Candidato:

Fabio Chillotti

Relatore:

Professor Andrea Loi

28 Novembre 2018

Anno accademico 2018/2019

I numeri cardinali e la loro aritmetica

«La paura dell'infinito è una forma di miopia che distrugge la possibilità di vederlo realmente»

George Cantor

$\aleph_0$

Università degli studi di Cagliari
Corso di Laurea in Matematica

Argomenti sui quali la tesi verte

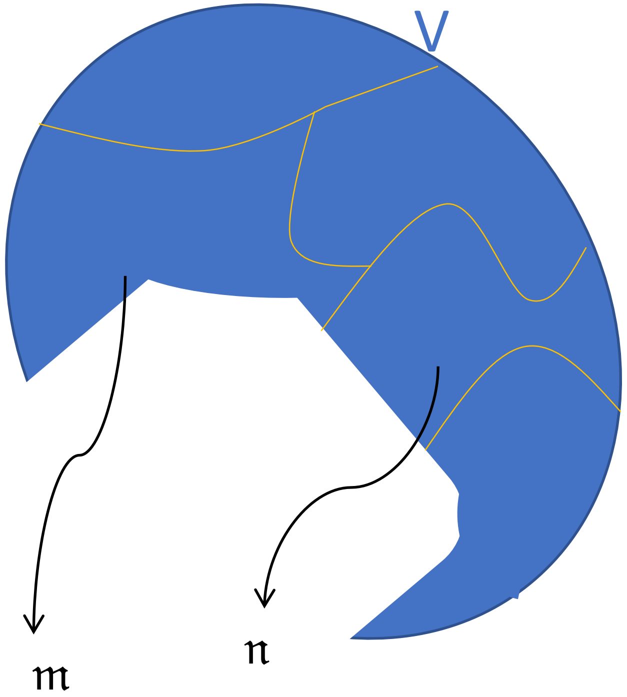
- Costruzione dei numeri cardinali
- Operazioni
- Ordine
- Esempi e proprietà

Costruzione

Sia $V = \{A \mid A \text{ sia un insieme}\}$ *la classe di tutti gli insiemi, definiamo su di essa la seguente relazione di equivalenza:*

$$A \sim B \Leftrightarrow \exists\, f : A \to B \text{ applicazione biunivoca}$$

Definiamo numero cardinale una classe di equivalenza $[A]_{\sim}$ *e rappresentiamo la classe dei numeri cardinali con la lettera* Γ



Prime osservazioni circa la definizione di cardinale

a) Ciascuna classe di equivalenza della partizione è un insieme e non una classe propria;
b) La classe dei cardinali è una classe propria, infatti:

$$V = \bigcup_{\mathfrak{m} \in \Gamma} \mathfrak{m}$$

c) Possiamo vedere ogni numero naturale con un numero cardinale, ad esempio:

$$1 = [\{1\}]_{\sim}$$

Operazioni elementari tra cardinali

Siano $\mathfrak{m}, \mathfrak{n} \in \Gamma$ *due cardinali qualsiasi.*

Consideriamo $M, N \in V$ *tali che* $|M| = \mathfrak{m}$ *e* $|N| = \mathfrak{n}$ *e* $M \cap N = \emptyset$

- Somma

Poniamo $S = M \cup N$ *da cui definiamo:*

$$|S| = \mathfrak{s} = \mathfrak{m} + \mathfrak{n}$$

- Prodotto

Poniamo $P = M \times N$ *da cui definiamo:*

$$|P| = \mathfrak{p} = \mathfrak{m} \cdot \mathfrak{n}$$

<u>OSS</u>: si noti che le due definizioni non dipendono dalla scelta degli insiemi M ed N

Proprietà

a) Dalle proprietà insiemistiche di unione e prodotto cartesiano si ottiene che $\forall\ \mathfrak{m}, \mathfrak{n}, \mathfrak{l} \in \Gamma$ *valgono le proprietà:*

i) $\mathfrak{m} + \mathfrak{n} = \mathfrak{n} + \mathfrak{m}$
ii) $\mathfrak{m} \cdot \mathfrak{n} = \mathfrak{n} \cdot \mathfrak{m}$
iii) $\mathfrak{l} \cdot (\mathfrak{m} + \mathfrak{n}) = \mathfrak{l} \cdot \mathfrak{m} + \mathfrak{l} \cdot \mathfrak{n}$
iv) $(\mathfrak{m} + \mathfrak{n}) + \mathfrak{l} = \mathfrak{m} + (\mathfrak{n} + \mathfrak{l})$
v) $(\mathfrak{m} \cdot \mathfrak{n}) \cdot \mathfrak{l} = \mathfrak{m} \cdot (\mathfrak{n} \cdot \mathfrak{l})$

b) Queste operazioni possono essere induttivamente generalizzate ad un numero finito $k \in \mathbb{N}$ *di cardinali* $\mathfrak{m}_1, \mathfrak{m}_2, \dots, \mathfrak{m}_k$*:*

$$\sum_{i=1}^{k} \mathfrak{m}_i = \mathfrak{m}_1 + \mathfrak{m}_2 + \cdots + \mathfrak{m}_k$$

$$\prod_{i=1}^{k} \mathfrak{m}_i = \mathfrak{m}_1 \cdot \mathfrak{m}_2 \cdot \cdots \cdot \mathfrak{m}_k$$

