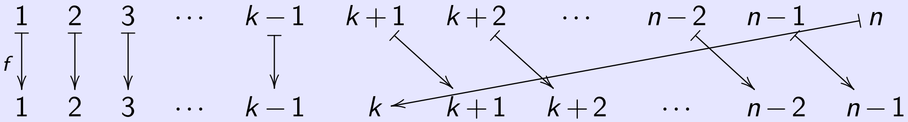
Sia $n \in \mathbb{N}, n \neq 0$. Allora, $\forall k \in I_n$ si ha $|I_n \setminus \{k\}| = |I_{n-1}|$.

Proof.

Dobbiamo costruire una biiezione $\alpha : I_n \setminus \{k\} \to I_{n-1}$.

Se $k = n$, allora $I_n \setminus \{k\} = I_n \setminus \{n\} = I_{n-1}$ e possiamo scegliere $\alpha := \mathrm{Id}_{I_{n-1}}$.

Se $k \neq n$, definiamo $\alpha : I_n \setminus \{k\} \to I_{n-1}$ ponendo $\alpha(n) := k$ e $\alpha(i) = i$ per ogni $i \neq n$.

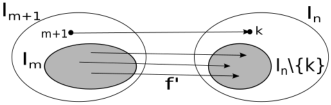


Proposizione (Principio dei cassetti)

Se esiste un'iniezione $f : I_m \to I_n$, allora $m \leq n$.

→ vale a dire che se $m > n$ ⇒ almeno due m devono essere assegnati allo stesso n ⇒ non è iniettiva

<u>DIMOSTRAZIONE</u>. Procediamo per induzione su m.
(PASSO INIZIALE) Se $m = 0$, è chiaro che $\forall n \in \mathbb{N}, m \leq n$.
(PASSO INDUTTIVO) Supponiamo l'enunciato vero per m (ipotesi induttiva) e dimostriamo che vale anche per $m+1$. Sia dunque $f : I_{m+1} \to I_n$ un'iniezione. Posto $k := f(m+1)$, possiamo definire $f' : I_m \to I_n \setminus \{k\}$, $i \mapsto f(i)$. Chiaramente f' è iniettiva (perché lo è f)



NON MI È CHIARA

Notiamo che $k \in I_n$ implica $I_n \neq \emptyset$ e quindi $n \neq 0$.
Per il lemma precedente esiste una biiezione $\alpha : I_n \setminus \{k\} \to I_{n-1}$.
Allora anche $\alpha \circ f' : I_m \to I_{n-1}$ è iniettiva come composizione di iniettive.
Per ipotesi induttiva abbiamo $m \leq n-1$ e dunque $m+1 \leq n$ come voluto.

Possiamo ora dimostrare il risultato voluto.

Corollario

$|I_m| = |I_n| \Rightarrow m = n$

Proof.

Se $|I_m| = |I_n|$ allora c'è una biiezione $f : I_m \to I_n$. Ora f biiettiva $\Rightarrow f$ invertibile $\Rightarrow$ esiste f^{-1}. Allora $f : I_m \to I_n$ e $f^{-1} : I_n \to I_m$ sono entrambe iniettive. Per il Principio dei cassetti, $m \leq n$ e $n \leq m$ da cui $m = n$. □

Se $|X| = |I_m|$ e $|X| = |I_n|$, allora $|I_m| = |I_n|$ e quindi $m = n$.
Pertanto ci può essere un unico n tale che $|X| = |I_n|$.
Questa osservazione giustifica la seguente definizione.

Se $|X| = |I_n|$, cioé se esiste una biiezione $X \to I_n$, si scrive semplicemente $|X| = n$ e si dice che X ha cardinalità n o che X ha n elementi.

Siccome $\mathrm{Id} : I_n \to I_n$ è biiettiva, vale $\boxed{|I_n| = n}$. In particolare $|\emptyset| = |I_0| = 0$.

