Capitolo 1

INSIEMI

Il concetto di insieme è così generale che non ha senso cercare di definirlo in termini di nozioni più semplici: quindi si darà qui una caratterizzazione assiomatica degli insiemi, scrivendo dei postulati che generalizzino ciò che alla nostra intuizione si presenta come "famiglia", "aggregato" o generica "collezione" di oggetti. Per evitare i paradossi della teoria ingenua degli insiemi distingueremo fra *classi* ed *insiemi* immaginando intuitivamente che le classi siano insiemi così grandi da non poter figurare come elementi di altri insiemi.

1.1 Un sistema di assiomi

Introduciamo alcuni assiomi[1] per determinare il concetto di classe: supponiamo di avere solo, oltre al concetto indefinibile di classe, un altro concetto primitivo, vale a dire la relazione di "inclusione" $x \in y$ che interpretiamo come l'appartenenza dell'elemento x alla classe y.

Il primo assioma stabilisce il legame fra il concetto logico di uguaglianza e quello insiemistico di appartenenza: intuitivamente equivale a dire che un insieme è determinato dagli elementi che gli appartengono, e da null'altro:

Assioma 1. (di estensionalità) *Se A e B sono classi allora $A = B$ se e solo se A e B hanno gli stessi elementi.*

Volendo questa può essere presa come una definizione della relazione di uguaglianza in termini di appartenenza: ovviamente, a meno che non si lavori come fanno i logici con i linguaggi al primo ordine, si può definire l'uguaglianza come un concetto logico, seguendo Leibniz:

Principio di identità degli indiscernibili. *Se $A = B$ allora per ogni proprietà P si ha $P(A) \iff P(B)$.*

[1] Si tratta sostanzialmente dell'assiomatica proposta da J. von Neumann, K. Gödel, e P. Bernays.

Quest'ultimo è uno *schema di assiomi*, perché da esso si può desumere un assioma data una qualsiasi proposizione[2] $P(x)$ che contenga una variabile libera x.

Quando tutti gli elementi di una classe A sono anche elementi di una classe B scriviamo $A \subset B$: questo si può definire come

1.1.1 Definizione *$A \subset B$ se e solo se per ogni $x \in A$ si ha pure $x \in B$.*

Se $A \subset B$ e $B \subset A$ allora le classi sono uguali: $A = B$; in vista del prossimo assioma la seguente definizione è cruciale:

1.1.2 Definizione *Una classe A è un* insieme *se esiste una classe B tale che $A \in B$.*

Il secondo assioma è appunto uno schema di assiomi

Assioma 2. (DI FORMAZIONE DELLE CLASSI) *Esiste una classe i cui elementi sono esattamente gli insiemi che soddisfano la proposizione $P(X)$.*

Si noti che la classe la cui esistenza è postulata dall'assioma 2 è formata dagli *insiemi* e non dalle classi che soddisfano P.

1.1.3 Esempio *Esibiamo una classe che non è un insieme: si consideri la proposizione $P(x)$ definita come $x \notin x$ (il segno $\notin$ è la negazione dell'appartenenza: cioè $x \notin y$ se e solo se non è vero che $x \in y$); allora possiamo formare la classe R degli insiemi tali che $P(x)$: cioè R contiene gli* insiemi *x tali che $x \notin x$; si noti che questa classe è univocamente determinata (assioma di estensionalità) ma* non può essere un insieme*: supponiamo infatti che R sia un insieme: allora possiamo chiederci se $R \in R$ e questo è vero se e solo se $P(R)$ cioè se e solo se $R \notin R$: un assurdo. Quindi R non è un insieme.*

La classe postulata dall'assioma 2 si denota

$$\{x \mid P(x)\}$$

Ad esempio la classe vuota si può definire come

$$\emptyset = \{x \mid x \neq x\}$$

Che questo sia un insieme, dobbiamo peró assumerlo assiomaticamente.[3]

[2] In una trattazione rigorosa bisognerebbe definire il concetto di "proposizione" e caratterizzare quelle che si possono utilizzare per generare istanze di questo schema di assiomi; in questo caso supporremo che le nostre proposizioni siano formate con i quantificatori $\forall$, $\exists$ ed i soliti operatori logici usati in matematica (e, o, implica, se e solo se)... ed impiegati per connettere termini che siano altri predicati, negazioni di altri predicati o relazioni della forma $t = s$ o $Y \in X$.

[3] Si potrebbe obiettare che la classe $\emptyset$ è elemento della classe $\{\emptyset\}$ (la classe che ha come elemento esattamente l'insieme vuoto): ma per formare questa classe, dobbiamo sapere che $\emptyset$ sia un insieme.

Assioma 3. *La classe $\emptyset$ è un insieme.*

L'unione e l'intersezione sono ovviamente $A \cup B = \{X \mid X \in A \text{ oppure } X \in B\}$ e $A \cap B = \{X \mid X \in A \text{ e } X \in B\}$.

In generale definiamo unione e intersezione di una famiglia di insiemi ("famiglia" è un altro sinonimo di "classe") come

$$\bigcup_{i \in I} A_i = \bigcup \{A_i\}_{i \in I} = \{X \mid \exists i \in I \ X \in A_i\}$$
$$\bigcap_{i \in I} A_i = \bigcap \{A_i\}_{i \in I} = \{X \mid \forall i \in I \ X \in A_i\}$$

Osserviamo che in queste costruzioni otteniamo in generale delle classi. Per garantire che questi procedimenti diano luogo ad insiemi, dobbiamo imporre qualche altro assioma.

Assioma 4. *Se A e B sono insiemi allora $\{A, B\}$ è un insieme.*

Assioma 5. *Se A è un insieme e $B \subset A$ allora B è un insieme.*

Dato che si dimostra facilmente che, se $j \in I$ allora $\bigcap_{i \in I} A_i \subset A_j$, questo assioma implica ad esempio che l'intersezione di una famiglia qualsiasi di insiemi è un insieme. Per l'unione, vale invece la relazione $j \in I \Rightarrow A_j \subset \bigcup_{i \in I} A_i$ e quindi non si può usare l'assioma 5.

Assioma 6. *Se A è un insieme di insiemi allora l'unione $\bigcup A$ è un insieme.*

Se A è un insieme, è naturale considerare l'*insieme delle parti* di A, ovvero la classe dei suoi sottoinsiemi: è pure naturale imporre che si tratti a sua volta di un insieme.

Assioma 7. *Se A è un insieme, allora*

$$P(A) = \{X \mid X \subset A\}$$

è un insieme.

L'assioma 2 consente anche la formazione di coppie ed in genere successioni ordinate di elementi:

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

In generale, una n-pla $(a_1, ..., a_n)$ si definisce iterando la definizione di coppia. L'insieme di tutte le possibili coppie di elementi di A e B è il prodotto (cartesiano) di A per B:

$$A \times B = \{(a, b) \mid a \in A \text{ e } b \in B\}$$

Se $A = B$ lo denotiamo anche A^2. Ricordiamo che

1.1.4 Definizione *Una* relazione *fra due classi A e B è una sottoclasse del prodotto $A \times B$.*

1.1.5 Definizione *Una funzione da A in B è una relazione fra A e B tale che un elemento di B non possa essere in relazione con piú di un elemento di A, cioè se $(a, b) \in f$ e $(a, c) \in f$ allora $c = b$.*

Definiamo

$$\mathrm{Dom}(f) = \{a \,|\, a \in A \text{ e } \exists b \in B \; b = f(a)\}$$

(dominio della funzione f) e

$$\mathrm{im}(f) = \{b \,|\, b \in B \text{ e } \exists a \in A \; b = f(a)\}$$

(immagine della funzione f).

Notiamo che se A è un insieme, certamente lo è $\mathrm{Dom}(f)$; non è detto che lo sia $\mathrm{im}(f)$.

Assioma 8. *Se $f : A \longrightarrow B$ è una funzione e A è un insieme, allora* $\mathrm{im}(f)$ *è un insieme.*

Siamo ora in grado di definire una nozione generale di prodotto di insiemi: se $\{A_i\}_{i \in I}$ è una famiglia di insiemi allora il loro insieme prodotto $\prod_{i_I} A_i$ è l'insieme delle funzioni $f : I \longrightarrow A$. Gli assiomi che abbiamo dato implicano che sia un insieme *a patto che sia gli A_i che I siano insiemi.* Se per ogni $i \in I$ è $A_i = A$ allora denotiamo $A^I = \prod_{i \in I} A_i$.

