# Istituzioni di A & G — ALGEBRA, lezioni 2-3

8 Marzo 2021

$R \subseteq X \times X$

**Definizione 1.** *Sia $X$ un insieme. Una* ***relazione*** *$R$ in $X$ è una corrispondenza da $X$ in $X$. La relazione $R$ si dice:*

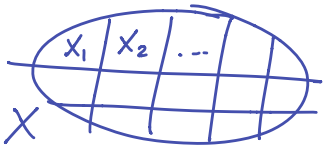
- ***riflessiva*** *se $x \; R \; x$ per ogni $x \in X$;*
- ***transitiva*** *se $x \; R \; y$ e $y \; R \; z$ implica $x \; R \; z$ per ogni $x, y, z \in X$;*
- ***simmetrica*** *se $x \; R \; y$ implica $y \; R \; x$ per ogni $x, y \in X$;*
- ***antisimmetrica*** *se $x \; R \; y$ e $y \; R \; x$ implica $x = y$ per ogni $x, y \in X$.*

**Definizione 2.** *Sia $X$ un insieme. Una relazione $\sim$ in $X$ si dice* ***relazione d'equivalenza*** *se è riflessiva, transitiva e simmetrica. Se $x \in X$ l'insieme*

$$[x] = \overline{x} = \{ \, y \in X \mid y \sim x \, \}$$

*è detto classe d'equivalenza di $x$.*

**Definizione 3.** *Sia $X$ un insieme. Una relazione $\prec$ si dice* ***relazione d'ordine*** *se è riflessiva, transitiva e antisimmetrica. Si dice* ***d'ordine totale*** *se è d'ordine e per ogni $x, y \in X$ o $x \prec y$ o $y \prec x$.*




**Definizione 4.** *Sia $X$ un insieme. Una* ***partizione*** *di $X$ è una famiglia $\{ X_i \}_{i \in I} \subseteq \mathcal{P}(X)$ di insiemi non vuoti tali che:*

$$(1)\ se \quad X_i \cap X_j \neq \emptyset \quad allora\ X_i = X_j \quad e \quad (2)\ \bigcup_{i \in I} X_i = X.$$

**Proposizione 5.** *Sia $X$ un insieme. Se $\sim$ è una relazione d'equivalenza in $X$ allora l'insieme delle classi di equivalenza $\{ \overline{x} \}_{x \in X}$ è una partizione di $X$.*

dim: osserviamo che $x \in \overline{x}$ $\forall x \in X$

$\Rightarrow \bigcup_{x \in X} \{x\} \subseteq \bigcup_{x \in X} \overline{x}$ cioè $X \subseteq \bigcup_{x \in X} \overline{x}$ ✓

$\bigcup_{x \in X} \{x\} = X$ ovvia $\supseteq$

Siano $\overline{x}$ e $\overline{y}$ 2 classi di equiv. t.c. $\overline{x} \cap \overline{y} \neq \emptyset$

Allora $\exists\ z \in \overline{x} \cap \overline{y}$

$z \in \overline{x}$, cioè $z \sim x$

$z \in \overline{y}$, cioè $z \sim y$

$\Rightarrow x \sim y \Rightarrow$ $x \in \overline{y}$, $\overline{x} \subseteq \overline{y}$ oppure $y \in \overline{x}$, $\overline{y} \subseteq \overline{x}$

in totale $\bar{x} = \bar{y}$ ⇏





**Definizione 6.** *Se $X$ è un insieme e $\sim$ è una relazione d'equivalenza in $X$ allora si definisce il* ***quoziente*** *di $X$ rispetto a $\sim$ come*

$$X/_\sim = \{\, \bar{x} \,\}_{x \in X}.$$

es: $\mathbb{Z}_n = \mathbb{Z}/_{\equiv_n}$ : $a \equiv_n b \iff a - b = n \cdot q \quad q \in \mathbb{Z}$

$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

es: le ore del giorno sono in $\mathbb{Z}_{24}$ $(\mathbb{Z}_{12})$

es: $\sim$ su $\mathbb{R}$ definita da:

$\forall x, y \in \mathbb{R}, \quad x \sim y \iff x - y \in \mathbb{Z}$

- rel. di equiv: $x \sim x$

  $x \sim y, y \sim z \implies x - y = m \in \mathbb{Z}$, $y - z = h \in \mathbb{Z}$