Un insieme X si dice finito se ha cardinalità n per qualche n, cioé se c'è una biiezione $f : X \to I_n$. Altrimenti diremo che X è infinito.

Lemma

Ogni insieme in biiezione con un insieme finito è finito.

Proof.

Sia A un insieme in biiezione con un insieme finito B. Allora $|A| = |B|$ e $|B| = |I_n|$. Allora $|A| = |I_n|$ e quindi A è finito. $\square$

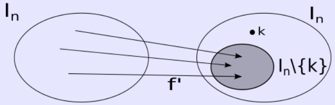
Vogliamo ora vedere che se A e B sono insiemi finiti della stessa cardinalità, ogni iniezione $f : A \to B$ è necessariamente una biiezione. Partiamo prima dal caso $A = B = I_n$.

Proposizione

Sia $f : I_n \to I_n$. Allora f iniettiva $\Rightarrow$ f suriettiva (e dunque biiettiva).

Proof.

Supponiamo che f non sia suriettiva. Esiste allora $k \in I_n$ (quindi $n \neq 0$) tale che $k \notin \mathrm{Im}(f)$. Possiamo allora definire $f' : I_n \to I_n \setminus \{k\}, i \mapsto f(i)$, che è iniettiva dato che lo è f.



Per il lemma esiste una biiezione $\alpha : I_n \setminus \{k\} \to I_{n-1}$. Allora anche $\alpha \circ f' : I_n \to I_{n-1}$ è iniettiva. Per il principio dei cassetti concludiamo che $n \leq n - 1$, assurdo. Pertanto f è suriettiva. $\square$

Proposizione

Siano A e B degli insiemi finiti della stessa cardinalità.
Se $f : A \to B$ è iniettiva, allora è anche suriettiva (e dunque biiettiva).

Proof.

Se A e B hanno cardinalità n, esistono delle biiezioni $\alpha : A \to I_n$ e $\beta : B \to I_n$. Definiamo $g := \beta \circ f \circ \alpha^{-1} : I_n \to I_n$.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\alpha"'] & B \arrow[d, "\beta"] \\ I_n \arrow[r, dotted, "g"] & I_n \end{tikzcd}$$

Allora $g : I_n \to I_n$ è iniettiva come composizione di iniettive.
Per la proposizione precedente g è suriettiva e quindi biiettiva.
Ma allora lo stesso vale per $\beta^{-1} \circ g \circ \alpha = \beta^{-1} \circ \beta \circ f \circ \alpha^{-1} \circ \alpha = f$. □

Ricordiamo che la funzione successore $s : \mathbb{N} \to \mathbb{N}, n \mapsto n+1$, è iniettiva ma non suriettiva ($0 \notin \mathrm{Im}(s)$). Questo conferma che $\mathbb{N}$ è un insieme [redacted].
INFINITO

Vogliamo dimostrare che ogni sottoinsieme di un insieme finito è finito. Prima ci serve il seguente risultato.

Proposizione

Ogni sottoinsieme A di I_n è finito.

Proof.

Dimostriamo che ogni sottoinsieme di I_n è finito per induzione su n.

- $n = 0$. In questo caso $I_n = \emptyset$. Pertanto se $A \subseteq I_0$ si ha $A \subseteq \emptyset$. Visto che l'altra inclusione vale sempre, allora $A = \emptyset$ e dunque A finito.
- Supponiamo che ogni sottoinsieme di I_n sia finito (ipotesi induttiva). Sia $A \subseteq I_{n+1}$. Abbiamo due casi: $n+1 \notin A$ o $n+1 \in A$.
  Se $n+1 \notin A$, allora $A \subseteq I_n$. Per l'ipotesi induttiva, A è finito.
  Se $n+1 \in A$, allora $A' := A \setminus \{n+1\} \subseteq I_n$ è finito per ipotesi induttiva. Posto $t := |A'|$, esiste una biiezione $\alpha' : A' \to I_t$. Definiamo la biiezione $\alpha : A \to I_{t+1}$ ponendo $\alpha(i) := \alpha'(i)$ se $i \in A'$ e $\alpha(n+1) := t+1$. Allora A è finito.