Nel caso di famiglie qualsiasi, se un prodotto di insiemi non è vuoto, possiamo dire che ognuno degli insiemi che figurano nel prodotto non è vuoto? Per rispondere questo quesito è necessario chiarire il significato della parola "infinito" in teoria degli insiemi.

Assioma 9. (ASSIOMA DELL'INFINITO) *Esiste un insieme U tale che $\emptyset \in U$ e se $u \in U$ allora $u \cup \{u\} \in U$.*

Questo assioma implica l'esistenza di un insieme infinito perché consente, ad esempio, di costruire i numeri naturali. L'insieme postulato da questo assioma contiene almeno un elemento, il vuoto, ma contiene anche l'insieme formato dal vuoto $\{\emptyset\}$, ed anche l'insieme $\{\emptyset, \{\emptyset\}\}$ e così via. Definiamo allora i numeri naturali come

$$0 = \emptyset \qquad 1 = \{\emptyset\} \qquad 2 = \{\emptyset, \{\emptyset\}\} \qquad ...$$

e quindi l'insieme $\mathbb{N}$ dei numeri naturali. Formalmente, basta considerare la classe degli insiemi X tali che $\emptyset \in X$ e se $x \in X$ allora $x \cup \{x\} \in X$; l'intersezione di questa classe è l'insieme $\mathbb{N}$.

Ora dimostriamo che si tratta esattamente dei numeri naturali, cioè che $\mathbb{N}$ soddisfa gli assiomi di Peano.

Intanto $0 = \emptyset \in \mathbb{N}$. Poi, definiamo $n + 1$ come $n \cup \{n\}$ e lo chiamiamo il *successore* di n; in questo modo se $n \in \mathbb{N}$ allora $n + 1 \in \mathbb{N}$ ed è ovvio che 0 non è mai della forma $n + 1$ per qualche $n \in \mathbb{N}$. Inoltre abbiamo che:

$$\forall n, m \in N \qquad n + 1 = m + 1 \Rightarrow n = m$$

Infatti $n + 1 = n \cup \{n\}$ e quindi $n + 1 = m + 1$ implica $n \cup \{n\} = m \cup \{m\}$ cioè, per ogni x $((x \in n$ oppure $x \in \{n\}) \iff (x \in m$ oppure $x \in \{m\}))$, il che è vero se e solo se $x = n = m$ oppure n e m hanno gli stessi elementi e quindi ancora $n = m$.

Infine vale il principio di induzione matematica:

$$\forall N \subset \mathbb{N} \quad 0 \in N \text{ e } (\forall x \in N \quad x + 1 \in N) \Rightarrow N = \mathbb{N}$$

Infatti l'insieme $\mathbb{N}$ è l'intersezione della classe degli insiemi che soddisfano le ipotesi del principio di induzione, quindi $\mathbb{N} \subset N$.

Abbiamo in questo modo i numeri naturali, ciascuno dei quali è un insieme. Allora, ricordando la seguente

1.1.6 Definizione *Una funzione $f : A \longrightarrow B$ si dice*

(1) iniettiva *se $f(a) = f(b)$ implica $a = b$ e si dice in tal caso che A va in B.*

(2) suriettiva *se* $\mathrm{im}(f) = B$ *e si dice in tal caso che A va su B.*

(3) biunivoca *se è iniettiva e suriettiva e si dice in tal caso che A è biunivoco a B.*

possiamo dare quella di insieme finito:

1.1.7 Definizione *Un insieme è* finito *se è biunivoco a un numero naturale; in caso contrario si dice* infinito.

Torniamo ora ai prodotti di insiemi: notiamo che se $\{A_i\}_{i \in I}$ è una famiglia di insiemi, e se per qualche $i \in I$ si ha che $A_i = \emptyset$ allora $\prod_{i \in I} A_i = \emptyset$, esattamente come nel caso dei numeri (se uno dei fattori è nullo anche il prodotto è nullo; il viceversa è pure una proprietà che sembra naturale imporre (la "legge di annullamento del prodotto"), ma che non è possibile dimostrare a partire dagli assiomi fin qui dati.

Assioma 10. (assioma moltiplicativo) *Se $\prod_{i \in I} A_i = \emptyset$ allora esiste $i \in I$ tale che $A_i = \emptyset$.*

Ora ricaviamo da questo assioma un altro famoso enunciato: l'*assioma di scelta*. Per formularlo, diamo una

1.1.8 Definizione *Una funzione* $f : A \longrightarrow B$ *si dice* funzione di scelta *se per ogni* $C \in \mathrm{Dom}(A)$ *si ha che* $f(C) \in C$.

1.1.9 Teorema (ASSIOMA DI SCELTA) *Ogni insieme non vuoto ha una funzione di scelta che lo ammette come dominio.*

DIMOSTRAZIONE: Consideriamo ora un insieme A: possiamo immaginarlo come una famiglia di insiemi (i suoi elementi) indicizzata da A stesso; cioè $A = \{A_a\}_{a \in A}$ (dove $A_a = a$). In questo modo, il prodotto $\prod_{a \in A} A_a$ della famiglia A è l'insieme delle funzioni da $A \longrightarrow A$, che in questo caso sono tutte funzioni di scelta (dato che $(f(a)) \in A_a = a$). Dunque, dato che esiste $a \in A$ in modo che A_a è non vuoto (un modo contorto di dire che $A \neq \emptyset$), l'assioma moltiplicativo ci dice che anche $\prod_{a \in A} A_a$ è non vuoto, cioè che l'insieme delle funzioni di scelta su A è non vuoto.
QED

L'ultimo assioma è il seguente:

Assioma 11. (ASSIOMA DI FONDAZIONE) *Ogni classe* A *non vuota contiene un elemento* X *tale che* $A \cap X = \emptyset$.

Il significato intuitivo di questo assioma è che un insieme non può contenere se stesso come elemento. Un modo equivalente di esprimerlo è dire che un insieme non può contenere catene infinite di elementi, cioè a dire se A è un insieme, non può aversi una catena di appartenenze

$$... \in A_n \in ... \in A_2 \in A_1 \in A$$

1.2 Ordinamento e Lemma di Zorn

Le seguenti definizioni catturano il concetto di "relazione" ed in particolare di "ordinamento":

1.2.1 Definizione *Una relazione* $R \subset A^2$ *su un insieme* A *si dice*

(1) *di* ordine parziale *se è riflessiva, antisimmetrica e transitiva, ovvero se per ogni* $a \in A$ $(a, a) \in R$, *per ogni* $a, b \in A$ $(a, b) \in R \Rightarrow (b, a) \in R$ *e per ogni* $a, b, c \in A$ $((a, b) \in R$ *e* $(b, c) \in R) \Rightarrow (a, c) \in R$;

(2) *di* ordine totale *se è di ordine e se per ogni* $a, b \in R$ $(a, b) \in R$ *oppure* $(b, a) \in R$;

(3) *di* buon ordinamento *se è di ordine totale e se ogni* $B \subset A$ *non vuoto possiede un elemento minimo* m *(cioè per ogni* $b \in B$ *tale che* $(b, m) \in R$ *segue che* $b = m$*).*

(4) *di* equivalenza *se è riflessiva, transitiva e simmetrica cio per ogni* $a, b \in R$ $(a, b) \in R$ *e* $(b, a) \in R \Rightarrow a = b$*.*

(5) *Un insieme* A *parzialmente ordinato da* R *è* diretto *se per ogni* $a, b \in A$ *esiste un* $c \in A$ *tale che* aRc *e* bRc*.*

Se R è una relazione in un insieme A, in genere si scrive aRb in luogo di $(a, b) \in R$.

1.2.2 Definizione *Sia* A *un insieme ordinato dalla relazione* $\leq$*.*

(1) *Una* catena C *in* A *è un sottoinsieme totalmente ordinato da* $\leq$*.*

(2) *Un* confine superiore (inferiore) *di un sottoinsieme* B *di* A *è un elemento* $s \in A$ *tale che per ogni* $b \in B$ *si abbia* $b \leq s$ $(s \leq b)$*.*

(3) *Un* massimale (minimale) *in* A *è un elemento* $m \in A$ *tale che per ogni* $a \in A$ *tale che* $m \leq a$ *si abbia* $a = m$ *(tale che* $a \leq m$ *si abbia* $a = m$*).*

(4) *Il* estremo inferiore (superiore) $\inf B$ $(\sup B)$ *di un sottoinsieme* $B \subset A$ *è il minimo dei confini superiori (massimo dei confini inferiori) di* B*.*

Si noti che un elemento massimale non è necessariamente un massimo.