  $\implies x - z = x - y + y - z = m + n$

  $x \sim y \iff y \sim x$

- $\mathbb{R}/_\sim = [0, 1)$

una relaz. d'ordine

**Definizione 7.** *Sia $X$ un insieme e sia $\prec$ un ordinamento su $X$.*

- *Dato $Y \subseteq X$, $x \in X$ è un* ***maggiorante*** *di $Y$ se $y \prec x$ per ogni $y \in Y$;*
- *$m \in X$ è* ***massimale*** *se per ogni $x \in X$ tale che $m \prec x$ risulta $x = m$.*

*Un insieme ordinato $X$ si dice* ***induttivo*** *se ogni $Y \subseteq X$ totalmente ordinato ha almeno un maggiorante in $X$.*

Attenzione: un elemento massimale può non essere maggiorante, inoltre di elementi massimali ne possono esistere più di uno.

- Ogni insieme con un numero finito di elementi è necessariamente induttivo.

oss: $x$ maggiorante di $Y \not\Rightarrow x \in Y$

es: $(\mathbb{Z}, \leq)$ insieme p.o. (ordine totale)
Il sottoinsieme $\mathbb{N} \subseteq \mathbb{Z}$ non ha maggioranti.

es: $(\mathbb{N}_0, |)$ $a|b$ se $a = p \cdot b$
$Y = \{6, 9, 15\}$
maggioranti di $Y$ = tutti i multipli di 90

Si può dimostrare che l'Assioma della scelta è equivalente al seguente enunciato

**Lemma di Zorn** *Sia $X$ un insieme ordinato induttivo. Allora $X$ ha elementi massimali.*

Utilizzeremo il Lemma di Zorn più volte durante il corso: ad esempio, si può usare per dimostrare l'esistenza di insiemi liberi di generatori per ogni spazio vettoriale non nullo, non necessariamente finito.

Ricordiamo: sia $V$ uno spazio vettoriale su un campo $k$. Sia $X = \{ v_i \}_{i \in I}$ un insieme, non necessariamente finito, di vettori di $V$. L'insieme $X$ si dice:

- un **insieme di generatori** di $V$ se per ogni $v \in V$ esistono indici $i_1, \dots, i_n \in I$ e scalari $\alpha_1, \dots, \alpha_n \in k$ tali che

$$v = \sum_{j=1}^{n} \alpha_j v_{i_j};$$

- un **insieme libero di vettori** di $V$ se per ogni scelta di indici $i_1, \dots, i_n \in I$ i vettori $v_{i_1}, \dots, v_{i_n}$ sono linearmente indipendenti, cioè se

$$\sum_{j=1}^{n} \alpha_j v_{i_j} = 0, \text{ con } \alpha_1, \dots, \alpha_n \in k \quad \Rightarrow \quad \alpha_1 = \cdots = \alpha_n = 0.$$

Nel corso di Algebra Lineare del primo anno avete visto che ogni spazio vettoriale non nullo e finitamente generato ammette una base. Ammettendo la validità dell'Assioma della scelta (e, quindi, del Lemma di Zorn) tale risultato si può estendere anche a spazi vettoriali non finitamente generati.

**Proposizione 8.** *Sia $V$ uno spazio vettoriale non nullo su un campo $k$. Allora esistono in $V$ insiemi liberi di generatori.*

↳ corrispondente delle basi nel caso ∞-

dim: $S \subseteq \mathcal{P}(V)$

$S$ = famiglia di tutti i sottoinsiemi liberi di $V$.

$V \neq \emptyset \Longrightarrow S \neq \emptyset$

Consideriamo in $S$ l'ordinamento per inclusione.

Sia $\mathcal{L} \subset S$ un sottoinsieme tot. ordinato.

$\mathcal{L} = \{L_i\}_{i \in I}$

$L = \bigcup_{i \in I} L_i$ è un maggiorante di $\mathcal{L}$ in $S$.

$\Rightarrow \begin{cases} S \text{ è un insieme induttivo.} \\ S \neq \emptyset \end{cases}$

$\Rightarrow$ Vale il lemma di Zorn: $S$ ha un elemento max, diciamo $M$.

$M$ è un insieme libero di vettori.

Se dimostro che $M$ genera, vinco.

Sia $v \in V$.

