Appunti di

Elementi di Teoria degli Insiemi

Carmine Frascella

29 Giugno 2014

Indice

CONNETTIVI LOGICI E QUANTIFICATORI
TABELLE DI VERITÀ

Iniziamo con qualche definizione.

Si definisce PROPOSIZIONE o ENUNCIATO un'affermazione di tipo matematico non ambigua, che rispetti cioè i principi di NON CONTRADDIZIONE (ossia non sia contemporaneamente vera e falsa) e DEL TERZO ESCLUSO (ossia sia o vera o falsa).

Un PREDICATO è invece un'affermazione il cui valore di verità dipende da una o più VARIABILI: una variabile è l'elemento fondamentale del calcolo letterale, che per l'appunto può variare, rendendo il predicato a volte vero, a volte falso. Indicheremo le variabili, talvolta indicizzate, in questi modi:

$$x, y, \lambda, \dots, x_n, x_k, \dots$$

Indicheremo solitamente con P, Q, o in maniera simile, gli enunciati; indicheremo con $P(x)$, $Q(x,y)$, o in maniera simile, i predicati.

Introduciamo ora i CONNETTIVI LOGICI più noti:

- la NEGAZIONE: "$\neg A$" significa "non A". Questo è l'unico connettivo UNARIO, gli altri sono tutti connettivi BINARI;
- la CONGIUNZIONE: "$A \wedge B$" significa "A e B";
- la DISGIUNZIONE: "$A \vee B$" significa "A o B": la "o" è alternativa ("vel"), non esclusiva ("aut");
- l'IMPLICAZIONE: "$A \Rightarrow B$" significa "se A allora B";
- la COIMPLICAZIONE: "$A \Leftrightarrow B$" significa "A se e solo se B".

Costruiamo dunque una cosiddetta TABELLA DI VERITÀ che ci dicono, a partire dai valori di verità delle proposizioni di partenza, se una determinata proposizione è vera o falsa.

Diremo in più due enunciati si diranno EQUIVALENTI se e solo se essi ammettono la medesima tabella di verità.

Costruiamo dunque la tabella:

P	Q	$P \wedge Q$	$P \vee Q$	$\neg P$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
V	V	V	V	F	V	V
V	F	F	V	F	F	F
F	V	F	V	V	V	F
F	F	F	F	V	V	V

OSSERVAZIONE

Dalla tabella di verità si evince che:

P	$\neg P$	$\neg\neg P$
V	F	V
F	V	F

Allora $\neg\neg P \equiv P$. In alcuni ambiti della matematica, come ad esempio la logica intuizionista, si ha $P \Rightarrow \neg\neg P$, ma non il viceversa.

OSSERVAZIONE

Indicheremo la o esclusiva ("aut") con il simbolo $\overline{\vee}$.

La questione è delicata soprattutto per quanto riguarda la tabella dell'implicazione e della coimplicazione. Infatti il valore di verità, in questo caso, viene attribuito d'ufficio nelle situazioni in cui esso non si possa attribuire con certezza. Dunque, se P e Q sono vere entrambe, $P \Leftrightarrow Q$ è vera anche se P e Q non sono di fatto proposizioni equivalenti; se però P è vera e Q è falsa, si sa con certezza che $P \Rightarrow Q$ e $P \Leftrightarrow Q$ sono false.

In ogni caso vale:

$$P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$$

Infatti, guardando la tabella di verità precedente:

P	Q	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$	$P \Leftrightarrow Q$
V	V	V	V
V	F	F	F
F	V	F	F
F	F	V	V

Notiamo che, se P e Q hanno medesimo valore di verità, $P \Leftrightarrow Q$ è vera; se P e Q hanno differente valore di verità, $P \Leftrightarrow Q$ è falsa.

OSSERVAZIONE

Il connettivo di negazione ha la precedenza sugli altri: negli altri così useremo le parentesi. Dunque:

$$(\neg P) \vee Q \equiv \neg P \vee Q \not\equiv \neg(P \vee Q)$$

Valgono le seguenti equivalenze (dimostreremo solo la prima):

- la negazione di una congiunzione è la disgiunzione delle negazioni:

$$\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$$

Infatti:

P	Q	$\neg(P \wedge Q)$	$(\neg P) \vee (\neg Q)$
V	V	F	F
V	F	V	V
F	V	V	V
F	F	V	V

;

- la negazione di una disgiunzione è la congiunzione delle negazioni:

$$\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q);$$

- $\neg(P \Rightarrow Q) \equiv P \wedge (\neg Q)$;
- vale la cosiddetta CONTRONOMINALE:

$$P \Rightarrow Q \equiv (\neg Q) \Rightarrow (\neg P).$$

Introduciamo ora i QUANTIFICATORI. Essi sono principalmente due:

- il QUANTIFICATORE UNIVERSALE: $\forall$, si legge "per ogni";
- il QUANTIFICATORE ESISTENZIALE: $\exists$, si legge "esiste".

Una FORMULA sarà per noi in sostanza un'espressione scritta mediante l'uso di connettivi logici, variabili e quantificatori.

Un predicato diventa così un enunciato se corredato da uno o più quantificatori, in modo che ogni variabile presente nel predicato sia legata da un quantificatore:

- $\exists\, x \ni' P(x)$ e $\forall\, x : P(x)$ sono enunciati;
- $\exists\, x \ni' Q(x, y)$ è ancora un predicato.

Attraverso l'uso delle tabelle di verità, si può dimostrare che:

- $\neg(\forall\, x : P(x)) \equiv \exists\, x \ni' (\neg P(x))$;
- $\neg(\exists\, x \ni' P(x)) \equiv \forall\, x : (\neg P(x))$.

I quantificatori possono essere anche combinati:

$$\forall\, x \;\exists\, y \ni' P(x, y)$$

A tal proposito, si ha:

- $\neg(\forall\, x, \forall\, y : P(x, y)) \equiv \exists\, x, \exists\, y \ni' (\neg P(x, y))$;
- $\neg(\forall\, x \;\exists\, y \ni' P(x, y)) \equiv \exists\, x \ni' \forall\, y : (\neg P(x, y))$;
- $\neg(\exists\, x \ni' \forall\, y : P(x, y)) \equiv \forall\, x \;\exists\, y \ni' (\neg P(x, y))$;
- $\neg(\exists\, x, \exists\, y \ni' P(x, y)) \equiv \forall\, x, \forall\, y : (\neg P(x, y))$.

A titolo di esempio, enunciamo e neghiamo la nozione di continuità di una funzione $f : I \subseteq \mathbb{R} \to \mathbb{R}$ in $x_0 \in I$:

- $\forall\, \varepsilon > 0 \;\exists\, \delta > 0 \ni' \forall\, x \in I : |x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \varepsilon$
- $\exists\, \varepsilon > 0 \ni' \forall\, \delta > 0 \;\exists\, x \in I \ni' |x - x_0| < \delta \wedge |f(x) - f(x_0)| \geq \varepsilon$

PRIMI PRINCIPI

Sia $P(x)$ un predicato.
La classe X degli oggetti a per cui $P(a)$ risulta vero si indica in questo modo:

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

$P(x)$ è anche detta PROPRIETÀ. In generale una proprietà è una formula nella quale compaiono soltanto connettivi, variabili, quantificatori, e i simboli di UGUAGLIANZA ($=$) e APPARTENENZA ($\in$).

OSSERVAZIONE
Per fissare la notazione:

$$\neg (x \in X) = x \notin X$$

L'ASSIOMA DEL LINGUAGGIO afferma che ogni proprietà è esprimibile nel linguaggio definito precedentemente.

L'ASSIOMA DI ESTENSIONALITÀ afferma che due insiemi sono uguali se e solo se essi hanno gli stessi elementi:
$\forall A, \forall B : (\forall x : x \in A \Leftrightarrow x \in B) \Leftrightarrow A = B$

Osserviamo che questa può essere anche una definizione di uguaglianza tra insiemi.
Osserviamo inoltre che, se $A = \{x \mid P(x)\}$ e $B = \{x \mid Q(x)\}$, e accade che $A \subseteq B$ e $B \subseteq A$, ossia $A = B$ (per l'assioma di estensionalità), non è necessariamente vero che P e Q siano predicati equivalenti.

OSSERVAZIONE
Per fissare le idee:

$$X \subseteq Y \Leftrightarrow \forall x : (x \in X \Rightarrow x \in Y)$$

Date due proprietà P e Q, se $\{x \mid P(x)\} \subseteq \{x \mid Q(x)\}$, allora:
$\forall x : P(x) \Rightarrow Q(x)$

Infine:

- $X \subsetneq Y \Leftrightarrow (X \subseteq Y \wedge X \neq Y)$;
- $X \nsubseteq Y \Leftrightarrow \exists x : x \in X \wedge x \notin Y$.

L'ASSIOMA DI ASTRAZIONE afferma che, data una proprietà "ammissibile" P, esiste un insieme i cui elementi sono gli oggetti che verificano P: tale insieme è unico per l'assioma di estensionalità. Useremo la notazione:

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

Si ha:

$$a \in \{ x \mid P(x) \} \Leftrightarrow P(a)$$

Dunque l'assioma afferma che:

$$\exists X \ni \forall x : (x \in X \Leftrightarrow P(x))$$

Infine, l'ASSIOMA DI COMPRENSIONE afferma che una sotto[illegible] di un insieme è un insieme. Sia infatti X un insieme e P una proprietà. Consideriamo:

$$B = \{ x \in A \mid P(x) \} = \{ x \mid x \in A \wedge P(x) \}$$

Si ha $B \subseteq X$, e B risulta un insieme per l'assioma appena enunciato.

Abbiamo parlato di proprietà "ammissibili": ciò è dovuto al fatto che non tutte le proprietà sono tali da generare un insieme di oggetti che la verifichino. Consideriamo la proprietà "$x \notin x$". La CLASSE DI RUSSELL è:

$$R = \{ x \mid x \notin x \}$$

Essa è la classe degli insiemi che non appartengono a loro stessi. Si ha dunque:

- $R \in R \Rightarrow R \notin R$;
- $R \notin R \Rightarrow R \in R$,

ossia quello che è noto come PARADOSSO DI RUSSELL.

COROLLARIO

La classe V di tutti gli oggetti non è un insieme.

Dim.

Ogni classe è inclusa in V: se V fosse un insieme, per il principio di comprensione lo sarebbe anche la classe R di Russell, ma ciò è assurdo, c.v.d.

INSIEME VUOTO, COPPIA ORDINATA, PRODOTTO CARTESIANO

Consideriamo la proprietà "eminentemente impossibile" $x \neq x$. Si definisce INSIEME VUOTO, per l'assioma di estrazione:

$$\emptyset \overset{\text{def}}{=} \{ x \mid x \neq x \}$$

Esso è unico, per il principio di estensionalità.

OSSERVAZIONE

Notiamo che $\emptyset \neq \{\emptyset\}$: infatti il secondo è un singoletto, ossia un insieme contenente solo un elemento (l'insieme vuoto). Possiamo dunque generare infiniti altri insiemi distinti a partire dal vuoto:

$$\{\{\emptyset\}\} \quad , \quad \{\emptyset, \{\emptyset\}\}$$

OSSERVAZIONE

Definiamo:

$$\mathbb{N} = \{ x \mid x \text{ è un naturale} \}$$

I cinque assiomi (di Peano) per i numeri naturali sono:

- $0 \in \mathbb{N}$;
- $n \in \mathbb{N} \Rightarrow n+1 \in \mathbb{N}$;
- se due numeri naturali hanno lo stesso successore, allora sono uguali;
- 0 non è successore: esso è l'unico con questa proprietà;
- se $X \subseteq \mathbb{N}$ è tale che

$$0 \in X \wedge (n \in \mathbb{N} \Rightarrow n+1 \in X),$$

allora $X = \mathbb{N}$.

L'ultimo è detto ASSIOMA DI INDUZIONE.

La definizione di $\mathbb{N}$, di VON NEUMANN, è la seguente:

- $0 \overset{\text{def}}{=} \emptyset$;
- $1 \overset{\text{def}}{=} \{0\} = \{\emptyset\}$;
- $2 \overset{\text{def}}{=} \{0, 1\} = \{\emptyset, \{\emptyset\}\}$;
- $n+1 \overset{\text{def}}{=} \{n, \{n\}\}$.

Ha senso, dunque, affermare che $\emptyset \in \mathbb{N}$.

OSSERVAZIONE

Gli assiomi presentati fin qui non garantiscono né l'esistenza, né la non esistenza, di oggetti che non siano insiemi. Entrambe le strade sono percorribili: noi sceglieremo la seconda. Modelleremo dunque tutti gli oggetti della matematica in modo insiemistico.

Un oggetto che non è un insieme, in teoria degli insiemi, è detto URELEMENTO o ATOMO. L'unico oggetto che non ha elementi, ossia non è un insieme, sarà dunque $\emptyset$.

La teoria degli insiemi che postula l'assenza di atomi è detta PURA.

Parliamo ora di contenimento. Per definizione:

$$A \subseteq B \Leftrightarrow \forall x \in A : x \in B \Leftrightarrow \forall x : (x \in A \Rightarrow x \in B)$$

Da qui segue che (aiutandosi con le tabelle di verità):

$$\forall B : \emptyset \subseteq B$$

Infatti la condizione $x \in \emptyset$ è sempre falsa. Dunque l'affermazione

$$\forall x : x \in \emptyset \Rightarrow x \in B,$$

stando alla tabella di verità, è vera (si dice, in questo caso, che essa è VERA A VUOTO), da cui $\emptyset \subseteq B$.

Si noti infine che:

$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A \Leftrightarrow \forall x : (x \in A \Leftrightarrow x \in B)$$

Dati ora due elementi a, b si definisce COPPIA ORDINATA il seguente oggetto:

$$c = (a, b)$$

Vogliamo tradurre in termini insiemistici quest'oggetto. La definizione dev'essere tale che risulti:

$$(a, b) = (a', b') \Leftrightarrow (a = a' \wedge b = b')$$

La seguente definizione, pertanto, non è buona:

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

Per il principio di estensionalità, infatti, si avrebbe:

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

e ciò non è vero in generale.

Definiamo dunque la COPPIA DI KURATOWSKI:

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

Questa è una buona definizione.

Se C è una coppia di Kuratowski, allora la sua prima componente è quell'unico elemento a tale che:

$\forall x \in C \quad a \in x$

Una volta noto a, la seconda componente è quell'unico elemento b tale che $\{a,b\} \in C$.

Si noti che, se $a = b$:

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

e ciò è comunque coerente con la richiesta fatta all'inizio.

Dati due insiemi A e B, si definisce PRODOTTO CARTESIANO:

$$A \times B = \{ x \mid \exists a \in A \wedge \exists b \in B \text{ t.c. } (a \in A \wedge b \in B \wedge$$
$$\wedge\ x = (a,b) \}$$

Quest'insieme è in accordo con l'assioma del linguaggio?

Effettuiamo una verifica:

$$\text{"}x = (a,b)\text{"} \rightsquigarrow \text{"}x = \{\{a\},\{a,b\}\}\text{"} \rightsquigarrow$$
$$\rightsquigarrow (\forall t : t \in x \Rightarrow \text{"}t = \{a\}\text{"} \vee \text{"}t = \{a,b\}\text{"}) \wedge$$
$$\wedge (\text{"}\{a\} \in x\text{"} \wedge \text{"}\{a,b\} \in x\text{"})$$

Ora:

- "$t = \{a\}$" $\rightsquigarrow \forall u : (u \in t \Leftrightarrow u = a)$;
- "$t = \{a,b\}$" $\rightsquigarrow \forall u : (u \in t \Leftrightarrow (u = a \vee u = b))$;
- $\{a\} \in x \rightsquigarrow \forall t : (\text{"}t = \{a\}\text{"} \Rightarrow t \in x)$;
- $\{a,b\} \in x \rightsquigarrow \forall t : (\text{"}t = \{a,b\}\text{"} \Rightarrow t \in x)$.

Definiamo ora, sulla base della definizione di coppia ordinata, la nozione di TERNA ORDINATA:

$$(a, b, c) \overset{\text{def}}{=} ((a, b), c)$$

Si definisce dunque il prodotto cartesiano di tre insiemi:

$$A \times B \times C \overset{\text{def}}{=} \{x \mid \exists a, \exists b, \exists c \ni' (a, b, c) = x\}$$

OSSERVAZIONE

Le formule:

$$\exists x \in A \ni' P(x)$$

$$\forall x \in A : P(x)$$

sono abbreviazioni di:

$$\exists x \ni' (x \in A \wedge P(x))$$

$$\forall x : (x \in A \Rightarrow P(x))$$

PROPOSIZIONE

Si ha:

$$(a, b) = (a', b') \Leftrightarrow a = a' \wedge b = b'$$

Dim.

Una implicazione è banale. Viceversa, sia $(a, b) = (a', b')$.

Vi sono due casi:

- $a \neq b$. Dunque $\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}$, da cui:
  $$\{a\} = \{a'\} \quad \wedge \quad \{a, b\} = \{a', b'\},$$
  da cui $a = a'$, e quindi $b = b'$;
- $a = b$. Dunque $\{\{a\}\} = \{\{a'\}, \{a', b'\}\}$. Allora:
  $$\{a\} = \{a'\} \quad \wedge \quad \{a\} = \{a', b'\},$$
  da cui $a = a'$ e $a = b'$, da cui $a = a' = b' = b$, c.v.d.

RELAZIONE BINARIA

Un insieme R è detto RELAZIONE BINARIA se tutti gli elementi di R sono coppie ordinate:

$\forall z \in R \; \exists x, \exists y \; \ni' \; z = (x, y)$

Diremo xRy, ossia che x è in relazione con y, se $(x, y) \in R$.

L'insieme delle prime coordinate delle coppie ordinate di R è chiamato DOMINIO:

$$\text{Dom}\, R = \{ x \mid \exists y \ni' (x, y) \in R \}$$

L'insieme delle seconde coordinate delle coppie ordinate di R è chiamato IMMAGINE:

$$\text{Im}\, R = \{ y \mid \exists x \ni' (x, y) \in R \}$$

Chiamiamo CAMPO di R:

$$\mathcal{F}(R) = \text{Dom}\, R \cup \text{Im}\, R$$

Se $\mathcal{F}(R) \subseteq X$, diremo che R è una relazione tra elementi di X.

Dato $A \subseteq X$, si hanno le definizioni seguenti:

$$R(A) = \{ y \in \text{Im}\, R \mid \exists x \in A \ni' (x, y) \in R \}$$
$$R^{-1}(A) = \{ x \in \text{Dom}\, R \mid \exists y \in A \ni' (x, y) \in R \}$$

Si definisce l'INVERSA di R:

$$R^{-1} = \{ z \mid z = (x, y) \wedge (y, x) \in R \}$$

Infine, date due relazioni R e S, si definisce la COMPOSIZIONE:

$$S \circ R = \{ (x, z) \mid \exists y \ni' (x, y) \in R \wedge (y, z) \in S \}$$

Ad esempio, definendo $\leq_{\mathbb{N}} = \{ (x, y) \in \mathbb{N} \times \mathbb{N} \mid x \leq y \}$, si ha:

$$(7 \leq 13) \Leftrightarrow (7, 13) \in \leq_{\mathbb{N}}$$

RELAZIONI DI EQUIVALENZA

Una relazione R tra elementi di A è detta RELAZIONE DI EQUIVALENZA se essa è:

- RIFLESSIVA: $\forall a \in A: aRa$;
- SIMMETRICA: $\forall a, b \in A: (aRb \Leftrightarrow bRa)$;
- TRANSITIVA: $\forall a, b, c \in A: ((aRb \wedge bRc) \Rightarrow aRc)$.

Data una relazione di equivalenza R su A, si definisce la CLASSE DI EQUIVALENZA:

$$[a]_R = \{ x \in A \mid xRa \}$$

Si ha che:

- $aRb \Leftrightarrow [a]_R = [b]_R$;
- $a \not R b \Leftrightarrow [a]_R \cap [b]_R = \emptyset$.

Si definisce allora l'insieme delle classi:

$$A/_R = \{ [a]_R \mid a \in A \}$$

Esso è una PARTIZIONE di A, in quanto:

- ogni classe è non vuota;
- $\bigcup_{a \in A} [a]_R = A$;
- $[a]_R \neq [b]_R \Rightarrow [a]_R \cap [b]_R = \emptyset$.

Viceversa, data una partizione S su A, si definisce la relazione indotta:

$$R_S = \{ (a, b) \in A \times A \mid \exists\, C \in S \ni a \in C \wedge b \in C \}$$

Si ha chiaramente $A/_{R_S} = S$. Inoltre, se R è una relazione di equivalenza e $A/_R = S$ allora $R_S = R$.

Infine, un sottoinsieme di A ($X \subseteq A$) è detto INSIEME DI RAPPRESENTANTI se:

$$\forall C \in A/_R : C \cap X = \{a\} \Leftrightarrow \forall C \in A/_R\ \exists!\, a \in C \cap X$$

RELAZIONI D'ORDINE

Una relazione R su A è detta ANTISIMMETRICA se $\forall a,b \in A : (aRb \wedge bRa) \Rightarrow a = b$

Una relazione R tra elementi di A è detta RELAZIONE D'ORDINE PARZIALE se risulta riflessiva, antisimmetrica e transitiva.

Dati $a, b \in A$, e una relazione d'ordine $\leq$ su A, diciamo che a, b sono COMPARABILI se:

$$a \leq b \vee b \leq a$$

Diciamo che a, b sono INCOMPARABILI se non sono comparabili.

Una relazione d'ordine parziale R su A è detta TOTALE se ogni coppia di elementi di A è comparabile. In tal caso, $(A, \leq)$ è detto INSIEME ORDINATO).

Ad esempio, dato $A = \mathbb{N}$, le relazioni seguenti:

$$R = \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid x \leq y\}$$
$$S = \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid x \mid y\}$$

sono rispettivamente totale e parziale.

FUNZIONI

Una relazione R su A si dice UNIVOCA se:
$\forall\, x \in \mathrm{Dom}\, R\ \exists!\ y \in \mathrm{Im}\, R$ t.c. $(x, y) \in R$

Una FUNZIONE è una relazione univoca. Equivalentemente:
$$[(x, y_1) \in R,\quad (x, y_2) \in R] \Rightarrow y_1 = y_2$$

Sia f una funzione. Allora, dato $x \in \mathrm{Dom}\, f$, l'unico $y \in \mathrm{Im}\, f$ per cui $(x, y) \in f$ verrà denotato con $f(x)$.

Una funzione è il suo grafico, ossia un insieme di coppie ordinate.

Se $\mathrm{Dom}\, f = A$ e $\mathrm{Im}\, f \subseteq B$, si usa scrivere $f: A \to B$. Essa è una formula, che afferma che f è un insieme di coppie $(x, y) \in A \times B$ tali che:
$\forall\, x \in A\ \exists!\ y \in B$ t.c. $y = f(x)$ $\quad(\ (x, y) \in f\ )$

Usando la NOTAZIONE funzionale, dato $X \subseteq A$, si scrive:
$$f(X) \stackrel{def}{=} \{ f(x) \mid x \in X \},$$
e si definisce la FUNZIONE RISTRETTA:
$$f|_X : X \to B$$
$$f(X) = \{ y \in B \mid \exists\, x \in X \text{ t.c. } (x, y) \in f \}$$

L'assioma di estensionalità applicato alle funzioni afferma che due funzioni F, G sono uguali se e solo se $\mathrm{Dom}\, F = \mathrm{Dom}\, G$ e:
$\forall\, x \in \mathrm{Dom}\, F : F(x) = G(x)$

Si definisce insieme delle immagini di $f: A \to B$:
$$f(A) = \{ f(a) \mid a \in A \} \subseteq B$$

Una funzione si dice SURIETTIVA se $f(A) = B$. Notiamo che, data $f: A \to B$, si può sempre restringere l'immagine a $f(A)$, generando così una funzione $f_1: A \to f(A)$ suriettiva. La definizione è quindi abbastanza vaga.

Una funzione $f: A \to B$ si dice invece INIETTIVA se:
$\forall a_1, a_2 \in \text{Dom } f: (a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2))$

Equivalentemente, per contronominale:
$\forall a_1, a_2 \in \text{Dom } f: (f(a_1) = f(a_2) \Rightarrow a_1 = a_2)$

PROPOSIZIONE
Una funzione $f: A \to B$ è iniettiva se e solo se ammette inversa destra:
$\exists\, g: B \to A \ni' \ g \circ f = Id_A$

Una funzione $f: A \to B$ è suriettiva se e solo se ammette inversa sinistra:
$\exists\, g: B \to A \ni' \ f \circ g = Id_B$

Dim.
Sia f iniettiva. Definiamo $f^{-1}: f(A) \to A$ nel seguente modo:

$$f^{-1} = \{ z = (x, y) \mid x = f(y) \}$$

Allora essa è una funzione:
$\forall x \in \text{Dom } f^{-1} \ \exists!\, y \in \text{Im } f^{-1} \ni' x = f(y)$

Se infatti fosse $x = f(y_1) = f(y_2)$, la funzione non sarebbe iniettiva, e ciò è assurdo. Si ha allora:

$\forall a \in \text{Dom } f: f^{-1}(f(a)) = a \Rightarrow f^{-1} \circ f = Id_A$

Viceversa, se f^{-1} è una funzione, allora f è iniettiva. Notiamo che:

$$f^{-1}(f(a)) = a \Leftrightarrow (f(a), a) \in f^{-1} \Leftrightarrow (a, f(a)) \in f$$

Concludiamo qui la dimostrazione: affronteremo il caso di f suriettiva più avanti, c.v.d.

OSSERVAZIONE
Vogliamo precisare che, date f, g funzioni tali che $\text{Im } f \subseteq \text{Dom } g$, si definisce FUNZIONE COMPOSTA:

$$g \circ f = \{ (x, z) \mid \exists\, y \in f(x) = y \wedge g(y) = z \}$$

SUCCESSIONI

Si definisce SUCCESSIONE o SEQUENZA una funzione:

$$f : \mathbb{N} \to X$$

Denotiamo per semplicità con a_n l'immagine di n secondo f:

$$f(n) = a_n$$

La sequenza si denota con:

$$< a_n \mid n \in \mathbb{N} > \quad \text{o} \quad (a_n)_{n \in \mathbb{N}}$$

L'immagine di f, invece, si denota con:

$$\mathrm{Im}\, f = \{ f(n) \mid n \in \mathbb{N} \} = \{a_n\}_{n \in \mathbb{N}}$$

Una successione è dunque una funzione con $\mathrm{Dom}\, f = \mathbb{N}$. Similmente, una I-SEQUENZA o I-SUCCESSIONE è una funzione con $\mathrm{Dom}\, f = I$:

$$< f(i) \mid i \in I >$$

Se $< A_i \mid i \in I >$ è una I-sequenza di insiemi:

$$\bigcup_{i \in I} A_i = \{ x \mid \exists\, i \in I \ \ni' \ x \in A_i \}$$

$$\bigcap_{i \in I} A_i = \{ x \mid \forall\, i \in I : x \in A_i \}$$

Sia $\mathcal{F}$ una famiglia non vuota di insiemi. Allora:

- $\bigcup \mathcal{F} \overset{\text{def}}{=} \bigcup_{F \in \mathcal{F}} F = \{ x \mid \exists\, F \in \mathcal{F} \ \ni' \ x \in F \}$
- $\bigcap \mathcal{F} \overset{\text{def}}{=} \bigcap_{F \in \mathcal{F}} F = \{ x \mid \forall\, F \in \mathcal{F} : x \in F \}$

Se $\mathcal{F} = \emptyset$:

- $\bigcup \mathcal{F} = \{ x \mid \exists\, F \in \mathcal{F} \ \ni' \ x \in F \} = \emptyset$, perché non esistono $F \in \mathcal{F}$;
- $\bigcap \mathcal{F} = \{ x \mid \forall\, F \in \mathcal{F} : x \in F \} = V$ (insieme di tutti gli insiemi, che abbiamo dimostrato non essere un insieme) perché la premessa è sempre falsa, dunque $(F \in \mathcal{F} \Rightarrow x \in F)$ è sempre vera. La definizione è dunque contraddittoria.

PRODOTTO CARTESIANO INFINITO

Sia $\langle A_i \mid i \in I \rangle$ una I-sequenza di insiemi (I infinito).
Si definisce PRODOTTO CARTESIANO INFINITO degli insiemi $(A_i)_{i \in I}$:

$$\prod_{i \in I} A_i = \{ f \mid f \text{ è una I-sequenza tale che } \forall i \in I,\ f(i) \in A_i \}$$

Gli elementi $f \in \prod_{i \in I} A_i$ si chiamano I-UPLE del prodotto cartesiano infinito.

$$\langle f(i) \mid i \in I \rangle$$

Si noti che il prodotto cartesiano di un numero finito di insiemi è costituito da n-uple ordinate; il prodotto cartesiano di un numero infinito di insiemi è invece costituito da I-sequenze, ossia, in sostanza, da funzioni.
Le due nozioni sono quindi differenti.

Dimostriamo ora un lemma, che ci servirà nel prossimo paragrafo.

LEMMA

Sia $A_1, \dots, A_n$ una sequenza finita di insiemi non vuoti: $\forall i = 1..n:\ A_i \neq \emptyset$.
Allora il prodotto cartesiano $\prod_{i=1}^{n} A_i$ è non vuoto.

Dim.

Si ha:

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

Ora:

$$\neg(A = \emptyset) \rightsquigarrow \neg(\forall t : (t \in A \Leftrightarrow t \neq t)) \rightsquigarrow$$
$$\rightsquigarrow \exists t \ni \neg(t \in A \Leftrightarrow t \neq t) \rightsquigarrow$$
$$\rightsquigarrow \exists t \ni ((t \in A \wedge t = t) \vee (t \notin A \wedge t \neq t))$$

Dato che $t = t$ è sempre vero, e $t \neq t$ è sempre falso:

$$\neg(A \neq \emptyset) = \exists t \ni t \in A$$

Allora:

$\forall i \in \{1, \ldots, n\} : A_i \neq \emptyset \Rightarrow \exists\, x_i \in A_i$

Allora:

$$(x_1, \ldots, x_n) \in \prod_{i \in I} A_i \Rightarrow \prod_{i \in I} A_i \neq \emptyset, \text{ c.v.d.}$$

OSSERVAZIONE

Abbiamo dunque provato il lemma senza il supporto di ulteriori assiomi. La scrittura finale è una formula, ossia una stringa finita di simboli. La dimostrazione, dunque, non può essere ripetuta nel caso di un prodotto cartesiano infinito, proprio perché una formula, per definizione, è una stringa finita di simboli. Occorre quindi un ulteriore assioma.