Potenze fra numeri cardinali

Siano $\mathfrak{m}, \mathfrak{n} \epsilon \Gamma$ *due cardinali qualsiasi.*

Consideriamo $M, N \epsilon V$ *tali che* $|M| = \mathfrak{m}$ *e* $|N| = \mathfrak{n}$

- Potenza fra due cardinali

Poniamo $M^N = \{f: N \to M \mid f\ applicazione\}$ da cui definiamo:

$$|M^N| = \mathfrak{m}^{\mathfrak{n}}$$

Proprietà

a) Come è lecito aspettarsi, $\forall\, \mathfrak{m} \in \Gamma$ *valgono le due uguaglianze:*

i) $\mathfrak{m}^1 = \mathfrak{m}$
ii) $1^{\mathfrak{m}} = 1$

Infatti, se M *è un insieme di cardinalità* $\mathfrak{m}$*, si ha che:*

$$M^{\{1\}} = \{f \mid f(1) = m\}_{m \in M} \sim M$$

$$\{1\}^M = \{f \mid f(m) = 1\ \forall\, m \in M\,\} \sim \{1\}$$

b) $\forall\, \mathfrak{m}, \mathfrak{m}_1, \mathfrak{m}_2, \mathfrak{n}, \mathfrak{n}_1, \mathfrak{n}_2, \mathfrak{p} \in \Gamma$ *si ha:*

i) $\mathfrak{m}^{\mathfrak{n}_1 + \mathfrak{n}_2} = \mathfrak{m}^{\mathfrak{n}_1} \cdot \mathfrak{m}^{\mathfrak{n}_2}$
ii) $(\mathfrak{m}_1 \cdot \mathfrak{m}_2)^{\mathfrak{n}} = \mathfrak{m}_1^{\mathfrak{n}} \cdot \mathfrak{m}_2^{\mathfrak{n}}$
iii) $(\mathfrak{m}^{\mathfrak{n}})^{\mathfrak{p}} = \mathfrak{m}^{\mathfrak{n} \cdot \mathfrak{p}}$

Esempi

Ricordando che l'unione di una famiglia finita di insiemi ha cardinalità pari alla cardinalità massima della famiglia otteniamo:

a) $\aleph_0 + \aleph_0 = \aleph_0$
b) $k \cdot \aleph_0 = \aleph_0 \ \forall\, k \in \mathbb{N}$
c) $\aleph_0 + \mathfrak{c} = \mathfrak{c}$
d) $k \cdot \mathfrak{c} = \mathfrak{c} \ \forall\, k \in \mathbb{N}$

Dove $\aleph_0$ *denota la cardinalità del numerabile e* $\mathfrak{c}$ *denota quella del continuo*

Ricordando che dati due insiemi infiniti M, N *si ha che* $|M \times N| = max\{|M|, |N|\}$ *desumiamo:*

e) $\aleph_0 \cdot \aleph_0 = \aleph_0$
f) $\aleph_0 \cdot \mathfrak{c} = \mathfrak{c}$

g) Notevole importanza riveste, circa le potenze tra cardinali, l'insieme delle parti di un insieme.
Questo fatto discenda relazione:

$$P(M) \sim \{0,1\}^M \;\; \forall\, M \,\epsilon\, V$$

Questo ci permette di asserire, tramite il linguaggio dei cardinali, che:

$$|P(M)| = 2^{|M|} \;\; \forall\, M \,\epsilon\, V$$

Ordine nella classe dei cardinali

Siano $\mathfrak{m}, \mathfrak{n} \in \Gamma$ *due cardinali qualsiasi e* M, N *tali che* $|M| = \mathfrak{m}$, $|N| = \mathfrak{n}$

Diremo che $\mathfrak{m}$ *è minore o uguale di* $\mathfrak{n}$ *e scriveremo* $\mathfrak{m} \leq \mathfrak{n}$ *se esiste un'iniezione da* M *ad* N.