$\square$

Proposizione

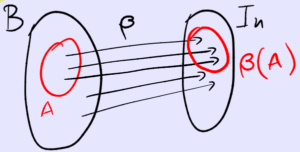
Ogni sottoinsieme di un insieme finito è finito.

Proof.

Sia B un insieme con $|B| = n$.
Esiste allora una biiezione $\beta : B \to I_n$.
Sia $A \subseteq B$. Consideriamo $\beta(A) = \{\beta(a) \mid a \in A\}$ e definiamo la funzione $f : A \to \beta(A), a \mapsto \beta(a)$.

$a \longmapsto a$

$$\begin{tikzcd} A \arrow[r, hook] \arrow[d, dotted, "f"'] & B \arrow[d, "\beta"] \\ \beta(A) \arrow[r, hook] & I_n \end{tikzcd}$$



Siccome β è iniettiva lo è anche f. Inoltre, per ogni $i \in \beta(A)$ esiste $a \in A$ tale che $i = \beta(a)$ e dunque $i = f(a)$, cioé f è suriettiva.
Pertanto $f : A \to \beta(A)$ è biiettiva.
D'altra parte, $\beta(A) \subseteq I_n$ è finito per la proposizione precedente.
Quindi anche A è finito perché in biiezione con un finito. ∎

Proposizione

Siano A e B insiemi finiti. Valgono le seguenti proprietà.

1. *Se $A \subseteq B$, allora $|A| \leq |B|$.*
2. *Se $A \subseteq B$ e $|A| = |B|$, allora $A = B$.*
3. *Se $A \subsetneq B$, allora $|A| < |B|$.*

Proof.

Se $|A| = a$ e $|B| = b$, esistono delle biiezioni $\alpha : A \to I_a$ e $\beta : B \to I_b$.
Sia $f : A \to B, a \mapsto a$, l'iniezione canonica.
1 La funzione $g := \beta \circ f \circ \alpha^{-1} : I_a \to I_b$ è iniettiva come composizione di iniettive. Per il principio dei cassetti, abbiamo $a \leq b$, cioé $|A| \leq |B|$.
2 Se $|A| = |B|$, allora f è un'iniezione tra insiemi della stessa cardinalità. Pertanto f è suriettiva. Allora preso $b \in B$ esiste $a \in A$ tale che $b = f(a)$, cioé $b = a$ e quindi $b \in A$. Pertanto $B \subseteq A$ e dunque $A = B$.
3 Se $A \subsetneq B$ allora $A \subseteq B$ e quindi $|A| \leq |B|$ per 1. Se fosse $|A| = |B|$, si avrebbe $A = B$ per 2. Ma questo va contro l'ipotesi. Pertanto $|A| \neq |B|$ e dunque $|A| < |B|$. $\square$

Corollario

Un insieme finito non è in biiezione con alcun suo sottoinsieme proprio.

Proof.

Sia B finito. Se B è in biiezione con $A \subseteq B$, allora anche A è finito e $|A| = |B|$. Da $A \subseteq B$ e $|A| = |B|$, per il risultato precedente, otteniamo $A = B$. Pertanto A non è un sottoinsieme proprio. □

$\rhd$ indipendente dal concetto di "insieme finito"

Per contrapposizione otteniamo che se un insieme è in biiezione con un qualche suo sottoinsieme proprio, allora è infinito (cioé non è finito). Questa proprietà venne utilizzata dal matematico Georg Cantor come definizione alternativa di insieme infinito: un insieme quindi è infinito se è in biiezione con un suo sottoinsieme proprio.