Possibilità 1: $v \in M$ ✓

Possibilità 2: $v \notin M$

$M \cup \{v\}$ non è libero

$\Rightarrow \exists\ \alpha, \alpha_1, \alpha_2 \dots \alpha_n$ t.c.

$$\alpha v + \sum_{i=1} \alpha_i v_i = 0 \qquad v_1 \dots v_n \in M$$

se $\alpha = 0 \rightsquigarrow \alpha_i = 0\ \forall i \rightsquigarrow 0 = 0$

se $\alpha \neq 0 \rightsquigarrow v = \sum_{i=1}^{n} \left(-\frac{\alpha_i}{\alpha}\right) v_i$

cioè $v$ è generato dai $v_i$ #

### Numeri naturali e principio di induzione

Ricordiamo l'insieme dei numeri naturali

$$\mathbb{N} = \{\ 1, 2, 3, 4, \dots, n, n+1, \dots\ \}.$$

Talvolta considereremo anche $\mathbb{N}_0 = \mathbb{N} \cup \{\ 0\ \}$. Spesso conviene pensare a $\mathbb{N}$ e $\mathbb{N}_0$ come sottoinsiemi dell'insieme dei numeri interi $\mathbb{Z}$.

In seguito indicheremo anche con $I_n$ l'insieme dei primi numeri naturali, cioè

$$I_n = \{\ 1, 2, 3, 4, \dots, n\ \} \subseteq \mathbb{N}.$$

Ricordiamo che in $\mathbb{N}$ sono definite un'operazione di somma e una di moltiplicazione t.c.

- $n + m = m + n$ per ogni $n, m \in \mathbb{N}$; commutativa
- $(n + m) + k = m + (n + k)$ per ogni $n, m, k \in \mathbb{N}$; associativa
- $nm = mn$ per ogni $n, m \in \mathbb{N}$; commutativa
- $(nm)k = m(nk)$ per ogni $n, m, k \in \mathbb{N}$; associativa
- $(n + m)k = nk + mk$ per ogni $n, m, k \in \mathbb{N}$. distributiva

Le operazioni di somma e prodotto sono **compatibili con l'ordinamento totale naturale definito su** $\mathbb{N}$, che come abbiamo imparato ieri è una relazione d'ordine.

Esiste una teoria assiomatica (la cosiddetta *assiomatica di Peano*) che permette di individuare univocamente l'insieme $\mathbb{N}$, le operazioni di somma e prodotto definite in esso, nonché la relazione d'ordine.

Uno degli strumenti più importanti legati a $\mathbb{N}$ è il

**Principio di induzione** *Sia $P(k)$ una proprietà che dipende da $k \in \mathbb{N}$. Se*

1. *$P(1)$ è vera;*
2. *per ogni $n \geqslant 1$, il fatto che $P(n)$ sia vera implica che $P(n+1)$ è vera;*

*allora $P(k)$ è vera per ogni $k \in \mathbb{N}$.*

Talvolta il Principio di induzione viene formulato in maniera leggermente diversa:
*Sia $P(k)$ una proprietà che dipende da $k \in \mathbb{N}$. Se*

1. *esiste $n_0 \in \mathbb{N}$ tale che $P(n_0)$ è vera;*
2. *per ogni $n \geqslant n_0$, il fatto che $P(n)$ sia vera implica che $P(n+1)$ è vera;*

*allora $P(k)$ è vera per ogni $k \in \mathbb{N}$, $k \geqslant n_0$.*

Diamo alcuni esempi di applicazione del Principio d'induzione.

Nelle dispense troverete (provate a leggere i dettagli da soli!) il principio di induzione usato per dimostrare che

- $I_n \approx I_m$ se e solo se $n = m$.

  ha lo stesso numero di elementi

- $x_1, \dots, x_n, y_1, \dots, y_m \in \mathbb{N}$, allora

$$\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{m} y_j\right) = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} x_i y_j\right);$$

  (proprietà distributiva generalizzata della somma rispetto all'addizione).