OSSERVAZIONE

In alcuni casi, data una I-sequenza infinita di insiemi non vuoti, $\prod_{i \in I} A_i \neq \emptyset$, e la dimostrazione non richiede ulteriori assiomi. Ad esempio, sia $\langle A_n \mid n \in \mathbb{N} \rangle$ una sequenza di sottoinsiemi non vuoti di $\mathbb{N}$. Allora la funzione:

$$f : \mathbb{N} \to \mathbb{N}$$
$$f(n) = \min A_n$$

appartiene a $\prod_{n \in \mathbb{N}} A_n$, da cui:

$$\prod_{n \in \mathbb{N}} A_n \neq \emptyset$$

ASSIOMA DELLA SCELTA

Data $\langle A_i \mid i \in I \rangle$, con I infinito, non sempre un elemento di $\prod_{i\in I} A_i$ è esprimibile esplicitamente: l'ASSIOMA DELLA SCELTA afferma, in ogni caso, che $\prod_{i\in I} A_i$ è non vuoto.

Ciò sembra banale, ma non deriva da quanto visto finora.
L'assioma della scelta ha segnato la nascita della teoria assiomatica degli insiemi: oggi è quasi universalmente accettato, sebbene all'inizio sia stato accolto con scetticismo.

OSSERVAZIONE

Sia $(A, \leq)$ un insieme parzialmente ordinato, e sia $B \subseteq A$.
B è una CATENA se:
$\forall x, y \in B : x \leq y \vee y \leq x$

In altre parole, B è una catena se l'ordinamento indotto è totale.

Un elemento $a \in A$ è detto MAGGIORANTE di B se:
$\forall b \in B : b \leq a$

Non è detto che $a \in B$.

Diciamo che $x \in A$ è un ELEMENTO MASSIMALE di $(A, \leq)$ se non esiste alcun $y \in A$ tale che $x \leq y$ e $x \neq y$.

Il LEMMA DI ZORN afferma che, se $(P, \leq)$ è un insieme parzialmente ordinato in cui ogni catena ha un maggiorante, allora esiste $x \in P$ elemento massimale.

Dimostreremo più avanti che il lemma di Zorn e l'assioma della scelta sono del tutto equivalenti.

L'assioma della scelta presenta varie definizioni equivalenti.

PROPOSIZIONE

Le definizioni seguenti sono equivalenti:

- per ogni famiglia $\mathcal{F}$ di insiemi non vuoti, $\prod_{F\in\mathcal{F}} F \neq \emptyset$;

- per ogni famiglia di insiemi non vuoti e disgiunti, esiste un "insieme di scelta", X, ossia un insieme X tale che $|X \cap F| = 1$ per ogni $F \in \mathcal{F}$;
- per ogni famiglia $\mathcal{F}$ di insiemi non vuoti, esiste una funzione di scelta f tale che $f(F) \in F$ per ogni $F \in \mathcal{F}$;
- per ogni funzione suriettiva $f : A \to B$ esiste $g : B \to A$ tale che $f \circ g = \mathrm{Id}_B$;
- $\bigcap_{i \in I} \bigcup_{j \in J} A_{ij} = \bigcup_{f : I \to J} \bigcap_{i \in I} A_{i, f(i)}$.

Dim.

Iniziamo dimostrando che 3) $\Rightarrow$ 5).

Si ha:

$$x \in \bigcap_{i \in I} \bigcup_{j \in J} A_{ij} \Leftrightarrow \forall\, i \in I \ \exists\, j \in J \ni' x \in A_{ij}$$

Supponendo vera la proposizione 3):

$$x \in \bigcap_{i \in I} \bigcup_{j \in J} A_{ij} \Leftrightarrow \exists\, f : I \to J \ni' \forall\, i \in I : x \in A_{i\, f(i)} \Leftrightarrow$$

$$\Leftrightarrow x \in \bigcup_{f : I \to J} \bigcap_{i \in I} A_{i,\, f(i)},$$

ossia la 5).

Dimostriamo ora che 1) e 3) sono equivalenti. Ciò è banale, perché, data una famiglia $\mathcal{F}$ di insiemi non vuoti, si ha:

$$\prod_{i \in I} A_i \neq \emptyset \Leftrightarrow \exists\, f \ni' f(A_i) \in A_i \ \forall\, i \in I$$

Dimostriamo ora che 2) e 3) sono equivalenti.

Se è vera la 3), esiste f tale che $f(A_i) \in A_i \ \forall\, i \in I$ (dunque $f(A_i) \notin A_j \ \forall\, j \neq i$). Allora $f(\mathcal{F}) = \{ f(A_i) \mid A_i \in \mathcal{F} \}$ è un insieme tale che $|f(\mathcal{F}) \cap A_i| = 1 \ \forall\, i \in I$.

Se invece 2) è vera, sia $\mathcal{F} = (A_i)_{i \in I}$ la famiglia di insiemi non vuoti e disgiunti, e sia $X = (x_i)_{i \in I}$ tale che $(X \cap A_i) = \{x_i\}$. Definendo la I-sequenza g tale che:
$\forall\, i \in I : g(A_i) = x_i \in A_i$,
si ha $\prod_{i \in I} A_i \neq \emptyset$, ossia la 1) ossia la 3).

Le definizioni 1), 2), 3) sono dunque equivalenti.

Dimostriamo ora che 2) e 4) sono equivalenti.

Se 2) è vera, allora:

$\forall y \in B : \{x \in A \mid f(x) = y\} = F_y \neq \emptyset$;

$\forall y_1, y_2 \in B : \{x \in A \mid f(x) = y_1\} \cap \{x \in A \mid f(x) = y_2\} = \emptyset$.

Allora, per la 2):

$\exists\, g \ni' \quad g(F_y) \in F_y \quad \forall\, F_y \in (F_y)_{y \in B} \Rightarrow$

$\Rightarrow \exists\, \tilde{g} : B \to A \ni' \tilde{g}(y) \overset{def}{=} g(F_y) \in F_y \quad \forall\, y \in B$,

da cui $\tilde{g}$ è una funzione tale che:

$$(f \circ \tilde{g})(y) = f(z),\ z \in F_y = y \Rightarrow (f \circ \tilde{g}) = 1_B .$$

Se invece vale la 4), la funzione seguente è suriettiva:

$$g : \bigcup_{F \in \mathcal{F}} F \to \mathcal{F}$$

$$f \mapsto F_f ,$$

ove F_f è l'unico $F \in \mathcal{F}$ tale che $f \in F$ (gli F di $\mathcal{F}$ sono non vuoti e disgiunti). La funzione inversa sinistra è, in effetti, una funzione di scelta: dunque vale 2).

Supponiamo ora vera la 5). Allora, in particolare, dato un insieme B e denotato con $X = \mathcal{P}(B) \setminus \emptyset$:

$$\bigcap_{x \in X} \bigcup_{b \in B} A_{x,b} = \bigcup_{f : X \to B} \bigcap_{x \in X} A_{x,f(x)}$$

Definiamo la seguente regola:

$$A_{x,b} = \begin{cases} \emptyset, & b \notin x \\ \{\emptyset\}, & b \in x \end{cases}$$

Allora:

$\forall\, x \in X : x \neq \emptyset \Rightarrow \exists\, b \in x \Rightarrow \forall\, x \in X : \bigcup_{b \in B} A_{x,b} = \{\emptyset\} \Rightarrow$

$\Rightarrow \{\emptyset\} \in \bigcap_{x \in X} \bigcup_{b \in B} A_{x,b} = \bigcup_{f : X \to B} \bigcap_{x \in X} A_{x,f(x)} \Rightarrow \bigcup_{f : X \to B} \bigcap_{x \in X} A_{x,f(x)} \neq \emptyset \Rightarrow$

$\Rightarrow \exists\, f : X \to B \ni' \{\emptyset\} \in \bigcap_{x \in X} A_{x,f(x)} \Rightarrow$

$\Rightarrow \exists\, f : X \to B \ni' \forall\, x \in X : \{\emptyset\} \in A_{x,f(x)} \Rightarrow f(x) \in x$,

ossia la 3), c.v.d.

CARDINALITÀ

Siano A, B due insiemi. Essi si dicono EQUIPOTENTI, e si dice che hanno la stessa cardinalità, se e solo se esiste una funzione bigettiva $f : A \to B$. In questo caso, si scrive:

$$|A| = |B|$$

La relazione di equipotenza ha le proprietà di relazione di equivalenza (e ciò è banale).

OSSERVAZIONE

Dimostreremo, ad esempio, che $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, e che dato A insieme qualsiasi $|A \times A| = |A|$ se e solo se vale l'assioma della scelta.

OSSERVAZIONE

La relazione di equipotenza, sebbene abbia le proprietà di relazione di equivalenza, non è una relazione di equivalenza.

Con gli insiemi finiti, si ha che due insiemi sono equipotenti se e solo se hanno la stessa cardinalità.

Valgono le seguenti relazioni (d'ora in poi, dati due insiemi A, B, l'insieme delle funzioni da B ad A verrà denotato con $Fun(B, A) = \{ f \mid f : B \to A \}$

$$|A^B \times A^C| = |A^{B \cup C}|, \quad B \cap C = \emptyset$$

$$|(A^B)^C| = |A^{B \times C}|$$

Infatti:

- alla funzione $(f, g) \in A^B \times A^C$, $f : B \to A$, $g : C \to A$, associamo la funzione $h : B \cup C \to A$ così definita:

$$h(x) \stackrel{def}{=} \begin{cases} f(x), & x \in B \\ g(x), & x \in C \end{cases}$$

  viceversa, data $f \in A^{B \cup C}$, si ha $(f|_B, f|_C) \in A^B \times A^C$;

- alla funzione $f : C \to Fun(B, A)$ così definita $\forall c \in C, \forall b \in B : f(c)(b) \in A$, associamo la funzione $g : (B \times C) \to A$ così definita: $f(b, c) \in A$.

Supponiamo ora di sapere che sia $2 = \{0,1\} = \{\emptyset, \{\emptyset\}\}$.
Si ha allora:

$$2^A \stackrel{def}{=} \mathrm{Fun}(A, \{0,1\})$$
$$2^A \stackrel{def}{=} \{ \chi \mid \chi : A \to \{0,1\} \}$$

Queste funzioni sono dette FUNZIONI CARATTERISTICHE, in quanto individuano univocamente un sottoinsieme di A (la controimmagine di 1 secondo la funzione). Viceversa, dato $B \subseteq A$, si definisce la funzione caratteristica di B:

$$\chi_B : A \to \{0,1\}$$
$$\chi_B(x) = \begin{cases} 1, & x \in B \\ 0, & x \notin B \end{cases}$$

Siano ora A e A' due insiemi equipotenti, e B e B' altri due insiemi equipotenti:

$$|A| = |A'| \quad , \quad |B| = |B'|$$

Allora:

- se $A \cap B = \emptyset$ e $A' \cap B' = \emptyset$, allora $|A \cup B| = |A' \cup B'|$;
- $|A \times B| = |A' \times B'|$;
- $|\mathrm{Fun}(A, B)| = |\mathrm{Fun}(B', A')|$;
- $|P(A)| \stackrel{def}{=} |\{B \mid B \subseteq A\}| = |P(A')|$.

Siano $f : A \to A'$ e $g : B \to B'$ due funzioni bigettive.
Consideriamo allora:

$$h : (A \cup B) \to (A' \cup B')$$
$$h(x) \stackrel{def}{=} \begin{cases} f(x) \in A', & x \in A \\ g(x) \in B', & x \in B \end{cases}$$

L'applicazione così costruita è bigettiva per costruzione:

- $\forall\ y \in A' \ \exists\ x \in A \ \ni'\ h(x) = f(x) = y$;
- $\forall\ y \in B' \ \exists\ x \in B \ \ni'\ h(x) = g(x) = y$;
- $h(x) = h(y) \in A' \Rightarrow f(x) = f(y) \Rightarrow x = y$;
- $h(x) = h(y) \in B' \Rightarrow g(x) = g(y) \Rightarrow x = y$.

Dunque h è bigettiva, e $|A \cup B| = |A' \cup B'|$, a patto che sia $A \cap B = A' \cap B' = \emptyset$.

Con dimostrazioni simili, l'applicazione:

$$h \equiv (f, g) \in \mathcal{F}un(A \times B, A' \times B')$$

è bigettiva:

- $\forall (y, y') \in A' \times B' \; \exists (x, x') \in A \times B \ni' h(x, x') = (f(x), g(x')) = (y, y')$;
- $h(x, y) = h(x', y') \Rightarrow (f(x), g(y)) = (f(x'), g(y')) \Rightarrow$
  $\Rightarrow x = x' \wedge y = y' \Rightarrow (x, y) = (x', y')$.

Si ha inoltre $|\mathcal{F}un(A, B)| = |\mathcal{F}un(A', B')|$. La costruzione è evidente:

$\forall h \in \mathcal{F}un(A, B) : g \circ h \circ f^{-1} \in \mathcal{F}un(A', B')$

$\forall h' \in \mathcal{F}un(A', B') : g^{-1} \circ h' \circ f \in \mathcal{F}un(A, B)$

In sostanza se $h \in \mathcal{F}un(A, B)$ mappa $a \in A$ in $b \in B$, $h' \in \mathcal{F}un(A', B')$ mappa $f(a) \in A'$ in $g(b) \in B'$.

Infine, se $|A'| = |A'|$, basta associare al generico sottoinsieme $B \subseteq A$ il sottoinsieme $f(B) \overset{def}{=} \{f(b) \mid b \in B\} \subseteq A'$. Dunque $|\mathcal{P}(A)| = |\mathcal{P}(A')|$.

La relazione di equipotenza è dunque coerente con le operazioni appena descritte.

TEOREMA DI CANTOR

TEOREMA

Sia A un qualunque insieme. Allora non esistono funzioni suriettive $f : A \to \mathcal{P}(A)$. In modo equivalente, $|\mathcal{P}(A)| \neq |A|$.

Dim.

Osserviamo preliminarmente il caso in cui $A = \emptyset$. Si ha:

$$\mathcal{P}(\emptyset) = \{\emptyset\} \neq \emptyset,$$

da cui non possono esistere funzioni suriettive dall'insieme vuoto all'insieme $\{\emptyset\}$ (che è di un elemento).

Sia ora $A \neq \emptyset$.

Esaminiamo il caso $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$. Sia, per assurdo, $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ una funzione surgettiva. Sia, per ogni $n \in \mathbb{N}$, $A_n \overset{def}{=} f(n)$.

Consideriamo $\langle A_n \mid n \in \mathbb{N} \rangle \subseteq \mathcal{P}(\mathbb{N})$. Consideriamo il seguente schema:

	1	2	3	4 ...
A_1	SI	NO	SI	...
A_2	NO	NO		*
A_3	:		SI	
	.	*		
A_4				.

Attuiamo dunque il PROCEDIMENTO DIAGONALE DI CANTOR.

Sia $B \subseteq \mathbb{N}$ tale che:

$\forall\, i \in \mathbb{N} : i \in B \Leftrightarrow i \notin A_i$

Per il principio di estensionalità, $B \neq A_i \ \forall\, i \in \mathbb{N}$, da cui $B \notin f(\mathbb{N})$, e f non è surgettiva.

Passiamo ora al caso generale. Data $f : A \to \mathcal{P}(A)$, definiamo:

$$B = \{ a \in A \mid a \notin f(a) \} \notin \operatorname{Im} f$$

Infatti, se esistesse $b \in \mathbb{N}$ tale che $f(b) = B$, allora:

- $b \in B = f(b) \Rightarrow b \notin B = f(b)$;
- $b \notin B = f(b) \Rightarrow b \in B = f(b)$,

e ciò è assurdo, c.v.d.

COROLLARIO

L'insieme seguente non esiste:

$$V = \{ x \mid x = x \}$$

La proprietà $x = x$, dunque, non è ammissibile.

Dim.

Se V fosse un insieme, avremmo:

$$V \subseteq \mathcal{P}(V) = \{ x \mid x \subseteq V \} \subseteq V,$$

da cui $Id: V \to \mathcal{P}(V)$ sarebbe suriettiva, in contraddizione con il Teorema di Cantor, c.v.d.

OSSERVAZIONE

Si ha, in particolare:

$$|\mathbb{N}| \neq |\mathcal{P}(\mathbb{N})|,$$

da cui $\mathcal{P}(\mathbb{N})$ ha cardinalità più che numerabile.

COMPLEMENTI SULLE CARDINALITÀ

Nel paragrafo precedente abbiamo introdotto la relazione di EQUIPOTENZA.

Diciamo ora che, dati A, B insiemi, la cardinalità di A è minore o uguale alla cardinalità di B (la notazione è $|A| \leq |B|$) se esiste $f : A \to B$ iniettiva.

Notiamo che, se $|A| = |A'|$, $|B| = |B'|$, $|A| \leq |B|$, allora:

$$|A'| \leq |B'|$$

Infatti, consideriamo il seguente schema:

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[d, "\wr\ \varphi_2"] \\ A' \arrow[u, "\varphi_1^{-1}\ \wr"] \arrow[r, dashed, "\tilde{f}"'] & B' \end{tikzcd}$$

Si ha effettivamente $\tilde{f} \overset{def}{=} \varphi_2 \circ f \circ \varphi_1^{-1}$ iniettiva, perché composizione di funzioni iniettive.

La relazione è banalmente riflessiva e transitiva. Dimostrare che essa è antisimmetrica è notevolmente più difficile: essa è infatti l'enunciato di un teorema di importanza fondamentale.

TEOREMA (DI CANTOR-BERNSTEIN) (SOLO ENUNCIATO)

Se $|B| \leq |A|$ e $|A| \leq |B|$, allora $|A| = |B|$.

OSSERVAZIONE

Ricordiamo che una successione indicizzata si indica con $\langle F_i \mid i \in I \rangle$, mentre:

$$\{F_i \mid i \in I\} = \operatorname{Im}(\langle F_i \mid i \in I \rangle),$$

secondo la funzione $\varphi : i \to F_i$.

Ad esempio, se $x : \mathbb{N} \to \{0, 1\}$, si ha la successione $\langle a_n \mid n \in \mathbb{N} \rangle$, ove per ogni $n \in \mathbb{N}$, $a_n = 0 \vee a_n = 1$, mentre:

$$\{a_n \mid n \in \mathbb{N}\} \subseteq \{0, 1\}$$

Imitando le dimostrazioni già viste, se $|A| \leq |A'|$ e $|B| \leq |B'|$, allora:

- se $A \cap B = A' \cap B' = \emptyset$, allora $|A \cup B| \leq |A' \cup B'|$;
- $|A \times B| \leq |A' \times B'|$;
- $|\mathrm{Fun}(A,B)| \leq |\mathrm{Fun}(A',B')|$;
- $|\mathcal{P}(A)| \leq |\mathcal{P}(A')|$.

PROPOSIZIONE

Siano A, B due insiemi tali che $|A| \leq |B|$. Allora:
$\exists\, g : B \to A$ suriettiva
Se si accetta l'assioma della scelta, vale anche il viceversa.

Dim.

Sia $f : A \to B$ una funzione iniettiva. (Studiamo il caso interessante in cui A e B sono non vuoti). Sia $a_* \in A$.
Sia $f : A \to B$. Definiamo allora g come segue:

$$g(y) = \begin{cases} f^{-1}(y), & y \in \mathrm{Im}\, f \\ a_*, & y \notin \mathrm{Im}\, f \end{cases},$$

ora $f^{-1} : \mathrm{Im}\, f \to A$ è ben definita ed è biiettiva.
Allora $\mathrm{Im}\, g = A$, ossia g è suriettiva.

Viceversa, sia $g : B \to A$. Allora:
$\forall a \in A : B_a \overset{def}{=} \{ y \in B \mid g(y) = a \} \neq \emptyset$
Utilizzando l'assioma della scelta:
$\forall a \in A \ \exists\, y_a \in B \ni' g(y_a) = a$

Definendo:

$$f : A \longrightarrow B$$
$$a \longrightarrow y_a,$$

f risulta iniettiva per costruzione da cui $|A| \leq |B|$, c.v.d.

PROPOSIZIONE

Sia R una relazione. Allora:

- $|\mathrm{Dom}\, f| \le |R|$;
- $|\mathrm{Im}\, f| \le |R|$.

Dim.

Consideriamo le seguenti funzioni:

$$\pi_1 : R \to \mathrm{Dom}\, f \qquad\qquad \pi_2 : R \to \mathrm{Im}\, f$$
$$(x,y) \to x \qquad\qquad (x,y) \to y$$

Le funzioni π_1 e π_2 sono suriettive. Utilizzando la proposizione precedente, allora, si ha la tesi (si noti che si è usato l'assioma della scelta), c.v.d.

OSSERVAZIONE

Sappiamo che vale:

$$|A| = |B| \Rightarrow |\mathcal{P}(A)| = |\mathcal{P}(B)|$$

Vale anche il viceversa?

$$|\mathcal{P}(A)| = |\mathcal{P}(B)| \Rightarrow |A| = |B|$$

La verità è che non si ha ancora la risposta a questa domanda. In altre parole, si è dimostrato che la proposizione è indimostrabile.

CARDINALITÀ NUMERABILE

Supponiamo di avere garantita l'esistenza di $\mathbb{N}$.
Diremo che un insieme A è NUMERABILE se $|A| = |\mathbb{N}|$.
Scriveremo allora:

$$|A| = \aleph_0$$

A proposito dell'ipotesi del continuo (che è un problema indecidibile), se si considera vera, si ha:

$$|\mathbb{R}| = \aleph_1,$$

e la cardinalità di $\mathbb{R}$ si dice CONTINUA (si ha $|\mathbb{N}| \lneq |\mathbb{R}|$)

Prima di continuare, un'altra definizione.
Un insieme A si dice INFINITO se si può porre in corrispondenza biunivoca con una sua parte propria. Un insieme si dice FINITO se non è infinito.
Utilizzando l'assioma della scelta, si può estrarre da A (insieme infinito) un sottoinsieme numerabile.
Per l'assioma di scelta, infatti, esiste:

$$f : \mathcal{P}(A) \setminus \emptyset \to A$$

$$f(A) \in A,$$

da cui si può generare la successione seguente:

- $a_1 := f(A) \in A$;
- $a_2 := f(A \setminus \{a_1\}) \in A \setminus \{a_1\}$;
- $a_{n+1} := f(A \setminus \{a_1, \dots, a_n\}) \in A \setminus \{a_1, a_2\}$,

e così via.

Esiste poi la categoria degli insiemi DEDEKIND-FINITI ma noi non li tratteremo.

PROPOSIZIONE
Se A è infinito, allora $|\mathbb{N}| \leq |A|$, ossia:
$\exists\, f : \mathbb{N} \to A$ iniettiva

Dim.
Consideriamo la funzione $f : \mathcal{P}(A) \setminus \emptyset \to A$ vista prima.
Essa è evidentemente suriettiva. Componiamo con la seguente funzione:

$$h : \mathrm{Im} f \to \mathbb{N},\ h(a_i) \overset{def}{=} i$$

Allora $h \circ f$ è suriettiva. Utilizzando l'assioma della scelta, esiste $g : \mathbb{N} \to A$ iniettiva (inversa sinistra), da cui $|\mathbb{N}| \leq |A|$, c.v.d.

COROLLARIO

Sia $A \subseteq \mathbb{N}$ un insieme infinito. Allora $|A| = |\mathbb{N}|$.

Dim.

Dimostreremo la tesi senza assumere l'assioma della scelta.

Consideriamo:

$$f : \mathcal{P}(\mathbb{N}) \setminus \emptyset \to \mathbb{N}$$

$$f(B) = \min B,$$

ove per ogni $B \neq \emptyset$, $\min B$ esiste per l'assioma del buon ordinamento. La funzione f induce una funzione:

$$f|_A : \mathcal{P}(A) \setminus \emptyset \to A$$

In altre parole, A può essere ordinato definendo:

- $a_0 = f(A) = \min A$;
- $a_1 = f(A \setminus \{a_0\}) = \min (A \setminus \{a_0\})$;
- $a_{k+1} = f(A \setminus \{a_0, \dots, a_k\}) = \min (A \setminus \{a_0, \dots, a_k\})$.

Definendo dunque:

$$g : \mathbb{N} \to A$$
$$n \to a_n$$
$$g^{-1} : A \to \mathbb{N}$$
$$a_n \to n,$$

si ha la tesi c.v.d.

PROPOSIZIONE

Si ha:

$$|\mathbb{N}| \lneq |\mathcal{P}(\mathbb{N})|$$

Dim.

Dal Teorema di Cantor sappiamo che, se $|\mathbb{N}| \leq |\mathcal{P}(\mathbb{N})|$, allora $|\mathbb{N}| \neq |\mathcal{P}(\mathbb{N})|$. Ma $|\mathbb{N}| \leq |\mathcal{P}(\mathbb{N})|$: la funzione $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$, $f(n) = \{n\}$ è infatti iniettiva, c.v.d.

PROPOSIZIONE

Si ha:

$$|\mathbb{N}| = |\mathbb{N} \times \{1, \dots, m\}| \quad \forall m \in \mathbb{N}$$

Dim.

Consideriamo le m copie di $\mathbb{N}$:

$$\mathbb{N} \times \{m\} = \{1, \dots, m, \dots\}$$

$$\vdots$$

$$\mathbb{N} \times \{2\} = \{1, \dots, n, \dots\}$$

$$\mathbb{N} \times \{1\} = \{1, \dots, 3, \dots\}$$

La seguente funzione:

$$\Phi : \mathbb{N} \times \{1, \dots, m\} \to \mathbb{N}$$

$$(n, k) \to (n-1)m + k$$

è iniettiva e suriettiva, da cui la tesi, c.v.d.

PROPOSIZIONE

Si ha:

$$|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$$

Dim.

Sappiamo che ogni $n \in \mathbb{N}$ ammette un unica fattorizzazione del tipo:

$$n = 2^u (2v - 1),$$

con $u \in \mathbb{N} \cup \{0\}$ e $v \in \mathbb{N}$. In particolare $|\mathbb{N}| = |2\mathbb{N}|$, da cui possiamo dimostrare che $|\mathbb{N} \times \mathbb{N}| = |2\mathbb{N}|$, e ottenere la tesi: questa volta però si ha $u \in \mathbb{N}$ $(u \geq 1)$.

La funzione:

$$\Phi : |\mathbb{N} \times \mathbb{N}| \to |2\mathbb{N}|$$

$$(u, v) \quad n = 2^u (2v - 1)$$

è iniettiva e suriettiva per le considerazioni effettuate.

Dunque:

$$|\mathbb{N} \times \mathbb{N}| = |2\mathbb{N}| = |\mathbb{N}|, \text{ c.v.d.}$$

OSSERVAZIONE

Dati due insiemi X, Y, si definisce DIFFERENZA SIMMETRICA:

$$X \Delta Y \overset{def}{=} (X \setminus Y) \cup (Y \setminus X) = (X \cup Y) \setminus (X \cap Y)$$

Si noti che:

$$X \Delta Y = Y \Delta X$$

PROPOSIZIONE

Sia X infinito, e sia Y un insieme tale $X \Delta Y$ finito.

Allora:

$$|X| = |Y| = |X \cap Y| = |X \cup Y|$$

Dim.

Premettiamo che è richiesto l'uso dell'assioma della scelta, quando si afferma che, se Z è infinito, allora esiste una funzione iniettiva $f : \mathbb{N} \to Z$.

Dimostreremo che $|X \cup Y| = |X \cap Y|$: la dimostrazione degli altri casi è del tutto identica. Alternativamente, notando che:

$$|X \cap Y| \leq |X|, |Y| \leq |X \cup Y|,$$

si potrebbe concludere subito con il teorema di Cantor-Bernstein.

Innanzitutto, notiamo che $X \cap Y$ è infinito: se $X \cap Y$ fosse finito, allora $X \cup Y = (X \cap Y) \cup (X \Delta Y)$ sarebbe finito, da cui $X \subseteq X \cup Y$ sarebbe finito, e ciò è assurdo. Si noti che abbiamo usato due fatti abbastanza intuitivi ma indimostrati: dati due insiemi finiti A e B, $A \cup B$ è finito, e un qualunque sottoinsieme $W \subseteq A$ è finito.

Dato che $X \cap Y$ è infinito, esiste $f : \mathbb{N} \to X \cap Y$ iniettiva, da cui esiste $\langle z_n \mid n \in \mathbb{N} \rangle \subseteq X \cap Y$. Inoltre:

$$X \setminus Y = \{a_1, \dots, a_k\}$$
$$Y \setminus X = \{b_1, \dots, b_h\}$$

Definiamo $\vartheta : X \cup Y \to X \cap Y$ come segue:

- $\forall\, a_i \in X \setminus Y : \vartheta(a_i) = z_i$, $\forall\, b_i \in Y \setminus X : \vartheta(b_i) = z_{k+i}$;
- $\forall\, z_n \in X \cap Y : \vartheta(z_n) = z_{k+h+n}$;
- $\forall\, x \in (X \cap Y) \setminus \{z_n \mid n \in \mathbb{N}\} : \vartheta(x) = x$.

La funzione è biettiva, da cui

$$|X \cup Y| = |X \cap Y|, \text{ c.v.d.}$$

COROLLARIO

Se X è numerabile (infinito) e $X \Delta Y$ è finito, allora:

$$|X| = |Y| = |X \cap Y| = |X \cup Y|$$

Dim.

La dimostrazione è simile a quella della proposizione precedente, ma non richiede l'uso dell'assioma della scelta.

Anche in questo caso, si ha:

$$X \setminus Y = \{a_1, \dots, a_k\}$$
$$Y \setminus X = \{b_1, \dots, b_h\}$$
$$X \cap Y = \{\partial_1, \dots, \partial_n, \dots\}$$

Definendo allora $d: X \cup Y \to X \cap Y$ come segue:

- $d(a_i) = \partial_i \quad \forall\, i \in \{1, \dots, k\}$;
- $d(b_j) = \partial_{k+j} \quad \forall\, j \in \{1, \dots, h\}$;
- $d(\partial_n) = \partial_{k+h+n} \quad \forall\, n \in \mathbb{N}$,

si ha la tesi, c.v.d.

PROPOSIZIONE

Se A e B sono insiemi numerabili, anche $A \cup B$ è numerabile.

Dim.

Per ipotesi, esistono le seguenti funzioni biunivoche:

$$\varphi: A \to \mathbb{N}$$
$$\psi: B \to \mathbb{N}$$

Vogliamo determinare una funzione biunivoca:

$$\theta: A \cup B \to \mathbb{N}$$

Definiamo:

$$\theta(x) = \begin{cases} 2\varphi(x), & x \in A \\ 2\psi(x) - 1, & x \in B \setminus A \end{cases}$$

Si noti che, per come è definita, $\theta: A \cup B \to \mathbb{N}$ è biunivoca se e solo se $A \cap B = \emptyset$; in ogni caso, θ è iniettiva.

Dunque:

$$|\mathbb{N}| \leq |A \cup B| \leq |\mathbb{N}|,$$

e per il Teorema di Cantor - Bernstein, $|A \cup B| = |\mathbb{N}|$, c.v.d.

PROPOSIZIONE

Si ha:

$$|\mathbb{Z}| = \aleph_0$$

Dim.