In simboli,

$$\mathfrak{m} \leq \mathfrak{n} \overset{def}{\Longleftrightarrow} \exists\, f : M \to N \text{ iniettiva}$$

Proprietà ed osservazioni circa l'ordine

Il teorema che segue pone in evidenza uno stretto legame con l'ordine usuale di $\mathbb{N}$.

Teorema

Siano $\mathfrak{m}, \mathfrak{n} \in \Gamma$ *due cardinali tali che* $\mathfrak{m} \leq \mathfrak{n}$, *allora esiste* $\mathfrak{p} \geq 0$ *tale che:*

$$\mathfrak{n} = \mathfrak{m} + \mathfrak{p}$$

Dimostrazione

Consideriamo due insiemi M, N *di cardinalità* $\mathfrak{m}, \mathfrak{n}$ *rispettivamente.*
Senza ledere la generalità possiamo pensare che $M \subseteq N$ *e definire l'insieme:*

$$P = N \setminus M \subseteq N, sia\ |P| = \mathfrak{p}$$

Naturalmente P *ed* M *sono due insiemi disgiunti, per la definizione di somma tra cardinali si ha* $\mathfrak{n} = \mathfrak{m} + \mathfrak{p}$ *come volevasi dimostrare.* $\square$

Mostriamo ora un risultato che permette di invertire il risultato appena dimostrato.

Lemma

Siano $\mathfrak{m}, \mathfrak{n}, \mathfrak{m}_1, \mathfrak{n}_1 \epsilon \Gamma$ *cardinali tali per cui* $\mathfrak{m} \leq \mathfrak{n}$ *e* $\mathfrak{m}_1 \leq \mathfrak{n}_1$. *Allora si ha:*

$$\mathfrak{m} + \mathfrak{m}_1 \leq \mathfrak{n} + \mathfrak{n}_1$$

Dimostrazione

Siano M, N, M_1, N_1 *insiemi di cardinalità* $\mathfrak{m}, \mathfrak{n}, \mathfrak{m}_1, \mathfrak{n}_1$ *rispettivamente. Dalle ipotesi possiamo supporre che* $M \subseteq N$ *e* $M_1 \subseteq N_1$ *da cui desumiamo:*

$$M \cup M_1 \subseteq N \cup N_1$$

Che permette di asserire ciò che volevasi dimostrare. □

Come anticipato questo lemma permette di invertire il risultato del teorema. Infatti se $\mathfrak{m}, \mathfrak{n}, \mathfrak{p} \epsilon \Gamma$ *sono tre cardinali tali che* $\mathfrak{n} = \mathfrak{m} + \mathfrak{p}$, *possiamo considerare il fatto che* $\mathfrak{m} \leq \mathfrak{m}$ *e* $\mathfrak{p} \geq 0$, *per il lemma otteniamo:*

$$\mathfrak{m} = \mathfrak{m} + 0 \leq \mathfrak{m} + \mathfrak{p} = \mathfrak{n}$$

Quindi potremmo definire la relazione d'ordine tra cardinali nello stesso modo in cui la si definisce tra numeri naturali.

In maniera del tutto analoga alla dimostrazione del lemma precedente si dimostra anche ciò che segue:

Lemma

Siano $\mathfrak{m}, \mathfrak{n}, \mathfrak{m}_1, \mathfrak{n}_1 \epsilon \Gamma$ *cardinali tali per cui* $\mathfrak{m} \leq \mathfrak{n}$ *e* $\mathfrak{m}_1 \leq \mathfrak{n}_1$. *Allora si ha:*

$$\mathfrak{m} \cdot \mathfrak{m}_1 \leq \mathfrak{n} \cdot \mathfrak{n}_1$$
$$\mathfrak{m}^{\mathfrak{m}_1} \leq \mathfrak{n}^{\mathfrak{n}_1}$$

Famiglie infinite di cardinali

Consideriamo una famiglia $\mathfrak{F} = \{\mathfrak{m}_i\}_{i \epsilon I}$ *infinita di cardinali, ci proponiamo di definire una somma e un prodotto dei cardinali della famiglia.*
Consideriamo la famiglia di insiemi $\mathcal{F} = \{M_i\}_{i \epsilon I}$ *tale per cui* $|M_i| = \mathfrak{m}_i$ $\forall i \epsilon I$ *e* $M_i \cap M_j = \emptyset \; \forall i \neq j$.

- Serie infinita

Poniamo

$$S = \bigcup_{i \epsilon I} M_i$$

da cui definiamo:

$$|S| = \mathfrak{s} = \sum_{i \epsilon I} \mathfrak{m}_i$$

- Prodotto infinito

Poniamo

$$P = \prod_{i \epsilon I} M_i$$

da cui definiamo:

$$|P| = \mathfrak{p} = \prod_{i \epsilon I} \mathfrak{m}_i$$

Proprietà ed osservazioni

a) «Perché è possibile definire la famiglia $\mathcal{F}$ *?».*

Domanda non banale dal momento che si è supposto I infinito.