1.2.3 Definizione *Sia* A *un insieme bene ordinato dalla relazione* $\leq_A$*. Un sottoinsieme* $B \subset A$ *si dice*

(1) Segmento iniziale *di* A *se per ogni* $a, b \in A$ *da* $a \in B$ *e* $b \leq_A a$ *segue che* $b \in B$*.*

(2) Segmento iniziale chiuso *di* A *se esiste un* $a \in A$ *tale che* $B = \{b \in A | b \leq_A a\}$ *e l'elemento* a *si dice* estremo *di* B*.*

(3) Segmento iniziale aperto *di* A *se esiste un* $a \in A$ *tale che* $B = \{b \in A | b <_A a\}$*.*

Osserviamo che $\emptyset$ è segmento iniziale di ogni insieme bene ordinato (notare l'analogia con le definizioni di intervalli aperti e chiusi a destra nei numeri reali). Passiamo ora alla dimostrazione del principale risultato che coinvolge queste definizioni:

Lemma di Zorn. *Sia* A *un insieme ordinato dalla relazione* $\leq$*; se ogni catena in* A *ha un confine superiore, allora* A *possiede un elemento massimale.*

DIMOSTRAZIONE: Consideriamo l'insieme

$$C = \{B \subset A \,|\, B \text{ è una catena in } A\}$$

e, per ogni $c \in C$, l'insieme

$$S(c) = \{a \in A \,|\, a \text{ è confine superiore di } C\}$$

Supponiamo per assurdo che A non possieda un massimale; allora la famiglia

$$F = \{S(B) \setminus B\}_{B \in C}$$

è formata da sottoinsiemi di A non vuoti. Per l'assioma di scelta esiste una funzione $f : C \longrightarrow A$ tale che, per ogni $B \in C$, $f(B) = S(B) \setminus B$.

Sia ora Z l'insieme delle catene B (non vuote) tali che per ogni segmento iniziale B' di B (diverso da B) di abbia

$$f(B') = \inf\{B \setminus B'\}$$

i.e. una catena B di A sta in Z se e solo se la funzione di scelta sceglie in ogni suo segmento iniziale un elemento che è piú piccolo di ogni elemento di B che non è in B'.

Ovviamente $f(\emptyset) \in Z$ che è quindi non vuoto e se $B', B'' \in Z$, dato che $f(\emptyset)$ è il minimo, in B' e B'' deve esistere un segmento iniziale comune a B' ed a B'', e quindi l'unione di tali segmenti è un insieme S non vuoto: si tratta naturalmente di un segmento iniziale sia per B' che per B''.

Per quanto si è visto, l'insieme $S \cup \{f(S)\}$ è ancora un segmento iniziale (la f sceglie un elemento apposta in questo modo) e quindi è un sottoinsieme di C: questo non può essere a meno che non sia $C = B'$ oppure $C = B''$.

Ne concludiamo che se $B', B'' \in Z$ allora deve aversi $B' \subset B''$ oppure $B'' \subset B'$; quindi l'insieme

$$B^* = \bigcup_{B \in Z} B$$

è una catena in A. Ma, di nuovo, $B^* \cup \{f(B^*)\} \in Z$ il che contraddice sia la definizione di B^* che il fatto $f(B^*) \in S(B^*) \setminus B^*$. L'assurdo deriva dunque dall'ipotesi che esistano elementi non vuoti nella famiglia F, e cioè dall'aver supposto l'insieme A privo di massimali.

QED

Il primo e principale esempio di applicazione del lemma di Zorn è il teorema di Zermelo secondo il quale ogni insieme è bene ordinabile: in séguito si avrà occasione di dare molte applicazioni del lemma di Zorn.

Teorema del Buon Ordinamento. (Zermelo) *Per ogni insieme A esiste una relazione d'ordine $\leq_A$ su A rispetto alla quale A è bene ordinato.*

Dimostrazione: Consideriamo l'insieme

$$W = \{(B, \leq_B) \,|\, B \subset A \text{ e } \leq_B \text{ è un buon ordinamento su } B\}$$

Definiamo su W un ordinamento $\ll$ come segue: $(B, \leq_B) \ll (B', \leq_{B'}) \iff B \subset B'$, $\leq_{B'}$ ristretto a B è $\leq_B$ e B è segmento iniziale di B.

Cioè un elemento $B \in W$ è piú piccolo di un altro $B' \in W$ se è piú piccolo come insieme ($B \subset B'$), se è pure piú piccolo come insieme ordinato (nel senso che la relazione di ordine su B' ristretta agli elementi di B sia esattamente la relazione di ordine su B) e se non esistano elementi in $B' \subset B$ piú piccoli di un qualsiasi elemento di B.

Ora consideriamo una catena $\{B_i\}_{i\in I}$ in W rispetto all'ordine parziale $\ll$. Allora l'insieme $B^* = \bigcup_{i\in I} B_i$ unione di questa catena è totalmente ordinato rispetto alla relazione unione delle relazioni d'ordine $\{\leq_{B_i}\}_{i\in I}$.

Sia C è un sottoinsieme non vuoto di B^*; ciò vuol dire che esiste un indice $i_0 \in I$ tale che $C \cap B_{i_0} \neq \emptyset$. L'insieme B_{i_0} è bene ordinato dalla sua relazione $\leq_{B_0}$ (per definizione) e quindi il suo sottoinsieme $C \cap B_{i_0}$ ha un elemento minimo c_0 (rispetto all'ordinamento $\leq_{B_{i_0}}$).

Ma B_{i_0} è segmento iniziale di A, e dunque c_0 è anche un minimo rispetto all'ordinamento di ogni altro B_i, col che c_0 è minimo rispetto all'ordinamento di B^*. Quindi $A \in W$.

è poi ovvio che A è un confine superiore per la catena $\{(B_i, \leq_i)\}_{i\in I}$ in W rispetto all'ordinamento $\ll$. Cioè l'insieme ordinato W soddisfa alle ipotesi del lemma di Zorn e quindi deve avere un elemento massimale $(M, \leq_M)$.

Per dimostrare il teorema basta far vedere che $M = A$. Se esistesse un elemento $a_0 \in A \setminus M$ allora $M \cup \{a_0\}$, con la relazione d'ordine che su M coincide con $\leq_M$ e che rende a_0 maggiore di ogni elemento di M, è ancora un elemento di W, il che contraddice la massimalità di M.

QED

1.3 Numeri ordinali e cardinali

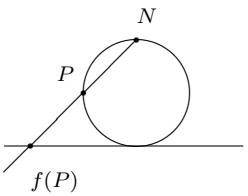
Contare gli elementi di un insieme finito significa metterli in corrispondenza biunivoca con un numero naturale: abbiamo così la possibilità di determinarne il numero di elementi di un insieme finito, che, in linguaggio insiemistico, si dice *cardinalità*. Vogliamo ora estendere il concetto di "numero di elementi di un insieme" anche al caso infinito.

1.3.1 Definizione *Due insiemi A e B si dicono* equipotenti *ovvero si dice che hanno la* stessa cardinalità *se sono biunivoci e si scrive in tal caso* $\mathrm{Card}(A) = \mathrm{Card}(B)$.

1.3.2 Esempio

(1) *Due numeri naturali sono equipotenti se e solo se sono uguali.*

(2) *L'insieme dei numeri reali $\mathbb{R}$ è equipotente all'intervallo $(0,1)$: un modo per vederlo è osservare che questo intervallo è equipotente ad una circonferenza del piano privata di un punto (ad esempio $t \longmapsto (\cos 2\pi t, \sin 2\pi t)$ è biunivoca fra $(0,1)$ e la circonferenza di centro l'origine e raggio 1 privata del punto $(1,0)$). Che poi una circonferenza privata di un punto sia equipotente a $\mathbb{R}$ si vede considerando un proiezione: se consideriamo ad esempio la circonferenza di centro $(0,1)$ e raggio 1 privata del punto $N = (0,2)$, possiamo associare ad un punto P di questo insieme l'unico punto $f(P)$ dell'asse reale $\{y = 0\}$ che interseca la retta per P e per il punto $(0,2)$.*



1.3.3 Definizione *Un insieme è* numerabile *se è equipotente a* $\mathbb{N}$.

Stabiliamo una notazione: avendo denotato col simbolo $\mathrm{Card}(A) = \mathrm{Card}(B)$ l'esistenza di una funzione biunivoca fra A e B, denotiamo col simbolo $\mathrm{Card}(A) \leq \mathrm{Card}(B)$ l'esistenza di una funzione iniettiva da A in B, e col simbolo $\mathrm{Card}(A) < \mathrm{Card}(B)$ l'esistenza di una funzione iniettiva fra A e B e la non esistenza di funzioni biunivoche fra A e B.