La seguente funzione è biunivoca:

$$\varphi : \mathbb{Z} \to \mathbb{N}$$

$$\varphi(k) = \begin{cases} 2k & , k > 0 \\ 1 & , k = 0 \\ -2k+1 & , k < 0 \end{cases}$$

Equivalentemente, usando la proposizione precedente, $\mathbb{Z}$ è numerabile perché unione di insiemi numerabili:

$$\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}, \text{ c.v.d.}$$

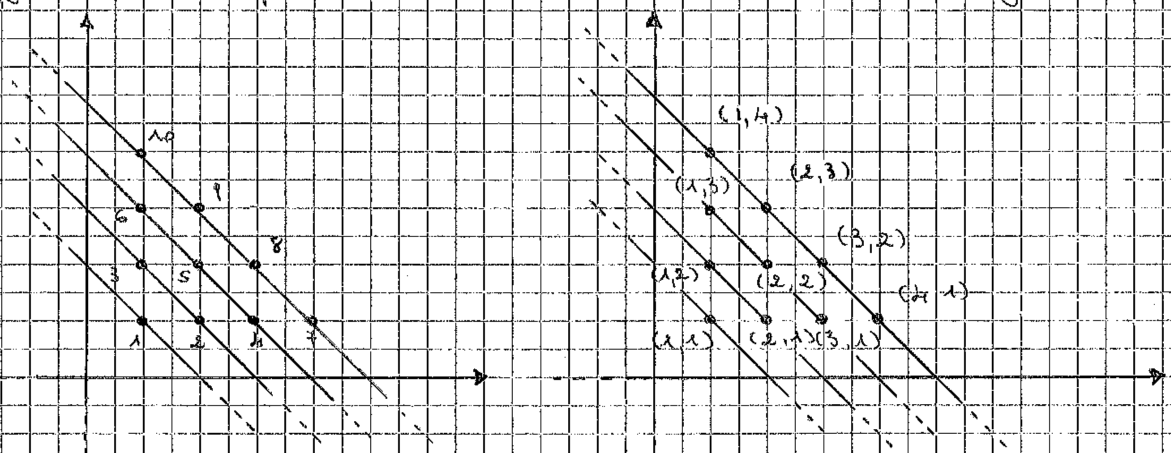
PROPOSIZIONE

Si ha:

$$|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$$

Dim.

Leggiamo le coppie di numeri naturali nel seguente modo:



Notiamo che ogni coppia viene letta, in questo modo. Numeriamo dunque le coppie in base all'ordine di lettura, come nel disegno.

Notiamo che su una retta diagonale si trovano coppie (x, y) tali che $x+y$ è costante. In particolare:

- si è una sola coppia la cui somma delle coordinate è 2;
- si sono due coppie la cui somma delle coordinate è 3;
- si sono $(n-1)$ coppie la cui somma delle coordinate è n.

In più, su una stessa retta le coppie sono ordinate in ordine crescente rispetto alla seconda componente.

Allora la generica coppia (n, m) viene mappata in:

$$\sum_{j=1}^{n+m-2} j + (n+m-1) - n + 1 =$$

$$= \sum_{j=1}^{n+m-2} j + m =$$

$$= \frac{(n+m-2)(n+m-1)}{2} + m$$

Definendo dunque:

$$\psi(n, m) = \frac{(n+m-2)(n+m-1)}{2} + m,$$

si ha la tesi, c.v.d.

OSSERVAZIONE

Abbiamo dunque dimostrato che $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ in due modi differenti. La proposizione si potrebbe dimostrare in un altro modo, sfruttando il teorema fondamentale dell'aritmetica, e il fatto che i numeri primi sono infiniti: l'idea verrà mostrata più avanti.

PROPOSIZIONE

Si ha:

$$|\mathbb{Q}| = |\mathbb{N}| = \aleph_0$$

Dim.

Sia $q \in \mathbb{Q}$. Allora $q = \frac{k}{m}$, ove $m \in \mathbb{N}$ e $k \in \mathbb{Z}$, e inoltre $k = 0$ o $(k, m) = 1$. Allora la funzione:

$$\psi : \mathbb{Q} \to (\mathbb{Z} \times \mathbb{N})$$
$$q \mapsto (k, m)$$

è iniettiva.

Notiamo che:

- si ha banalmente $|\mathbb{N}| \leq |\mathbb{Q}|$;
- si ha $|\mathbb{Z} \times \mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$, dato che $|\mathbb{Z}| = |\mathbb{N}|$.

Allora:

$$|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}| \leq |\mathbb{Q}|,$$

da cui:

$$|\mathbb{Q}| = |\mathbb{N}| = \aleph_0,$$

e la tesi si ha usando il teorema di Cantor-Bernstein, c.v.d.

PROPOSIZIONE

Se $\langle A_i \mid i \in I \rangle$ è una sequenza dove $|I| \leq \aleph_0$ e $|A_i| \leq \aleph_0$ per ogni $i \in I$, allora:

$$\left| \bigcup_{i \in I} A_i \right| \leq \aleph_0$$

Come conseguenza immediata, un'unione numerabile di insiemi è numerabile.

Dim.

Sia $\varphi : \mathbb{N} \to I$ una funzione suriettiva. Sia, per ogni $i \in I$, $\psi_i : \mathbb{N} \to A_i$ una funzione suriettiva.

Allora, usando l'assioma della scelta:

$$\langle \psi_i \mid i \in I \rangle \in \prod_{i \in I} \{ g : \mathbb{N} \to A_i \mid g \text{ è suriettiva} \}$$

Definiamo allora:

$$F : \mathbb{N} \times \mathbb{N} \to \bigcup_{i \in I} A_i$$

$$(n, m) \mapsto \psi_{\varphi(n)}(m) \in A_{\varphi(n)}$$

La funzione è suriettiva per costruzione. Dunque:

$$\left| \bigcup_{i \in I} A_i \right| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}| \Rightarrow \left| \bigcup_{i \in I} A_i \right| \leq \aleph_0 \text{ c.v.d.}$$

SEQUENZE FINITE E INSIEMI FINITI

ANELLI DI POLINOMI

Definiamo ora, dato un insieme X, le SEQUENZE FINITE di elementi di X (talvolta dette anche STRINGHE):

$$FS(X) \overset{def}{=} \{ a : \{1, \dots, n\} \to X \text{ per qualche } n \in \mathbb{N} \text{ (} a \text{ è una funzione), } \operatorname{Im} a \subseteq X \} =$$

$$= \{ < x_1, \dots, x_n > \mid x_i \in X, n \in \mathbb{N} \}$$

Per convenzione:

$$< \cdot > = \emptyset$$

Denotiamo invece con $Fin(X)$ l'insieme dei sottoinsiemi finiti di X:

$$Fin(X) = \{ A \mid A \subseteq X \wedge |A| = n, n \in \mathbb{N} \}$$

PROPOSIZIONE

Se $|X| \leq |X'|$, allora $|FS(X)| \leq |FS(X')|$ e $|Fin(X)| \leq |Fin(X')|$

Se $|X| = |X'|$, esse sono tutte uguaglianze.

Dim

Sia $|X| \leq |X'|$, sia $\varphi : X \to X'$ iniettiva. Allora:

$\forall < x_1, x_2, \dots x_n > \in FS(X) \ \exists < \varphi(x_1), \dots \varphi(x_n) > \in FS(X')$,

da cui:

$$\bar{\varphi} : FS(X) \to FS(X')$$
$$< x_1 \dots x_n > \to < \varphi(x_1) \dots \varphi(x_n) >$$

è iniettiva.

Inoltre:

$\forall A \in Fin(X), A = \{x_1, \dots x_n\} \ \exists \ \varphi(A) \in Fin(X')$

$\varphi(A) \overset{def}{=} \{ \varphi(x_1) \dots \varphi(x_n) \}$,

da cui:

$$\tilde{\varphi} : Fin(X) \to Fin(X)$$
$$\{x_1 \dots x_n\} \to \{ \varphi(x_1) \dots \varphi(x_n) \}$$

è iniettiva, c.v.d.

PROPOSIZIONE

Si ha:

$$|FS(\mathbb{N})| = |Fin(\mathbb{N})| = |\mathbb{N}|$$

Dim.

Si ha:

- $|\mathbb{N}| \leq |Fin(\mathbb{N})|$: la funzione $f: \mathbb{N} \to Fin(\mathbb{N})$, $f(n) = \{n\}$ è iniettiva;
- $|Fin(\mathbb{N})| \leq |FS(\mathbb{N})|$: sia $F \subseteq \mathbb{N}$ finito. Esso può essere ordinato in maniera crescente:

$$F = \{a_1, \dots a_k\}$$

Allora:

$$\Phi : Fin(\mathbb{N}) \to FS(\mathbb{N})$$
$$F = \{a_1, \dots a_k\} \to \langle a_1, \dots, a_k \rangle$$

è iniettiva;

- $|FS(\mathbb{N})| \leq |\mathbb{N}|$: consideriamo $\langle p_k \mid k \in \mathbb{N} \rangle$, la sequenza crescente e infinita dei numeri primi. La funzione:

$$\Lambda : FS(\mathbb{N}) \to \mathbb{N}$$
$$\langle a_1, \dots, a_k \rangle \to p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$$

è iniettiva (per definizione $\Lambda(\langle\rangle) = 1$. Non lo sarebbe stato se avessimo posto $0 \in \mathbb{N}$, ma così non è:

$$\Lambda(0,0) = 2^0 3^0 = 1$$
$$\Lambda(0,0,0,0) = 2^0 3^0 5^0 7^0 = 1$$

Dunque:

$$|\mathbb{N}| \leq |Fin(\mathbb{N})| \leq |FS(\mathbb{N})| \leq |\mathbb{N}|,$$

e si conclude con il teorema di Cantor - Bernstein, c.v.d.

PROPOSIZIONE

$|\mathbb{Z}[x]| = |\mathbb{Q}[x]| = \aleph_0$.

Dim.

La dimostrazione è identica nei due casi. Si ha $|\mathbb{N}| \leq |\mathbb{Z}[x]|$, e ciò è ovvio. Ora, si ha che la seguente funzione è iniettiva:

$$\Psi : \mathbb{Z}[x] \to FS(\mathbb{Z})$$
$$a_0 + a_1 x + \dots + a_n x^n \to \langle a_0, a_1, \dots, a_n \rangle$$

Allora:

$$|\mathbb{Z}[x]| \leq |FS(\mathbb{Z})| = |FS(\mathbb{N})| = |\mathbb{N}|$$

$$|\mathbb{Q}[x]| \leq |FS(\mathbb{Q})| = |FS(\mathbb{N})| = |\mathbb{N}|,$$

e si conclude con il Teorema di Cantor - Bernstein, c.v.d.

TEOREMA DI CANTOR

Consideriamo il campo $\mathbb{R}$ dei reali, e l'anello dei polinomi $\mathbb{Z}[x]$.

Un elemento $\alpha \in \mathbb{R}$ si dice:

- ALGEBRICO, se esiste $P(x) \in \mathbb{Z}[x]$ tale che $P(\alpha) = 0$;
- TRASCENDENTE in caso contrario.

TEOREMA (DI CANTOR)

Sia T l'insieme dei reali trascendenti, e A l'insieme dei reali algebrici.

Allora $|T| \gneq \aleph_0$.

Dim.

Supponiamo di sapere che $|\mathbb{R}| \gneq \aleph_0$.

Ogni polinomio di grado n ha al più n radici reali.

Dato $P(x) \in \mathbb{Z}[x]$, l'insieme

$$\mathrm{Root}(P) \overset{def}{=} \{ a \in \mathbb{R} \mid P(a) = 0 \}$$

è finito, dunque meno che numerabile.

Allora, dato che $|\mathbb{Z}[x]| = \aleph_0$:

$$|A| = \left| \bigcup_{P(x) \in \mathbb{Z}[x]} \mathrm{Root}(P) \right| \leq |\mathbb{N}| = \aleph_0$$

Ovviamente $|\mathbb{N}| \leq |A|$, da cui, per il Teorema di Cantor-Bernstein, $|A| = \aleph_0$. Se $|T| \leq \aleph_0$, avremmo:

$$|\mathbb{R}| = |T \cup A| = \aleph_0,$$

e ciò è assurdo. Dunque la tesi, c.v.d.

CARDINALITÀ DEL CONTINUO

Supporremo garantita l'esistenza di $\mathbb{R}$.
La CARDINALITÀ DEL CONTINUO è la cardinalità di $\mathbb{R}$:

$$c = |\mathbb{R}|$$

Il primo teorema che dimostreremo afferma che $\mathbb{R}$ ha cardinalità più che numerabile.
Prima di enunciarlo, ricordiamo che:

$$B^A = \mathcal{F}un(A, B) = \{ f \mid f : A \to B \},$$

e che in particolare:

$$|2^{\mathbb{N}}| = |\mathcal{F}un(\mathbb{N}, 2)| = |\mathcal{F}un(\mathbb{N}, \{0,1\})| = |\mathcal{P}(\mathbb{N})|$$

Si ha infatti, data:

$$\chi : \mathbb{N} \to \{0,1\},$$

che il seguente è un sottoinsieme di $\mathbb{N}$:

$$A_\chi \overset{\text{def}}{=} \{ n \in \mathbb{N} \mid \chi(n) = 1 \} \in \mathcal{P}(\mathbb{N})$$

Allora:

$$F : \chi \longrightarrow A_\chi$$

è una bigezione. Infatti, dato $B \in \mathcal{P}(\mathbb{N})$ la funzione caratteristica $\chi_B : \mathbb{N} \to \{0,1\}$ così definita

$$\chi_B(n) = \begin{cases} 1 & , n \in B \\ 0 & , n \notin B \end{cases}$$

è tale che $F(\chi_B) = B$. Dunque $|2^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})|$

PROPOSIZIONE
Si ha:

$$|\mathbb{R}| = |2^{\mathbb{N}}|$$

Dim.
Assegnata $\chi : \mathbb{N} \to \{0,1\}$, consideriamo:

$$\sum_{n=1}^{+\infty} \frac{\chi(n)}{10^n}$$

Dimostriamo che la funzione:

$$\Phi : \chi \longrightarrow \sum_{n=1}^{+\infty} \frac{\chi(n)}{10^n}$$

è iniettiva.

Per dimostrarlo, supponiamo che le funzioni χ, χ' siano distinte. Allora:

$$\exists\, k \in \mathbb{N} \ni' \ \forall\, h < k : \chi(h) = \chi'(h), \quad \chi(k) \neq \chi'(k)$$

Ad esempio, nel caso di:

$$\chi \to x_1 = 0,010101100\ldots$$
$$\chi' \to x_2 = 0,010010111\ldots$$
$$\uparrow$$
$$k$$

si ha $k = 4$.

Allora si ha:

$$\sum_{n=k}^{+\infty} \frac{\chi(n)}{10^n} \geq \frac{1}{10^k} > \frac{1}{10^k \cdot 9} = \sum_{n=k+1}^{+\infty} \frac{1}{10^n} \geq \sum_{n=k}^{+\infty} \frac{\chi'(n)}{10^n},$$

da cui l'iniettività.

Notiamo ora che:

$$|\mathcal{P}(\mathbb{Q})| = |\mathcal{P}(\mathbb{N})| = |2^{\mathbb{N}}|,$$

da cui è sufficiente dimostrare che:

$$|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})|$$

La funzione così definita:

$$\Psi : \mathbb{R} \to \mathcal{P}(\mathbb{Q})$$
$$r \to \{q \in \mathbb{Q} \mid q < r\}$$

tale funzione è iniettiva perché $\mathbb{Q}$ è denso in $\mathbb{R}$.

Se $r \neq r'$, allora (supponiamo $r < r'$):

$$\exists\, q \in \mathbb{Q} \ni' q < r',\ q > r \Rightarrow q \in \Psi(r') \setminus \Psi(r),$$

da cui $\Psi(r') \neq \Psi(r)$. Dunque $|\mathbb{R}| \leq |2^{\mathbb{N}}|$.

Per il Teorema di Cantor-Bernstein:

$$c = |\mathbb{R}| = |2^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})| > |\mathbb{N}| = \aleph_0, \text{ c.v.d.}$$

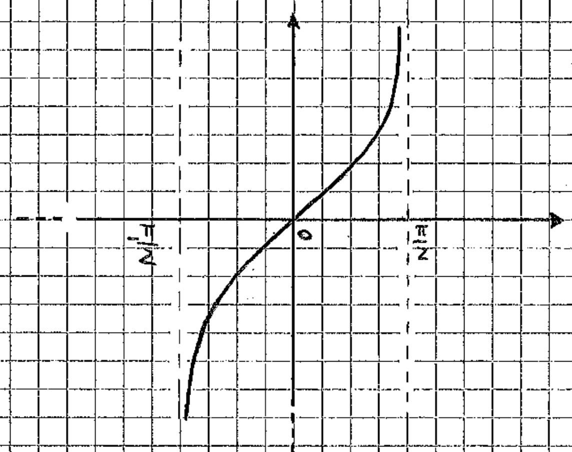
L'IPOTESI DEL CONTINUO (indimostrabile) afferma che non esistono cardinalità intermedie tra $\aleph_0$ e c, ossia non esistono insiemi tali che $\aleph_0 \lneq |A| \lneq c$:

$$\forall A : \aleph_0 \lneq |A| \Rightarrow c \leq |A|$$

OSSERVAZIONE

Sia $]a,b[\subseteq \mathbb{R}$. Allora $|]a,b[| = c$. La funzione TANGENTE, infatti, è una bigezione tra $]-\frac{\pi}{2}, \frac{\pi}{2}[$ e $\mathbb{R}$, e una sua opportuna riparametrizzazione è una bigezione tra $]a,b[$ e $\mathbb{R}$:

$$Tg: \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[\to \mathbb{R}$$



Si può poi dimostrare, con il Teorema di Cantor-Bernstein, che per ogni intervallo $I \subseteq \mathbb{R}$, si ha $|I| = |\mathbb{R}|$. Si può anche procedere trovando una bigezione esplicita:

$$f: [0,1[\to]0,1[$$

Consideriamo i sottoinsiemi:

- $A = \left\{ 1 - \frac{1}{2^n} \mid n \in \mathbb{N} \right\} = \left\{ 0, \frac{1}{2}, \frac{3}{4}, \dots \right\} \subseteq [0,1[$;
- $B = \left\{ 1 - \frac{1}{2^{n+1}} \mid n \in \mathbb{N} \right\} = \left\{ \frac{1}{2}, \frac{3}{4}, \frac{7}{8}, \dots \right\} \subseteq]0,1[$

Allora definiamo:

$$f: [0,1[\to]0,1[$$

$$f(x) = \begin{cases} x, & x \notin A \\ 1 - \frac{1}{2^{n+1}}, & x = 1 - \frac{1}{2^n},\ n \in \mathbb{N} \end{cases}$$

È evidente che f sia una bigezione. Dunque $|[0,1[| = |]0,1[| = c$. In generale un qualsiasi intervallo reale ha la cardinalità del continuo.

Usando il Teorema di Cantor-Bernstein invece:

$$]a,b[\subseteq [a,b[\subseteq]a-1,b[\Rightarrow$$

$$c = |]a,b[| \leq |[a,b[| \leq |]a-1,b[| = c \Rightarrow$$

$$\Rightarrow |[a,b[| = c$$

COMPLEMENTI SULLA CARDINALITÀ DEL CONTINUO

Si sa che $|\mathbb{N}\times\mathbb{N}| = |\mathbb{N}|$.
In effetti vale anche $|\mathbb{R}\times\mathbb{R}| = |\mathbb{R}|$. Infatti:

$$|\mathbb{R}\times\mathbb{R}| = |2^{\mathbb{N}}\times 2^{\mathbb{N}}| = |2^{D}\times 2^{P}| = |2^{P\cup D}| =$$
$$= |2^{\mathbb{N}}| = c,$$

ove D e P sono gli insiemi dei numeri dispari e pari, rispettivamente.

Esistono insiemi a cardinalità più che continua. Ad esempio, per il teorema di Cantor:

$$|\mathcal{P}(\mathbb{R})| \gneq c = |\mathbb{R}|$$

L'IPOTESI GENERALIZZATA DEL CONTINUO afferma che, se A è un insieme infinito, non esistono insiemi B tali che $|A| < |B| < |\mathcal{P}(A)|$. Essa è indecidibile.

PROPOSIZIONE
Se $|A| = c$ e $B \subseteq A$ è tale che $|B| < c$, allora $|A\setminus B| = c$. Se in particolare $|B| \leq \aleph_0$, $|A\setminus B| = c$ si può dimostrare senza l'assunzione dell'assioma della scelta, che è invece necessario nel caso generale.

Dim.
Senza perdita di generalità, sia $A = \mathbb{R}\times\mathbb{R}$: se dimostriamo la tesi in questo caso particolare, attraverso una bigezione avremo dimostrato la tesi in generale.
Se $B \subseteq A$, B è una relazione. Si ha, assumendo l'assioma della scelta:

$$|\operatorname{dom} B| \leq |B|$$

Allora, dato che $|\operatorname{dom} B| < c$, $\operatorname{dom} x \neq \mathbb{R}$, da cui:
$\exists\ \bar{x} \in \mathbb{R} \setminus \operatorname{dom} B$

Si ha $\{\bar{x}\}\times\mathbb{R} \subseteq B^c$, con:

$$\lambda: \mathbb{R} \to \{\bar{x}\}\times\mathbb{R}$$
$$t \mapsto (\bar{x}, t)$$

bigettiva.

Allora:

$$|B^c| \le |\mathbb{R}| \quad , \quad |B^c| \ge |\{x\} \times \mathbb{R}| = |\mathbb{R}|,$$

da cui, per il Teorema di Cantor-Bernstein:

$$|B^c| = |\mathbb{R}| = c$$

Nel caso generale, considerata una bigezione:

$$\psi : A \to \mathbb{R} \times \mathbb{R}$$

Se $B \subseteq A$, allora $\psi(B) \subseteq \mathbb{R} \times \mathbb{R}$, da cui:

$$|\psi(B)| = |B| < c$$

Per quanto dimostrato:

$$|\psi(A \setminus B)| = |(\mathbb{R} \times \mathbb{R}) \setminus \psi(B)| = c \Rightarrow$$

$$\Rightarrow |(A \setminus B)| = |\psi(A \setminus B)| = c$$

L'assunzione dell'assioma della scelta non è necessaria se $|B| \le \aleph_0$, perché si può usare una bigezione con $\mathbb{N}$, e usare come funzione di scelta la funzione $\varphi : \mathcal{P}(\mathbb{N}) \to \mathbb{N}$, tale che $\varphi(A) = \min A$, c.v.d.

Calcoliamo ora la cardinalità di qualche insieme noto.

Consideriamo:

$$\mathrm{Fin}(\mathbb{R})$$

Si ha che la seguente funzione:

$$\varphi : \mathrm{Fin}(\mathbb{R}) \to \mathrm{FS}(\mathbb{R})$$

$$A \mapsto \langle a_1, \dots, a_n \rangle$$

ove $A = \{a_1, \dots, a_n\}$ e gli a_i sono disposti in maniera ad esempio crescente, è iniettiva. Dunque:

$$|\mathrm{Fin}(\mathbb{R})| \le |\mathrm{FS}(\mathbb{R})|$$

Inoltre $|\mathbb{R}| \le |\mathrm{Fin}(\mathbb{R})|$, in quanto $\psi : \mathbb{R} \to \mathrm{Fin}(\mathbb{R})$, $\psi(x) = \{x\}$ è iniettiva. Infine si ha banalmente $\mathrm{Fin}(\mathbb{R}) \subseteq \mathcal{P}(\mathbb{R})$, da cui

$$|\mathrm{Fin}(\mathbb{R})| \le |\mathcal{P}(\mathbb{R})|$$

Consideriamo a questo punto, per ogni $n \in \mathbb{N}$:

$$S_n \overset{def}{=} \{ f \in FS(\mathbb{R}) \mid \# f = n \}$$

Allora:

$$|FS(\mathbb{R})| = \left| \bigcup_{n \geq 0}^{+\infty} S_n \right| = \sum_{n=0}^{+\infty} |S_n|,$$

dato che per ogni coppia di insiemi l'intersezione è vuota.

Ora, si ha che

$$\varphi_n : S_n \to \mathbb{R}^n$$
$$\langle a_1, \dots, a_n \rangle \to (a_1, \dots, a_n)$$

è iniettiva, da cui:

$$|S_n| \leq |\mathbb{R}^n| = |\mathbb{R}| \leq |S_n|,$$

dato che:

$$\lambda_n : \mathbb{R} \to S_n$$
$$x \to \langle x, \dots, x \rangle$$

è iniettiva.

Per il Teorema di Cantor-Bernstein, allora:

$\forall n \in \mathbb{N} : |S_n| = |\mathbb{R}|$

Dunque $FS(\mathbb{R})$ è un'unione numerabile di insiemi aventi la cardinalità del continuo. La dimostrazione che afferma che unioni numerabili di insiemi numerabili sono numerabili può essere adattata al caso di insiemi continui.

Allora:

$$|FS(\mathbb{R})| = |Fin(\mathbb{R})| = |\mathbb{R}|$$

Consideriamo ora $Fun(\mathbb{N}, \mathbb{N})$ e $Fun(\mathbb{N}, \mathbb{R})$. Si ha:

- si ha $|Fun(\mathbb{N}, \mathbb{R})| = |\mathbb{R}^{\mathbb{N}}| = |(2^{\mathbb{N}})^{\mathbb{N}}| = |2^{\mathbb{N} \times \mathbb{N}}| = |2^{\mathbb{N}}| = |\mathbb{R}| = \mathfrak{c}$;
- si ha $|Fun(\mathbb{N}, \mathbb{N})| \leq |Fun(\mathbb{N}, \mathbb{R})| = \mathfrak{c}$, e $|Fun(\mathbb{N}, \mathbb{N})| \geq |Fun(\mathbb{N}, 2)| = |2^{\mathbb{N}}| = |\mathbb{R}| = \mathfrak{c}$, e per il Teorema di Cantor-Bernstein, $|Fun(\mathbb{N}, \mathbb{N})| = \mathfrak{c}$.

Consideriamo:

$$\mathcal{F}un(\mathbb{R},\mathbb{R}) = \mathbb{R}^{\mathbb{R}}$$

Si ha:

$$|\mathcal{F}un(\mathbb{R},\mathbb{R})| = |\mathbb{R}^{\mathbb{R}}| = |(2^{\mathbb{N}})^{\mathbb{R}}| = |2^{\mathbb{N}\times\mathbb{R}}| = |2^{\mathbb{R}}| =$$
$$= |\mathcal{P}(\mathbb{R})| > c,$$

ove:

- $|\mathbb{R}| = |2^{\mathbb{N}}|$ (già visto);
- $|\mathbb{N}\times\mathbb{R}| = |\mathbb{R}|$: infatti $|\mathbb{R}| \leq |\mathbb{N}\times\mathbb{R}|$ perché la funzione $\varphi:\mathbb{R}\to\mathbb{N}\times\mathbb{R}$, $\varphi(x) = (1,x)$ è iniettiva, e d'altra parte si ha $|\mathbb{N}\times\mathbb{R}| \leq |\mathbb{R}\times\mathbb{R}| = |\mathbb{R}| = c$, da cui la tesi.

Consideriamo ora:

$$\mathcal{C}^0(\mathbb{R}) = \{ f:\mathbb{R}\to\mathbb{R} \mid f \text{ è continua} \}$$

Innanzitutto:

$$\begin{aligned} \psi : \mathbb{R} &\to \mathcal{C}^0(\mathbb{R}) \\ c &\to K_c : \mathbb{R}\to\mathbb{R} \\ &\qquad\quad x \to c \end{aligned}$$

è iniettiva. Ma anche:

$$\begin{aligned} \varphi : \mathcal{C}^0(\mathbb{R}) &\to \mathbb{R}^{\mathbb{Q}} = \mathcal{F}un(\mathbb{Q},\mathbb{R}) \\ f &\to f|_{\mathbb{Q}} \end{aligned}$$

è iniettiva. Essendo $\overline{\mathbb{Q}} = \mathbb{R}$ due funzioni coincidono su $\mathbb{Q}$ se e solo se coincidono su $\mathbb{R}$.

Infine:

$$|\mathbb{R}^{\mathbb{Q}}| = |\mathbb{R}^{\mathbb{N}}| = |(2^{\mathbb{N}})^{\mathbb{N}}| = |2^{\mathbb{N}\times\mathbb{N}}| = |2^{\mathbb{N}}| = |\mathbb{R}|,$$

da cui, per Cantor-Bernstein:

$$|\mathbb{R}^{\mathbb{Q}}| = |\mathbb{R}|$$
$$|\mathcal{C}^0(\mathbb{R})| = |\mathbb{R}|$$

COROLLARIO

Si ha:

- la cardinalità di $\mathbb{R}\setminus\mathbb{Q}$ è c;
- la cardinalità dei trascendenti è c.

Indichiamo ora con $\mathcal{O}(\mathbb{R}^2)$ l'insieme degli aperti di $\mathbb{R}^2$.
Quanto vale:

$$|\mathcal{O}(\mathbb{R}^2)|?$$

Sicuramente:

$$\alpha: \mathbb{R}^2 \to \mathcal{O}(\mathbb{R}^2)$$
$$(x,y) \mapsto \mathbb{R}^2 \setminus \{(x,y)\}$$

è iniettiva, da cui:

$$\mathfrak{c} \le |\mathcal{O}(\mathbb{R}^2)|$$

Dato ora un aperto $A \subseteq \mathbb{R}^2$, sia:

$$\psi(A) = \{(q_1, q_2, q_3) \in \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}^+ \mid B((q_1, q_2),\ ) \subseteq A\} \in \mathcal{P}(\mathbb{Q}^3)$$

Si ha

$$|\mathcal{P}(\mathbb{Q}^3)| = |\mathcal{P}(\mathbb{N}^3)| = |\mathcal{P}(\mathbb{N})| = |\mathbb{R}| = \mathfrak{c},$$

e per Cantor-Bernstein $|\mathcal{O}(\mathbb{R}^2)| = \mathfrak{c}$, a patto di dimostrare che ψ è iniettiva.

Se $A \neq A'$, allora (senza perdere di generalità):
$\exists\ \bar{x} \in A \setminus A'$. Allora:
$\forall (q_1, q_2, \varepsilon) \in \mathbb{Q}^3,\ (q_1, q_2) = \bar{x} : (q_1, q_2, \varepsilon) \notin A'$,
e d'altra parte:
$\exists\, \varepsilon > 0$ t.c. $(q_1, q_2, \varepsilon) \in A$,
da cui $\psi(A) \neq \psi(A')$.

Introduciamo ora un nuovo insieme. Dato un insieme A e un cardinale b, si definisce:

$$[A]^b = \{S \subseteq A \mid |S| = b\},$$

e con abuso di notazione:

$$[A]^{\le b} = \{S \subseteq A \mid |S| \le b\}$$

PROPOSIZIONE
Siano A, B, D insiemi, tali che $|A| = |B|$. Allora:

$$|[A]^{|D|}| = |[B]^{|D|}|$$

Dim.