- Formula del binomio di Newton: se $a, b, n \in \mathbb{N}$ allora

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i},$$

  ove per $1 \leqslant i \leqslant n-1$

$$\binom{n}{0} = \binom{n}{n} = 1, \qquad \binom{n}{i} = \frac{n!}{i!(n-i)!}.$$

Osserviamo che la formula di Newton ha come conseguenza interessante che $\mathcal{P}(I_n)$ ha $2^n$ elementi. Infatti $\mathcal{P}(I_n)$ contiene un solo sottoinsieme di $I_n$ con 0 elementi (cioè $\emptyset$); $n$ sottoinsiemi di $I_n$ con un solo elemento; in generale $\binom{n}{i}$ sottoinsiemi con $i$ elementi.

Quindi $\mathcal{P}(X)$ contiene in totale

$$\sum_{i=0}^{n} \binom{n}{i} = \sum_{i=0}^{n} \binom{n}{i} 1^i 1^{n-i} = (1+1)^n = 2^n$$

sottoinsiemi di $I_n$. Questo è uno dei motivi per cui talvolta si scrive anche $2^X$ in luogo di $\mathcal{P}(X)$.

Vediamo insieme un altro esempio: ~~dimostreremo~~ per induzione che per ogni $n \in \mathbb{N}$ si ha

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

$n=1$: $\sum_{i=1}^{1} i = \frac{1\cdot(1+1)}{2}$

$1 = 1$ ✓

$n \geq 2$: supponiamo che sia vera per $n$.

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) \overset{\text{hp induttiva}}{=} \frac{n(n+1)}{2} + (n+1)$$

$$= \frac{n^2+n+2n+2}{2} = \frac{(n+1)(n+2)}{2} \quad \#$$

Esercizio. Dimostrare che, per ogni $z \in \mathbb{Z}$, $z^3 - z$ è divisibile per 6.

La formulazione data del Principio d'induzione viene anche detta *Principio di induzione in forma debole* per distinguerla dalla seguente che ha, apparentemente, delle ipotesi più restrittive: in realtà si può dimostrare che le due formulazioni sono, di fatto, equivalenti.

**Principio di induzione in forma forte** *Sia $P(k)$ una proprietà che dipende da $k \in \mathbb{N}$. Se*

1. *$P(1)$ è vera;*
2. *$\forall\, n \geqslant 1$, il fatto che $P(m)$ sia vera per ogni $m \leqslant n$ implica che $P(n+1)$ è vera;*

*allora $P(k)$ è vera per ogni $k \in \mathbb{N}$.*

Nelle dispense viene usato il Principio di induzione in forma forte per dimostrare che ogni $n \in \mathbb{N} \setminus \{\, 1 \,\}$ si scrive come prodotto finito di numeri primi [1].

Vale un risultato analogo anche per ogni intero diverso da 0 e $\pm 1$ definendo come numeri primi in $\mathbb{Z}$ i numeri positivi privi di divisori propri. In tal caso, ogni $x \in \mathbb{Z}$ si può scrivere come il prodotto di $\pm 1$ per un numero finito di numeri primi.

Verificheremo in seguito che tale scomposizione è unica a meno dell'ordine dei fattori.

[1] Un numero $p \in \mathbb{N}_0$ si dice primo se non ha divisori propri, cioè i suoi unici divisori sono 1 e $p$: convenzionalmente 1 non viene considerato primo.

$n \in \mathbb{N}$, $n \geq 2 \Longrightarrow$ $n$ è prodotto di # finito di primi

Vediamo insieme i dettagli.

$n=2$: viene da dim. perché 2 è primo

$n \geq 2$: Supponiamo che la tesi sia vera per ogni $m \leq n$. Guardiamo $n+1$.

- $n+1$ è primo ✓
- $n+1$ non è primo, cioè $\exists$ un divisore proprio: $1 < a < n+1$ t.c. $\exists\ b : n+1 = ab$ ovviamente $1 < b < n+1$.

Per $a$ e $b$ vale l'hp induttiva:

$$a = \prod_{i=1}^{\alpha} p_i, \quad b = \prod_{j=1}^{\beta} q_j \Longrightarrow n+1 = a \cdot b = \prod_{i=1}^{\alpha} p_i \prod_{j=1}^{\beta} q_j \quad \#$$

Il Principio di induzione implica il seguente **Principio di buon ordinamento**:

**Proposizione 9.** *Ogni sottoinsieme non vuoto $S \subseteq \mathbb{N}$ ha un primo elemento.*

dim: dimostriamo che se $S$ non ha un primo elemento, allora $S = \emptyset$, cioè $\mathbb{N} \setminus S = \mathbb{N}$.