1.3.4 Teorema (CANTOR–SCHRÖDER–BERNSTEIN)

$$\mathrm{Card}(A) \leq \mathrm{Card}(B) \ e \ \mathrm{Card}(B) \leq \mathrm{Card}(A) \Rightarrow \mathrm{Card}(A) = \mathrm{Card}(B)$$

DIMOSTRAZIONE: (Birkhoff–MacLane) Osserviamo preliminarmente che, come in ogni questione riguardante la cardinalità, possiamo considerare gli insiemi A e B disgiunti (cioè $A \cap B = \emptyset$), dato che se non lo sono, possiamo considerare $C = A \cap B$ e porre $B' = (B \setminus C) \cup C'$ con C' insieme equipotente a C e disgiunto da C in modo che, ovviamente, $\mathrm{Card}(B) = \mathrm{Card}(B')$.

Dimostriamo quindi il teorema nell'ipotesi che sia $A \cap B = \emptyset$; consideriamo due funzioni (che esistono per ipotesi) $f : A \longrightarrow B$ e $g : B \longrightarrow A$ iniettive. Definiamo per un elemento a di A o B un suo discendente come un elemento che sia stato ottenuto con applicazioni successive delle funzioni f e g (ad esempio $g(f(g(b))) \in A$ è discendente di $b \in B$). Allora possiamo decomporre A in tre insiemi: A_P che consiste degli elementi di A che hanno un numero pari di discendenti, A_D che consiste degli elementi di A che hanno un numero dispari di discendenti e A_I che consiste degli elementi di A con un numero infinito di discendenti. Analogamente decomponiamo B ed osserviamo che f manda A_P su B_D e A_I su B_I e che g^{-1} manda A_D su B_P. Quindi la funzione che, su $A_P \cup A_I$ è definita come f e che su A_D è definita come g^{-1} è biunivoca da A in B.

QED

1.3.5 Teorema (Cantor) *Se A è un insieme, allora* $\mathrm{Card}(A) < \mathrm{Card}(P(A))$.

Dimostrazione: Che si abbia $\mathrm{Card}(A) \leq \mathrm{Card}(P(A))$ è ovvio: la funzione $f : A \longrightarrow P(A)$ definita come $f(a) = \{a\}$ è manifestamente iniettiva. Ora dimostriamo per assurdo che $\mathrm{Card}(A) \neq \mathrm{Card}(P(A))$.

Supponiamo cioè che esista una funzione biunivoca $f : A \longrightarrow P(A)$, e definiamo l'insieme

$$B = \{a \in A \,|\, a \notin f(a)\}$$

Per definizione è $B \subset A$ e quindi $B \in P(A)$. Deve allora esistere un unico elemento $a_B \in A$ tale che $f(a_B) = B$; ma se $a_B \in B$ allora $a_B \notin f(a_B) = B$ che è assurdo; quindi deve aversi $a_B \notin B$, cioè a dire $a_B \in f(a_B) = B$ che è un altro assurdo.

Quindi la funzione biunivoca f non può esistere.

QED

Osserviamo che i numeri che abbiamo incontrato finora (i naturali e ω stesso) sono insiemi che hanno due particolarità, espresse dalle definizioni seguenti:

1.3.6 Definizione

(1) *Un insieme A è* pieno *se per ogni $B \in A$ si ha pure $B \subset A$.*

(2) *Un insieme A è* transitivo *se per ogni $B \in A$ e per ogni $C \in B$ si ha che $C \in A$.*

(3) *Un* numero ordinale *è un insieme pieno e transitivo.*

Cioè un ordinale contiene come elementi esattamente i suoi sottoinsiemi e gli elementi dei suoi elementi.

1.3.7 Teorema *Un numero ordinale è bene ordinato dalla relazione* $\in$.

DIMOSTRAZIONE: Consideriamo un numero ordinale α: che la relazione $\in$ sia un ordinamento parziale in α è ovvio; dimostriamo che ogni sottoinsieme A non vuoto di α ha un primo elemento. Per l'assioma di fondazione v'è un elemento $a \in A$ tale che $a \cap A = \emptyset$ e quindi nessun elemento di a appartiene ad A, il che vuol dire che a è il primo elemento di A.

QED

1.3.8 Lemma *Sia* α *un ordinale.*

(1) *Se* $A \subset \alpha$, $A \neq \alpha$ *e* A *è pieno allora* $A \in \alpha$.

(2) *Se* β *è un ordinale allora* $\alpha \subset \beta$ *oppure* $\beta \subset \alpha$.

(3) *Se* β *è un ordinale allora* $\alpha \in \beta$ *oppure* $\beta \in \alpha$ *oppure* $\beta = \alpha$.

(4) *Se* $A \in \alpha$ *allora* A *è un ordinale.*

DIMOSTRAZIONE:

(1) Per transitività di A esiste un $B \in A$ tale che $A = \{a \in \alpha | a \in B\}$. Infatti l'insieme $\alpha \setminus A$ ha un primo elemento B per la relazione $\in$, ed è un esercizio vedere che A è formato dagli elementi che appartengono a questo B. Per concludere basta allora osservare che, essendo ogni elemento di B anche elemento di α ne segue che $A = B$.

(2) L'insieme $\alpha \cap \beta$ è piena e per (1) è $\alpha = \alpha \cap \beta$ oppure $\alpha \cap \beta \in \alpha$; nel primo caso troviamo immediatamente $\alpha \subset \beta$, mentre nel secondo caso, otteniamo $\alpha \cap \beta \notin \beta$ (dato che $\alpha \cap \beta \in \alpha \cap \beta$), e quindi, per (1), $\alpha \cap \beta = \beta$ (dato che $\alpha \cap \beta \notin \beta$) sicché $\beta \subset \alpha$.

(3) Ovvio!

(4) Che A sia pieno segue dal fatto che lo è α; per vedere che è transitivo, si osservi che α è bene ordinato da $\in$ e che $A \in \alpha$: allora se $C \in B$ e $B \in A$ allora $C \in A$.

QED

1.3.9 Definizione *Una funzione* $f : A \longrightarrow B$ *fra due insiemi totalmente ordinati* A *e* B *si dice un* isomorfismo (ordinale) *se è suriettiva e monotona:*

$$\forall a, b \in A \quad a \leq_A b \Rightarrow f(a) \leq_B f(b)$$

Un isomorfismo ordinale è necessariamente iniettivo ed il suo inverso è un isomorfismo ordinale.

1.3.10 Lemma *Siano A e B insiemi totalmente ordinati.*

(1) *Se $f : A \longrightarrow B$ è un isomorfismo ordinale e S è un segmento iniziale (aperto, chiuso) in A, allora $f(S)$ è un segmento iniziale (aperto, chiuso) in B.*

(2) *Se S è un segmento iniziale di A e A è bene ordinato, allora (se $S \neq A$) S è aperto.*

(3) *Se $f : A \longrightarrow B$ e $g : B \longrightarrow A$ sono isomorfismi ordinali fra un insieme bene ordinato A ed un segmento iniziale di un insieme totalmente ordinato B allora $f = g$.*

1.3.11 Teorema *Per ogni insieme A bene ordinato dalla relazione $\leq$ esiste un unico ordinale α che sia isomorfo (con la relazione $\in$) ad A come insieme ordinato.*

Dimostrazione: L'unicità segue facilmente dalla (3) del lemma precedente. Dimostriamo l'esistenza di α: denotiamo con B l'insieme di tutti gli $a \in A$ tali che esistano un ordinale α_a e un isomorfismo f_a dell'insieme bene ordinato α_a sul segmento chiuso S_a di estremo a: notiamo che per il lemma precedente questa funzione f_a è univocamente determinata da a.

Ora sia $c \in B$ tale che $b \leq c$. Allora l'insieme $\alpha_0 = \{f_c^{-1}(a)\}_{a \in S_b}$ è un numero ordinale. la funzione f ristretta a α_0 è un isomorfismo su S_b e quindi $b \in B$ e $f_b = f_c|_{\alpha_0}$. In altri termini $f_b \subset f_c$.