Sia $\varphi : A \to B$ una bigezione. Allora:

$\forall\ S \in [A]^{|D|} : \varphi(S) = \{\varphi(x) \mid x \in S\} \in [B]^{|D|}$

$\forall\ T \in [B]^{|D|} : \varphi^{-1}(T) = \{\varphi^{-1}(x) \mid x \in T\} \in [A]^{|D|}$

Inoltre le funzioni:

$$\Phi : [A]^{|D|} \to [B]^{|D|} \qquad\qquad \Psi : [A]^{|D|} \to [B]^{|D|}$$
$$S \to \varphi(S) \qquad\qquad T \to \varphi^{-1}(T)$$

sono una l'inversa dell'altra: dunque la tesi.

Analizziamo ora $[\mathbb{R}]^{\aleph_0}$. Per quanto appena dimostrato:

$$|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}| \Rightarrow |[\mathbb{R} \times \mathbb{R}]^{\aleph_0}| = |[\mathbb{R}]^{\aleph_0}|$$

Consideriamo la funzione:

$$\Lambda : \mathbb{R}^{\mathbb{N}} \to [\mathbb{R} \times \mathbb{R}]^{\aleph_0}$$
$$f : \mathbb{N} \to \mathbb{R} \ \to \ ((n, a_n))_{n \in \mathbb{N}}$$
$$n \to a_n$$

Λ è iniettiva, da cui $\mathbb{R}^{\mathbb{N}} \leq [\mathbb{R} \times \mathbb{R}]^{\aleph_0}$, da cui:

$$c = |\mathbb{R}^{\mathbb{N}}| \leq |[\mathbb{R} \times \mathbb{R}]^{\aleph_0}| = |[\mathbb{R}]^{\aleph_0}|$$

Sia, viceversa, $A \in [\mathbb{R}]^{\aleph_0}$. Allora $A = \{a_n \mid n \in \mathbb{N}\}$, ove la numerazione scelta è arbitraria. Consideriamo ora:

$$\beta : [\mathbb{R}]^{\aleph_0} \to \mathrm{Fun}(\mathbb{N}, \mathbb{R})$$
$$A = \{a_0, a_1 \dots\} \to f : \mathbb{N} \to \mathbb{R}$$
$$i \to a_i$$

β è iniettiva (è ben definita se per ogni insieme fissiamo una numerazione). Allora:

$$|[\mathbb{R}]^{\aleph_0}| \leq |\mathbb{R}^{\mathbb{N}}| = c,$$

e per Cantor-Bernstein:

$$|[\mathbb{R}]^{\aleph_0}| = c.$$

Consideriamo:

$$\mathcal{F}_1 = \{ f : \mathbb{N} \to \mathbb{N} \mid \forall n \in \mathbb{N} : f(n) \neq n \} \subseteq Fun(\mathbb{N}, \mathbb{N})$$

Sappiamo che $|Fun(\mathbb{N},\mathbb{N})| = \mathfrak{c}$. Allora $|\mathcal{F}_1| \leq \mathfrak{c}$.

Cerchiamo ora un insieme A tale che $|A| = \mathfrak{c}$ e una funzione iniettiva:

$$\psi : A \to \mathcal{F}_1,$$

così da avere $\mathfrak{c} \leq |\mathcal{F}_1|$, e per Cantor-Bernstein $|\mathcal{F}_1| = \mathfrak{c}$.

Consideriamo $A = \mathcal{P}(\mathbb{N})$, definiamo:

$$\psi(A)(n) = \begin{cases} n+1, & n \notin A \\ n+2, & n \in A \end{cases},$$

ossia:

$$\psi(A) = \mathrm{Id}_{\mathbb{N}} + \chi_A + 1$$

La funzione è iniettiva, da cui:

$$\mathfrak{c} \leq |\mathcal{F}_1| \Rightarrow \mathfrak{c} = |\mathcal{F}_1|.$$

Sia ora:

$$\mathcal{F}_2 = \{ f : \mathbb{N} \to \mathbb{N} \mid f \text{ è bigettiva} \} \subseteq Fun(\mathbb{N}, \mathbb{N})$$

Sicuramente $|\mathcal{F}_2| \leq \mathfrak{c}$.

Per ogni $A \subseteq \mathbb{N}$ tale che $|A| = \aleph_0$ (ossia $A = (a_n)_{n \in \mathbb{N}}$), consideriamo:

$$\sigma_A : \mathbb{N} \to \mathbb{N}, \quad \begin{cases} \forall k \in \mathbb{N}^+ : \sigma(a_{2k}) = a_{2k-1}, \ \sigma(a_{2k-1}) = a_{2k} \\ \sigma(n) = n \ \forall n \notin A \end{cases}$$

Notiamo che la corrispondenza è iniettiva:

$$A^c = \{ n \in \mathbb{N} \mid \sigma_A(n) = n \}$$

Dunque:

$$\Sigma : [\mathbb{N}]^{\aleph_0} \longrightarrow \mathcal{F}_2$$
$$A \longrightarrow \sigma_A$$

è iniettiva, da cui $|\mathcal{F}_2| \geq \mathfrak{c}$ e quindi $|\mathcal{F}_2| = \mathfrak{c}$.

Consideriamo ora:

$$\mathcal{F}_3 = \{ f : \mathbb{N} \to \mathbb{N} \mid f \text{ è limitata} \}$$

Esso contiene l'insieme:

$$\Lambda = \{ f : \mathbb{N} \to \mathbb{N} \mid f : \mathbb{N} \to \{1, 2\} \}$$

Si ha inoltre che $|\Lambda| = |2^{\mathbb{N}}| = |\mathbb{R}| = c$, da cui:

$$|\mathcal{F}_3| \geq c$$

Ma $|Fun(\mathbb{N}, \mathbb{N})| = c$, da cui $|\mathcal{F}_3| = c$.

Consideriamo adesso:

$$\mathcal{F}_4 = \{ f : \mathbb{N} \to \mathbb{N} \mid f \text{ è illimitata} \}$$

Consideriamo:

$$\begin{aligned} \psi : \mathcal{P}(\mathbb{N}) &\to \mathcal{F}_4 \\ A &\longrightarrow f_A : \mathbb{N} \to \mathbb{N} \\ & \qquad f_A = Id_{\mathbb{N}} + \chi_A \end{aligned}$$

Essa è iniettiva, e inoltre $|Fun(\mathbb{N}, \mathbb{N})| = c$. Allora:

$$|\mathcal{F}_4| = c$$

Sia ora:

$$\mathcal{F}_5 = \{ f : \mathbb{N} \to \mathbb{N} \mid f \text{ è definitivamente costante} \}$$

Sia $f \in \mathcal{F}_5$. Definiamo:

$$k_f = \min \{ k \mid \forall n \geq k \;\; f(n) = f(k) \}$$

Sia ora:

$$\begin{aligned} \varphi \quad \mathcal{F}_5 &\longrightarrow FS(\mathbb{N}) \\ f &\longrightarrow \langle f(1), \dots, f(k) \rangle \end{aligned}$$

Essa è iniettiva, da cui:

$$|\mathcal{F}_5| \leq FS(\mathbb{N}) = \aleph_0,$$

da cui in definitiva:

$$|\mathcal{F}_5| = \aleph_0$$

Consideriamo ora $[\mathbb{N}]^{\aleph_0}$. Sicuramente $|[\mathbb{N}]^{\aleph_0}| \leq c$.

Notiamo che, se $A \subseteq \mathbb{N}$, esiste una bigezione con $2\mathbb{N}$

$$\begin{aligned} \varphi : \mathcal{P}(\mathbb{N}) &\longrightarrow \mathcal{P}(2\mathbb{N}) \\ A &\longrightarrow 2A = \{ 2n \mid n \in A \} \end{aligned}$$

Componiamo ora con:

$$\psi : \mathcal{P}(2\mathbb{N}) \to [\mathbb{N}]^{\aleph_0}$$
$$B \mapsto B \cup D,$$

dove $D = \{2k+1 \mid k \in \mathbb{N} \wedge k \neq 0\}$.

Allora $|[\mathbb{N}]^{\aleph_0}| \geq c$, allora si ha l'uguaglianza.

PROPOSIZIONE

Sia A un insieme con cardinalità 2^c, e sia $B \subseteq A$ tale che $|B| \leq c$. Allora $|A \setminus B| = 2^c$.

Dim.

Senza perdita di generalità, assumiamo che sia $A = \mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R})$. Si ha $|B| \leq c$, da cui esiste $f : \mathbb{R} \to B$ suriettiva (non si usa l'assioma di scelta).

Consideriamo ora:

$$\pi_1 : B \to \mathrm{Dom}\, B$$

Si ha $\mathrm{Dom}\, B \neq \mathcal{P}(\mathbb{R})$, altrimenti:

$$\pi_1 \circ f : \mathbb{R} \to \mathcal{P}(\mathbb{R})$$

sarebbe suriettiva, in contraddizione con il teorema di Cantor. Allora:

$\exists\, X \in \mathcal{P}(\mathbb{R}) \setminus \mathrm{Dom}(B) \Rightarrow \{X\} \times \mathcal{P}(\mathbb{R}) \subseteq A \setminus B$, $|\{X\} \times \mathcal{P}(\mathbb{R})| = 2^c$, da cui:

$$|A \setminus B| = 2^c, \text{ c.v.d.}$$

OSSERVAZIONE

L'enunciato si può generalizzare: se $|A| = |\mathcal{P}(Y)|$ e $B \subseteq A$, $|B| \leq |Y|$, allora $|A \setminus B| = |\mathcal{P}(Y)|$.

OSSERVAZIONE

Dato che $|C^0(\mathbb{R}, \mathbb{R})| = c$, e $|\{f : \mathbb{R} \to \mathbb{R}\}| = 2^c$, allora l'insieme delle $g : \mathbb{R} \to \mathbb{R}$ discontinue ha cardinalità 2^c.

OSSERVAZIONE

Abbiamo usato il fatto che $|\mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R})|$: lo dimostreremo in seguito. In generale $|\mathcal{P}(Y) \times \mathcal{P}(Y)| = |\mathcal{P}(Y)|$ è equivalente all'assioma della scelta.

Un altro modo per dimostrare che $|[\mathbb{R}]^{\aleph_0}| = c$ è considerare la seguente catena:

$$c \le |[\mathbb{R}]^{\aleph_0}| \le |[\mathbb{R}]^{\le \aleph_0}| \le |\mathbb{R}^{\mathbb{N}}| = c$$

e le funzioni:

$$\varphi : \mathbb{R} \to [\mathbb{R}]^{\aleph_0} \qquad\qquad \psi : \mathbb{R}^{\mathbb{N}} \to [\mathbb{R}]^{\le \aleph_0}$$

$$r \mapsto r + \mathbb{N} = \{ n + r \mid n \in \mathbb{N} \} \qquad\qquad a \mapsto \operatorname{Im} a,$$

la prima iniettiva, la seconda suriettiva.

Sia ora:

$$\mathcal{F} = \{ f : \mathbb{R} \to \mathbb{R} \mid f \text{ è non decrescente} \}$$

Per $f \in \mathcal{F}$, definiamo:

$$\Gamma(f) = \{ x \in \mathbb{R} \mid f \text{ è discontinua in } x \}$$

Si ha $|\Gamma(f)| \le \aleph_0$. Per $x \in \Gamma(f)$, definiamo:

$$I_x = \left] \sup_{\tilde{x} < x} f(\tilde{x}) \,,\, \inf_{\tilde{x} > x} f(\tilde{x}) \right[$$

Se $x_1 \neq x_2$, allora:

$$I_{x_1} \cap I_{x_2} = \emptyset$$

Inoltre, dato che $\overline{\mathbb{Q}} = \mathbb{R}$, possiamo affermare (anche senza l'uso dell'assioma della scelta) che:

$\forall\, I_x ,\ x \in \Gamma(f) : \exists\, q_x \in I_x \cap \mathbb{Q}$,

da cui la seguente funzione è iniettiva:

$$\psi : \Gamma(f) \to \mathbb{Q}$$
$$x \mapsto q_x$$

Consideriamo allora:

$$\Theta : \mathcal{F} \to \bigcup_{A \in [\mathbb{R}]^{\le \aleph_0}} C^0(\mathbb{R} \setminus A) \times \mathbb{R}^A$$
$$f \mapsto \left(f|_{\mathbb{R} \setminus \Gamma(f)} \,,\, f|_{\Gamma(f)} \right),$$

e l'applicazione è iniettiva.

Sicuramente $|\mathcal{F}| \ge c$ (consideriamo le funzioni costanti).
Ma vale anche $|\mathcal{F}| \le c$, perché vale:

$$\left| \bigcup_{A \in [\mathbb{R}]^{\le \aleph_0}} C^0(\mathbb{R} \setminus A) \times \mathbb{R}^A \right| = c$$

La dimostrazione consta di due parti:

- $\forall\, A \in [\mathbb{R}]^{\leq \aleph_0} \setminus \{\emptyset\}\ \ |C(\mathbb{R}\setminus A) \times \mathbb{R}^A| = \mathfrak{c}$.

Innanzitutto, se $|A| \leq \aleph_0$, allora:

$$\mathfrak{c} = |\mathbb{R}| \leq |\mathbb{R}^A| \leq |\mathbb{R}^{\mathbb{N}}| = \mathfrak{c},$$

e per Cantor-Bernstein:

$$|\mathbb{R}^A| = \mathfrak{c}$$

Vogliamo ora dimostrare che, se $|A| \leq \aleph_0$, allora $\mathbb{R} \setminus A$ è separabile:

$$\exists\, D \subseteq \mathbb{R}\setminus A \text{ t.c. } |D| \leq \aleph_0 \wedge \overline{D} = \mathbb{R}\setminus A$$

In questo modo potremo ricondurci alla dimostrazione usata per dimostrare che $C^0(\mathbb{R},\mathbb{R})$ ha cardinalità continua. In particolare D sarà una "copia" di $\mathbb{Q}$, dunque la dimostrazione sarà perfettamente adattabile.

Definiamo la relazione di equivalenza su $\mathbb{R}$:

$$r \sim r' \Leftrightarrow r - r' \in \mathbb{Q}$$

Allora:

$$[r]_\sim = r + \mathbb{Q} \overset{\text{def}}{=} \{r + q \mid q \in \mathbb{Q}\}$$

Sicuramente si ha:

$$|\mathbb{R}/_\sim| > \aleph_0,$$

altrimenti risulterebbe $|\mathbb{R}| \leq \aleph_0$, assurdo. Allora:

$\exists\, r^* \in \mathbb{R}$ t.c. $r^* + \mathbb{Q} \cap A = \emptyset$,

da cui la tesi.

- se $\langle A_i \mid i \in I\rangle$, con $|I| \leq \mathfrak{c}$ e $|A_i| \leq \mathfrak{c}$ per ogni $i \in I$, allora:

$$\left|\bigcup_{i\in I} A_i\right| \leq \mathfrak{c}$$

In effetti, sia $\varphi : \mathbb{R} \to I$ una funzione suriettiva, e sia, per $i \in I$, $\psi_i : \mathbb{R} \to A_i$ una funzione suriettiva. Usando l'assioma della scelta:

$$\langle \psi_i \mid i \in I\rangle \in \prod_{i\in I} \{\sigma : \mathbb{R} \to A_i \mid \sigma \text{ è suriettiva}\}$$

Definiamo allora $F : \mathbb{R} \times \mathbb{R} \to \bigcup_{i\in I} A_i$ in questo modo:

$$F(\lambda, \mu) = \psi_{\varphi(\lambda)}(\mu)$$

La funzione è suriettiva per costruzione. Allora:

$$\left|\bigcup_{i\in I} A_i\right| \leq |\mathbb{R}\times\mathbb{R}| = |\mathbb{R}| = c \Rightarrow \left|\bigcup_{i\in I} A_i\right| \leq c.$$

Con l'ultima dimostrazione vista, possiamo risolvere un quesito lasciato in sospeso:

$$|\mathcal{P}(\mathbb{R})\times\mathcal{P}(\mathbb{R})| \leq |\mathcal{P}(\mathbb{R})|$$

In effetti:

$$|\mathcal{P}(\mathbb{R})\times\mathcal{P}(\mathbb{R})| = |2^{2^{\mathbb{N}}}\times 2^{2^{\mathbb{N}}}| = |2^{2^{\mathbb{N}}\cup 2^{\mathbb{N}}}| = |2^{2^{\mathbb{N}}}| =$$

$$= |2^{\mathbb{R}}| = |\mathcal{P}(\mathbb{R})|$$

Quanto a $\mathbb{R}/_\sim$, si ha sicuramente $|\mathbb{R}/_\sim| \leq c$. Utilizzando l'assioma della scelta, e la seguente funzione:

$$\pi : \mathbb{R} \longrightarrow \mathbb{R}/_\sim$$
$$x \longrightarrow [x]_\sim,$$

banalmente suriettiva si ha la tesi.

Per dimostrare che $c \leq |\mathbb{R}/_\sim|$ non è necessario l'assioma della scelta.

Innanzitutto $|[0,1]| = c$, $|\mathbb{Q}\cap[0,1]| = \aleph_0$, da cui $|(\mathbb{R}\setminus\mathbb{Q})\cap[0,1]| = c$.
Sia $X \overset{def}{=} (\mathbb{R}\setminus\mathbb{Q})\cap[0,1]$, e sia $r \in X$. Allora:

$$r = 0,a_1a_2a_3a_4\ldots \quad a_i \in \{0,\ldots 9\}\ \forall i\in\mathbb{N},$$

e non vi sono periodi. Sia $Y \subseteq X$ il sottoinsieme di X dei reali tali che:

$$s = 0,a_1a_2a_3a_4,\ldots \quad a_i \in \{1,\ldots 9\}\ \forall i\in\mathbb{N}$$

Chiaramente $|Y| = c$. Sia:

$$\varphi : Y \longrightarrow \mathbb{R}\setminus\mathbb{Q}$$

$$\varphi(0,a_1a_2\ldots) = 0,a_1 0 a_1a_2 00 a_1a_2a_3 000\ldots$$

Sia $\psi = \pi\circ\varphi$. Se $r > r'$, allora:

$$\exists k\in\mathbb{N} \ni' a_{k,r} \neq a_{k,r'} \wedge a_{h,r} = a_{h,r'}\ \forall h < k \Rightarrow$$
$$\Rightarrow \exists \varphi(r-r') \in \mathbb{R}\setminus\mathbb{Q} \Rightarrow \psi(r-r') \neq [0],$$

ossia $[r] \neq [r']$, da cui $\psi(r) \neq \psi(r')$. Allora $\psi : Y \to \mathbb{R}/_\sim$ è iniettiva, da cui, senza usare l'assioma della scelta:

$$c \leq |\mathbb{R}/_\sim|$$

TEORIA ASSIOMATICA DEGLI INSIEMI

Iniziamo una trattazione più rigorosa della teoria degli insiemi.

Partiamo dalle FORMULE. Se x, y sono variabili, si dicono FORMULE ATOMICHE:

- $x = y$ (uguaglianza);
- $x \in y$ (appartenenza).

L'uso dei connettivi consente di amplificare la gamma delle formule. Se P, Q sono formule, allora sono formule le seguenti

$$P \vee Q \qquad P \wedge Q \qquad \neg P \qquad P \Rightarrow Q \qquad P \Leftrightarrow Q$$

In particolare, le variabili x e y citate sopra sono variabili LIBERE. Un caso in cui una variabile è invece LEGATA si ha quando si usano i quantificatori.

Se $P(x)$ è una formula, dove x è libera, sono formule le seguenti:

- $\exists\ x : P(x)$;
- $\forall\ x : P(x)$.

In questo caso x è LEGATA.

Notiamo invece che, se P e Q sono formule, l'uso dei connettivi logici non altera lo stato di variabile libera o legata delle variabili coinvolte.

Una formula dove tutte le variabili sono legate si dicono ENUNCIATI. Essa rispetta i principi di non contraddizione e del terzo escluso.

Una formula che presenta invece variabili libere si dice PREDICATO. Il suo valore di verità dipende dal valore attribuito alle variabili libere.

Enunciamo ora alcuni assiomi.

ASSIOMA (DI ESTENSIONALITÀ)

Siano X, Y insiemi. Allora:

$$(\forall t : t \in X \Leftrightarrow t \in Y) \Leftrightarrow X = Y$$

ASSIOMA (DELL' INSIEME VUOTO)

Esiste un unico insieme (per l'assioma di estensionalità), detto INSIEME VUOTO, tale che:

$$\forall t : t \notin X$$

Si scriverà $X = \emptyset$.

ASSIOMA (DELLA COPPIA)

Dati due insiemi A e B, $C = \{A, B\}$ è un insieme.

ASSIOMA (DELL' UNIONE)

Data una famiglia di insiemi x, esiste un insieme $y = \bigcup_{t \in x} t \overset{def}{=} \bigcup x$, ossia tale che:

$$\forall s : (s \in y \Leftrightarrow \exists t \in x : s \in t)$$

ASSIOMA (DI POTENZA)

Dato un insieme X, esiste Y tale che $Y = P(X)$.

ASSIOMA (DI SEPARAZIONE O ASTRAZIONE LIMITATA)

Si ha:

$$\forall x_1 \dots x_n, \forall y \; \exists z : z = \{t \in y \mid \varphi(t, x_1, \dots x_n)\}$$

Questo assioma è diverso dai precedenti: esso è dunque detto SCHEMA DI SEPARAZIONE. La formula $\varphi(t, x_1, \dots, x_n)$ è un predicato in cui $t, x_1 \dots x_n$ sono tutte e sole le variabili libere.

Ex. Per lo schema di separazione, dato un insieme qualunque y, esiste l'insieme:

$$V = \{t \in y \mid t \notin t\}$$

Vogliamo ora dimostrare che, per ogni coppia di insiemi A, B esistono i seguenti insiemi:

$C_1 = A \cap B$ $\quad$ $C_2 = A \cup B$ $\quad$ $C_3 = A \setminus B$

$C_4 = (A, B)$ $\quad$ $C_5 = A \times B$ $\quad$ $C_6 = \mathrm{Fun}(A, B) = B^A$

Dimostriamo l'esistenza di C_1. Si ha:

$$C_1 = \{ x \in A \mid x \in B \}$$

L'assioma di estrazione limitata ci dice che:

$\forall x, \forall y \; \exists z \; t.c. \; z = \{ t \in y \mid \varphi(t, x) \}$

Scegliendo:

- $x = B$;
- $y = A$;
- $\varphi(t, x) = t \in x$,

si ha che esiste:

$$C_1 = \{ t \in A \mid t \in B \}$$

Dimostriamo l'esistenza di C_2. Per l'assioma della coppia, dati A, B, esiste $\{A, B\}$. Per l'assioma dell'unione, esiste:

$$C_2 = \bigcup \{A, B\} \overset{\text{def}}{=}$$
$$\overset{\text{def}}{=} \{ x \mid \exists \, t \in \{A, B\} : x \in t \} =$$
$$= A \cup B$$

Dimostriamo l'esistenza di C_3. Si ha:

$$C_3 = \{ x \in A \mid x \notin B \}$$

Scegliendo:

- $x = B$;
- $y = A$;
- $\varphi(x, t) = x \notin t$,

si prova l'esistenza di C_3:

$$\exists \; C_3 = \{ x \in A \mid x \notin B \}$$

Dimostriamo l'esistenza di C_4. Usando ripetutamente l'assioma della coppia, dati A e B insiemi:

- $\exists \ \{A, A\} = \{A\}$,
- $\exists \ \{A, B\}$,

da cui:

$$\exists \{\{A\},\{A,B\}\} = (A,B)$$

Dimostriamo ora l'esistenza di C_5. Usando due volte l'assioma della potenza:

- $\exists \ \mathcal{P}(A \cup B)$;
- $\exists \ \mathcal{P}(\mathcal{P}(A \cup B))$.

In particolare:

$$\{a\}, \{a,b\} \in \mathcal{P}(A \cup B) \Rightarrow$$
$$\Rightarrow (a,b) = \{\{a\},\{a,b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$$

Usando ora lo schema di separazione:

$$A \times B = \{ x \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid \exists a \ \exists b : a \in A \wedge b \in B \wedge (a,b) = x \}$$

Dimostriamo ora l'esistenza di C_6. Per l'assioma di potenza, infatti, esiste $\mathcal{P}(A \times B)$ (sapendo che $A \times B$ esiste). Usando ora lo schema di estrazione, con:

$$\varphi(t, A, B) = \forall a \in A \ \exists! \ b \in B : (a,b) \in t,$$

si ha:

$$C_6 = \{ t \in \mathcal{P}(A \times B) \mid \varphi(t, A, B) \}$$

In maniera simile, esiste l'INSIEME QUOZIENTE:

$$\psi(t, R) = \forall x \in t, \ \forall y \in t : (x,y) \in R$$

$$A/R = \{ t \in \mathcal{P}(A \times B) \mid \psi(t,R) \},$$

dove ovviamente $R \subseteq A \times A$ è una relazione di equivalenza

INSIEMI E CLASSI

Esistono tre principali assiomatizzazioni della Teoria degli insiemi:

- la Teoria di ZERMELO - FRAENKEL (ZF);
- la Teoria di VON NEUMANN - BERNAYS - GÖDEL (NBG);
- la Teoria di MORSE - KELLEY (MK).

Le differenze tra i diversi approcci riguardano in sostanza il modo in cui viene affrontato il problema della distinzione tra INSIEMI e CLASSI, e in particolare lo "status" che viene attribuito a quest'ultime.

Ad oggi, la più comune nel mondo matematico è ZF; tuttavia, vi sono casi in cui conviene disporre della nozione di classe, per cui si usa NGB.

Ad esempio, la classe di Russell non è un insieme (in NGB):

$$R = \{ x \mid x \notin x \}$$

In ZF, non essendo definita la nozione di classe, si dice che non esiste un insieme che contenga tutti e soli gli x tali che $x \notin x$.

Un insieme è dunque una particolare classe che appartiene ad almeno un'altra classe. Una classe è detta PROPRIA se non è un insieme. Le seguenti, ad esempio, sono CLASSI PROPRIE:

$$R = \{ x \mid x \notin x \}$$
$$V = \{ x \mid x = x \}$$

Altri esempi, come la classe di tutti gli ORDINALI, verranno analizzati più avanti.

ASSIOMA DELLA SCELTA

OSSERVAZIONE

Sia $\langle A_i \mid i \in I \rangle$ una sequenza. Allora, dato:

$$f : i \to A_i,$$

si può dimostrare che esiste:

$$\mathrm{Im}\ f = \{ A_i \mid i \in I \}$$

Per l'assioma dell'unione, esiste:

$$\bigcup_{i \in I} A_i$$

Allora esiste:

$$\mathrm{Fun}\left(I, \bigcup_{i \in I} A_i \right),$$

e per l'assioma di separazione esiste:

$$\prod_{i \in I} A_i = \left\{ f \in \mathrm{Fun}\left(I, \bigcup_{i \in I} A_i \right) \;\middle|\; \forall i \in I : f(i) \in A_i \right\}$$

Non si sa se $\prod_{i \in I} A_i$ è vuoto o no; sicuramente, se esiste $i \in I$ per cui $A_i = \emptyset$, allora $\prod_{i \in I} A_i = \emptyset$.

ASSIOMA (DELLA SCELTA)

Se $\langle A_i \mid i \in I \rangle$ è una sequenza infinita di insiemi non vuoti, allora $\prod_{i \in I} A_i \neq \emptyset$.

Resta da dimostrare che $\mathrm{Im}\ f$ esiste.

Data una coppia $(a, b) \in f$, si ha:

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

Allora si ha:

$$A \cup B = \bigcup \left[\bigcup_{(a,b) \in A \times B} (a, b) \right]$$

Da qui, usando lo schema di estrazione:

$$\mathrm{Im}\ f = \{ b \in A \cup B \mid \exists\, a \in A \cup B \text{ t.c. } (a, b) \in f \}$$

NUMERI NATURALI

Definiamo:

$$0 \overset{def}{=} \emptyset$$

$$1 \overset{def}{=} \{\emptyset\}$$

$$2 \overset{def}{=} \{\emptyset, \{\emptyset\}\}$$

$$3 \overset{def}{=} \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\},$$

e così via. In generale:

$$n \overset{def}{=} \{(n-1) \cup \{n-1\}\}$$

Gli assiomi ci garantiscono l'esistenza di questi insiemi, ma nessun assioma ci garantisce l'esistenza dell'insieme contenente tutti e soli quegli insiemi.

Notiamo che, fino ad ora, l'esistenza di insiemi di cardinalità infinita non è garantita dagli assiomi presentati finora.

ASSIOMA (DELL'INFINITO)

Esistono insiemi INDUTTIVI ossia tali che:

- $\emptyset \in X$;
- $x \in X \Rightarrow \hat{x} = x \cup \{x\} \in X$.

Un insieme n si dice NUMERO NATURALE (di Von Neumann) se n appartiene ad ogni insieme induttivo: è palese che $0, 1, 2, \dots$ siano numeri naturali.

TEOREMA

Esiste l'insieme ω di tutti e soli i numeri naturali. ω è il più piccolo tra gli insiemi induttivi: infatti ω stesso è induttivo.

Dim.

Per l'assioma dell'infinito, esiste X induttivo. Allora basta considerare:

$$\omega = \{x \in X \mid x \text{ è numero naturale}\}$$

PRINCIPIO DI INDUZIONE

TEOREMA

Sia $A \subseteq \omega$. Se $0 \in A$ e $\forall n \in \omega : n \in A \Rightarrow \hat{n} = n+1 \in A$, allora $A = \omega$.

Una forma alternativa è la seguente.

TEOREMA

Sia $P(x, y_1, \dots, y_k)$ una formula. Per ogni $A_1, \dots, A_k$, se:

- $P(0, A_1, \dots, A_k)$;
- $\forall n \in \omega : P(n, A_1, \dots, A_k) \Rightarrow P(n+1, A_1, \dots, A_k)$,

allora:

$\forall n \in \omega : P(n, A_1, \dots, A_k)$

Le due formulazioni non sono equivalenti. La cardinalità delle formule è infatti numerabile, mentre la cardinalità delle parti è continua.

Dim.

Le ipotesi dicono semplicemente che A è un insieme induttivo. Allora $\omega \subseteq A$, ossia $A = \omega$, c.v.d.

La versione presentata è detta INDUZIONE DEBOLE, per distinguerla da quella che viene detta INDUZIONE FORTE.

TEOREMA

Sia $P(x)$ una proprietà. Se valgono le seguenti:

- $P(0)$;
- $[\forall x < y : P(x)] \Rightarrow P(y)$,

allora $P(x)$ è vera per ogni $x \in \omega$.

Le due forme di induzione, in ogni caso, sono equivalenti, assumendo che:

$\forall y \in \omega \setminus \{0\} : \exists x \in \omega$ t.c. $y = x+1$

OSSERVAZIONI SUI NUMERI NATURALI

LEMMA

Sia $n \in \omega$, $n \neq 0$. Allora $0 \in n$.

Dim.

Consideriamo la seguente proprietà:

$$P(n): (n \in \omega, n \neq 0) \Rightarrow 0 \in n$$

Ragioniamo per induzione su n.

CASO BASE

$n = 0$

La proprietà è vera "a vuoto", perché l'ipotesi è :

$P(0)$ è dunque vera.