$1 \notin S$, se $1 \in S$, sarebbe un primo elemento

$\rightsquigarrow 1 \notin S$, cioè $1 \in \mathbb{N} \setminus S$

Supponiamo $I_n = \{1, 2, \dots, n\} \subseteq \mathbb{N} \setminus S$.

se $n+1 \notin \mathbb{N} \setminus S \Longrightarrow n+1 \in S$, e $n+1$ sarebbe il primo elt. di $S$ no

$\Longrightarrow n+1 \in \mathbb{N} \setminus S \Longrightarrow I_n \subseteq \mathbb{N} \setminus S \ \forall n$

cioè $\mathbb{N} \setminus S = \mathbb{N}$ #

In realtà si può dimostrare che il Principio del buon ordinamento implica il Principio di induzione.

Sia $S \subseteq \mathbb{N}$ t.c. $1 \in S$ e t.c. $S$ ha la proprietà $n \in S \Rightarrow n+1 \in S$: vogliamo dim. che $S = \mathbb{N}$, cioé $\mathbb{N} \setminus S = \emptyset$.

Se fosse $\mathbb{N} \setminus S \neq \emptyset$, per il buon ordinamento, $\mathbb{N} \setminus S$ avrebbe un primo elemento, $m \in \mathbb{N} \setminus S$.

$1 \in S \Rightarrow 1 \notin \mathbb{N} \setminus S \Rightarrow m > 1$.

Poiché $m$ é il primo elt. di $\mathbb{N} \setminus S$, $m-1 \notin \mathbb{N} \setminus S$, cioé $m-1 \in S$.

Ma allora $(m-1)+1 \in S$ $m \in S$ ↯ ※

attenzione: la dim. scritta in viola è stata risistemata rispetto alla confusione fatta a lezione!



Chiaramente il Principio del buon ordinamento vale anche per ogni sottoinsieme di $\mathbb{Z}$ avente un primo elemento, per esempio $\mathbb{N}_0$.

In $\mathbb{N}_0$ vale l'**Algoritmo euclideo di divisione**, cioè per ogni $a \in \mathbb{N}_0$ e $b \in \mathbb{N}$ esistono unici $q, r \in \mathbb{N}_0$ (detti rispettivamente quoziente e resto) con $0 \leqslant r < b$ tali che $a = qb + r$.
In particolare $b$ è divisore di $a$ se e solo se il resto della divisione intera di $a$ per $b$ è 0.

$a \geq b$

oss: posso anche considerare la divisione in $\mathbb{Z}$ (e eliminare la condizione $a \geq b$)

dim: sia $a \in \mathbb{N}_0$, $b \in \mathbb{N}$ e definiamo

$$S = \{ a - qb \mid q \in \mathbb{N}_0 \} \subseteq \mathbb{N}_0$$

Poiché $a = a - 0 \cdot b \in S \Longrightarrow S \neq \emptyset$.

$\rightsquigarrow$ possiamo applicare il principio del buon ordinamento: $S$ ha un primo elemento, che chiamiamo $r$.

- $r \in S \Longrightarrow r = a - qb \rightsquigarrow a = qb + r$
- $r \geq 0$ - Inoltre $r < b$, perché se $r \geq b$, allora avremmo

$$0 \leq r - b = (a - qb) - b = a - (q+1)b \in S$$

cioè $r - b \in S$, $r - b \leq r \rightsquigarrow$ assurdo ↯

Quindi $\exists\, q, r$ t.c. $0 \leq r < b$ e $a = qb + r$.

Per l'unicità: se $\exists\, q', r'$ t.c.

$$a = q'b + r' = qb + r \Longrightarrow b(q - q') = r' - r.$$

Se $q \neq q'$ (diciamo $q > q'$)

$$\Longrightarrow b < b(q - q') = r' - r \leq b \quad \text{↯}$$

$$\Longrightarrow q = q' \text{ e } r = r' \quad \#$$

È interessante osservare che quanto dimostrato finora implica anche che **i numeri primi (in $\mathbb{N}$ o $\mathbb{Z}$) sono infiniti**.