Ma allora la funzione $f_0 = \bigcup_{a \in B} f_a$ è un isomorfismo dell'ordinale $\beta_0 = \bigcup_{a \in B} \alpha_a$ su B. Ora, se $A = B$ il teorema è dimostrato, altrimenti, se $A \neq B$, comunque B è segmento iniziale di A, che è bene ordinato, sicché deve esistere un $a_0 \in A$ tale che $B = S_{a_0}$. Dunque $f_0 \cup \{(\beta_0, \alpha_0)\}$ è un isomorfismo dell'ordinale $\beta_0 + 1 = \beta_0 \cup \{\beta_0\}$ su $B \cup \{\alpha_0\} = S_{a_0}$ il che implica $a_0 \in B$ che è un assurdo. Quindi $A = B$.

QED

Dato che ogni insieme è bene ordinato, per una opportuna relazione d'ordine totale, dal teorema precedente segue che ogni insieme è isomorfo a un numero ordinale: in particolare un isomorfismo è una funzione biunivoca e quindi

1.3.12 Corollario *Ogni insieme è equipotente a un numero ordinale.*

Un insieme qualsiasi è ordinato dalla relazione di uguaglianza: $a \leq a$ se e solo se $a = a$. Questo è un ordinamento banale, che non aggiunge alcuna ulteriore informazione alla natura dell'insieme stesso e definiamo i numeri cardinali come gli ordinali che tengano conto di questa relazione.

1.3.13 Definizione *Un numero ordinale α è un* numero cardinale *se per ogni ordinale $\beta \leq \alpha$[4], β e α* non *sono equipotenti.*

Dimostriamo ora che per ogni insieme A possiamo trovare un solo numero cardinale che sia equipotente ad A; chiameremo questo numero la *cardinalità* di A e lo indicheremo con $\mathrm{Card}(A)$

1.3.14 Teorema *Per ogni insieme A esiste un unico cardinale $\mathfrak{a}$ ad esso equipotente.*

DIMOSTRAZIONE: Dato che A è bene ordinabile, per il corollario 1.3.12 esiste un unico ordinale α isomorfo (in particolare equipotente) a A; ora vogliamo trovare un cardinale $\mathfrak{a}$ equipotente a α (e quindi ad A). Questo è facilissimo: dato che α è bene ordinato da $\in$ esiste un ordinale $\mathfrak{a} \leq \alpha$ equipotente a α ma i cui elementi siano tutti non equipotenti a α; questo $\mathfrak{a}$ è quindi un cardinale.

L'unicità di $\mathfrak{a}$ segue dall'unicità di α sancita nel corollario 1.3.12 e dalla definizione di numero cardinale.

QED

1.3.15 Corollario *Per ogni numero ordinale α esiste un unico numero cardinale equipotente a α.*

1.3.16 Teorema *Se A è un insieme infinito, allora* $\mathrm{Card}(A^2) = \mathrm{Card}(A)$.

DIMOSTRAZIONE: Consideriamo la funzione

$$\begin{aligned} f : A &\longrightarrow A^2 \\ a &\longmapsto (a, a) \end{aligned}$$

Dato che è iniettiva, abbiamo subito che $\mathrm{Card}(A) \leq \mathrm{Card}(A^2)$. Ora procediamo per assurdo: supponiamo che non valga la $\mathrm{Card}(A^2) \leq \mathrm{Card}(A)$; allora l'insieme C dei cardinali infiniti $\mathfrak{a}$ tali che

$$\mathfrak{a} \leq \mathrm{Card}(A) \text{ e } \mathfrak{a} < \mathrm{Card}(\mathfrak{a}^2)$$

è non vuoto e, i cardinali sono bene ordinati, sia $\mathfrak{a}_0$ il suo minimo. Sull'insieme $\mathfrak{a}_0^2$ definiamo una relazione d'ordine $\leq$ come

$$\begin{aligned} (\alpha, \alpha') \leq (\beta, \beta') \iff & \max(\alpha, \alpha') < \max(\beta, \beta') \text{ oppure} \\ & \alpha < \beta \text{ e } \max(\alpha, \alpha') < \max(\beta, \beta') \text{ oppure} \\ & \alpha = \beta \text{ e } \alpha' \leq \beta' \text{ e } \max(\alpha, \alpha') < \max(\beta, \beta') \end{aligned}$$

[4]Ricordiamo che per gli ordinali la relazione $\leq$ significa $\in$.

In questo modo $\mathfrak{a}^2$ è totalmente ordinato; ma è pure bene ordinato: per ogni insieme non vuoto $B \subset \mathfrak{a}^2$ i seguenti sottoinsiemi sono non vuoti (in virtù della definizione della relazione $\leq$ su $\mathfrak{a}^2$):

$$B_1 = \{(\alpha, \alpha') \in B | \forall (\beta, \beta') \in B \ \max(\alpha, \alpha') \leq \max(\beta, \beta')\}$$
$$B_2 = \{(\alpha, \alpha') \in B_1 | \forall (\beta, \beta') \in B_1 \ \alpha < \beta\}$$
$$B_3 = \{(\alpha, \alpha') \in B_2 | \forall (\beta, \beta') \in B_2 \ \alpha' < \beta'\}$$

e B_3 non può che contenere esattamente un elemento, che è proprio il minimo in B rispetto alla relazione $\leq$. Dato che $\mathfrak{a}_0 < \mathrm{Card}(\mathfrak{a}_0^2)$, l'insieme bene ordinato (dalla relazione $\in$) $\mathfrak{a}_0$ è isomorfo al segmento iniziale S (aperto di estremo (α_0, β_0)) dell'insieme bene ordinato $\mathfrak{a}_0^2$. Ora consideriamo il massimo δ_0 fra α_0 e β_0; evidentemente deve aversi

$$B \subset (\delta \cup \{\delta\})^2$$

(notare che $\delta + 1 = \delta \cup \{\delta\}$). Ma α_0 è infinito e quindi anche B e δ_0 lo sono e si ha

$$\mathrm{Card}(\delta_0 + 1) = \mathrm{Card}(\delta_0) < \mathfrak{a}_0$$

Allora, per minimalità di $\mathfrak{a}_0$ in C, abbiamo

$$\mathfrak{a}_0 = \mathrm{Card}(B) \leq \mathrm{Card}((\delta_0 + 1)^2) \leq \mathrm{Card}(\delta_0 + 1) \leq \mathfrak{a}_0$$

che è assurdo. Quindi l'insieme C è vuoto e il teorema è dimostrato.

QED

1.3.17 Corollario *Siano A e B insiemi, con A infinito.*

(1) *Se $B \neq \emptyset$ allora* $\mathrm{Card}(A \times B) = max(\mathrm{Card}(A), \mathrm{Card}(B))$.

(2) $\mathrm{Card}(A \cup B) = max(\mathrm{Card}(A), \mathrm{Card}(B))$.

(3) *Se $n \in \mathbb{N}$ oppure se $n = \mathbb{N}$ allora* $\mathrm{Card}(A^n) = \mathrm{Card}(A)$.

Si può dimostrare che il teorema precedente non solo è conseguenza, ma equivale al teorema del buon ordinamento. Concludiamo riportando alcuni fondamentali risultati dovuti a Cantor.

Ricordiamo che possiamo identificare i numeri razionali con le frazioni $\frac{n}{m}$ (con $n, m \neq 0$ interi) e quindi delle coppie $(n, m) \in \mathbb{N} \times \mathbb{N} \setminus \{0\}$ modulo la relazione di equivalenza $(n, m) \equiv (n', m') \iff \exists a \in \mathbb{Z} \ an = n', am = m'$. Usando il teorema precedente abbiamo che $\mathbb{Q}$ è numerabile.

1.3.18 Definizione *Una* successione *in un insieme A è una funzione $s : \mathbb{N} \longrightarrow A$; si denota pure $\{s_n\}_{n \in \mathbb{N}}$ e si scrive quindi $s(n) = s_n$.*

1.3.19 Teorema (CANTOR) *L'insieme* $\mathbb{R}$ *non è numerabile.*

DIMOSTRAZIONE: Basta dimostrare la non numerabilità dell'intervallo $I = (0, 1)$ che è infatti biunivoco con $\mathbb{R}$. Supponiamo per assurdo che I sia numerabile: allora deve esistere una successione $\{r_n\} = I$. Un elemento di $r_n \in I$ è un numero reale positivo minore di 1, che ha dunque uno sviluppo decimale della forma

$$r_n = c_{n1}10^{-1} + c_{n2}10^{-2} + c_{n3}10^{-3} + ... = \sum_{k=1}^{\infty} c_{nk}10^{-k}$$

(le c_{nk} sono le cifre dello sviluppo decimale di r_n). La successione $\{r_n\}$ dà quindi luogo ad una "tabella infinita"

$$\begin{array}{l} r_0 \longleftrightarrow r_{01}\ r_{02}\ r_{03}... \\ r_1 \longleftrightarrow r_{11}\ r_{12}\ r_{13}... \\ r_2 \longleftrightarrow r_{21}\ r_{22}\ r_{23}... \\ \quad\vdots \qquad\quad \vdots \end{array}$$

Ora, combinando arbitrariamente una successione di cifre a_1, a_2, a_3,... possiamo costruire il numero reale $r \in I$ il cui sviluppo è $\sum_{k\in\mathbb{N}^+} a_k 10^{-k}$ e questo deve figurare da qualche parte nella successione (r_n), deve cioè esistere un n_0 (dipendente da (a_m)) tale che $r = r_{n_0}$.