PASSO INDUTTIVO

$n \Rightarrow \hat{n}$

Supponendo $P(n)$, vogliamo dimostrare $P(\hat{n})$.

Si hanno due casi:

- $n = 0 \Rightarrow \hat{0} \in \{0\} = \hat{0} = \hat{n}$;
- $n \neq 0$: per ipotesi induttiva, $0 \in n \subseteq \hat{n} \Rightarrow 0 \in \hat{n}$, c.v.d.

OSSERVAZIONE

$A = \{\{\emptyset\}\} \neq \omega$ perché $A \neq \emptyset$, ma $\emptyset \notin A$.

LEMMA

Se $x \in y$, allora $\hat{x} \in \hat{y}$.

Dim.

Ragioniamo per induzione su y, con la proprietà:

$$P(y) = \forall x : x \in y \Rightarrow \hat{x} \in \hat{y}$$

CASO BASE

$y = 0$

Anche in questo caso $P(0)$ è vera a vuoto.

PASSO INDUTTIVO

$y \rightarrow \hat{y}$

Assumiamo $P(y)$; vogliamo dimostrare $P(\hat{y})$.

Si ha:

$$x \in \hat{y} = y \cup \{y\} \Rightarrow \begin{cases} x \in y \Rightarrow \hat{x} \in \hat{y} \subseteq \hat{\hat{y}} \\ x \in \{y\}, \text{ ossia } x = y \Rightarrow \hat{x} = \hat{y} \in \hat{\hat{y}} \end{cases}, \text{ c.v.d.}$$

PROPOSIZIONE

$(\omega, \in)$ è un insieme totalmente ordinato.

Dim.

Dobbiamo dimostrare le seguenti proprietà:

- $x \notin x$;
- $x \in y \wedge y \in z \Rightarrow x \in z$;
- $\forall x, y$, vale una sola delle seguenti possibilità:
  - $x \in y$;
  - $y \in x$;
  - $x = y$.

Cominciamo con la seconda proprietà:

$$P(z) = \forall x \ \forall y : (x \in y \wedge y \in z) \Rightarrow x \in z$$

Ragioniamo per induzione su z. Come si vede $P(0)$ è vera a vuoto. Assumiamo $P(z)$, e dimostriamo che:

$$x \in y \wedge y \in \hat{z} \Rightarrow x \in \hat{z}$$

Sia $y \in \hat{z}$. Allora:

- se $y \in z$, per ipotesi induttiva, da $(x \in y \wedge y \in z) \Rightarrow$
  $\Rightarrow x \in z \subseteq \hat{z}$;
- se $y = z$, $x \in y = z$, ossia $x \in z \subseteq \hat{z}$,

ossia la tesi.

Dimostriamo ora la prima proprietà, con la proprietà:

$$P(x) = x \notin x$$

$P(0)$ è vera a vuoto. Assumiamo $P(x)$, allora dobbiamo dimostrare che $\hat{x} \notin \hat{x}$. È equivalente dimostrare che:

$$\hat{x} \in \hat{x} \Rightarrow x \in x$$

Se $\hat{x} \in \hat{x}$, allora:

- se $\hat{x} \in x$, allora $x \in \hat{x} \in x \Rightarrow x \in x$;
- se $\hat{x} = x$, allora $\hat{x} \in \hat{x}$ equivale a $x \in x$.

Rimane da provare la terza proprietà:

$\forall\, m, n \in \omega \quad m \in n \ \dot{\vee}\ m = n \ \dot{\vee}\ n \in m$

Useremo un'induzione "doppia": ragioniamo per induzione su n.

CASO BASE

$n = 0$

Per ogni $m \in \omega$, si ha $m \notin 0$. Inoltre abbiamo dimostrato che:

$$m \neq 0 \Rightarrow 0 \in m,$$

da cui:

$\forall\, m \in \omega : \ m \in 0 \ \dot{\vee}\ m = 0 \ \dot{\vee}\ 0 \in m$

è vero (parzialmente a vuoto).

PASSO INDUTTIVO

Supponiamo la proprietà vera per n:

$\forall\, m \in \omega : \ m \in n \ \dot{\vee}\ m = n \ \dot{\vee}\ n \in m$

Dimostriamo la proprietà per $\hat{n}$. Sia $m \in \omega$. Allora:

- $m \in n \Rightarrow m \in n,\ n \in \hat{n} \Rightarrow m \in \hat{n}$;
- $m = n \Rightarrow m = n \in \hat{n} \Rightarrow m \in \hat{n}$;
- $n \in m$. Ragioniamo per induzione su $m \in \omega$:

  $$P(m) : \quad n \in m \Rightarrow \left[\hat{n} = m \ \dot{\vee}\ \hat{n} \in m\right]$$

  CASO BASE

  La proprietà è vera a vuoto, perché $\hat{n} \notin 0 \quad \forall\, \hat{n} \in \omega$.

  PASSO INDUTTIVO

  Supponiamo vera $P(m)$. Allora, se $n \in \hat{m}$, allora:

  - $n \in m \Rightarrow \hat{n} \in m \ \dot{\vee}\ \hat{n} = m$, per ipotesi induttiva, dunque in particolare $\hat{n} \in \hat{m}$;
  - $n = m \Rightarrow \hat{n} = \hat{m}$.

L'induzione su m è completa. Allora è completa anche l'induzione su n, e la proposizione è dimostrata, c.v.d.

CARDINALITÀ DI ω

PROPOSIZIONE

La funzione seguente è una bigezione:

$$S: \omega \to \omega \setminus \{0\}$$
$$n \mapsto \hat{n}$$

Dim.

Iniettività:

$$\hat{n} = \hat{m} \Rightarrow n = m$$

Infatti:

$$n \in \hat{n} = \hat{m} = m \cup \{m\} \begin{cases} n \in m \\ n = m \end{cases}$$

$$m \in \hat{m} = \hat{n} = n \cup \{n\} \begin{cases} m \in n \\ m = n \end{cases}$$

Se fosse $n \neq m$, allora sarebbe $n \in m$, $m \in n \Rightarrow n \in n$, assurdo. Dunque $n = m$. Dunque S è iniettiva.

Dimostriamo ora la suriettività. La proprietà è:

$$P(n) \equiv (n \neq 0 \Rightarrow \exists m : \hat{m} = n)$$

Se ovvio, $P(0)$ è vera a vuoto. Quanto al passo induttivo, assumendo $P(n)$, si ha:

$$m = \hat{n} \neq 0 \Rightarrow \exists m = n : \hat{m} = \hat{n},$$

ossia $P(\hat{n})$ è vera, c.v.d.

OSSERVAZIONE

$S: \omega \to \omega \setminus \{0\}$ è una bigezione: dunque ω è infinito.

OSSERVAZIONE

Siano $x, y \in \omega$. Allora:

$$\hat{x} \in \hat{y} \Rightarrow x \in y$$

Infatti, se $\hat{x} \in \hat{y}$, le possibilità sono due:

- $\hat{x} \in y$, $x \in \hat{x} \Rightarrow x \in y$;
- $\hat{x} \in \{y\} \Rightarrow \hat{x} = y \Rightarrow x \in \hat{x} = y \Rightarrow x \in y$.

OSSERVAZIONE

Sia $x \in n \in \omega$. Allora $x \in \omega$. Ragioniamo per induzione su n, con la proprietà:

$$P(n) = \forall x : x \in n \Rightarrow x \in \omega$$

Il caso base, per $n=0$, è vero a vuoto. Supponendo vero $P(n)$, se $x \in \hat{n}$:

- $x \in n \Rightarrow x \in \omega$, per ipotesi induttiva;
- $x \in \{n\} \Rightarrow x = n \Rightarrow x \in \omega$.

OSSERVAZIONE

Sia $n \in \omega$. Allora $\hat{n}$ è il SUCCESSORE di n, ossia:

$\forall m \in \omega : n \in m \Rightarrow m = \hat{n} \;\dot\vee\; \hat{n} \in m$

Sappiamo infatti che:

$\forall n, m \in \omega : m \in \hat{n} \;\dot\vee\; m = \hat{n} \;\dot\vee\; \hat{n} \in m$,

dunque è sufficiente dimostrare la seguente proprietà:

$$P(m) = n \in m \Rightarrow [\hat{n} = m \;\dot\vee\; \hat{n} \in m]$$

Ragioniamo con un'induzione su m.

CASO BASE

$m=0$

La proprietà è vera a vuoto.

PASSO INDUTTIVO

Supponiamo vera $P(m)$. Allora, se $n \notin \hat{m}$, la proprietà è vera a vuoto. Se invece $n \in \hat{m}$, allora $n \in m$, e per ipotesi induttiva $\hat{n} \in \hat{m}$, oppure $n \in \{m\}$, ossia $n = m$, ossia $\hat{n} = \hat{m}$, e la proprietà è vera.

D'ora in avanti scriveremo $n+1$ in favore di $\hat{n}$: è molto più familiare, come notazione.

PRINCIPIO DI INDUZIONE
PRINCIPIO DI BUON ORDINAMENTO

TEOREMA

Sia $(N, <)$ un insieme ordinato, con minimo 0.
Allora sono proprietà equivalenti:

- ogni $A \subseteq N$ non vuoto, A ammette minimo;
- per ogni proprietà $P(x)$, se vale:
  - $P(0)$;
  - $[\forall x < y : P(x)] \Rightarrow P(y)$,

  allora $P(x)$ è vera per ogni $x \in N$.

Un insieme che rispetta queste due proprietà, l'insieme si dice BENE ORDINATO.

Dim.

Sia $Q(x)$ una proprietà che soddisfa $Q(0)$ e $[\forall x < y : Q(x)] \Rightarrow$ $\Rightarrow Q(y)$, tale che $\{x \in N \mid \neg Q(x)\} \neq \emptyset$: neghiamo dunque il principio di induzione. Allora, se $E \overset{def}{=} \{x \in N \mid \neg Q(x)\}$, E non ammette minimo. Se infatti esistesse $e = \min E$, innanzitutto $e \neq 0$ perché $Q(0)$ è vera. Dato che $y \in E$:
$\forall z < y : Q(z) \Rightarrow Q(y)$,
assurdo.
Per contronominale, il buon ordinamento implica il principio di induzione.

Neghiamo ora il buon ordinamento: sia $X \neq \emptyset$ senza minimo. Sia:

$$P(x) = x \notin X$$

Allora $0 \in X \Rightarrow 0 = \min X$, assurdo. Dunque $0 \notin X$, ossia $P(0)$ è vera. Inoltre:
$\forall z < y : P(z) \Rightarrow P(y)$,
altrimenti $y = \min X$, assurdo. Dunque:

$$\forall x \in X : P(x) \Rightarrow \forall x \in X : x \notin X,$$

ossia $X = \emptyset$, una contraddizione.
Per contronominale, il principio di induzione implica il principio del buon ordinamento, c.v.d.

TEOREMA DI RICORSIONE NUMERABILE

Dato $n \in \mathbb{N}$, il fattoriale di n, $n!$, è definito spesso in questo modo, detto RICORSIVO:

$$\begin{cases} 0! = 1 \\ (n+1)! = n!\,(n+1) \end{cases}$$

Con questa definizione, stiamo implicitamente affermando che esiste un'unica successione $\langle a_n \mid n \in \mathbb{N} \rangle$ tale che $a_0 = 1$, $a_{n+1} = a_n (n+1)$.

TEOREMA

Sia A un insieme, $\tilde{a} \in A$ un elemento di A, $g : \omega \times A \to A$ una funzione. Allora esiste ed è unica la successione $\langle a_n \mid n \in \mathbb{N} \rangle$ di elementi di A tale che:

- $a_0 = \tilde{a}$;
- $a_{n+1} = g(n, a_n)$.

Dim.

Nel caso di approssimazioni finite, si ha l'esistenza e l'unicità dei primi termini:

- $a_0 = \tilde{a}$;
- $a_1 = g(0, \tilde{a})$;
- $a_2 = g(1, g(0, \tilde{a}))$,

e così via.

In generale, φ è un' APPROSSIMAZIONE FINITA se esiste $k \in \omega$ tale che $\mathrm{Dom}\,\varphi = \{0, \dots k-1\}$, con $\varphi(0) = \tilde{a}$ e, per ogni $n+1 \in \mathrm{Dom}\,\varphi$, con $n \in \mathrm{Dom}\,\varphi$:

$$\varphi(n+1) = g(n, \varphi(n)).$$

LEMMA (SOLO ENUNCIATO)

Sia $\mathcal{F}$ una famiglia di funzioni.

L'unione $F = \bigcup_{f \in \mathcal{F}} f$ è una funzione se e solo se le funzioni in $\mathcal{F}$ sono compatibili a due a due, ossia:

$\forall f, g \in \mathcal{F}, \forall x \in \mathrm{Dom}\,f \cap \mathrm{Dom}\,g : f(x) = g(x)$

Dobbiamo allora dimostrare che:

- $\forall k \in \omega$ esiste φ_k approssimazione finita con Dom φ_k = $= k = \{0, \dots, k-1\}$;
- Se φ e ψ sono due approssimazioni finite, allora per ogni $x \in$ Dom $\varphi \cap$ Dom ψ si ha $\varphi(x) = \psi(x)$.

Nel nostro caso

- Dom $\varphi = k = \{0, \dots, k-1\}$;
- Dom $\psi = h = \{0, \dots, h-1\}$.

Bisogna allora verificare che valga:

$$\varphi \subseteq \psi \quad o \quad \psi \subseteq \varphi$$

Dopo aver dimostrato ciò, l'unione F di tutte le approssimazioni finite è tale che $a_n = F(n)$ soddisfa la tesi.

Prima di continuare, osserviamo che l'insieme delle approssimazioni finite è contenuto in $\omega \times A$, dunque esiste per lo schema di separazione.

Dimostriamo prima la seconda proposizione. Procediamo ancora una volta, per induzione su n.

CASO BASE

Se $0 \in$ Dom $\varphi \cap$ Dom ψ, per definizione di approssimazione finita:

$$\varphi(0) = \bar{a} = \psi(0)$$

PASSO INDUTTIVO

Sia $(n+1) \in$ Dom $\varphi \cap$ Dom ψ. Allora:

- $\varphi(n+1) = g(n, \varphi(n))$
- $\psi(n+1) = g(n, \psi(n))$

Inoltre:

$$(n+1) \in \text{Dom } \varphi \cap \text{Dom } \psi \Rightarrow n \in \text{Dom } \varphi \cap \text{Dom } \psi,$$

e per ipotesi induttiva:

$$\varphi(n) = \psi(n) \Rightarrow g(n, \varphi(n)) = g(n, \psi(n)),$$

ovvia:

$$\varphi(m+1) = \psi(m+1).$$

Dimostriamo ora la prima proposizione, sempre per induzione.

CASO BASE

La funzione:

$$\varphi_0 : \{0\} \to A$$
$$0 \to \tilde{a}$$

è un'approssimazione finita del tipo richiesto.

PASSO INDUTTIVO

Supponiamo che $\varphi_m : \{0, \dots, m\} \to A$ esista. Allora definiamo:

$$\varphi_{m+1} \quad \{0, \dots, m+1\} \to A$$

$$\varphi_{m+1}(x) = \begin{cases} \varphi_m(x), & x \in \{0, \dots, m\} \\ g(m, \varphi_{m+1}(m)), & x = m+1 \end{cases}$$

φ_{m+1} è in effetti un'approssimazione finita del tipo richiesto.

Ciò conclude la dimostrazione, c.v.d.

ESERCIZIO

Siano $n, m \in \omega$. Vogliamo dimostrare che:

$$n \cap m \in \omega$$
$$n \cup m \in \omega,$$

ove, informalmente:

$$n \cap m = \min\{n, m\}$$
$$n \cup m = \max\{n, m\}$$

Ragioniamo per induzione su n, con la proprietà:

$$P(n) = \forall m : n \cap m,\ n \cup m \in \omega$$

CASO BASE

$n = 0$

Si ha banalmente:

$\forall m \in \omega : 0 \cap \omega = 0 \in \omega,\ 0 \cup m = m \in \omega$

da cui $P(0)$ è vero.

PASSO INDUTTIVO

Supponiamo che sia vera $P(n)$. Ragioniamo per induzione su m:

$$Q(m) = n \cap m,\ n \cup m \in \omega$$

CASO BASE

$m = 0$

Si ha banalmente $\hat{n} \cap 0 = 0$, $\hat{n} \cup 0 = \hat{n} \in \omega$,

da cui $Q(0)$ è vero.

PASSO INDUTTIVO

Supponiamo che regga $Q(m)$. Allora:

- $\hat{n} = \hat{m} \Rightarrow \hat{n} \cap \hat{m} = \hat{n} \cup \hat{m} = \hat{n} \in \omega$;
- $\hat{n} \in \hat{m} \Rightarrow \hat{n} \cap \hat{m} = \hat{n} \in \omega,\ \hat{n} \cup \hat{m} = \hat{m} \in \omega$;
- $\hat{m} \in \hat{n} \Rightarrow \hat{n} \cap \hat{m} = \hat{m} \in \omega,\ \hat{n} \cup \hat{m} = \hat{n} \in \omega$

Allora $Q(\hat{m})$ è vera, dunque anche $P(\hat{n})$, dunque l'asserto.

TEOREMA DI CANTOR-BERNSTEIN

Dimostriamo ora un teorema che in passato abbiamo solamente enunciato.

TEOREMA (DI CANTOR-BERNSTEIN)

Se $|X| \leq |Y|$ e $|Y| \leq |X|$, allora $|X| = |Y|$.

Dim.

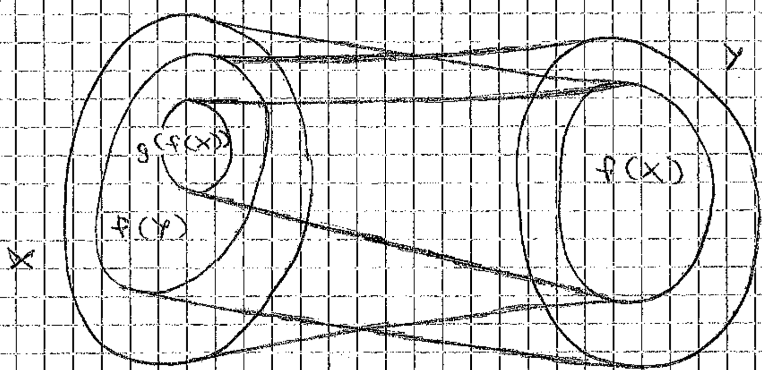
Fissiamo due funzioni iniettive:

$$f: X \to Y \qquad g: Y \to X$$

Si ha:

- $f(X) \subseteq Y$, $|f(X)| = |X|$;
- $g(f(X)) \subseteq g(Y) \subseteq X$, $|g(f(X))| = |f(X)| = |X|$, $|g(Y)| = |Y|$.

Un disegno chiarisce le idee:



Dunque abbiamo:

$$g(f(X)) \subseteq g(Y) \subseteq X,$$
$$|g(f(X))| = |X|$$

E' sufficiente allora dimostrare che, se A, B, C sono tali che:

$$A \supseteq B \supseteq C, \quad |A| = |C|,$$

allora $|A| = |B| = |C|$.

Fissiamo una bigezione $\varphi: A \to C$. Vogliamo trovare una bigezione $\psi: A \to B$. Sia $D = A \setminus B$.

Per il teorema di ricorsione numerabile, definiamo una successione di insiemi:

$$\begin{cases} E_0 = \varphi(D) \\ E_{n+1} = \varphi(E_n) \end{cases}$$

Sia $E \overset{def}{=} \bigcup_{n\in\omega} E_n$.

Definiamo allora:

$$\psi(a) \overset{def}{=} \begin{cases} \varphi(a), & a \in D \cup E \\ a, & a \in B \setminus E \end{cases}$$

Dobbiamo controllare che ψ sia una bigezione:

- ψ è suriettiva su B. Sia $b \in B$. Allora:
  - se $b \in B \setminus E$, allora $b = \psi(b)$;
  - se $b \in E_0 = \varphi(D)$, allora esiste $d \in D$ tale che $\psi(d) = \varphi(d) = b$;
  - se $b \in E_{n+1}$, allora esiste $k \in E_n$ tale che $\psi(k) = \varphi(k) = b$;
- ψ è iniettiva. Infatti ψ si ottiene da due funzioni con dominio disgiunto, ossia:

$$\varphi|_{D\cup E} \qquad \mathrm{Id}|_{B\setminus E}$$

Esse sono iniettive, e gli insiemi immagine sono disgiunti, da cui ψ è iniettiva perchè $\varphi|_{D\cup E}$ e $\mathrm{Id}|_{B\setminus E}$ lo sono.

Dunque ψ è una bigezione, da cui, tornando indietro:

$$|g(f(X))| = |g(Y)| = |X|$$
$$|g(Y)| = |Y|$$
$$|Y| = |X| \text{, c.v.d}$$

INSIEMI FINITI

Un insieme A si dice FINITO se:

$\exists\, n \in \omega \ni |A| = |n|$

Dimostriamo subito una proprietà

PROPOSIZIONE

Si ha:

$\forall A, \forall n \in \omega : (A \subsetneq n \Rightarrow \exists\, m \in n \ni' |A| = |m|)$.

Dim.

Procediamo per induzione su n.

CASO BASE

Per ogni insieme A, $A \subsetneq \emptyset$ è sicuramente falsa, da cui la proprietà è vera a vuoto.

PASSO INDUTTIVO

Sia $A \subsetneq \{0, \ldots, n\} = n+1$. I casi sono due:

- $n \notin A \Rightarrow A \subseteq n$. In questo caso:
  - se $A = n$, si ha $|A| = |n| < |n+1|$;
  - se $A \subsetneq n$, si ha, per ipotesi induttiva:
    $\exists\, m \quad m \in n+1 \ni' |A| = |m|$;
- $n \in A \Rightarrow \exists\, k \in n \ni' k \notin A$. Allora $A' = A \setminus \{n\}$ è tale che $A' \subsetneq n$, da cui, per ipotesi induttiva:
  $\exists\, m' \in n \ni' |A'| = |m'|$
  Ciò vuol dire che esiste $f : A' \to m'$ biunivoca. Sia dunque:
  $$g \overset{def}{=} f \cup \{(n, m')\}$$
  $$g : A' \cup \{n\} \to m' \cup \{m'\}$$
  $$g : A \to m'+1$$
  g è una bigezione, da cui $|A| = |m'+1|$. Ma:
  $$m' \in n \Rightarrow m'+1 \in n+1,$$
  e ciò conclude la dimostrazione, c.v.d.

COROLLARIO

Se $B \subseteq A$, con A finito, B è finito.

Dim

Per ipotesi esiste $f: A \longrightarrow n$, $n \in \omega$, bigettiva. Allora:

$$f(A) = \{0, \ldots, n-1\}$$

$$f(B) \subseteq f(A)$$

Si ha in ogni caso $f(B) \subsetneq n+1$, da cui, per la proprietà dimostrata:

$\exists\ m \in n+1 \ni' |f(B)| = |m|$

Ma $|f(B)| = |B|$, da cui B è finito, c.v.d.

OSSERVAZIONE

D'ora in poi scriveremo $n < m$ in favore di $n \in m$: è una notazione nettamente più familiare. Nella proposizione precedente, si noti che $(n+1)$ è il successore di n, da cui $|f(B)| \leq$ $\leq |f(A)|$.

PRINCIPIO DEI CASSETTI

PROPOSIZIONE (PIGEON-HOLE)

Sia $n > m$ e $f : n \to m$. Allora f non è iniettiva.

Dim.

Procediamo per induzione su m.

CASO BASE

Per $m = 0$ l'ipotesi è falsa, dunque la proposizione è vera a vuoto.

PASSO INDUTTIVO

Sia $n+1 > m$ e sia $f : n+1 \to m$.

Supponiamo per assurdo che f sia iniettiva. Sia:

$$A \overset{def}{=} f(\{0, \dots, n-1\}) = \{f(0), \dots, f(n-1)\}$$

Osserviamo che $A \neq m$, infatti:

$$f(n) \in A \setminus f(\{0, \dots, n-1\}),$$

perché $n \notin A$ e f è iniettiva. Allora:

$\exists\, k < m$ t.c. $|A| = |k| \Rightarrow \exists\, g : A \to k$ biunivoca

La funzione composta:

$$h : n \to k$$

$$h = g \circ f|_{\{0, \dots, n-1\}}$$

è iniettiva, con $k < m < n+1 \Rightarrow k < m \leq n \Rightarrow k < n$, assurdo, c.v.d.

COROLLARIO

Si ha:

- $n < m \iff |n| < |m|$;
- $n = m \iff |n| = |m|$.

Dim.

Se $n < m$, allora ogni funzione $f : m \to n$ non può essere iniettiva, da cui $|n| < |m|$.

Allo stesso modo, se $n > m$, si ha $|n| > |m|$.

Se $n = m$, l'identità è una bigezione tra n e m, da cui $|n| = |m|$, c.v.d.

OSSERVAZIONE

Se A è finito, allora:

$\exists !\ n \in \omega \ni' |A| = |n|$

Scriveremo dunque $|n| = n$, e $|A| = n$. In questo caso i numeri naturali sono visti come CARDINALI FINITI.

PROPOSIZIONE

Se A è finito e $f : A \to A$, sono proprietà equivalenti:

- f è iniettiva;
- f è suriettiva;
- f è biunivoca.

Dim.

L'unica proposizione non banale da dimostrare è che la 1) e la 2) sono equivalenti.

Sia f non iniettiva. Allora:

$\exists\ n_1, n_2 \in A \ni' f(n_1) = f(n_2) \Rightarrow |f(A)| < |A| \Rightarrow$

$\Rightarrow |f(A)| \neq |A|$ ossia f non è suriettiva.

Sia f non suriettiva. Allora $|f(A)| < |A|$, da cui non può essere $f : A \to f(A)$ iniettiva, c.v.d.

APPLICAZIONI DEL TEOREMA DI RICORSIONE NUMERABILE

Vediamo ora un paio di applicazioni del teorema di ricorsione numerabile, che ci aiuteranno a sistematizzare quanto visto finora.

PROPOSIZIONE

Sia X un insieme finito, e sia $Y \subseteq X$. Allora $|Y| \leq |X|$.

Dim.

Assumiamo che Y sia non vuoto, e che sia:

$$X = \{x_0, \dots, x_{n-1}\},$$

ove:

$\forall\, i \neq j : \quad x_i \neq x_j$

Usiamo ora il teorema di ricorsione numerabile. Sia:

- k_0 è elemento di indice minimo $x_{k_0} \in Y$;
- k_{i+1} è elemento di indice minimo tra gli indici maggiori dell'indice di k_i, tale che $x_{k_{i+1}} \in Y$, se questo esiste.

Si ha dunque l'esistenza e unicità della sequenza $\langle k_0, \dots, k_{m-1} \rangle$.

Allora:

$$Y = \{k_0, \dots, k_{m-1}\},$$

da cui Y è finito. In più, ragionando per induzione su i, si ha $|Y| \leq |X|$. Infatti consideriamo:

$$P(i) = (k_i = x_j \Rightarrow i \leq j)$$

CASO BASE

$i = 0$

Qualunque sia $x_k = k_0$, si ha $0 \leq k$.

PASSO INDUTTIVO

Supponiamo che sia $k_{i+1} = x_j$. Allora, per ipotesi induttiva, $k_i = x_h$, con $i \leq h$. Per definizione $j > h$, da cui $j \geq h+1$.

$$i \leq h \Rightarrow i+1 \leq h+1 \leq j.$$

Da qui si ha che, se $k_{m-1} = x_j$, allora $m-1 \leq j \leq n-1$, ossia $|Y| \leq |X|$. L'uguaglianza, in effetti, non si ha se e solo se $Y \subsetneq X$, c.v.d.

PROPOSIZIONE

Sia X un insieme finito, e sia $f: X \to Y$ una funzione, con Y insieme qualunque. Allora $|f(X)| \leq |X|$, da cui $f(X)$ è finito.

Dim.

Usiamo il Teorema di ricorsione, definendo:

- $k_0 = 0$;
- k_{i+1} il minimo $k > k_i$, $k < n$ tale che:
  $\forall\, j \leq i : f(x_k) \neq f(x_{k_j})$,
  se esiste.

Ancora una volta, con considerazioni simili a quelle viste nella dimostrazione precedente si ha $f(X) = \{y_0, \dots, y_{m-1}\}$, con $m \leq n$, e $m = n$ se e solo se f è iniettiva, o suriettiva, c.v.d.

PROPOSIZIONE

Se A è finito e $B \subsetneq A$ è una sua parte propria, allora $|B| < |A|$.

Dim.

Immediata conseguenza della prima proposizione dimostrata, c.v.d.

OSSERVAZIONE

Il fatto che $B \subsetneq A$, A finito $\Rightarrow |B| < |A|$ sarà ancora più chiaro dopo aver visto che $|A \cup B| = |A| + |B|$, con $A \cap B = \emptyset$. Si avrà, in particolare, $|A| = |B| + |A \setminus B|$, con $A \setminus B \neq \emptyset \Rightarrow$
$\Rightarrow |A \setminus B| > 0$ se $B \subsetneq A$ è un sottoinsieme proprio.

PROPOSIZIONE

ω è infinito.

Dim.

Abbiamo dimostrato che un insieme finito non può essere in bigezione con una sua parte propria, e la funzione successore è una bigezione tra ω e $\omega \setminus \{0\} \subsetneq \omega$, c.v.d.

ANCORA SUGLI INSIEMI FINITI

PROPOSIZIONE

Siano A, B insiemi finiti. Allora $A \cup B$ è finito, e in più si ha $|A \cup B| \leq |A| + |B|$, e se $A \cap B = \emptyset$ allora $|X \cup Y| = |A| + |B|$.

Dim.

Siano:

$$A = \{a_0, a_1, \dots a_{m-1}\},$$
$$B = \{b_0, b_1, \dots b_{n-1}\},$$

ove $\langle a_0, \dots, a_{m-1} \rangle$ e $\langle b_0, \dots, b_{n-1} \rangle$ sono sequenze iniettive.
Consideriamo la sequenza seguente:

$$s = \langle c_0, \dots c_{m-1}, c_m, \dots c_{m+n-1} \rangle,$$

ove:

$$c_i \overset{def}{=} \begin{cases} a_i, & i \in \{0, \dots m-1\} \\ b_{i-m} & i \in \{m, m+n-1\} \end{cases}$$

s mappa $m+n$ su $A \cup B$ suriettivamente, da cui $A \cup B$ è finito, e $|A \cup B| \leq |A| + |B|$. Se $A \cap B = \emptyset$, allora s è iniettiva, da cui $|A \cup B| = |A| + |B|$, c.v.d.

COROLLARIO

Sia $\mathcal{F}$ una famiglia finita di insiemi finiti. Allora $\bigcup \mathcal{F}$, ossia $\bigcup_{F \in \mathcal{F}} F$, è finito, e in più $\left| \bigcup_{F \in \mathcal{F}} F \right| \leq \sum_{F \in \mathcal{F}} |F|$, e l'uguaglianza si ha se gli insiemi, ad esempio, sono a due a due disgiunti.