Infatti: se esistesse un # finito di primi $p_1, p_2, \dots, p_t$ –

Allora $$q = \left(\prod_{i=1}^{t} p_i\right) + 1$$

$q \neq p_i$, perché $q > p_i \ \forall i$ –

Inoltre $q$ ha una scomposizione in fattori primi, ma nessuno dei $p_i$ può essere fattore di $q$, perché la divisione di $q$ per $p_i$ ha sempre resto $1 \neq 0$ – ↯ #

# INSIEMI FINITI/INFINITI



**Def:** $X$ insieme. $X$ si dice finito se o $X=\emptyset$, o $\exists\, n\in\mathbb{N}$ t.c. $X\approx I_n$ ($X$ equipotente a $I_n$, cioè ha lo stesso # di elementi).
$X$ si dice infinito se non è finito.

- Ogni sottoinsieme di un insieme finito è finito.
- Ogni insieme equipotente a un insieme infinito è infinito.
- Se $X$ contiene un insieme infinito, allora $X$ è infinito.

→ è equivalente all'assioma della scelta

**Prop:** $X$ un insieme. Se $X$ è infinito, allora $\exists$ un'applicazione iniettiva $\varphi : \mathbb{N} \longrightarrow X$.

**dim:** Prendiamo la famiglia

$$\mathcal{X} = \{Y\}_{Y \in \mathcal{P}(X) \setminus \emptyset}$$

Allora $\exists$ una funzione di scelta

$$f : \mathcal{P}(X) \setminus \emptyset \longrightarrow \bigcup_{\mathcal{P}(X)\setminus\emptyset} Y$$

t.c. $f(Y) \in Y$.

Chiamiamo:

$$a_1 := f(X)$$
$$a_2 := f(X \setminus \{a_1\})$$
$$a_3 := f(X \setminus \{a_1, a_2\})$$
$$\vdots$$

La funzione $\varphi: \mathbb{N} \longrightarrow X$, $n \longmapsto a_n$ è iniettiva,

perché se $n \neq m \Longrightarrow a_n \neq a_m$ #

## CRITERIO DI DEDEKIND

$X$ un insieme.

$X$ è infinito $\Longleftrightarrow X \approx Y$ a un suo sottoins. proprio $Y \subset X$.

dim:

($\Longleftarrow$) supp $\exists\, Y \subset X$, $Y \approx X$. Supp per assurdo che $|X| = n < \infty$.

Poiché $Y \subset X$, $\exists\, \varphi: Y \longrightarrow I_n$ iniettiva ma non suriettiva.

Cioè $\exists\, m < n$, $m \neq n$ t.c. $Y \approx I_m$.

Allora: $I_n \approx X \approx Y \approx I_m$ con $n \neq m$ ↯

($\Longrightarrow$) Supp $X$ sia infinito.
Per quanto dim prima, $\exists\ \varphi: \mathbb{N} \hookrightarrow X$ iniettiva.

Sia $Z = \mathrm{Im}(\varphi)$.
Sia $Z' = Z \setminus \varphi(1) \neq Z$

oss: $\varphi: \mathbb{N} \longrightarrow Z$ è biettiva per def.
$\varphi': \mathbb{N}\setminus\{1\} \longrightarrow Z'$ biettiva per def
$\sigma: \mathbb{N} \longrightarrow \mathbb{N}\setminus\{1\}$ biettiva
$n \longmapsto n+1$

$\rightsquigarrow$ la composizione


è biettiva.

Sia $Y = X \setminus \{\varphi(1)\}$.
Allora $Y = (X \setminus Z) \cup Z' \neq X = (X \setminus Z) \cup Z$

**Def:** $X$ insieme

- $X$ si dice **numerabile** se $X \approx \mathbb{N}$.
- $X$ si dice **al più numerabile** se $X$ è finito o numerabile.
- $X$ si dice **più che numerabile** (non numerabile) in tutti gli altri casi.

$$\begin{array}{ccc} 1 & \longleftrightarrow & x_1 \\ 2 & \longleftrightarrow & x_2 \\ 3 & \longleftrightarrow & x_3 \\ \vdots & & \vdots \end{array}$$

Li posso contare

**Teorema:** (CANTOR-SCHRÖDER-BERNSTEIN)

$X$ e $Y$ insiemi. Se esistono applicazioni iniettive $f: X \longrightarrow Y$ e $g: Y \longrightarrow X$ allora $X \approx Y$.

**Corol1:** Ogni sottoinsieme di un insieme al più numerabile è al più numerabile.