Come successione (a_m) prendiamo quella il cui elemento m-mo a_m è zero se il termine r_{mm} della tabella precedente è diverso da zero, e 1 se il termine r_{mm} della tabella precedente è uguale a zero. L'elemento r non potrà mai figurare nella tabella, cioè la successione (a_m) non corrisponde a nessuna (r_{nk}); infatti se fosse $a_m = r_{n_0 m}$ per un certo numero naturale n_0 allora, se $a_{n_0} = 0$ avremmo $r_{n_0 n_0} \neq 0$ e quindi $a_{n_0} \neq 0$ e se $a_{n_0} \neq 0$ avremmo $r_{n_0 n_0} = 0$ e quindi $a_{n_0} = 0$. In ogni caso un assurdo, e quindi la successione (r_n) non può esistere.

QED

1.3.20 Teorema (CANTOR) $\mathrm{Card}(\mathbb{R}) = 2^{\mathbb{N}}$.

Il significato di $2^{\mathbb{N}}$ è evidente: 2 è l'insieme con due elementi $2 = \{0, 1\}$. Allora se A è un insieme e B è un altro insieme, poniamo per definizione

$$\mathrm{Card}(A)^{\mathrm{Card}(B)} = \mathrm{Card}(A^B)$$

In questo modo definiamo l'esponenziale per i numeri cardinali. Se A è finito e B è numerabile allora $\mathrm{Card}(A^B) = 2^{\mathbb{N}}$. Il teorema di Cantor afferma che la cardinalità dei numeri reali (che si dice *cardinalità del continuo*) è proprio questa.

Per dimostrarlo si tenga presente il fatto che 2^A è semplicemente l'insieme delle funzioni da A in $\{0,1\}$ cioè un insieme di cifre binarie indicizzato da A; ogni numero reale ammette sviluppi in base due (abbiamo usato prima quelli in base dieci) ove, ad esempio, i numeri 0,111111... e 1 sono esattamente lo stesso (in base due... in base dieci l'esempio è 0,999999... = 1).

1.4 Categorie e funtori

Sarà utile, nel seguito, il linguaggio astratto delle categorie.

1.4.1 Definizione *Una* categoria $\mathcal{C}$ *è determinata da una classe* $\mathrm{Ob}\,\mathcal{C}$ *i cui elementi si dicono* oggetti *della categoria e da due funzioni:*

(1) *Una funzione che ad ogni coppia di oggetti* X, Y *associ un insieme* $\hom(X,Y)$ *i cui elementi si diranno* morfismi.

(2) *Una funzione che, per ogni tripla di oggetti* X, Y, Z *associ una funzione*

$$\hom(Y,Z) \times \hom(Y,X) \longrightarrow \hom(X,Z)$$

(denotata con $(f,g) \longmapsto g \circ f$ *e che si dirà* composizione *dei morfismi* f *e* g*), tale che valgano i seguenti assiomi:*

$$h \circ (g \circ f) = (h \circ g) \circ f$$
$$1_Y \circ f = f \ \ e \ \ g \circ 1_Y = g$$

Il morfismo 1_Y si dice *identità* e la classe dei morfismi $\{\hom(X,Y)\}_{X,Y \in \mathrm{Ob}\,\mathcal{C}}$ si denota con $\mathrm{Mor}\,\mathcal{C}$. Vediamo alcuni esempi importanti di categorie.

La categoria $\mathbb{S}$: i suoi oggetti sono tutti gli insiemi e, se X, Y sono insiemi un morfismo è una qualsiasi funzione $f : X \longrightarrow Y$. La composizione è esattamente la composizione di funzioni e le identità sono esattamente le funzioni identità di ciascun insieme. Ovviamente gli oggetti di $\mathbb{S}$ ed i suoi morfismo sono classi che non sono insiemi.

La categoria $\mathbb{G}$ dei gruppi: i suoi oggetti sono tutti i gruppi (si noti che una classe C non può essere un gruppo, perché per definire l'operazione bisogna considerare una funzione $C \times C \longrightarrow C$) ed i suoi morfismi gli omomorfismi fra i gruppi. Si tratta di una sottocategoria di $\mathbb{S}$ nel senso della seguente

1.4.2 Definizione *Se* $\mathcal{C}$ *è una categoria, una sua* sottocategoria *è una categoria* $\mathcal{D}$ *tale che* $\mathrm{Ob}\,\mathcal{D} \subset \mathrm{Ob}\,\mathcal{C}$*. Una sottocategoria* $\mathcal{D}$ *di una categoria* $\mathcal{C}$ *si dice* piena *se per ogni* $X, Y \in \mathrm{Ob}\,\mathcal{D} \subset \mathrm{Ob}\,\mathcal{C}$ *si ha che* $\hom_{\mathcal{D}}(X,Y) = \hom_{\mathcal{C}}(X,Y)$ *ove* $\hom_{\mathcal{C}}(X,Y)$ *denota i morfismi fra* X *e* Y *nella categoria* $\mathcal{C}$*.*

1.4.3 Esempio *La categoria $\mathbb{AB}$ dei gruppi abeliani (i suoi oggetti sono gruppi abeliani e i morfismi gli omomorfismi) è una sottocategoria piena della categoria $\mathbb{G}$ dei gruppi.*

In generale, tutte le categorie che avremo modo di considerare sono sottocategorie di $\mathbb{S}$: ogni qual volta si definisce una struttura su un insieme ed una classe di applicazioni che preserva tale struttura, si può considerare la categoria associata: gli anelli, gli spazi vettoriali, i campi,... sono tutti esempi di categorie.

Non ogni esempio di categoria sorge in questo modo: se K è un anello commutativo, possiamo considerare la categoria $\mathbb{M}_K$ i cui oggetti sono gli interi positivi e i cui morfismi $\hom(m,n)$ sono le matrici $M_{n,m}(K)$ $m \times n$ a coefficienti in K. La composizione di morfismi sarà il prodotto di matrici.

Non bisogna cioè pensare che i morfismi di una categoria siano necessariamente applicazioni fra insiemi.

1.4.4 Esempio *Se P è un insieme parzialmente ordinato dalla relazione $\leq$ allora individua una categoria $\mathcal{P}$ i cui oggetti sono gli elementi di P (i.e. $\mathrm{Ob}\,\mathcal{P} = P$) ed i morfismi sono così definiti:*

$$\hom(p,q) = \begin{cases} \{i_{pq}\} & \text{se } p \leq q \\ \emptyset & \text{altrimenti} \end{cases}$$

Cioè esiste un solo morfismo fra p e q (che è un simbolo univocamente determinato da p e q) se $p \leq q$; altrimenti non esiste nessun morfismo (si noti che le identità sono i simboli i_{pp}).

In generale, dato un qualsiasi grafo composto da vertici e frecce orientate, questo definisce una categoria, i cui oggetti sono i vertici ed i cui morfismi le frecce.

1.4.5 Esempio *Un gruppo G induce una categoria $\mathbb{C}(G)$ con: $\mathrm{Ob}\,\mathbb{C}(G) = \{e\}$ (identità del gruppo) e $\hom(e,e) = G$; la composizione è il prodotto del gruppo.*

In questo esempio abbiamo una proprietà particolare: per ogni morfismo f esiste un *inverso* i.e. un morfismo g tale che $f \circ g = 1$ e $g \circ f = 1$. è un esercizio verificare che ogni categoria i cui morfismi siano tutti invertibili è della forma $\mathbb{C}(G)$ per un opportuno gruppo G.

Evidentemente fra due categorie $\mathbb{C}(G)$ e $\mathbb{C}(H)$ esistono delle applicazioni che è naturale considerare, e che sono indotte dagli omomorfismi del gruppo G nel gruppo H. Si tratta di un caso particolare della nozione seguente.