Dim.

Ragioniamo per induzione sulla cardinalità di $\mathcal{F}$.

CASO BASE

Se $|\mathcal{F}| = 0$, la proposizione è vera a vuoto.

PASSO INDUTTIVO

Sia $|\mathcal{F}| = n+1$, ossia $\mathcal{F} = \{X_0, \dots, X_n\}$. Allora per ipotesi induttiva, $\bigcup_{g=0}^{n-1} X_g$ è finito e $\left| \bigcup_{g=0}^{n-1} X_g \right| \leq \sum_{g=0}^{n-1} X_g$, e l'uguaglianza sussiste se $X_0, \dots, X_{n-1}$ sono a due a due disgiunti.

Allora:

$$\bigcup_{g=0}^{n} X_g = \left(\bigcup_{g=0}^{n-1} X_g\right) \cup X_n$$

è finito, e in più:

$$\left|\bigcup_{g=0}^{n} X_g\right| \leq \left|\bigcup_{g=0}^{n-1} X_g\right| + |X_n| \leq \sum_{g=0}^{n} |X_g|,$$

e l'uguaglianza si ha se $\bigcup_{g=0}^{n-1} X_g \cap X_n = \emptyset$, ossia $X_0, \ldots X_n$ sono a due a due disgiunti, c.v.d.

PROPOSIZIONE

Se A, B sono finiti, allora $A \cap B$ è finito.

Dim.

È semplice conseguenza di quanto visto finora, dato che:

$$A \cap B \subseteq A \quad , \quad A \cap B \subseteq B$$

Inoltre si ha $|A \cap B| \leq \min\{|A|, |B|\}$, c.v.d.

PROPOSIZIONE

Se A, B sono finiti, allora $A \times B$ è finito, e $|A \times B| = |A||B|$.

Dim.

Siano:

$$A = \{a_0, \ldots, a_{m-1}\}$$
$$B = \{b_0, \ldots, b_{n-1}\}$$

ove $\langle a_0, \ldots, a_{m-1} \rangle$ e $\langle b_0, \ldots, b_{n-1} \rangle$ sono sequenze iniettive.

Consideriamo la sequenza seguente:

$$z = \langle x_0, \ldots, x_j, \ldots, x_{(m+1)(n+1)-1} \rangle,$$

ove (la notazione verrà spiegata alla fine della dimostrazione):

$$x_j \stackrel{def}{=} (a_{j/n}, b_{j\%n})$$

Allora si ha che mn si mappa bigettivamente mediante z su $A \times B$ (l'iniettività deriva dalla definizione di coppia ordinata e dall'esistenza e unicità della divisione euclidea), da cui $|A \times B| = mn$ ($A \times B$ è dunque finito), c.v.d.

OSSERVAZIONE

Se $a = qb + r$, con $b > 0$ e $0 \leq r < b$, si ha:

- $a / b = q$;
- $a \% b = r$.

OSSERVAZIONE

Equivalentemente, $B \times A$ è finito, e $|B \times A| = nm$. La seguente è una bigezione:

$$i : A \times B \to B \times A$$
$$(a, b) \to (b, a),$$

da cui $|A \times B| = |B \times A|$, ossia $mn = nm$.

PROPOSIZIONE

Sia A un insieme finito. Allora $\mathcal{P}(A)$ è finito.

Dim.

Ragioniamo per induzione su $n = |A|$.

CASO BASE

Se $n = 0$, allora $A = \emptyset$, e $\mathcal{P}(A) = \{\emptyset\}$ è finito.

PASSO INDUTTIVO

Sia $n+1 = |A|$. Si ha:

$$A = \{x_0, \ldots, x_n\},$$

ove $\langle x_0, \ldots x_n \rangle$ è una sequenza finita iniettiva.

Si ha:

$$\mathcal{P}(A) = \{B \subseteq A \mid x_n \in B\} \cup \{B \subseteq A \mid x_n \notin B\} \overset{def}{=} C_1 \cup C_0$$

Si ha una bigezione naturale:

$$\mathcal{X} : C_1 \to C_0$$
$$B \to B \setminus \{x_n\}$$

$$\mathcal{X}^{-1} : C_0 \to C_1$$
$$B' \to B' \cup \{x_n\}$$

In più si ha un'altra bigezione naturale $\Phi : C_0 \to \mathcal{P}(A \setminus \{x_n\})$. Dato che $|A \setminus \{x_n\}| = n$, per ipotesi induttiva $|\mathcal{P}(A \setminus \{x_n\})| = |C_0| = |C_1| = k \in \omega$, da cui $\mathcal{P}(A)$ è finito, c.v.d.

OSSERVAZIONE

Con una facile aggiunta alla dimostrazione appena vista, si può dimostrare che:

$$|A| = k \Rightarrow |\mathcal{P}(A)| = 2^k$$

PROPOSIZIONE

Se A, B sono insiemi finiti, allora $Fun(B, A) = A^B$ è finito.

Dim

Poniamo innanzitutto $A \neq \emptyset$, $B \neq \emptyset$, in modo che sia ben definito $Fun(B, A)$: i casi in cui $Fun(B, A) = \emptyset$ non sono interessanti.

Ricalchiamo la dimostrazione appena vista. Procediamo per induzione doppia su $m = |B|$ e su $n = |A|$.

CASO BASE

Sia $m = 1$. Allora:

$\forall n \in \omega : (A = n \Rightarrow Fun(B, A) = n)$

Infatti, se $A = \{x_0, \dots, x_{n-1}\}$, allora

$$Fun(B, A) = \{\varphi_{x_i} \mid x_i \in A\},$$

ove:

$$\varphi_{x_i} : B \longrightarrow A$$
$$b_0 \longrightarrow x_i$$

PASSO INDUTTIVO

Supponiamo che:

$\forall k \leq m : (|B| = k \Rightarrow (\forall n \in \omega : |A| = n \Rightarrow |A^B| = n^k))$

Sia $B = m+1$. Allora:

$$B = \{x_0, \dots x_m\} = \{x_0, \dots x_{m-1}\} \cup \{x_m\},$$

con $B' \overset{def}{=} \{x_0, \dots, x_{m-1}\}$ tale che $|B'| = m$. Per cominciare il passo induttivo doppio, notiamo che se $|A| = 1$ allora $|Fun(B, A)| = 1$ (l'unica funzione, se $A = \{y_0\}$, manda tutto in y_0), e supponiamo che:

$\forall h \leq n : (|A| = n \Rightarrow |Fun(B, A)| = n^k)$

Sia $|A| = n+1$. Allora, prima di usare l'ipotesi induttiva, definiamo (se $A = \{y_0, \dots y_n\}$):

$\forall\ j = 0, \ldots, m : D_j \overset{def}{=} \{ f \in Fun(B, A) \mid f(x_m) = y_j \}$

Si ha allora:

$$Fun(B, A) = \bigcup_{j=0}^{m} D_j$$

Dovrebbe ora essere chiaro che esistono delle bigezioni canoniche:

$$\phi_{ij} : D_i \longrightarrow D_j,$$

e delle bigezioni canoniche:

$$\psi_i : D_i \longrightarrow Fun(B', A)$$

Per ipotesi induttiva $|Fun(B', A)| = (m+1)^n$. Allora:

$$Fun(B, A) = \bigcup_{j=0}^{m} D_j \Rightarrow$$

$$\Rightarrow |Fun(B, A)| = (m+1) \cdot |Fun(B', A)| =$$
$$= (m+1) \cdot (m+1)^n = (m+1)^{n+1}, \text{ c.v.d.}$$

OSSERVAZIONE

Abbiamo volutamente usato le usuali operazioni aritmetiche tra cardinali finiti, senza in effetti definirle. Ciò sarà fatto in seguito: per ora abbiamo mostrato alcuni risultati relativi alla cardinalità dei vari insiemi considerati.

Per ora notiamo solamente che la somma può essere definita come la cardinalità dell'unione di insiemi disgiunti:

$$n + m \overset{def}{=} |A \cup B|, \ |A| = n, \ |B| = m, \ A \cap B = \emptyset,$$

e il prodotto come la cardinalità del prodotto cartesiano:

$$n \cdot m \overset{def}{=} |A \times B|, \ |A| = n, \ |B| = m$$

Se la commutatività della somma è del tutto ovvia, la commutatività del prodotto non è così banale: l'applicazione bigettiva $i : A \times B \longrightarrow B \times A$, in ogni caso, la dimostra.

ESERCIZI VARI E COMPLEMENTI

Sia V uno spazio vettoriale reale o complesso di dimensione finita. Innanzitutto:

$$|\mathbb{C}| = |\mathbb{R}|,$$

in quanto:

$$\phi : \mathbb{C} \longrightarrow \mathbb{R} \times \mathbb{R}$$
$$a+ib \quad (a,b)$$

è bigettiva, e $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$.

Inoltre

$\exists\ k \in \mathbb{N}$ t.c. $V \cong \mathbb{R}^k \Rightarrow |V| = |\mathbb{R}^k| = |\mathbb{R} \times \ldots \times \mathbb{R}| = |\mathbb{R}| = c$.

Sia ora V uno spazio vettoriale di dimensione infinita, tale che ogni base di V abbia cardinalità numerabile. Sia $\mathcal{B}$ una base di V. Allora:

$\forall\ v \in V \ \exists!\ (\alpha_i)_{i=1}^{m} \subseteq \mathbb{K}$ t.c. $v = \sum_{i=1}^{+\infty} \alpha_i b_{k_i}$

Sia $B \subseteq \mathcal{B}$ un sottoinsieme finito, definiamo:

$$V_B = \mathrm{Span}(B) = \left\{ \sum_{i=1}^{m} \lambda_i b_{k_i} \;\middle|\; \lambda_i \in \mathbb{K},\ b_{k_i} \in B,\ |B| = m \right\}$$

Allora, al variare di $B \subseteq \mathcal{B}$, vale:

$$V = \bigcup_{B \subseteq \mathcal{B}} V_B$$

Si ha $|V_B| = c \ \forall\ B \subseteq \mathcal{B}$, visto che $V_B \cong \mathbb{R}^{|B|}$. Si ha ora:

$$|\mathcal{B}|^{<\aleph_0} = |\mathbb{N}|^{<\aleph_0} = \bigcup_{k \in \mathbb{N}} |\mathbb{N}|^k = |\mathbb{N}| = \aleph_0,$$

da cui un'unione numerabile di insiemi di cardinalità continua ha cardinalità continua. Allora:

$$|V| \leq c,$$

e chiaramente:

$$|\mathrm{Span}(v)| = c \Rightarrow c \leq |V|,$$

e per Cantor-Bernstein:

$$|V| = c.$$

Notiamo che un'unione continua di insiemi a cardinalità continua ha cardinalità continua. Dunque se V è uno spazio vettoriale tale che una qualsiasi sua base ablia cardinalità convenuta, esso ha cardinalità continua.

Per completezza dimostriamo un lemma che però è stato già visto e dimostrato in precedenza.

LEMMA

Un unione $A = \bigcup_{i \in I} A_i$, ove $|I| \leq c$ e $|A_i| \leq c$ $\forall i \in I$ ha cardinalità al più continua.

Dim

Per ipotesi:

$\exists \; \varphi : \mathbb{R} \to I$ suriettiva;

$\forall i \in I \; \exists \; \psi_i : \mathbb{R} \to A_i$ suriettiva

Definiamo:

$$\Sigma : \mathbb{R} \times \mathbb{R} \longrightarrow \bigcup_{i \in I} A_i$$
$$(r, s) \to \psi_{\varphi(r)}(s) \in A_{\varphi(r)}$$

Questa funzione è suriettiva per costruzione. Allora:

$$\left| \bigcup_{i \in I} A_i \right| \leq |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|,$$

e sottolineiamo che comunque è indispensabile l'assunzione dell'assioma della scelta, c.v.d

Siano ora V, W due spazi vettoriali di dimensione infinita, aventi basi numerabili. Qual è la cardinalità di
$$\mathrm{Hom}(V, W) \;?$$

PREMESSA

Se V, W avessero dimensione finita allora si avrebbe:

$$\mathrm{Hom}(V, W) \cong M(n, m, \mathbb{R}) \cong$$
$$\cong \mathbb{R}^{m \times n} \Rightarrow$$
$$\Rightarrow |\mathrm{Hom}(V, W)| = |\mathbb{R}| = c$$

Sia $\mathcal{B}$ una base di V. Allora $\varphi : V \to W$ lineare è univocamente determinata dai valori che assume sulla base $\mathcal{B}$.

Allora:

$$|Hom(V,W)| = |Hom(\mathcal{B},W)| = |Fun(\mathcal{B},W)| =$$
$$= |W^{\mathcal{B}}| = |\mathbb{R}^{\mathbb{N}}| = c \Rightarrow |Hom(V,W)| = c$$

Più velocemente, possiamo notare che $L(V,W)$ è uno spazio vettoriale a base numerabile, dunque avente cardinalità continua. Se $\mathcal{B}=(v_i)_{i\in\mathbb{N}}$ e $\mathcal{B}'=(w_j)_{j\in\mathbb{N}}$ sono basi numerabili di V e W rispettivamente, allora $\mathcal{G} = \{ f_{ij} : \mathcal{B} \to \mathcal{B}' \mid f_i(v_i) = w_j,\ f_i(v_k)=0 \}$ è una base di $L(V,W)$.

Sia ora:

$$T = \{ X \subseteq \mathcal{P}(\mathbb{R}) \mid |X| = \aleph_0,\ \forall x \in X : |x| = n \in \mathbb{N} \}$$

Dim

Sia $X \in T$. Allora X è una famiglia di sottoinsiemi di $\mathbb{R}$. Precisamente X è una famiglia numerabile di insiemi finiti. Elenchiamo un po' di fatti noti:

- $|[\mathbb{N}]^{\aleph_0}| = |[\mathbb{R}]^{\aleph_0}| = c$;
- $|[\mathbb{R}]^{c}| = 2^c$;
- $|[\mathbb{N}]^{<\aleph_0}| = \aleph_0$;
- $|[\mathbb{R}]^{<\aleph_0}| = c$.

Ricordiamo anche che:

$$|Fin(\mathbb{R})| = \left|\bigcup_{n\in\mathbb{N}} \mathbb{R}^n\right| = c$$

$$|Fun(\mathbb{N},\mathbb{R})| = c$$

Dunque:

$$T = [Fin(\mathbb{R})]^{\aleph_0},$$

e dato che $|Fin(\mathbb{R})| = |\mathbb{R}|$, $|T| = [\mathbb{R}]^{\aleph_0} = c$.

Vogliamo ora studiare la cardinalità di:

$$B = \{ \text{partizioni di } \mathbb{N} \}$$

Sappiamo bene che le partizioni di un insieme sono date da relazioni di equivalenza. Si ha dunque

$$|B| = |\{\text{relazioni di equivalenza su } \mathbb{N}\}| \leq$$
$$\leq \{\text{relazioni su } \mathbb{N}\} \leq |\mathcal{P}(\mathbb{N}\times\mathbb{N})| = |\mathcal{P}(\mathbb{N})| = |\mathbb{R}| = c$$

Consideriamo ora la funzione:

$$\vartheta : \mathcal{P}(\mathbb{N}) \longrightarrow B$$
$$A \longmapsto \{A, A^c\}$$

Questa funzione, dato $A \in \mathcal{P}(\mathbb{N})$, genera la partizione di $\mathbb{N}$ data da A e A^c. Essa è palesemente non iniettiva:

$$\vartheta(A) = \vartheta(A^c),$$

ma si ha che:

$$\forall\; X \in \vartheta(\mathcal{P}(\mathbb{N})) : |\vartheta^{-1}(X)| = 2,$$

da cui la funzione che va da $\mathcal{P}(\mathbb{N})/\sim$ (ove $A \sim B \Leftrightarrow A = B \vee A = B^c$) in B è iniettiva (e ben definita):

$$\vartheta : \mathcal{P}(\mathbb{N})/\sim \longrightarrow B$$
$$[A] \longmapsto \{A, A^c\}$$

Si ha banalmente:

$$|\mathcal{P}(\mathbb{N})| = |\mathcal{P}(\mathbb{N})/\sim| = c,$$

da cui $c \leq |B|$, e per il Teorema di Cantor-Bernstein:

$$|B| = c$$

Alternativamente, la funzione:

$$\sigma : \mathcal{P}(\mathbb{N}) \longrightarrow B$$
$$A \longmapsto \{(2A), (2A)^c\},$$

ove:

$$2A \overset{\text{def}}{=} \{2 \cdot n \mid n \in A\},$$

è iniettiva, da cui, ancora, si ha $c \leq |B|$

Consideriamo ora le partizioni numerabili di $\mathbb{R}$:

$$A = \{\text{partizioni numerabili di } \mathbb{R}\}$$

Si ha:

$$A \subseteq [\mathcal{P}(\mathbb{R})]^{\aleph_0} \Rightarrow |A| \leq |[\mathcal{P}(\mathbb{R})]^{\aleph_0}| \leq |[\mathcal{P}(\mathbb{R})]^{\mathbb{N}}| =$$
$$= |[2^{\mathbb{R}}]^{\mathbb{N}}| = |2^{\mathbb{R}\times\mathbb{N}}| = |2^{\mathbb{R}}| = 2^c$$

In particolare, per $Q \in [\mathcal{P}(\mathbb{R})]^{\aleph_0}$ associo $\sigma_Q : \mathbb{N} \to Q \subseteq \mathcal{P}(\mathbb{R})$. Si ha che σ_Q è una bigezione per ogni $Q \in [\mathcal{P}(\mathbb{R})]^{\aleph_0}$. In più la seguente funzione è iniettiva:

$$\tau : [\mathcal{P}(\mathbb{R})]^{\aleph_0} \longrightarrow \mathcal{P}(\mathbb{R})^{\mathbb{N}}$$
$$Q \longmapsto \sigma_Q,$$

Siano infatti $\sigma_{\mathcal{A}} = \sigma_{\mathcal{B}}$, con $\mathcal{A}, \mathcal{B} \in \mathcal{P}(\mathbb{R})^{\aleph_0}$.

Allora:

$$\sigma_{\mathcal{A}}(\mathbb{N}) = \sigma_{\mathcal{B}}(\mathbb{N}), \quad \sigma_{\mathcal{A}}(\mathbb{N}) \overset{def}{=} \mathcal{A}, \quad \sigma_{\mathcal{B}}(\mathbb{N}) \overset{def}{=} \mathcal{B} \Rightarrow \mathcal{A} = \mathcal{B}$$

Dimostriamo ora l'altra disuguaglianza:

$$2^c \le |[\mathcal{P}(\mathbb{R})]^{\aleph_0}|$$

Innanzitutto:

$$2^c = |\mathcal{P}(\mathbb{R})| = |\mathcal{P}(]0,1[)|$$

Definiamo:

$$\Theta : \mathcal{P}(]0,1[) \to A$$
$$B \subseteq]0,1[\mapsto \{B,]-1,0],]-2,-1], \dots, \mathbb{R}^+ \setminus B\}$$

Θ è iniettiva. Allora:

$$2^c = |\mathcal{P}(]0,1[)| \le |A| \le |[\mathcal{P}(\mathbb{R})]^{\aleph_0}| \le |\mathcal{P}(\mathbb{R})^{\mathbb{N}}| = 2^c,$$

e per il teorema di Cantor Bernstein:

$$|A| = 2^c$$

Definiamo ora la seguente relazione di equivalenza su $\mathcal{P}(\mathbb{R})$:

$$\forall A, B \in \mathcal{P}(\mathbb{R}) : A \sim B \Leftrightarrow |A \triangle B| \overset{def}{=} |(A \setminus B) \cup (B \setminus A)| = n \in \mathbb{N}$$

La seguente è una relazione di equivalenza: l'unica proprietà non banale è l'ultima. Si ha:

$\forall A, B, C \in \mathcal{P}(\mathbb{R}) : \quad A \triangle C \subseteq (A \triangle B) \cup (B \triangle C)$,

da cui l'asserto.

Qual è la cardinalità di $\mathcal{P}(\mathbb{R})/\sim$?

Studiamo la cardinalità, dato $A \in \mathcal{P}(\mathbb{R})$, di $[A] \overset{def}{=} \{B \in \mathcal{P}(\mathbb{R}) \mid B \sim A\}$.

Si ha che la seguente è una bigezione:

$$\varphi : Fin(A) \times Fin(A^c) \to [A]$$
$$(F, G) \mapsto B \overset{def}{=} (A \setminus F) \cup G \in [A]$$

Dunque, dato che $A \cup A^c = \mathbb{R}$, da cui uno tra A e A^c (anche entrambi) ha cardinalità c, ed entrambi non hanno cardinalità superiore a c, si ha:

$$|[A]| = |Fin(A) \times Fin(A^c)| = c$$

Ora, sicuramente $c < \left|{}^{\mathcal{P}(\mathbb{R})}/_{\sim}\right|$. Se infatti fosse $c \geq \left|{}^{\mathcal{P}(\mathbb{R})}/_{\sim}\right|$, si avrebbe:

$$|\mathcal{P}(\mathbb{R})| = \left| \bigcup_{[A] \in \mathcal{P}(\mathbb{R})/_{\sim}} [A] \right| = c,$$

assurdo.

In effetti, dato che:

$$|\mathcal{P}(\mathbb{R})| = |\mathcal{P}(]0,1[)| = 2^{c},$$

e che:

$$\Psi : \mathcal{P}(]0,1[) \to {}^{\mathcal{P}(\mathbb{R})}/_{\sim}$$

$$A \subseteq]0,1[\mapsto [A + \mathbb{N}] \overset{def}{=}$$

$$\overset{def}{=} [\{a + n \mid a \in A,\ n \in \mathbb{N}\}]$$

è iniettiva (lo dimostreremo tra poco), si ha:

$$2^{c} \leq \left|{}^{\mathcal{P}(\mathbb{R})}/_{\sim}\right| \leq 2^{c}$$

(la disuguaglianza $\left|{}^{\mathcal{P}(\mathbb{R})}/_{\sim}\right| \leq |\mathcal{P}(\mathbb{R})| = 2^{c}$ è banale), e per il teorema di Cantor - Bernstein:

$$\left|{}^{\mathcal{P}(\mathbb{R})}/_{\sim}\right| = 2^{c}$$

Resta da dimostrare che Ψ è iniettiva. Siano $A, A' \in \mathcal{P}(]0,1[)$, con A A'. Senza perdere di generalità:

$\exists\, x \in A \setminus A' \Rightarrow (x + \mathbb{N}) \subseteq (A + \mathbb{N}),\ (x + \mathbb{N}) \cap (A' + \mathbb{N}) = \emptyset \Rightarrow$

$\Rightarrow (x + \mathbb{N}) \subseteq (A + \mathbb{N}) \,\Delta\, (A' + \mathbb{N}),\ |(x + \mathbb{N})| = |\mathbb{N}| = \aleph_0,$

da cui, dato che $(x + \mathbb{N})$ è infinito:

$$\Psi(A) \neq \Psi(A').$$

ARITMETICA DEI NUMERI NATURALI

Dati A, B insiemi finiti, sappiamo che è ben definita la loro cardinalità:

$$|A| = n, \quad |B| = m$$

Si definisce allora la SOMMA tra cardinali finiti:

$$n+m \overset{def}{=} |A \cup B|, \quad |A| = n, \quad |B| = m, \quad A \cap B = \emptyset$$

Si definisce poi il PRODOTTO tra cardinali finiti:

$$n \cdot m \overset{def}{=} |A \times B|, \quad |A| = n, \quad |B| = m$$

Le definizioni sono ben poste, in quanto insiemi aventi stessa cardinalità sono equipotenti.

Prima di continuare, parliamo dell'ARITMETICA DI PEANO.
Un MODELLO DI P.A. consiste di un insieme N, contenente un elemento "zero" $0 \in N$, tale che:

- esiste la funzione SUCCESSORE $S: N \to N$
- vi è una SOMMA $+: N \times N \to N$
- vi è un PRODOTTO $\cdot : N \times N \to N$,

ove vengono soddisfatte le seguenti proprietà:

- (PA 1) Tutti e soli gli elementi di $N \setminus \{0\}$ sono successori:
  $$\forall x : (x \neq 0 \Rightarrow \exists y : S(y) = x)$$
- (PA 2) Numeri diversi hanno successori diversi:
  $$\forall x, \forall y : (x \neq y \Rightarrow S(x) \neq S(y))$$
- (PA 3) Si ha:
  - $\forall x : x + 0 = x$;
  - $\forall x, \forall y : x + S(y) = S(x+y)$;
- (PA 4) Si ha:
  - $\forall x : x \cdot 0 = 0$;
  - $\forall x, \forall y : x \cdot S(y) = x \cdot y + x$;

- (PA 5) Si considera la formulazione dell' INDUZIONE AL SECONDO ORDINE: se $A \subseteq \mathbb{N}$ è tale che $0 \in A$, e:
$$\forall x \ (x \in A \Rightarrow S(x) \in A),$$
allora $A = \mathbb{N}$.

OSSERVAZIONE
Per quanto riguarda il quinto assioma di Peano, vi è una formulazione di INDUZIONE AL PRIMO ORDINE: se $P(x)$ è una formula tale che:
$$P(0) \wedge (\forall x : P(x) \Rightarrow P(S(x))),$$
allora
$\forall x \in \mathbb{N} : P(x)$

Le due formulazioni sono non equivalenti. Infatti:
- $|\{\text{formule di PA}\}| = \aleph_0$;
- $|\{\text{sottoinsiemi di } \mathbb{N}\}| = c$.

OSSERVAZIONE
Considerando l'induzione al primo ordine si possono generare modelli dell' aritmetica di Peano non isomorfi tra di loro; se invece consideriamo l'induzione al secondo ordine, allora due qualsiasi modelli dell' aritmetica di Peano sono tra loro isomorfi.

Sono teoremi dell' aritmetica di Peano:
- la proprietà associativa:
$$\forall x, \forall y, \forall z : \quad x + (y + z) = (x + y) + z$$
$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \ ;$$
- la proprietà commutativa:
$$\forall x, \forall y : \quad x + y = y + x$$
$$xy = yx \ ;$$
- la proprietà distributiva.

È utile però dimostrare prima un lemma.

LEMMA

Si ha:

$$\forall\, x \in \mathbb{N}: 0 + x = x \;,\quad 0 \cdot x = 0$$

Dim.

Per induzione su x, usando (PA 3) e (PA 4). Il caso base è vero banalmente. Quanto al passo induttivo:

- $0 + S(x) = S(0 + x) = S(x)$;
- $0 \cdot S(x) = 0 \cdot x + 0 = 0 + 0 = 0$, c.v.d.

Dimostriamo ora, con un'induzione doppia, la commutatività delle operazioni. Il caso base è fornito dal lemma, e lo Teleoremma. Quanto al passo induttivo:

- $S(x) + S(y) = S(S(x) + y) = S(y + S(x)) = S(S(y + x)) =$
  $= S(S(x + y)) = S(x + S(y)) = S(S(y) + x) = S(y) + S(x)$;
- $S(x) \cdot S(y) = S(x) \cdot y + S(x) = y \cdot S(x) + S(x) =$
  $= (y \cdot x + y) + S(x) = S(y \cdot x + y + x) = S(x \cdot y + x + y) =$
  $= (x \cdot y + x) + S(y) = x \cdot S(y) + S(y) = S(y) \cdot x + S(y) =$
  $= S(y) \cdot S(x)$.

Le proprietà associativa e distributiva si dimostrano in maniera simile, magari facendo attenzione ai casi base. Vediamo ad esempio la proprietà distributiva. Avendo dimostrato che le operazioni sono commutative, è sufficiente dimostrare che:

$$\forall x, \forall y, \forall z: x(y + z) = x \cdot y + x \cdot z$$

Il caso base è banale:

$$0 \cdot (0 + 0) = 0 \cdot 0 = 0 = 0 + 0 = 0 \cdot 0 + 0 \cdot 0$$

Si ha ora:

$$S(x)\left[S(y) + S(z)\right] = S(x)\left[S(S(y) + z)\right] = S(x)\left[S(z + S(y))\right] =$$
$$= S(x)\left[S(S(z + y))\right] = S(x)\, S(z + y) + S(x) =$$
$$= S(x)(z + y) + S(x) + S(x) = (z + y)x + (z + y) + S(x) + S(x) =$$
$$= zx + yx + z + y + S(x) + S(x) = zx + z + yx + y + S(x) + S(x) =$$
$$= z\, S(x) + y\, S(x) + S(x) + S(x) = S(x)\, z + S(x) + S(x)\, y + S(x) =$$
$$= S(x)\, S(z) + S(x)\, S(y) = S(x)\, S(y) + S(x)\, S(z).$$

ORDINE TOTALE DEI NATURALI

Definiamo la seguente relazione:

$$x < y \overset{def}{\Leftrightarrow} \exists\, z \neq 0 \ \ni' \ x + z = y$$

Allora $<$ è un ordine totale.

Dobbiamo provare che:

- $\forall x : x \not< x$;
- $\forall x, y : (x < y \Rightarrow y \not< x)$;
- $\forall x, y, z : (x < y,\ y < z \Rightarrow x < y)$;
- $\forall x, y : (x \neq y \Rightarrow x < y \ \vee \ y < x)$.

Dunque:

- Si ha $x + 0 = x$, da cui, se esistesse $z \neq 0$ tale che $x + z = x$, sarebbe $z = 0$, assurdo;
- Se per assurdo valesse $y < x$, si avrebbe per la proprietà transitiva (che per ora accettiamo) $x < y,\ y < x \Rightarrow x < x$, assurdo, da cui $(x < y \Rightarrow y \not< x)$;
- Siano $x < y$, $y < z$. Allora:
  $\exists\, a \neq 0, b \neq 0 \ \ni' \ x + a = y,\ y + b = z$
  Allora:
  $\exists\, a + b \neq 0 \ \ni' \ x + a + b = (x + a) + b = y + b = z$,
  da cui $x < z$;
- Notiamo innanzitutto che:
  - $x < y \Leftrightarrow \exists\, z \neq 0 \ \ni' \ x + z = y \Leftrightarrow \exists\, z \neq 0 \ \ni' \ S(x + z) = S(x) + z = S(y) \Leftrightarrow$
    $\Leftrightarrow S(x) < S(y)$,
  - $S : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ è iniettiva, da cui $x = y \Leftrightarrow S(x) = S(y)$.

Ragioniamo con induzione doppia: il caso base è vero e vuoto perché $0 = 0$. Quanto al passo induttivo, se $S(x) \neq S(y)$, ossia $x \neq y$, allora o $x < y$ (e in tal caso $S(x) < S(y)$) o $x > y$ (e in tal caso $S(x) > S(y)$).

L'ordine $<$ è dunque un ordine totale.