Esempio

Torniamo alla funzione successore $s : \mathbb{N} \to \mathbb{N}, n \mapsto n+1$. La sua corestrizione $f : \mathbb{N} \to \mathbb{N} \setminus \{0\}, n \mapsto n+1$, è biiettiva. Quindi $\mathbb{N} \setminus \{0\}$ è un sottoinsieme proprio di $\mathbb{N}$ che è in biiezione con $\mathbb{N}$.
Questo conferma ancora che $\mathbb{N}$ è infinito.

Abbiamo dimostrato che una funzione iniettiva tra insiemi finiti della stessa cardinalità è anche suriettiva. Vediamo che vale anche il viceversa.

~~Corollario~~ Proposizione

Siano A e B insiemi finiti della stessa cardinalità.
Se $f : A \to B$ è suriettiva, allora è anche iniettiva (e dunque biiettiva).

molto confusa

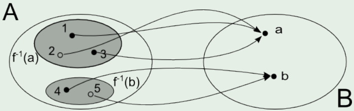
DIMOSTRAZIONE. Definiamo $g : B \to A$ associando ad ogni b una sua controimmagine (tramite f) a scelta (vedere esempio sotto). Allora $\boxed{f \circ g = \mathrm{Id}}$ e dunque g è iniettiva. Pertanto $g : B \to A$ è un'iniezione tra insiemi finiti della stessa cardinalità e quindi è biiettiva. Ma allora f è biiettiva, come composizione di biiettiva anche $\underline{(f \circ g)} \circ g^{-1} = f \circ \mathrm{Id} = f$.

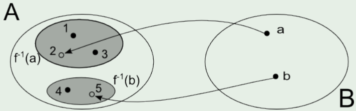
$f[g(b)] = b$

Esempio

$\mathrm{Id} \circ g^{-1} = g^{-1} \Rightarrow f = g^{-1}$

Sia $f : A \to B$ la funzione suriettiva descritta dal grafo di sinistra qui di seguito. Il grafo o destra è una possibile funzione g tale che $f \circ g = \mathrm{Id}$.





Osservazione

Consideriamo un insieme X e due funzioni $f, g : X \to X$ tali che $f \circ g = \mathrm{Id}_X \neq g \circ f$. Vediamo cosa possiamo dire su X, f e g. Notiamo prima di tutto che, poiché $f \circ g = \mathrm{Id}_X$, allora f è suriettiva e g è iniettiva. Ora se g fosse suriettiva, sarebbe biiettiva e quindi invertibile e dunque $f = f \circ g \circ g^{-1} = \mathrm{Id} \circ g^{-1} = g^{-1}$ da cui $g \circ f = g \circ g^{-1} = \mathrm{Id}_X$, assurdo. Pertanto g non è suriettiva. Similmente f non è iniettiva. Ne deduciamo che X non è un insieme finito.

Esercizio

Trovare un insieme X e funzioni $f, g : X \to X$ tali che $f \circ g = \mathrm{Id}_X \neq g \circ f$.

<u>SOLUZIONE</u>. Consideriamo $g : \mathbb{N} \to \mathbb{N}, n \mapsto 2n$ ed $f : \mathbb{N} \to \mathbb{N}$ così definita

$$f(n) := \begin{cases} \frac{n}{2} & \text{se } n \text{ è pari;} \\ 3n+1 & \text{se } n \text{ è dispari.} \end{cases}$$

congettura Collatz

Allora $f(g(n)) = f(2n) = n$ per ogni $n \in \mathbb{N}$ e quindi $f \circ g = \mathrm{Id}_{\mathbb{N}}$. Invece $g(f(n)) = 2f(n) \neq n$ se n è dispari. Dunque $g \circ f \neq \mathrm{Id}_{\mathbb{N}}$. N.B.: al posto di $3n+1$ avremmo potuto inserire qualunque altra espressione diversa da $\frac{n}{2}$.