1.4.6 Definizione *Se $\mathcal{C}$ e $\mathcal{D}$ sono categorie, un* funtore $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ *è determinato da*

(1) *Una funzione* $\mathcal{F} : \mathrm{Ob}\,\mathcal{C} \longrightarrow \mathrm{Ob}\,\mathcal{D}$.

(2) *Una funzione* $\mathcal{F} : \mathrm{Mor}\,\mathcal{C} \longrightarrow \mathrm{Mor}\,\mathcal{D}$.

in modo che

$$\forall X \in \mathrm{Ob}\,\mathcal{C} \quad \mathcal{F}(1_X) = 1_{\mathcal{F}(X)}$$

$$\forall f \in \hom(Y, Z) \forall g \in \hom(X, Y) \quad \mathcal{F}(f \circ g) = \mathcal{F}(f) \circ \mathcal{F}(g)$$

Quindi un funtore è un "morfismo" fra categorie, nel senso che preserva la struttura categorica. In particolare, se un funtore $\mathcal{F}$ è tale che le applicazioni $\mathcal{F} : \mathrm{Ob}\,\mathcal{C} \longrightarrow \mathrm{Ob}\,\mathcal{D}$ e $\mathcal{F} : \mathrm{Mor}\,\mathcal{C} \longrightarrow \mathrm{Mor}\,\mathcal{D}$ sono biunivoche si dice una *equivalenza* fra le categorie $\mathcal{C}$ e $\mathcal{D}$: questo significa che, anche se realizzate con insiemi diversi, dal punto di vista categorico $\mathcal{C}$ e $\mathcal{D}$ vanno considerate come indistinguibili. Ovviamente se $\mathcal{C}$ è una categoria esiste sempre il funtore identico $1 : \mathcal{C} \longrightarrow \mathcal{C}$ e due funtori si possono comporre.

1.4.7 Definizione *Una categoria è* piccola *se la classe dei suoi oggetti è un insieme.*

Osserviamo che, in virtù degli assiomi che abbiamo dato per le classi, una funzione $f : S \longrightarrow C$ ove S sia un insieme e C una classe è un insieme: infatti il suo grafico $\{(s, f(s))\}_{s \in S}$ è l'immagine della funzione $s \longmapsto (s, f(s))$ e quindi, per l'assioma 8 del §1, è un insieme. Se ora $\mathcal{C}$ è una categoria piccola, la classe $\mathrm{Ob}\,\mathcal{C} \times \mathrm{Ob}\,\mathcal{C}$ è un insieme e quindi lo è l'insieme dei morfismi $\mathrm{Mor}\,\mathcal{C}$.

In altri termini, esiste la categoria delle categorie piccole: i suoi oggetti sono tutte le categorie ed i cui morfismi sono i funtori.

Per le categorie costruite a partire da insiemi esiste sempre il funtore "distratto": ad esempio se $\mathbb{G}$ è la categoria dei gruppi, il suo funtore distratto è $\mathcal{F} : \mathbb{G} \longrightarrow \mathbb{S}$ (nella categoria degli insiemi) che assegna ad un oggetto $G \in \mathrm{Ob}\,\mathbb{G}$ se stesso (in quanto insieme) e ad ogni morfismo $f \in \mathrm{Mor}\,\mathbb{G}$ se stesso in quanto funzione: questo funtore dimentica quindi la struttura gruppale.

In molti casi il concetto di funtore non soddisfa pienamente le proprietà che si vorrebbero: ad esempio se $\mathbb{V}$ è la categoria degli spazi vettoriali, esiste una applicazione $^* : \mathbb{V} \longrightarrow \mathbb{V}$ che ad ogni spazio vettoriale associa il suo duale: non si tratta però di un funtore, perché

$$(f \circ g)^* = g^* \circ f^*$$

Cioè * "inverte il senso delle frecce". Si tratta di un nuovo tipo di funtore:

1.4.8 Definizione *Se $\mathcal{C}$ e $\mathcal{D}$ sono categorie, un* funtore controvariante $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ *è determinato da*

(1) *Una funzione* $\mathcal{F} : \mathrm{Ob}\,\mathcal{C} \longrightarrow \mathrm{Ob}\,\mathcal{D}$.

(2) *Una funzione* $\mathcal{F} : \mathrm{Mor}\,\mathcal{C} \longrightarrow \mathrm{Mor}\,\mathcal{D}$.

in modo che

$$\forall X \in \mathrm{Ob}\,\mathcal{C} \quad \mathcal{F}(1_X) = 1_{\mathcal{F}(X)}$$

$$\forall f \in \hom(Y, Z)\ \forall g \in \hom(X, Y) \quad \mathcal{F}(f \circ g) = \mathcal{F}(g) \circ \mathcal{F}(f)$$

Spesso anziché scrivere identità fra morfismi si scrivono diagrammi e si dichiara che sono *commutativi*, cioè che le applicazioni ottenute componendo frecce che inizino e finiscano sugli stessi vertici sono uguali. Ad esempio anziché scrivere $f \circ g = h \circ i$ si dice che il diagramma

$$\begin{array}{ccc} X & \xrightarrow{g} & Y \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle f} \\ Z & \xrightarrow{h} & W \end{array}$$

è commutativo. Quindi, se $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ è un funtore controvariante, la seconda proprietà che lo definisce equivale alla commutatività del diagramma

$$\begin{array}{ccc} \mathcal{F}(Z) & \xrightarrow{\mathcal{F}(f)} & \mathcal{F}(Y) \\ & \searrow^{\mathcal{F}(f\circ g)} & \downarrow{\scriptstyle \mathcal{F}(g)} \\ & & \mathcal{F}(X) \end{array}$$

Così il funtore $^* : \mathbb{V} \longrightarrow \mathbb{V}$ è controvariante (i funtori propriamente detti si dicono anche *covarianti*). In generale il funtore che a un oggetto $V \in \mathbb{V}$ associa lo spazio $\hom(V, W)$ (ove $W \in \mathrm{Ob}\,\mathbb{V}$) è controvariante da $\mathbb{V}$ in $\mathbb{V}$. Osserviamo che questa asserzione è imprecisa: per meglio formalizzarla introduciamo la

1.4.9 Definizione *Se* $\mathcal{C}$ *è una categoria, la sua* categoria opposta $\mathcal{C}^{op}$ *è la categoria così determinata:* $\mathrm{Ob}\,\mathcal{C}^{op} = \mathrm{Ob}\,\mathcal{C}$ *e ogni* $X \xrightarrow{f} Y \in \mathrm{Mor}\,\mathcal{C}$ *determina univocamente un* $Y \xrightarrow{f^{op}} X \in \mathrm{Mor}(\mathcal{C}^{op})$*, in modo che*

$$(f \circ g)^{op} = g^{op} \circ f^{op}$$

Quindi fra una categoria e la sua opposta esiste un funtore controvariante $^{op} : \mathcal{C} \longrightarrow \mathcal{C}^{op}$. è ovvio che questo funtore è una equivalenza di categorie e che il suo funtore inverso è $^{op} : \mathcal{C}^{op} \longrightarrow (\mathcal{C}^{op})^{op} = \mathcal{C}$. Questa dualità è simile alla dualità degli spazi vettoriali di dimensione finita.

1.4.10 Esempio *Esiste fra la categoria degli insiemi* $\mathbb{S}$ *e la sua opposta* $\mathbb{S}^{op}$ *il funtore controvariante* $\mathcal{P} : \mathbb{S}^{op} \longrightarrow \mathbb{S}$ *dato dall'insieme potenza: fissato un insieme* X *il funtore* $Y \longmapsto X^Y$ *è controvariante.*

Analizziamo meglio l'esempio (che ha dato origine alla teoria) della dualità per gli spazi vettoriali: sappiamo che il funtore $^* : \mathbb{V} \longrightarrow \mathbb{V}^{op}$ è controvariante come pure lo è $^* : \mathbb{V}^{op} \longrightarrow \mathbb{V}$. Il fatto che abbia l'isomorfismo canonico i fra uno spazio vettoriale V ed il suo biduale V^{**} è di natura puramente categorica: se $f : V \longrightarrow W$ è un morfismo di spazi vettoriali (i.e. un'applicazione lineare) allora il seguente diagramma è commutativo

$$\begin{array}{ccc} V & \xrightarrow{i} & (V^*)^* \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle (f^*)^*} \\ W & \xrightarrow{i} & (W^*)^* \end{array}$$

Quindi la mappa i in un certo senso trasforma il funtore identità nel funtore **.