UNICITÀ DEI NATURALI

PROPOSIZIONE

Tutti i modelli dell'aritmetica di Peano, ove la formulazione del quinto assioma è al second'ordine, sono tra loro isomorfi. In altre parole, se:

$$\mathcal{M} = (N, 0, S, +, \cdot) \quad , \quad \mathcal{M}' = (N', 0', S', \oplus, \odot)$$

sono due modelli, allora:

$\exists\ \Theta : N \to N'$ biunivoca,

tale che:

- $\Theta(0) = 0'$;
- $\Theta(S(y)) = S'(\Theta(y))$;
- $\Theta(x+y) = \Theta(x) \oplus \Theta(y)$;
- $\Theta(x \cdot y) = \Theta(x) \odot \Theta(y)$.

Dim.

Enunciamo dapprima la seguente proposizione

PROPOSIZIONE (SOLO ENUNCIATO)

La struttura $\Sigma = (\omega, \emptyset, \hat{\ }, +, \cdot)$ è un modello di aritmetica di Peano, ove il quinto assioma è al second'ordine.

Dim.

Abbiamo già dimostrato che:

$$\hat{\ } : \omega \to \omega \setminus \{0\}$$
$$n \to n+1,$$

dunque le prime due proprietà sono dimostrate:

- $\forall n \in \omega : (n \neq \emptyset \Rightarrow \exists m \in \omega \text{ t.c. } m+1 = n)$;
- $\forall x, \forall y : (x \neq y \Rightarrow x+1 \neq y+1)$

Quanto alla terza proprietà:

- $n + 0 \overset{\text{def}}{=} |n \cup \emptyset| = |n| = n$;
- $n + (m+1) = (n+m)+1$. Siano:

$$|A| = n \quad , \quad |B| = m+1 \quad , \quad A \cap B = \emptyset$$

Sia $* \in B$ un qualsiasi elemento. Si ha:

$$m + (m+1) = |A \cup B| = |(A \cup (B \setminus \{*\})) \cup \{*\}|$$

Basta verificare che $|A \cup (B \setminus \{*\})| = n + m$.

Siano:

$$\varphi : A \to n \quad , \quad \psi : B \to m+1$$

due bigezioni. Senza perdere di generalità, sia:

$$\psi(*) = m$$

Definiamo:

$$\vartheta : C = A \cup (B \setminus \{*\}) \to n + m$$

$$\vartheta(x) = \begin{cases} \varphi(x) & , x \in A \\ n + \psi(x), & x \in B \setminus \{*\} \end{cases}$$

ϑ è banalmente una bigezione, da cui:

$$|A \cup (B \setminus \{*\})| = n + m$$

La proprietà del tipo della moltiplicazione è sostanzialmente analoga.

L'ultima proprietà, infine, è l'induzione su ω, c.v.d.

Senza perdita di generalità, sia $\mathcal{M} = (\omega, \emptyset, {}^{\wedge}, +, \cdot)$

definiamo per ricorsione numerabile:

$$\Theta : \omega \to N'$$

tale che:

- $\Theta(\emptyset) = 0'$;
- $\Theta(n+1) = S'(\Theta(n))$.

Dunque:

- $\Theta(0) = 0'$, direttamente dalla definizione;
- Θ è suriettiva. Ragioniamo per induzione in N':
  - $0' \in \mathrm{Im}(\Theta)$, infatti $\Theta(0) = 0'$;
  - se $x \in \mathrm{Im}(\Theta)$, ossia $x = \Theta(n)$ per qualche $n \in \omega$, allora $\Theta(n+1) = S'(\Theta(n)) = S'(x)$, da cui $S'(x) \in \mathrm{Im}\,\Theta$,

da cui Θ è suriettiva;

- Θ è iniettiva. Sia:

$$X_{in} \overset{def}{=} \{n \in \omega \mid \forall m \in \omega : \Theta(n) = \Theta(m) \Rightarrow n = m\}$$

è equivalente dimostrare che $X_{in} = \omega$. Ragioniamo per induzione su $n \in \omega$:

- $0 \in X$. Infatti, preso $m \in \omega$ tale che $\Theta(0) = \Theta(m)$, se $m \neq 0$, per (PA 1) esiste $n \in \omega$ t.c. $n+1 = m$, da cui: $\Theta(m) = \Theta(n+1) = S'(\Theta(n)) \neq 0' = \Theta(0)$, per (PA 1) in N', e si è giunti a un assurdo. Dunque $m = 0$, e $0 \in X$;
- Sia $n \in X$, e sia $m \in \omega$ tale che $\Theta(m) = \Theta(n+1) = S'(\Theta(n))$. Vogliamo dimostrare che vale $m = n+1$. Osserviamo che $\Theta(m) = S'(\Theta(n))$ è un successore, dunque è diverso da $0'$. Allora esiste $k \in \omega$ tale che $k+1 = m$. Dunque, usando le proprietà di S' e l'ipotesi induttiva, si ha:

$S'(\Theta(k)) = S'(\Theta(n)) \Rightarrow \Theta(k) = \Theta(n) \Rightarrow k = n \Rightarrow m = n+1$;

- Consideriamo:

$$X_+ \overset{def}{=} \{n \in \omega \mid \forall m \in \omega : \Theta(n+m) = \Theta(n) \oplus \Theta(m)\}$$

Ragioniamo per induzione su $n \in \omega$, per dimostrare che $X_+ = \omega$:

- $0 \in X_+ : \forall m \in \omega : \Theta(0+m) = \Theta(m) = 0' \oplus \Theta(m) =$
$= \Theta(0) \oplus \Theta(m)$;
- $n \in X_+ \Rightarrow \forall m \in \omega : \Theta((n+1)+m) = \Theta((n+m)+1) =$
$= S'(\Theta(n+m)) = S'(\Theta(n) \oplus \Theta(m)) = S'(\Theta(n)) \oplus \Theta(m) =$
$= \Theta(n+1) \oplus \Theta(m) \Rightarrow (n+1) \in X_+$;

- Consideriamo:

$$X_\cdot \overset{def}{=} \{n \in \omega \mid \forall m \in \omega : \Theta(n \cdot m) = \Theta(n) \odot \Theta(m)\}$$

Allora, per induzione su $n \in \omega$ si ha $X_\cdot = \omega$:

- $0 \in X_\cdot : \forall m \in \omega : \Theta(0 \cdot m) = \Theta(0) = 0' = 0' \odot \Theta(m) =$
$= \Theta(0) \odot \Theta(m)$;
- $n \in X_\cdot \Rightarrow \forall m \in \omega : \Theta((n+1) \cdot m) = \Theta(m \cdot n + m) =$
$= \Theta(m \cdot n) \oplus \Theta(m) = \Theta(m) \odot \Theta(n) \oplus \Theta(m) =$
$= \Theta(m) \odot S'(\Theta(n)) = S'(\Theta(n)) \odot \Theta(m) =$
$= \Theta(n+1) \odot \Theta(m) \Rightarrow (n+1) \in X_\cdot$, c.v.d.

ANELLO DEGLI INTERI

Definiamo:

$$\mathbb{Z} \stackrel{def}{=} \mathbb{N}\times\mathbb{N} / \sim,$$

ove:

$$(a,b)\sim(c,d) \stackrel{def}{\Leftrightarrow} a+d=b+c$$

Innanzitutto $\sim$ è una relazione di equivalenza:

- $(a,b)\sim(a,b)$, dato che $a+b=b+a$;
- $(a,b)\sim(c,d) \Leftrightarrow a+d=b+c \Leftrightarrow c+b=d+a \Leftrightarrow$
  $\Leftrightarrow (c,d)\sim(a,b)$;
- $(a,b)\sim(c,d),\ (c,d)\sim(e,f) \Leftrightarrow a+d=b+c,\ c+f=d+e \Rightarrow$
  $\Rightarrow a+d+c+f=b+c+d+e \Rightarrow a+f=b+e \Rightarrow (a+b)\sim(e,f)$.

Consideriamo le classi di equivalenza: c'è un unico elemento in ognuna, della forma $(0,0)$, oppure $(n,0)$, con $n>0$, oppure $(0,m)$, con $m>0$.

Allora identifichiamo:

- $[(n,0)]$ con $n\in\omega$;
- $[(0,n)]$ con $-n\in -\omega \stackrel{def}{=} \{-n \mid n\in\omega\setminus\{0\}\}$
- $[(0,0)]$ con 0.

Allora:

$$\mathbb{Z} = \omega \cup -\omega$$

Definiamo ora:

$$[(a,b)]+[(c,d)] \stackrel{def}{=} [(a+c,\ b+d)]$$
$$[(a,b)]\cdot[(c,d)] \stackrel{def}{=} [(ac+bd,\ bc+ad)]$$

PROPOSIZIONE

$(\mathbb{Z},+,\cdot,0,1)$ è un anello ordinato discreto.

Dim.

PREMESSA

Tralasceremo la dimostrazione del fatto che $\mathbb{Z}$ è un anello.

Definiamo il seguente ordine stretto:

$$[(a,b)] < [(c,d)] \overset{def}{\Longleftrightarrow} a+d > b+c$$

Dunque:

- $\forall\, [(a,b)] \in \mathbb{Z} : a+b \not> a+b \Rightarrow [(a,b)] \not< [(a,b)]$;
- $\forall\, [(a,b)], [(c,d)], [(e,f)] \in \mathbb{Z} : [(a,b)] < [(c,d)]$, $[(c,d)] < [(e,f)] \Rightarrow a+d > b+c,\ c+f > d+e \Rightarrow$ $\Rightarrow a+d+c+f > b+c+d+e \Rightarrow a+f > b+e \Rightarrow$ $\Rightarrow [(a,b)] < [(e,f)]$;
- $\forall\, [(a,b)], [(c,d)] \in \mathbb{Z} : ([(a,b)] < [(c,d)] \Rightarrow$ $\Rightarrow [(c,d)] \not< [(a,b)])$.
  Infatti, per la proprietà transitiva e quella antiriflessiva:
  $[(a,b)] < [(c,d)]$, $[(c,d)] < [(a,b)] \Rightarrow [(a,b)] < [(a,b)]$, assurdo;
- $\forall\, [(a,b)], [(c,d)] \in \mathbb{Z}$, $[(a,b)] \neq [(c,d)] \Rightarrow$ $\Rightarrow ([(a,b)] < [(c,d)] \vee [(a,b)] > [(c,d)])$,
  e ciò dipende dal fatto che $(\mathbb{N}, <)$ è totalmente ordinato.

Dunque $\mathbb{Z}$ è un anello ordinato.
Per vedere che $\mathbb{Z}$ è discreto, è sufficiente dimostrare che $0 = [(0,0)] \in \mathbb{Z}$ ha un successore. Ciò è immediato: se $[(a,b)] \in \mathbb{Z}$ è tale che $[(0,0)] < [(a,b)]$, allora:

$$a > b \Rightarrow a = b+1 \ \vee\ a > b+1,$$

da cui $[(a,b)] = [(1,0)] \vee [(a,b)] > [(1,0)]$, da cui $[(1,0)]$ è il successore di $[(0,0)]$, c.v.d.

CAMPO DEI RAZIONALI

Definiamo:
$$\mathbb{Q} = \mathbb{Z} \times (\mathbb{N} \setminus \{0\}) /_{\sim},$$
ove:
$$(x, y) \sim (x', y') \overset{def}{\iff} x y' = x' y$$

Esso è il campo delle frazioni di $\mathbb{Z}$.

PROPOSIZIONE
$(\mathbb{Q}, <)$ è denso: dati due elementi in $\mathbb{Q}$ distinti, ove esiste un terzo maggiore del minore dei due e minore del maggiore dei due.

Dim.
Siano $(a, b), (c, d) \in \mathbb{Q}$, e supponiamo che $(a, b) < (c, d)$, ossia, com'è prevedibile:
$$ad < bc$$
Consideriamo:
$$(ad + bc, 2bd),$$
ove $2bd \overset{def}{=} bd + bd$. Usando tutte le proprietà dimostrate o deducibili da quelle, si ha:

- $a(bd + bd) < bad + bcb \iff abd < bcb \iff ad < bc$, da cui $(a, b) < (ad + bc, 2bd)$;
- $(ad + bc)d < (bd + bd)c \iff add < bdc \iff ad < bc$, da cui $(ad + bc, 2bd) < (c, d)$,

ossia $\mathbb{Q}$ è denso, c.v.d.

BUONI ORDINI

Quando si introducono i numeri naturali, si è motivati dal bisogno di formalizzare il processo di "conteggio": in particolare, si definisce la funzione SUCCESSORE:

$$S(x) \overset{def}{=} x \cup \{x\}$$

Sarebbe auspicabile continuare questo "conteggio" oltre i numeri naturali.

Sappiamo che:

$$n = \{0, 1, \dots, n-1\}$$
$$\omega = \{0, 1, \dots\}$$

ω è allora il minimo NUMERO TRANSFINITO.

La funzione successore può essere allora estesa:

$$S(\omega) \overset{def}{=} \omega + 1 \overset{def}{=} \omega \cup \{\omega\}$$

Si ha allora una successione del tipo:

$$0 < 1 < 2 < \dots < \omega < \omega + 1 < \dots < \omega + \omega < \dots < \omega \cdot \omega < \dots$$
$$\dots < \omega^{\omega} < \dots < \omega^{\omega^{\omega}} < \dots$$

OSSERVAZIONE

In quest'ambito, un "insieme ordinato" sarà, salvo avviso esplicito, un insieme totalmente ordinato.

Un insieme ordinato $(A, <)$ è un BUON ORDINE se ogni sottoinsieme non vuoto $X \subseteq A$, $X \neq \emptyset$ ammette minimo.

Sia $(A, <)$ un buon ordine. Allora possiamo definire ricorsivamente:

$$\begin{cases} 0_A \overset{def}{=} \min A \\ 1_A \overset{def}{=} \min (A \setminus \{0_A\}) \\ \vdots \\ (N+1)_A \overset{def}{=} \min (A \setminus \{0_A, \dots, N_A\}) \end{cases}$$

Se $\omega \in A$, la successione per ricorsione non ordina tutto A.

Ex. Sia S un insieme finito e ordinato. Allora S ammette massimo e minimo (se esso è non vuoto).

Ragioniamo per induzione su $n = |S|$: se $n=1$ la tesi è banale.

Se la proposizione vale per n, allora, se $S = \{x_0, \dots, x_n\}$ è un insieme di $n+1$ elementi, si ha:

$$S = \{x_0\} \cup \{x_1, \dots, x_n\}$$

Per ipotesi induttiva, esistono $\max\limits_{i=1..n} x_i$ e $\min\limits_{i=1..n} x_i$.

Definiamo allora:

$$X = \begin{cases} x_0, & x_0 > \max\limits_{i=1..n} x_i \ \vee \ x_0 = \max\limits_{i=1..n} x_i \\ \max\limits_{x=1..n} x_i, & x_0 < \max\limits_{i=1..n} x_i \end{cases}$$

$$Y = \begin{cases} x_0, & x_0 < \max\limits_{i=1..n} x_i \ \vee \ x_0 = \max\limits_{i=1..n} x_i \\ \min\limits_{x=1..n} x_i, & x_0 > \max\limits_{i=1..n} x_i \end{cases}$$

Si ha, per costruzione $X = \max S$ e $Y = \min S$, da cui la tesi.

Ex. Ogni insieme $S \neq \emptyset$ ordinato e finito è un buon ordine.

Sia $X \subseteq S$, $X \neq \emptyset$. Allora, per l'esercizio precedente (X è un insieme finito e ordinato con l'ordinamento indotto) X ammette minimo.

Per definizione, allora, S è un buon ordine.

Ex. Due insiemi ordinati finiti ed equipotenti sono tra loro isomorfi mediante un isomorfismo d'ordine (si assume che gli insiemi siano non vuoti).

Ragioniamo per induzione su $n = |X| = |Y|$.

Il caso base è vero banalmente: se $X = \{x_1\}$, $Y = \{y_1\}$, allora $\Theta_1 : X \to Y$, $\Theta(x_1) \overset{\text{def}}{=} y_1$ è un isomorfismo d'ordine.

Siano ora $|X| = |Y| = n+1$, supponendo vera la tesi per n.

Per un esercizio precedente, si ha che:

$\exists\ \mathcal{X} = \max X$, $\mathcal{Y} = \max Y$,

da cui:

$$X = (X \setminus \{\mathcal{X}\}) \cup \{\mathcal{X}\}, \quad Y = (Y \setminus \{\mathcal{Y}\}) \cup \{\mathcal{Y}\}$$

Si ha $|X \setminus \{x\}| = |Y \setminus \{y\}| = n$, da cui:

$\exists\ \theta_{n+1} : X \setminus \{x\} \to Y \setminus \{y\}$ isomorfismo d'ordine.

A questo punto definiamo $\theta_{n+1} : X \to Y$ in questo modo:

$$\theta_{n+1} : X \to Y$$

$$\theta_{n+1}(x) = \begin{cases} \theta_{n+1}(x), & x \neq \max Y \\ \max Y, & x = \max X \end{cases}$$

Per costruzione, $\theta_{n+1} : X \to Y$ è un isomorfismo d'ordine da cui X e Y sono isomorfi.

PROPOSIZIONE

$(A, <)$ è un insieme bene ordinato se e solo se non esistono catene discendenti, ossia della forma:

$$a_1 > a_2 > a_3 > \dots > a_{n-1} > a_n > a_{n+1} > \dots,$$

con $a_i \in A\ \forall i \in \omega$.

Dim.

Un'implicazione è ovvia, se esiste una catena discendente, allora $X = \{a_i \mid i \in \omega\} \subseteq A$, $X \neq \emptyset$ non ammette minimo e quindi $(A, \leq)$ non è bene ordinato.

Dunque, per contronominale, la prima implicazione è dimostrata.

Sia ora $(A, <)$ non bene ordinato, e sia $X \neq \emptyset$, $X \subseteq A$ un sottoinsieme privo di minimo: immediatamente, per gli esercizi svolti precedentemente, X è infinito. Utilizzando l'assioma della scelta (necessario), sia:

$$f : \mathcal{P}(X) \setminus \emptyset \to X,$$

tale che:

$\forall Z \subseteq X : f(Z) \in Z$

(Sia dunque f una funzione di scelta su X).

Definiamo ora per ricorsione numerabile:

$$\begin{cases} a_1 = f(X) \\ a_{n+1} = f(\{x \in X \mid x < a_n\}) \end{cases}$$

La successione è ben definita, in quanto X non ammette minimo, dunque:

$\forall x \in X : \{y \in X \mid y < x\} \neq \emptyset$

Per costruzione, si ottiene dunque una catena discendente:

$$a_1 > a_2 > \dots > a_n > a_{n+1} > \dots,$$

proprio perché X non ha minimo.
Per contronominale, allora, la seconda implicazione è dimostrata, e con essa l'intera proposizione, c.v.d.

SEGMENTI INIZIALI

Sia $(A, <)$ un insieme ordinato. Un sottoinsieme $S \subseteq A$ (per non cadere nel banale, supponiamo $S \neq \emptyset$) si dice SEGMENTO INIZIALE se e solo se:

$\forall x, \forall y : (x < y \wedge y \in S \Rightarrow x \in S)$

Come suggerisce anche l'intuizione:

- $]-\infty, 1[\subseteq \mathbb{R}$ è un segmento iniziale;
- $S = \{ q \in \mathbb{Q} \mid q < 0 \vee q^2 < 2 \} \subseteq \mathbb{Q}$ è un segmento iniziale.

Sia $S \subseteq A$, $S \neq \emptyset$ un segmento iniziale. Esso si dice GENERATO da $a \in A$ se:

$$S = A_a \overset{\text{def}}{=} \{ x \in A \mid x < a \}$$

PROPOSIZIONE

Se $(A, <)$ è un buon ordine, allora ogni segmento iniziale $S \neq A$ è generato da un opportuno $a \in A$, ossia:

$\exists a \in A$ t.c. $S = A_a$.

Dim.

Si ha $S \neq A \Rightarrow A \setminus S \neq \emptyset$, da cui $(A \setminus S)$ ammette minimo:

$\exists a = \min (A \setminus S)$

Allora:

- $x \notin S \Rightarrow x \in A \setminus S \Rightarrow a \leq x \Rightarrow x \nless a \Rightarrow x \notin A_a$,

  o equivalentemente:

  $x \in A_a \Rightarrow x < a \Rightarrow x \in S$,

  da cui $A_a \subseteq S$;
- $x \notin A_a \Rightarrow x \nless a \Rightarrow a \leq x \Rightarrow x \notin S$,

  perché se fosse $x \in S$ (segmento iniziale), sarebbe $a \leq x \Rightarrow a \notin S$, assurdo.

  Dunque $S \subseteq A_a$.

da cui la Tesi, c.v.d.

OSSERVAZIONE

Nella notazione della proposizione, se $a \in (A,<)$, A_a è un insieme bene ordinato se $(A,<)$ è bene ordinato, mediante l'ordinamento indotto:

$$<_{A_a} \overset{def}{=} < \cap \, (A_a \times A_a)$$

OSSERVAZIONE

Sia $A = (\mathbb{Z}, <)$. Allora ogni segmento iniziale è generato, ma $(\mathbb{Z}, <)$ non è un buon ordine.

Dunque il viceversa della proposizione precedente è falso.

Ex. Se $\mathfrak{F}$ è una famiglia di insiemi ordinati, uno sottoinsieme dell'altro, ossia:

$\forall (A, <_A), (B, <_B) \in \mathfrak{F} : (A \subseteq B \Rightarrow (<_B) \cap (A \times A) = <_A)$

(ossia $\forall a, a' \in A : a <_A a' \Leftrightarrow a <_B a'$)

Allora $\bigcup \mathfrak{F} = \bigcup_{(A,<) \in \mathfrak{F}} (A,<)$ è un insieme ordinato.

Per le proprietà di $\mathfrak{F}$, dati $a, b \in \bigcup \mathfrak{F}$, si ha una di queste due possibilità:

- $\forall S \in \mathfrak{F},\ S \supseteq \{a,b\} : a <_S b$;
- $\forall S \in \mathfrak{F},\ S \supseteq \{a,b\} : a \not<_S b$.

Definiamo dunque la seguente relazione d'ordine, ben definita:

$\forall a, b \in \bigcup \mathfrak{F} : a <_* b \Leftrightarrow \exists S \in \mathfrak{F},\ \{a,b\} \subseteq S$ t.c. $a <_S b$.

Inoltre, dato che gli insiemi sono uno sottoinsieme dell'altro, per ogni insieme finito di elementi di $\bigcup \mathfrak{F}$, esiste $D \in \mathfrak{F}$ che li contiene tutti.

Dunque:

- $\forall a \in \bigcup \mathfrak{F},\ \forall S \in \mathfrak{F}$ t.c. $a \in S : a \not<_S a \Rightarrow a \not<_* a$;
- $\forall a, b, c \in \bigcup \mathfrak{F},\ \forall S \in \mathfrak{F},\ S \supseteq \{a,b,c\} : a <_* b,\ b <_* c \Rightarrow$
  $\Rightarrow a <_S b,\ b <_S c \Rightarrow a <_S c \Rightarrow a <_* c$;
- $\forall a, b \in \bigcup \mathfrak{F},\ \forall S \in \mathfrak{F},\ S \supseteq \{a,b\} : a <_* b \Rightarrow a <_S b \Rightarrow$
  $\Rightarrow b \not<_S a \Rightarrow b \not<_* a$;
- $\forall a, b \in \bigcup \mathfrak{F},\ \forall S \in \mathfrak{F},\ S \supseteq \{a,b\} : (a \neq b \Rightarrow a <_S b \vee b <_S a) \Rightarrow$

$\Rightarrow (a \neq b \Rightarrow a <_* b \lor b <_* a)),$

da cui $(\bigcup \mathcal{F}, <_*)$ è un insieme totalmente ordinato.

OSSERVAZIONE

La proprietà esposta nell'esercizio precedente non vale più, in genere, se si parla di buoni ordini anziché di ordini totali.

Ad esempio, se consideriamo $\mathcal{F} = \{A_n \mid n \in \mathbb{N}\}$, ove:

$$A_n \overset{def}{=} \mathbb{Z} \cap [-n, +\infty[,$$

si ha che $A_n \simeq (\mathbb{N}, <)$ è un buon ordine per ogni $n \in \mathbb{N}$, ma $\mathbb{Z} = \bigcup_{n \in \mathbb{N}} A_n$ non è bene ordinato.

Vi sono però casi in cui ciò vale, come spiega il prossimo esercizio.

Ex. Sia $\mathcal{F}$ una famiglia di buoni ordini, tali che essi siano uno un segmento iniziale dell'altro (nel senso dell'esercizio precedente). Allora $\bigcup \mathcal{F}$ è un buon ordine.

In base all'esercizio precedente, sappiamo che $(\bigcup \mathcal{F}, <_*)$, ove:

$$a <_* b \Leftrightarrow \exists\, S \in \mathcal{F},\ S \supseteq \{a, b\} \ni' a <_S b,$$

è un insieme ordinato.

Sia ora $X \subseteq \bigcup \mathcal{F}$, $X \neq \emptyset$. Sia $x \in X$, e sia $S \in \mathcal{F}$ un insieme contenente x. Allora si ha:

$$\{y \in X \mid y <_* x\} = S \cap \{y \in X \mid y <_* x\}$$

Le possibilità sono due:

- $S \cap \{y \in X \mid y <_* x\} = \emptyset$, dunque $x = \min X$ ed esiste il minimo di X.
- $S \cap \{y \in X \mid y <_* x\} \neq \emptyset$. Ma S è un buon ordine, dunque esiste $z = \min\{y \in X \mid y <_* x\}$. Si ha in effetti $z = \min X$, dato che, per $d \in X$:
  - $d \in \{y \in X \mid y <_* x\} \Rightarrow z \leq_* d$;
  - $d \notin \{y \in X \mid y <_* x\} \Rightarrow z <_* x \leq d \Rightarrow z <_* d$,

da cui $(\bigcup \mathcal{F}, <_*)$ è, in questo caso, un buon ordine.

PROPOSIZIONE

Sia $(A,<)$ un buon ordine. Allora:

- Se $\varphi : A \to A$ preserva l'ordine, allora $\varphi(a) \geq a \ \forall a \in A$;
- $\forall a \in A$, $A \not\cong A_a$;
- Se $a \neq a'$, allora $A_a \not\cong A_{a'}$;
- L'unico automorfismo $\varphi : A \to A$ ordinato è l'identità.

Dim.

- Se per assurdo la tesi fosse falsa, esisterebbe:
$$b = \min T, \quad T \overset{def}{=} \{ x \in A \mid \varphi(x) < x \}$$
Se φ preserva l'ordine, si avrebbe dunque:
$$\varphi(b) < b \Rightarrow \varphi(\varphi(b)) < \varphi(b) \Rightarrow \varphi(\varphi(b)) < \varphi(b), \varphi(b) < b,$$
assurdo per la minimalità di $b = \min T$;
- Se per assurdo avessimo $\varphi : A \to A_a$ isomorfismo ordinato, avremmo $\varphi(a) \notin A_a$ perché $\varphi(a) \geq a$, e questo è assurdo;
- Sia ad esempio $a < a'$. Sia $B = A_{a'}$. Allora $A_a = B_a$, e per la proposizione precedente $B_a \not\cong B$, ossia $A_a \not\cong A_{a'}$;
- Se la tesi fosse falsa, esisterebbe:
$$b = \min \{ a \in A \mid \varphi(a) \neq a \}$$
Dato che $\varphi : A \to A$ è un automorfismo ordinato, si avrebbe:
$$\varphi(b) \geq b, \quad \varphi(b) \neq b \quad \Rightarrow \quad \varphi(b) > b$$
Si avrebbe allora:
  - $\forall x < b : \varphi(x) = x < b$;
  - $\forall x \geq b : \varphi(x) \geq \varphi(b) > b$,

da cui $b \notin \operatorname{Im} \varphi$, e questo è assurdo, c.v.d.

OSSERVAZIONE

Osserviamo che $]0,1[\subseteq \mathbb{R}^+$ è un segmento iniziale, e:
$$\varphi : \mathbb{R}^+ \to]0,1[$$
$$x \longmapsto \frac{x}{x+1}$$
è un isomorfismo ordinato. Dunque $\mathbb{R}^+$ non è bene ordinato (come già si sapeva).

OSSERVAZIONE

È possibile che esistano un buon ordine $(A, \leq_A)$ e un sottoinsieme $B \subseteq A$ (ordinato tramite l'ordinamento indotto $\leq_B = \leq_A \cap (B \times B)$) tali che:

$$(B, \leq_B) \cong (A, \leq_A)$$

Basta considerare i seguenti esempi:

- $[-2, +\infty[\, \cap \, \mathbb{Z} \to \mathbb{N}$
- $\mathbb{N} \to 2\mathbb{N} \overset{def}{=} \{2n \mid n \in \mathbb{N}\}$

Come ci si aspettava, i sottoinsiemi non sono mai segmenti iniziali.

PROPOSIZIONE

Sia $(A, <)$ un insieme ordinato tale che ogni segmento iniziale $S \neq A$ (compreso il segmento vuoto $S = \emptyset$) è generato, ossia $\exists\, a \in A \ni S = A_a$. Allora $(A, <)$ è un buon ordine.

Dim.

Sia $X \subseteq A$, $X \neq \emptyset$. Consideriamo:

$$S_X = \{y \in A \mid y < x \ \forall\, x \in X\} \neq A$$

Allora $S_X = A_a$ per un opportuno $a \in A$. Allora si ha:

$$a = \min X$$

CONFRONTABILITÀ DEI BUONI ORDINI

TEOREMA (TRICOTOMIA DEI BUONI ORDINI)

Siano $(A,<)$ e $(B,<)$ dei buoni ordini. Allora vale una e una sola delle seguenti proprietà (introdurremo nel frattempo una notazione):

- $A \cong B$ (ossia $ot(A) = ot(B)$, o $A \approx B$);
- $\exists\, b \in B \ni' A \cong B_b$ (ossia $ot(A) < ot(B)$, o $A \prec B$);
- $\exists\, a \in A \ni' A_a \cong B$ (ossia $ot(A) > ot(B)$ o $A \succ B$).

Tra gli ordini vi è dunque una relazione d'ordine totale.

Dim.

PREMESSA

Alcuni facili esempi sono i seguenti:

$$ot(n) < ot(m) \iff n < m$$

$$ot(n) < ot(\omega) \quad \forall\, n \in \omega$$

Più avanti giustificheremo scritture del tipo:

$$ot(\omega+\omega+17) < ot(\omega+\omega+\omega)$$

$$ot(\omega+\omega) < ot(\omega^\omega)$$

Innanzitutto, non possono valere simultaneamente due proprietà. Supponiamo che valgano 1) e 2) (il caso 1) e 3) è identico). Allora si ottiene:

$$A \cong B \cong A_a \Rightarrow A \cong A_a,$$

assurdo.

Enunciamo ora un lemma, che dimostreremo in seguito.

LEMMA (SOLO ENUNCIATO)

Sia $\psi : C \to D$ un isomorfismo tra buoni ordini. Allora:

$\forall\, c \in C : \psi|_{C_c} : C_c \to D_{\psi(c)}$ è un isomorfismo.