La risposta viene fornita dall'assioma della scelta, il motivo di questo giace nel fatto che la famiglia $\mathfrak{F}$ *è una famiglia di insiemi a tutti gli effetti e determinare la famiglia* $\mathcal{F}$ *è equivalente a determinare una funzione di scelta:*

$$f : I \to \bigcup_{i \in I} \mathfrak{m}_i \; con \; f(j) \in \mathfrak{m}_j \; \forall j \in I$$

b) Il prodotto insiemistico dato nella definizione necessita di qualche parola.
Ciò che si intende nella definizione altro non è che una generalizzazione del prodotto cartesiano di una famiglia finita di insiemi, nella fattispecie:

$$\prod_{i \epsilon I} M_i = \left\{ f : I \to \bigcup_{i \epsilon I} M_i \mid f \text{ } applicazione \text{ } tale \text{ } che \text{ } f(j) \epsilon M_j \; \forall j \epsilon I \right\}$$

Cioè è l'insieme delle funzioni di scelta possibili, il suo essere non vuoto è dunque garantito dall'assioma della scelta.
Dunque la definizione di prodotto infinito necessita dell'utilizzo doppio dell'assioma della scelta.

Esempi

a) Consideriamo una famiglia numerabile di naturali $\mathfrak{F} = \{m_i\}_{i \epsilon \mathbb{N}^*}$, *allora si ha:*

$$\sum_{i=1}^{\infty} m_i = \left| \bigcup_{i=1}^{\infty} M_i \right| = |\mathbb{N}| = \aleph_0$$

Dove $|M_i| = \mathfrak{m}_i \ \forall i \ \epsilon \ I$ *e* $M_i \cap M_j = \emptyset \ \forall i \neq j.$

Quindi potremmo dire anche che:

$$\sum_{i=0}^{\infty} 1 = \aleph_0$$

$$\sum_{i=0}^{\infty} i = \aleph_0$$

b) Si può dimostrare uno dei risultati precedenti più in generale: sia M un insieme di cardinalità $\mathfrak{m}$, *allora:*

$$\sum_{\mathfrak{x} \epsilon M} 1 = \mathfrak{m}$$

c) In particolare se $\mathfrak{m} = \mathfrak{m}_i = \mathfrak{m}_j \ \forall i, j \ \epsilon \ \mathbb{N} = I$ *ed M è un insieme di cardinalità* $\mathfrak{m}$ *allora il prodotto infinito è la cardinalità dell'insieme delle successioni a valori in M. In simboli:*

$$\prod_{i \epsilon I} \mathfrak{m}_i = \prod_{i=0}^{\infty} \mathfrak{m} = \mathfrak{m}^{\aleph_0}$$

In particolare:

$$\prod_{i=0}^{\infty} 2 = 2^{\aleph_0} = \mathfrak{c}$$

d) Diremo che un cardinale $\mathfrak{m}$ *divide un cardinale* $\mathfrak{n}$ *se esiste un cardinale* $\mathfrak{p}$ *tale per cui:*

$$\mathfrak{n} = \mathfrak{p} \cdot \mathfrak{m}$$

Consideriamo ora un gruppo G qualsiasi. Preso un sottogruppo H di G, possiamo definire due relazioni di equivalenza che partizionano il gruppo G: una partiziona il gruppo nella famiglia $\mathcal{F}_d = \{xH\}_{x \epsilon G}$ *e una nella famiglia* $\mathcal{F}_s = \{Hx\}_{x \epsilon G}$.

Si ha che:

$$|\mathcal{F}_d| = |\mathcal{F}_s| \overset{\text{def}}{=} [G: H] \text{ } e \text{ } |xH| = |Hx| = |H|$$

Consideriamo $\mathcal{F}_d$*, essendo una partizione di G si ha:*

$$G = \bigcup_{xH \epsilon \mathcal{F}_d} xH$$

Le classi laterali sono tutte disgiunte (essendo $\mathcal{F}_d$ una partizione) quindi possiamo asserire che:

$$|G| = \sum_{xH \in \mathcal{F}_d} |xH| = \sum_{xH \in \mathcal{F}_d} |H| = |H| \cdot \sum_{xH \in \mathcal{F}_d} 1 = |H| \cdot |\mathcal{F}_d| = |H| \cdot [G:H]$$

Quindi abbiamo dimostrato il seguente:

Teorema *(di Lagrange)*

Sia G un gruppo qualunque e H un suo sottogruppo, allora:

$$|G| = |H| \cdot [G:H]$$

Quindi la cardinalità di un sottogruppo, divide la cardinalità del gruppo.