1.4.11 Definizione *Se* $\mathcal{F}, \mathcal{G} : \mathcal{C} \longrightarrow \mathcal{D}$ *sono funtori, una* trasformazione naturale $\mathfrak{t} : \mathcal{F} \longrightarrow \mathcal{G}$ *è una funzione che ad ogni oggetto* $X \in \mathrm{Ob}\,\mathcal{C}$ *associa un morfismo* $\mathcal{F}(X) \xrightarrow{\mathfrak{t}_X} \mathcal{G}(X) \in \mathrm{Mor}\,\mathcal{D}$ *in modo che per ogni morfismo* $X \xrightarrow{f} Y \in \mathrm{Mor}\,\mathcal{C}$ *il seguente diagramma sia commutativo:*

$$\begin{array}{ccc} \mathcal{F}(X) & \xrightarrow{\mathfrak{t}_X} & \mathcal{G}(X) \\ {\scriptstyle \mathcal{F}(f)}\downarrow & & \downarrow{\scriptstyle \mathcal{G}(f)} \\ \mathcal{F}(Y) & \xrightarrow{\mathfrak{t}_Y} & \mathcal{G}(Y) \end{array}$$

Quindi una trasformazione naturale è in un certo senso un morfismo fra funtori: precisamente, se $\mathcal{C}$ è una categoria piccola e $\mathcal{D}$ una categoria qualsiasi, per l'assioma 8 del §1 una funzione $\mathrm{Ob}\,\mathcal{C} \longrightarrow \mathrm{Ob}\,\mathcal{D}$ è un insieme: quindi i funtori $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ sono insiemi. Possiamo cioè considerare l'insieme $\mathrm{Fun}(\mathcal{C}, \mathcal{D})$ dei funtori $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$; ora dimostriamo che la classe delle trasformazioni naturali $\mathfrak{t} : \mathcal{F} \longrightarrow \mathcal{G}$ del funtore $\mathcal{F} \in \mathrm{Fun}(\mathcal{C}, \mathcal{D})$ nel funtore $\mathcal{G} \in \mathrm{Fun}(\mathcal{C}, \mathcal{D})$, è, some applicazione, è un insieme. Evidentemente, dato che $\mathcal{C}$ è piccola e $\mathcal{F}, \mathcal{G}$ sono insiemi, la classe $\mathcal{M} = \bigcup_{X \in \mathrm{Ob}\,\mathcal{C}} \hom(\mathcal{F}(X), \mathcal{G}(X))$ è un insieme (assioma 6 del §1) ed una trasformazione naturale è una funzione $\mathfrak{t} : \mathrm{Ob}\,\mathcal{C} \longrightarrow \mathcal{M}$ ed il suo grafico è una sottoclasse del prodotto $\mathcal{C} \times \mathcal{M}$ che è un insieme. Ma l'insieme $\mathfrak{P}(\mathcal{C} \times \mathcal{M})$ potenza di un insieme è un insieme (assioma 7 del §1) e quindi la classe delle trasformazioni naturali da $\mathcal{F}$ in $\mathcal{G}$ è una sottoclasse di un insieme, cioè (assioma 5 del §1) è un insieme essa stessa.

Fatte tutte queste verifiche, che sono ovvie ma che abbiamo voluto esplicitare per mostrare l'importanza dell'assiomatica insiemistica, possiamo considerare l'insieme dei funtori $\mathrm{Fun}(\mathcal{C},\mathcal{D})$ e definire una categoria che ha come insieme degli oggetti proprio $\mathrm{Fun}(\mathcal{C},\mathcal{D})$, e come classe di morfismi le trasformazioni naturali fra elementi di $\mathrm{Fun}(\mathcal{C},\mathcal{D})$. Questa categoria è la *categoria dei funtori*.

Una trasformazione naturale $\mathfrak{t} : \mathcal{F} \longrightarrow \mathcal{G}$ si dice *equivalenza naturale* se per ogni $X \in \mathrm{Ob}\,\mathcal{C}$ il morfismo $\mathfrak{t}_X$ è invertibile in $\mathrm{Mor}\,\mathcal{D}$.

Quindi la teoria della dualità degli spazi vettoriali di dimensione finita si riassume nella frase: esiste una equivalenza naturale fra il funtore identità e il funtore ** effettuata dalla funzione $\mathfrak{i}_V : x \in V \longmapsto (\varphi \longmapsto \varphi(x)) \in V^{**}$ tale che, per ogni morfismo $f : V \longrightarrow W$:

$$\begin{array}{ccc} V & \xrightarrow{\mathfrak{i}_V} & V^{**} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f^{**}} \\ W & \xrightarrow[\mathfrak{i}_W]{} & W^{**} \end{array}$$

Per concludere questa rapida rassegna sul concetto di categoria, introduciamo i concetti forse più importanti della teoria.

1.4.12 Definizione *Se $\mathcal{F} : \mathcal{C} \longrightarrow \mathbb{S}$ è un funtore da una categoria nella categoria degli insiemi, una* rappresentazione *di $\mathcal{F}$ è determinata da un oggetto $R \in \mathrm{Ob}\,\mathcal{C}$ e da una famiglia di trasformazioni naturali*

$$\{\varphi_X : \hom_{\mathcal{C}}(R,X) \longleftrightarrow \mathcal{F}(X)\}_{X\in \mathrm{Ob}\,\mathcal{C}}$$

In altri termini, una rappresentazione di $\mathcal{F}$ è una equivalenza naturale $\mathfrak{f} : \mathcal{F} \longrightarrow \mathcal{H}_R$ ove $\mathcal{H}_R : \mathcal{C} \longrightarrow \mathbb{S}$ è il funtore (covariante)

$$\mathcal{H}_r(X) = \hom_{\mathcal{C}}(R,X)$$

Osserviamo che una rappresentazione $\mathfrak{t}$ del funtore $\mathcal{F}$ determina un elemento $S \in \mathcal{F}(R)$ tale che per ogni $Y \in \mathrm{Ob}\,\mathcal{C}$ e per ogni $T \in \mathcal{F}(Y)$ esiste un unico morfismo $f : R \longrightarrow X$ tale che $\mathcal{F}(f)S = T$. L'oggetto S si dice allora *universale* per la rappresentazione del funtore.

Moltissimi oggetti dell'algebra astratta sono determinati da proprietà universali: ad esempio il prodotto tensoriale, i gruppi liberi, l'insieme quoziente modulo una relazione, &c.

1.4.13 Lemma (YONEDA) *Se $\mathcal{F} : \mathcal{C} \longrightarrow \mathbb{S}$ è un funtore covariante, e se $X, Y \in \mathrm{Ob}\,\mathcal{C}$ allora esiste una biiezione canonica fra la classe delle trasformazioni naturali di $\mathcal{H}_X \longrightarrow \mathcal{H}_Y$ e $\hom_{\mathcal{C}}(X,Y)$.*

DIMOSTRAZIONE: Ogni $g \in \hom(X, Y)$ induce una trasformazione naturale di funtori $\mathfrak{t}_g(f) = f \circ g$. Ovviamente $g = \mathfrak{t}_g(1_X)$. Viceversa, una trasformazione naturale $\mathfrak{t} : \mathcal{H}_X \longrightarrow \mathcal{H}_Y$ dà luogo, per ogni $X \xrightarrow{f} Z \in \operatorname{Mor}\mathcal{C}$ al diagramma commutativo

$$\begin{array}{ccc} \mathcal{H}_X(X) & \xrightarrow{\mathfrak{t}_X} & \mathcal{H}_Y(X) \\ {\scriptstyle \mathcal{H}_X(f)}\downarrow & & \downarrow{\scriptstyle \mathcal{H}_Y(f)} \\ \mathcal{H}_X(Z) & \xrightarrow[\mathfrak{t}_Z]{} & \mathcal{H}_Y(Z) \end{array}$$

Allora definiamo un morfismo in $g \in \hom(X, Y)$ ponendo $g = \mathfrak{t}_X(1_X)$: che si tratti di un morfismo segue dal diagramma: $f = f \circ 1_X = \mathcal{H}_X(f)(1_X)$ e $\mathfrak{t}_Z(f) = \mathcal{H}_Y(f)(\mathfrak{t}_X(1_X)) = f \circ g$.

QED

Il seguente risultato è un modo diverso di esprimere il lemma di Yoneda:

1.4.14 Teorema *La categoria $\mathcal{C}^{op}$ opposta a $\mathcal{C}$ è equivalente alla categoria dei funtori rappresentabili, che è una sottocategoria piena della categoria dei funtori.*