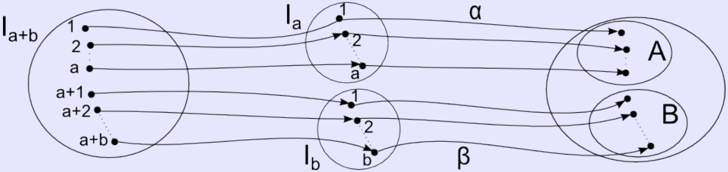
Ricordiamo che due insiemi A e B si dicono disgiunti se $A \cap B = \emptyset$.

Proposizione (Principio della somma)

Se A e B sono insiemi finiti e disgiunti, allora $A \cup B$ è finito con $|A \cup B| = |A| + |B|$.

Proof.

Mettiamo che $|A| = a$ e $|B| = b$. Esistono allora delle biiezioni $\alpha : I_a \to A$ e $\beta : I_b \to B$. Definiamo $f : I_{a+b} \to A \cup B$ ponendo $f(i) := \alpha(i)$ se $1 \le i \le a$ e $f(i) := \beta(i - a)$ se $a + 1 \le i \le a + b$.



Si vede facilmente che si tratta di una biiezione (essendo A e B disgiunti) e dunque $|A \cup B| = a + b$. □

Il principio della somma appena enunciato può essere facilmente generalizzato al seguente risultato.

Proposizione (Principio della somma generalizzato)

Siano $A_1, \ldots, A_n$ *degli insiemi finiti a due a due disgiunti, cioé tali che* $A_i \cap A_j = \emptyset$ *per ogni* $i \neq j$*. Allora* $A_1 \cup \cdots \cup A_n$ *è finito con* $|A_1 \cup \cdots \cup A_n| = |A_1| + \cdots + |A_n|$.

Esempio

Se X è un insieme finito e $\mathscr{F} = \{A_i \mid i \in I\}$ è una sua partizione, allora gli insiemi della partizioni sono a due a due disgiunti e quindi, per il principio della somma generalizzato si ha

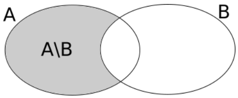
$$|X| = \sum_{i \in I} |A_i|$$

dove notiamo che la somma è finita perché I è necessariamente finito visto che lo è X.

Proposizione (Principio di Inclusione-Esclusione)

Se A e B sono insiemi finiti, allora $|A \cup B| = |A| + |B| - |A \cap B|$.

<u>DIMOSTRAZIONE</u>. E' facile verificare che $A \cup B = (A \setminus B) \cup B$.



Notiamo che $A \setminus B \subseteq A$ e quindi è finito come B. Siccome $A \setminus B$ e B sono disgiunti, possiamo applicare il principio della somma per dire che $A \cup B = (A \setminus B) \cup B$ è finito e scrivere

$$|A \cup B| = |(A \setminus B) \cup B| = |A \setminus B| + |B|.$$

Analogamente si vede che $A = (A \setminus B) \cup (A \cap B)$ ed essendo anche questa una unione di insiemi disgiunti otteniamo $|A| = |A \setminus B| + |A \cap B|$. Ricavando $|A \setminus B|$ da questa uguaglianza e sostituendola in quella precedente si conclude.

Esercizio

In una classe di 20 *studenti si parlano due lingue: l'italiano e l'inglese. Gli studenti che parlano italiano sono* 14 *e quelli che parlano inglese sono* 10*. Determinare quanti studenti parlano entrambe le lingue.*

SOLUZIONE. Indichiamo con

- A l'insieme degli studenti della classe che parlano italiano;
- B l'insieme degli studenti della classe che parlano inglese.

Si ha allora che

- $A \cup B$ è l'insieme degli studenti che parlano l'italiano oppure l'inglese, cioé tutti gli studenti della classe;
- $A \cap B$ è proprio l'insieme degli studenti della classe che parlano entrambe le lingue.

Pertanto $|A| = 14$, $|B| = 10$ e $|A \cup B| = 20$. Il Principio di Inclusione-Esclusione ci dice che $|A \cup B| = |A| + |B| - |A \cap B|$ cioé, sostituendo, che $20 = 14 + 10 - |A \cap B|$. Ricavando il termine ignoto otteniamo $|A \cap B| = 14 + 10 - 20 = 4$.

Proposizione (Cardinalità dell'insieme della parti)

Se A è un insieme finito, si ha $|P(A)| = 2^{|A|}$.

<u>DIMOSTRAZIONE</u>. Ogni biiezione $f : A \to B$ induce una biiezione $P(A) \to P(B), S \mapsto f(S)$. Posto $n = |A|$, si avrà una biiezione $A \to I_n$ e dunque una biiezione $P(A) \to P(I_n)$. Resta da dimostrare che $P(I_n)$ è finito con $|P(I_n)| = 2^n$. Procediamo per induzione su n.

- $n = 0 \Rightarrow P(I_n) = P(I_0) = P(\emptyset) = \{\emptyset\} \Rightarrow |P(I_n)| = 1 = 2^n$.
- Supponiamo $|P(I_n)| = 2^n$ e dimostriamo $|P(I_{n+1})| = 2^{n+1}$.
  Si ha che $P(I_{n+1}) := A \cup B$ dove A e B sono gli insiemi disgiunti:

$$\begin{aligned} A &:= \{S \subseteq I_{n+1} \mid n+1 \notin S\} = P(I_n). \\ B &:= \{S' \subseteq I_{n+1} \mid n+1 \in S'\} = \{S \cup \{n+1\} \mid S \in P(I_n)\}. \end{aligned}$$

  Per ipotesi induttiva $|A| = |P(I_n)| = 2^n$. Inoltre $A \to B, S \to S \cup \{n+1\}$ è una biiezione e dunque $|B| = |A| = 2^n$.
  Per il principio della somma,
  $|P(I_{n+1})| = |A \cup B| = |A| + |B| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$.

Proposizione (Cardinalità del prodotto cartesiano)

Se A e B sono insiemi finiti, allora $|A \times B| = |A| \cdot |B|$.

<u>DIMOSTRAZIONE</u>. Siano $a := |A|$ e $b := |B|$. Allora esistono biiezioni $\alpha : I_a \to A$ e $\beta : I_b \to B$. Ma allora anche $\alpha \times \beta : I_a \times I_b \to A \times B, (x,y) \mapsto (\alpha(x), \beta(y))$ è una biiezione.
Resta quindi da dimostrare che $I_a \times I_b$ è finito con $|I_a \times I_b| = a \cdot b$.
Notiamo che

$$I_a \times I_b = (\{1\} \times I_b) \cup (\{2\} \times I_b) \cup \cdots \cup (\{a\} \times I_b).$$

Inoltre $\{t\} \times I_b \to I_b,\ (t,x) \mapsto x$ è una biiezione e quindi $|\{t\} \times I_b| = b$.
Pertanto quella di sopra è un'unione di insiemi finiti a due a due disgiunti.
Per il principio della somma generalizzato, abbiamo che

$$|I_a \times I_b| = |\{1\} \times I_b| + |\{2\} \times I_b| + \cdots + |\{a\} \times I_b| = \underbrace{b + b + \cdots + b}_{a \text{ volte}} = ab.$$

Corollario

Sia $A \neq \emptyset$ un insieme finito. Allora $|A^n| = |A|^n$ per ogni $n \in \mathbb{N}$.

Proof.

Procediamo per induzione su n.
$n = 0$) Si ha $A^0 = \{\emptyset\}$ e dunque $|A^0| = 1 = |A|^0$.
Notiamo che $|A| \neq 0$ perchè $A \neq \emptyset$.

$n \Rightarrow n+1$) Se l'enunciato è vero per n allora

$$|A^{n+1}| = |A^n \times A| = |A^n| \cdot |A| = |A|^n \cdot |A| = |A|^{n+1}$$

cioè vale anche per $n+1$. $\square$