Se valgono 2) e 3), si ha $B \cong A_a$. Inoltre esiste:

$$\psi : A \to B_b,$$

$$\psi|_{A_a} : A_a \to (B_b)_{\psi(a)} = B_{\psi(a)},$$

da cui:

$$B \cong B_{\psi(a)},$$

assurdo.

Completeremo dopo la dimostrazione, dimostrando il lemma e l'uguaglianza sopra vista:

$$(B_b)_{\psi(a)} = B_{\psi(a)}$$

Definiamo ora:

$$T \overset{def}{=} \{(a,b) \in A \times B \mid A_a \cong B_b\}$$

Allora:

- $(0_A, 0_B) \in T$ perché $A_{0_A} = \emptyset = B_{0_B}$;
- $(1_A, 1_B) \in T$ perché $A_{1_A} = \{0_A\} \cong \{0_B\} = B_{0_B}$,

e così via.

T è una relazione, dimostriamo che è una funzione. È sufficiente dimostriamo che:

$$(a,b), (a,b') \in T \Rightarrow b = b'$$

Per una proposizione precedente:

$$\begin{matrix}(a,b) \in T \\ (a,b') \in T\end{matrix} \Rightarrow A_a \cong B_b \wedge A_a \cong B_{b'} \Rightarrow B_b \cong B_{b'} \Rightarrow b = b'$$

Dimostriamo ora che $\mathrm{Dom}\,T$ è un segmento iniziale di A, potendo essere anche $\mathrm{Dom}\,T = A$.

Sia $a' < a$, con $a \in \mathrm{Dom}\,T$. Sia $b \in B$, con $(a,b) \in T$.

Allora esistono:

$$\psi\ A_a \to B_b$$

$$\psi|_{A_{a'}} : A_{a'} \to B_{\psi(a')}$$

isomorfismi, da cui $(a', \psi(a')) \in T$, ossia $a' \in \mathrm{Dom}\,T$, e in più $T(a') = \psi(a') < b = T(a)$, da cui T preserva l'ordine.

Per simmetria, anche $\operatorname{Im} T$ è un segmento iniziale (di B, potendo essere $\operatorname{Im} T = B$).

A questo punto distinguiamo 4 casi:

- $\operatorname{Dom} T = A \wedge \operatorname{Im} T \neq B$, ossia $\operatorname{Im} T = B_b$, $b \in B$. Allora:
$$T : A \to B_b$$
è un isomorfismo, dunque vale la 2);
- $\operatorname{Dom} T \neq A \wedge \operatorname{Im} T = B$. Allora, in maniera analoga al precedente caso, vale la 3);
- $\operatorname{Dom} T = A \wedge \operatorname{Im} T = B$. Allora si ha l'isomorfismo:
$$T : A \to B,$$
da cui vale la 1);
- $\operatorname{Dom} T \neq A \wedge \operatorname{Im} T \neq B$, ossia $\operatorname{Dom} T = A_a \wedge \operatorname{Im} T = B_b$. Allora si ha:
$$T : A_a \to B_b$$
isomorfismo, da cui, per definizione di T:
$$(a, b) \in T \Rightarrow a \in \operatorname{Dom} T = A_a,$$
assurdo.

Dunque si ha la tesi c.v.d.

Giustifichiamo ora l'uguaglianza:
$$(B_b)_{\psi(a)} = B_{\psi(a)}$$
Un'inclusione è ovvia:
$$(B_b)_{\psi(a)} = \{x \in B_b \mid x < \psi(a)\} \subseteq \{x \in B \mid x < \psi(a)\} = B_{\psi(a)}$$
L'altra uguaglianza si ottiene subito, ricordando che $\psi(a) < b$. Infatti, se $\psi : A \to B_b$, allora $\psi(a) \in B_b \Rightarrow \psi(a) < b$. Si ha dunque:
$$B_{\psi(a)} = \{x \in B \mid x < \psi(a)\} = \{x \in B \mid x < \psi(a) < b\} \subseteq$$
$$\subseteq \{x \in B_b \mid x < \psi(a)\} = (B_b)_{\psi(a)}$$

Dimostriamo ora il lemma esposto precedentemente.

La restrizione di una funzione iniettiva ad un sottoinsieme qualsiasi del dominio rimane iniettiva. Dunque bisogna dimostrare che effettivamente sia $(\psi|_{C_c})(C_c) = D_{\psi(c)}$.

In effetti, si può semplicemente dimostrare che:

$$\psi^{-1}|_{D_{\psi(c)}} : D_{\psi(c)} \to C_c$$

è iniettiva.

Per concludere, basta notare che $\psi|_{C_c}(c) = \psi(c)$, da cui:

$$\psi|_{C_c}(C_c) \subseteq D_{\psi(c)}$$

Analogamente:

$$\psi^{-1}|_{D_{\psi(c)}}(D_{\psi(c)}) \subseteq C_c,$$

e dato che:

$$\psi|_{C_c} \circ \psi^{-1}|_{D_{\psi(c)}} = Id_{D_{\psi(c)}}$$

$$\psi^{-1}|_{D_{\psi(c)}} \circ \psi|_{C_c} = Id_{C_c},$$

si conclude che $\psi|_{C_c} : C_c \to D_{\psi(c)}$ è un isomorfismo.

ESERCIZI VARI

1. Sia $(A, <)$ un insieme ordinato infinito.
Le proprietà seguenti sono equivalenti:

- $(A, <) \cong (\omega, \in)$;
- Ogni segmento iniziale $S \neq A$ è finito;
- Nessun $X \subseteq A$ infinito ha massimo.

Dimostriamo che 1) $\Rightarrow$ 2)
I segmenti iniziali di ω (buon ordine) sono generati, ossia della forma $\omega_n = \{x \in \omega \mid x < n\} = \{0, \dots, n-1\} = n$, da cui $|\omega_n| = |n| = n$, e ω_n è finito.

Dimostriamo che 1) $\Rightarrow$ 3).
Se $B \subseteq \omega$ ha massimo m, allora:

$$\max B = m \Rightarrow B \subseteq \{0, \dots, m\} = m+1,$$

da cui:

$$|B| \leq |m+1| = m+1 \Rightarrow B \text{ è finito.}$$

Dimostriamo che 2) $\Rightarrow$ 1).
Si ha che $(A, <)$ è un buon ordine. Se così non fosse, esisterebbe $a_1 > a_2 > a_3 > \dots$ catena discendente. Ma allora $S = A_{a_1} \neq A$ sarebbe un segmento iniziale infinito, e ciò è assurdo. Si noti che, per dimostrare l'esistenza della catena discendente si è usato l'assioma della scelta.

Possiamo allora usare la tricotomia dei buoni ordini: dato che sia ω che A sono infiniti, e ogni segmento iniziale proprio di ω (di A) è finito, si deduce facilmente, per esclusione, che vale $(A, <) \cong (\omega, \in)$.

Dimostriamo che 3) $\Rightarrow$ 1).
Innanzitutto A è un buon ordine: se così non fosse, (utilizzando l'assioma della scelta) la catena discendente risulterebbe un insieme infinito avente massimo, e ciò è assurdo.

Usiamo ancora la tricotomia dei buoni ordini.

Non può essere $A \cong n$ per $n \in \omega$, perché A è infinito.
Non può essere $\omega \cong A_a$ per qualche $a \in A$, altrimenti $A_a \cup \{a\}$ sarebbe un sotto insieme di A infinito e con massimo uguale ad a.
Allora $(A, <) \cong (\omega, \in)$.

2. Sia $(A, <)$ un buon ordine, e sia $B \subseteq A$. Allora:

$$ot(B) \leq ot(A)$$

Innanzitutto, $B \subseteq A$ è un buon ordine. Se non lo fosse, esisterebbe in B (dunque a fortiori in A) una catena discendente e ciò è assurdo.

Usiamo allora la tricotomia dei buoni ordini. Se per assurdo fosse $ot(A) < ot(B)$, cioè:
$\exists\, b \in B \ni' A \cong B_b$,
si avrebbe:

$$ot(A) = ot(B_b) \leq ot(A_b),$$

assurdo. Dunque $ot(B) \leq ot(A)$.

3. Sia $\mathcal{F}$ una famiglia non vuota di buoni ordini. Allora esiste $(A, <) \in \mathcal{F}$ di TIPO D'ORDINE MINIMO, cioè tale che:
$\forall (B, <) \in \mathcal{F} : ot(A) \leq ot(B)$

Sia $(A, <) \in \mathcal{F}$. Consideriamo l'insieme:

$$\Lambda = \{(C, <) \in \mathcal{F} \mid ot(C) < ot(A)\}$$

Se $\Lambda = \emptyset$, allora abbiamo finito. Altrimenti, dato che:
$\forall (C, <) \in \Lambda \ \exists\, a_C \in A \ni' A_{a_C} \cong C$,
possiamo definire la seguente funzione:

$$\begin{aligned} \Psi : \Lambda &\to A \\ (C, <) &\mapsto a_C \end{aligned}$$

Dato che A è un buon ordine, l'insieme non vuoto:

$$\mathcal{B} = \{a \in A \mid a = a_C \text{ per un } (C, <) \in \mathcal{F}\}$$

ammette minimo h.
Detto $\bar{X} \in \mathcal{B}$ tale che $\Psi(\bar{X}, <) = h$, $\bar{X}$ è un buon ordine di tipo d'ordine minimo.

Infatti:

- $\forall (U, <) \in \mathcal{F}$, $ot(A) \leq ot(U)$: $ot(\overline{X}) < ot(A) \leq ot(U)$;
- $\forall (U, <) \in \mathcal{F}$, $ot(A) > ot(U)$: $(U, <) \in \Lambda \Rightarrow U \cong A_{a_0}$, $a_0 \geq h \Rightarrow$
$\Rightarrow ot(\overline{X}) = ot(A_h) \leq ot(A_{a_0}) = ot(U)$.

4. Sia $(A, <) \subseteq (\mathbb{R}, <)$ un buon ordine. Allora $|A| \leq \aleph_0$.

Dato $x \in A$, sia $S(x) \in A$ il successore di x in A. Se $x \in A$ non ha successori, definiamo $S(x) = q_0$, con $q_0 \in \mathbb{Q}$, $q_0 > x$.
Gli intervalli di $\mathbb{R}$ del tipo $]x, S(x)[$, $x \in A$ sono non vuoti e disgiunti.
Per densità di $\mathbb{Q}$, allora, esiste un razionale in ogni intervallo del tipo $]x, S(x)[$, $x \in A$, da cui la seguente composizione di funzioni iniettive che preserva l'ordine:

$$\begin{array}{ccccc} A & \longrightarrow & \{\,]x, S(x)[\; \mid x \in A\} & \longrightarrow & \mathbb{Q} \\ x & \longrightarrow &]x, S(x)[& \longrightarrow & q_x \in\,]x, S(x)[\end{array}$$

è iniettiva.
Allora:

$$|A| \leq |\mathbb{Q}| = \aleph_0$$

5. Siano $A, B \subseteq \mathbb{R}$ buoni ordini. Allora è un buon ordine:

$$A + B = \{a + b \mid a \in A,\ b \in B\}$$

Per assurdo, sia la seguente una catena discendente:

$$a_1 + b_1 > a_2 + b_2 > \dots > a_m + b_m > \dots = c_1 > c_2 > \dots > c_m > \dots$$

Siano, ricorsivamente:

- $a_{m_1} \stackrel{def}{=} \min \{a_m \mid m \in \mathbb{N}\}$;
- $a_{m_{k+1}} = \min \{a_m \mid m > m_k\}$.

Si ha allora una sottosuccessione:

- $a_{m_1} + b_{m_1} > a_{m_2} + b_{m_2} > \dots$;
- $a_{m_1} \leq a_{m_2} \leq \dots$.

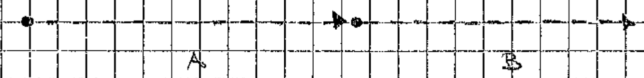
Allora $b_{m_1} > b_{m_2} > \dots$, assurdo.

SOMMA E PRODOTTO DI BUONI ORDINI

Siano $(A,<)$ e $(B,<)$ buoni ordini. Allora si definisce:

$$A \oplus B$$

l'insieme formato "giustapponendo" B ad A:



Vogliamo però dare una definizione più formale. Definiamo allora l'UNIONE DISGIUNTA di A e B:

$$A \amalg B \overset{def}{=} (A \times \{0\}) \cup (B \times \{1\}) =$$
$$= \{(a,0) \mid a \in A\} \cup \{(b,1) \mid b \in B\}$$

Allora $A \oplus B$ è l'insieme $A \amalg B$, con l'ordine definito in questo modo:

- $(a,0) < (a',0) \iff a <_A a'$;
- $(b,1) < (b',1) \iff b <_B b'$;
- $\forall a \in A, \forall b \in B : (a,0) < (b,1)$.

L'insieme $A \oplus B$ può essere definito anche nel caso in cui A e B sono solamente insiemi ordinati. Tuttavia, vale quanto segue:

- A e B sono buoni ordini se e solo se $A \oplus B$ è un buon ordine;
- se $A \cong A'$ e $B \cong B'$, allora $A \oplus B \cong A' \oplus B'$.

Dimostreremo tali proposizioni in seguito.

Notiamo ora che, aggiungendo a sinistra un elemento $*$ a ω, si ha banalmente:

$$\omega \cong \omega \oplus \{*\}$$

Se invece aggiungiamo $*$ a destra, $\omega \not\cong \omega \oplus \{*\}$, da cui, in particolare, si ha:

$$(\omega \oplus \{*\})_* = \omega \Rightarrow$$
$$\{*\} \oplus \omega = \omega < \omega \oplus \{*\},$$

e la somma così definita non è commutativa. In particolare, si dice che ω "assorbe a sinistra".

Vogliamo ora presentare il prodotto. Consideriamo:

$$\underbrace{\omega \oplus \omega \oplus \dots \oplus \omega}_{10 \text{ volte}}$$

Chiameremo tale insieme $\omega \odot 10$.

Intuitivamente, $A \odot B$ si costruisce "ripetendo A B-volte", ossia rimpiazzando ogni elemento di B con una copia di A.

Si noti che $\omega \odot 10 \neq 10 \odot \omega$: nel secondo caso, si hanno ω copie di $\{0, \dots, 9\} = 10$.

Si può ora definire formalmente il prodotto di buoni ordini:

$$A \otimes B$$

Definiamo $A \otimes B$ come l'insieme $A \times B$ con l'ordine definito dall'ORDINE ANTI-LESSICOGRAFICO:

$$(a,b) < (a',b') \Leftrightarrow \begin{cases} b < b' \\ b = b' \ \wedge \ a < a' \end{cases}$$

Ad esempio:

$$A \oplus A \oplus A \oplus A \cong A \otimes \{0, 1, \dots, 3\},$$

dove si noti che l'isomorfismo non è un'uguaglianza.

Alcune proprietà sono le seguenti:

- $(A \oplus B) \oplus C \cong A \oplus (B \oplus C)$;
- $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$;
- $A \otimes (B \oplus C) \cong (A \otimes B) \oplus (A \otimes C)$;
- $(B \oplus C) \otimes A \ncong (B \otimes A) \oplus (C \otimes A)$;

Dimostriamo ora un po' di fatti.

LEMMA

A e B sono buoni ordini se e solo se $A \otimes B$ è un buon ordine.

Dim.

La prima implicazione è banale, in quanto se A, B sono buoni ordini, per come è definito $A \otimes B$, esso è un buon ordine.

Viceversa, ogni sottoinsieme di un buon ordine è un buon ordine, da cui $A \cong A \times \{0\}$ e $B \cong B \times \{1\}$ sono buoni ordini, c.v.d.

LEMMA

Se $A \cong A'$ e $B \cong B'$, allora $A \oplus B \cong A' \oplus B'$.

Dim.

La dimostrazione è immediata. Presi:

$$\phi : A \to A' \qquad \psi : B \to B',$$

definiamo:

$$\eta : A \oplus B \to A' \oplus B'$$

$$(x, t) \mapsto \begin{cases} (\phi(x), t), & t = 0 \\ (\psi(x), t), & t = 1, \end{cases}$$

e questo è un isomorfismo, c.v.d.

Vediamo ora perché non vale la proprietà distributiva a destra.

Siano:

$$A = \omega, \qquad B = 1 = \{0\} = C$$

Allora:

- $(B \oplus C) \otimes A = 2 \otimes \omega \cong \omega;$
- $B \otimes A \oplus C \otimes A = 1 \otimes \omega \oplus 2 \otimes \omega \cong \omega + \omega \not\cong \omega.$

L'INSIEME $\mathbb{R}$ DEI REALI

Un sottoinsieme $X \subseteq \mathbb{Q}$ è un TAGLIO DI DEDEKIND:

- X è un segmento iniziale non banale, ossia $\emptyset \neq X \neq \mathbb{Q}$;
- X non ha massimo.

Ad esempio, per ogni $q \in \mathbb{Q}$, $X_q = \{x \in \mathbb{Q} \mid x < q\}$ è un taglio di Dedekind. Infatti:

- $q-1 \in X_q \Rightarrow X_q \neq \emptyset$; $q \notin X_q \Rightarrow X \neq \mathbb{Q}$;
- X_q non ha massimo perché $\mathbb{Q}$ è denso in $\mathbb{R}$.

Possiamo identificare X_q con q. Infatti:

$$q < q' \Rightarrow (q+q')\frac{1}{2} \in X_{q'} \setminus X_q \Rightarrow X_q \subsetneq X_{q'}$$

Definiamo allora:

$$\mathbb{R} \overset{\text{def}}{=} \{ X \subseteq \mathbb{Q} \mid X \text{ è un taglio di Dedekind} \}$$

Dato che gli insiemi $X = X_q$, $q \in \mathbb{Q}$ sono tagli di Dedekind, allora ha senso scrivere $\mathbb{Q} \subseteq \mathbb{R}$.
Definiamo ora, per X, Y tagli di Dedekind, ossia $X, Y \in \mathbb{R}$

$$X \leq Y \overset{\text{def}}{\Longleftrightarrow} X \subseteq Y$$

PROPOSIZIONE
$(\mathbb{R}, \leq)$ è un insieme ordinato e completo, che ammette $\mathbb{Q}$ come sottoinsieme numerabile e denso.

Dim.
Sicuramente l'inclusione $\subseteq$ è un ordine parziale, ma vogliamo dimostrare che $\leq$ è un ordine totale, ossia che, dati $X, Y \in \mathbb{R}$:

$$(X \neq Y \Rightarrow X \subsetneq Y \vee Y \subsetneq X)$$

Se per assurdo valesse il contrario, avremmo:

- $\exists\, x \in X \setminus Y$;
- $\exists\, y \in Y \setminus X$.

Chiaramente $x \neq y$.

Se ad esempio vale $x < y$, Y non è un segmento iniziale perché $x \notin Y$, $x < y$, $y \in Y$. Ciò è assurdo.
Dunque $(\mathbb{R}, \leq)$ è ordinato.

Vogliamo ora dimostrare che $\mathbb{Q}$ è denso in $\mathbb{R}$.
Vogliamo, in altre parole, determinare $q \in \mathbb{Q}$ tale che:

$$X \subsetneq X_q \subsetneq Y,$$

assumendo $X \subsetneq Y$.
Sia $q' \in Y \setminus X$. Dato che potrebbe essere $X = X_{q'}$, consideriamo $q > q'$, $q \in Y$, e si ha:

$$X \subsetneq X_q \subsetneq Y$$

Tale q esiste perché $Y \subseteq \mathbb{Q}$ non ha massimo.

Dimostriamo ora la completezza.
Sia $\mathcal{X} \subseteq \mathbb{R}$, $\mathcal{X} \neq \emptyset$, un insieme SUPERIORMENTE LIMITATO.
Sia:

$$Y = \bigcup \mathcal{X} = \bigcup_{X \in \mathcal{X}} X$$

Allora $Y = \sup \mathcal{X} \in \mathbb{R}$. Per dimostrarlo effettuiamo le verifiche:

- $\mathcal{X} \neq \emptyset \Rightarrow \exists\, X \in \mathcal{X} \Rightarrow Y = \bigcup \mathcal{X} \neq \emptyset$;
- per ipotesi, esiste $Z \in \mathbb{R} \ni' X \subseteq Z$ per ogni $X \in \mathcal{X}$.
  Sia $z \notin Z$. Allora $z \notin X$ per nessun $X \in \mathcal{X}$; ciò è banale.
  Allora $Y \neq \mathbb{Q}$.
- Y non ha massimo, e ciò è banale;
- Y è segmento iniziale perché unione di segmenti iniziali;
- Si ha:
  $\forall\, X \in \mathcal{X} : X \subseteq Y \Rightarrow X \leq Y$
  Inoltre, se $W \supseteq X$ $\forall\, X \in \mathcal{X}$, ossia W è un maggiorante di $\mathcal{X}$, allora:

$$W \supseteq \bigcup \mathcal{X} = \bigcup_{X \in \mathcal{X}} X = Y,$$

da cui Y è il minimo dei maggioranti di $\mathcal{X}$:

$$Y = \sup \mathcal{X} \in \mathbb{R}, \text{ c.v.d.}$$

Definiamo ora l'operazione di SOMMA in $\mathbb{R}$:

$$X+Y \overset{def}{=} \{ q+q' \mid q\in X,\ q'\in Y \}$$

Quanto segue è solo enunciato:

- $X+Y$ è un taglio di Dedekind;
- $(\mathbb{R},+)$ è un gruppo Abeliano, e il suo elemento neutro è:
$$0=\{ q\in\mathbb{Q} \mid q<0 \}$$

Da definizione, dunque, si ha:

$$X>0 \iff \exists\, q\in X \text{ t.c. } q>0$$

Definiamo, allora:

- se $X\equiv X_q,\ q\in\mathbb{Q}$: $-X = -X_q \overset{def}{=} X_{-q}$;
- in caso contrario:
$$-X \overset{def}{=} \{ -q \mid q\notin X \}$$

Dati ora $X>0$, $Y>0$, definiamo il PRODOTTO in $\mathbb{R}^+$:

$$X\cdot Y \overset{def}{=} \{ x\in\mathbb{Q} \mid x\le 0 \} \cup \{ qq' \mid q\in X,\ q'\in Y,\ q,q'>0 \}$$

Estendiamo allora il prodotto in $\mathbb{R}$ in questo modo:

$$X\cdot Y = -[(-X)\cdot Y]$$

Si possono allora dimostrare i seguenti fatti:

- $(\mathbb{R},+,\cdot,\le)$ è un campo ordinato completo;
- le operazioni definite sono coerenti con quelle di $\mathbb{Q}$, ossia:
$$\forall\, q, q'\in\mathbb{Q}:\ X_q+X_{q'}=X_{q+q'},\quad X_q\cdot X_{q'}=X_{q\cdot q'}$$
- due campi ordinati e completi sono isomorfi.

ORDINI TOTALI E BUONI ORDINI

Su $Fin(\mathbb{N})$ definiamo:

- $A <_1 B \overset{def}{\iff} A \neq B \wedge \min(A \Delta B) \in B$
- $A <_2 B \overset{def}{\iff} A \neq B \wedge \max(A \Delta B) \in B$,

ove:

$$A \Delta B \overset{def}{=} (A \setminus B) \cup (B \setminus A)$$

Il primo si chiama ORDINE DELLA MINIMA DIFFERENZA, ed è un ordine totale, ma non un buon ordine.

Questo non è un buon ordine, perché la seguente è una catena discendente:

$$\{1\} >_1 \{2\} >_1 \{3\} >_1 \dots$$

L'unica proprietà non banale per dimostrare che $<_1$ è un ordine è totale è la proprietà transitiva.

Supponiamo che $A, B, C \in Fin(\mathbb{N})$ siano tali che:

$$A <_1 B <_1 C$$

Allora:

- $\exists m_1 = \min(A \Delta B) \in B \setminus A$
- $\exists m_2 = \min(B \Delta C) \in C \setminus B$

Innanzitutto $m_1 \neq m_2$, perché $m_1 \in B$, $m_2 \notin B$. I casi sono due, dunque:

- $m_1 < m_2$. Si ha allora:

$\forall k < m_2 : (k \in B \wedge k \in C) \vee (k \notin B \wedge k \notin C)$

Dato che $m_1 < m_2$, e $m_1 \notin A$, $m_1 \in B \Rightarrow m_1 \in C$, e che:
$\forall h < m_1 : k \notin (A \Delta B) \cup (B \Delta C)$,
si ha $m_1 = \min(A \Delta C) \in C$, da cui $A <_1 C$;

- $m_2 > m_1$: si ragiona in modo analogo

Il secondo si chiama ORDINE DELLA MASSIMA DIFFERENZA, ed è un buon ordine.

Prima di dimostrarlo, notiamo che:

- $\emptyset$ è il minimo di $(Fin(\mathbb{N}), <_2)$. Infatti:
  $\forall A \neq \emptyset : \exists \max A \in A \setminus \emptyset \Rightarrow \emptyset <_2 A$
- $\{1\}$ è il minimo di $(Fin(\mathbb{N}) \setminus \{\emptyset\}, <_2)$. Infatti:
  $\forall A \neq \emptyset,\ A \neq \{1\} : \exists \max A > 1 \Rightarrow \{1\} <_2 A$

Si generalizza facilmente:

$$\emptyset <_2 \{1\} <_2 \{2\} <_2 \{1,2\} <_2 \{3\} <_2 \{1,3\} <_2 \{2,3\} <_2$$
$$<_2 \{1,2,3\} <_2 \{4\} <_2 \{1,4\} <_2 \{2,4\} <_2 \{1,2,4\} <_2$$
$$<_2 \{3,4\} <_2 \{1,3,4\} <_2 \{2,3,4\} <_2 \{1,2,3,4\} <_2 \dots$$

Dimostriamo che $(Fin(\mathbb{N}), <_2)$ è totalmente ordinato.
L'unica proprietà non banale è la transitiva.

Siano $A, B, C \in Fin(\mathbb{N})$ tali che:

$$A <_2 B <_2 C$$

Allora:

- $\exists m_1 = \max(A \Delta B) \in B \setminus A$
- $\exists m_2 = \max(B \Delta C) \in C \setminus B$

Chiaramente $m_1 \neq m_2$ perché $m_1 \in B$, $m_2 \notin B$. I casi sono due:

- $m_1 < m_2$. Si ha allora:
  $\forall k > m_1 : (k \in B \wedge k \in A) \vee (k \notin B \wedge k \notin A)$

  Dato che $m_1 < m_2$, e che $m_2 \in C$, $m_2 \notin B \Rightarrow m_2 \notin A$, e che:
  $\forall h > m_2 : h \notin (A \Delta B) \cup (B \Delta C)$,
  si ha: $m_2 = \max(A \Delta C) \in C \setminus A$ da cui $A <_2 C$.

- $m_1 < m_2$: si ragiona in modo analogo.

Dimostrare a questo punto che $<_2$ è facile: dimostreremo che non esistono catene discendenti infinite.
Per assurdo, sia $\langle a_i \mid i \in \mathbb{N} \rangle$ una catena discendente:
$\forall i \in \mathbb{N} \quad a_{i+1} <_2 a_i \quad , a_i \in Fin(\mathbb{N})$

Sia $h = \max a_1 \in \mathbb{N}$. Allora:

$\forall\ i \in \mathbb{N} : a_i <_2 a_1 \Rightarrow \forall\ i \in \mathbb{N},\ \forall\ k > h : k \notin a_i \Rightarrow$

$\Rightarrow \forall\ i \in \mathbb{N} : a_i \in Fin(\{0, \dots, h\}) = Fin(h+1) = \mathcal{P}(h+1)$,

e tale insieme è finito perché insieme delle parti di un insieme finito. Ciò è assurdo, dunque $(Fin(\mathbb{N}), <_2)$ è un buon ordine.

OSSERVAZIONI E COMPLEMENTI SULLO STUDIO DI $\mathbb{R}$

OSSERVAZIONE

Possiamo notare come la costruzione dei reali sia stata sostanzialmente più complicata rispetto a quelle di $\mathbb{Z}$ e $\mathbb{Q}$. Infatti in questo caso si sta usando l'insieme delle parti, che determina dunque un "salto di cardinalità":

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0 \quad , \quad |\mathbb{R}| = 2^{\aleph_0} = c$$

OSSERVAZIONE

Per ogni $q \in \mathbb{Q}$, il seguente è un taglio di Dedekind:

$$X_q \overset{\text{def}}{=} \{ q' \in \mathbb{Q} \mid q' < q \}$$

Vi sono però tagli di Dedekind che non sono di quella forma. Consideriamo ad esempio:

$$X_{\sqrt{2}} \overset{\text{def}}{=} \{ q \in \mathbb{Q} \mid q \leq 0 \vee q^2 < 2 \}$$

Si ha:

- $1^2 = 1 < 2 \Rightarrow 1 \in X_{\sqrt{2}} \Rightarrow X_{\sqrt{2}} \neq \emptyset$;
- $3^2 = 9 > 2 \Rightarrow 3 \notin X_{\sqrt{2}} \Rightarrow X_{\sqrt{2}} \neq X$;
- $X_{\sqrt{2}}$ non ha massimo per densità di $\mathbb{Q}$;
- $X_{\sqrt{2}}$ è segmento iniziale per costruzione;
- $X_{\sqrt{2}}$ non è della forma X_k, $k \in \mathbb{Q}$. Se infatti così fosse, dovrebbe essere $k > 0$, $k^2 = 2$. Dunque:

$$k = \frac{p}{q} \Rightarrow k^2 = \frac{p^2}{q^2} = 2 \Rightarrow p^2 = 2q^2,$$

e ciò è assurdo per il Teorema fondamentale dell'aritmetica (unicità della fattorizzazione).

Ex. Sia $X \in \mathbb{R}$. Sia $\varepsilon > 0$ un razionale. Allora:

$\exists\, x \in X,\ y \notin X \ ,\ y - x < \varepsilon$

Siano $\xi \in X$, $\eta \notin X$, $m \in \mathbb{N}$ con $m > \frac{1}{\varepsilon}$ ($\mathbb{Q}$ è banalmente Archimedeo). Sia:

$$A = \{ k \in \mathbb{N} \mid \xi + \frac{k}{m} \notin X \}$$

Se $k > (\eta - \xi)m$, allora $\xi + \frac{k}{m} > \xi + \frac{(\eta - \xi)m}{m} = \eta \notin X$, da cui $A \neq \emptyset$. Allora esiste $\bar{m} = \min A > 0$.

Dunque:

$$x = \xi + \frac{m-1}{n} \in X, \quad y = \xi + \frac{m}{n} \notin X,$$

$$y - x = \frac{1}{n} < \varepsilon,$$

come voluto.

OSSERVAZIONE

Siano $q, q' \in \mathbb{Q}$. Allora: $X_q \leq X_{q'} \Leftrightarrow q \leq q'$.

Identificando allora ogni $q \in \mathbb{Q}$ con il suo taglio di Dedekind corrispondente $X_q \in \mathbb{R}$, si ha:

$$(\mathbb{Q}, \leq) \subseteq (\mathbb{R}, \leq),$$

e $\mathbb{Q}$ è dunque un sottoinsieme ordinato di $\mathbb{R}$.

OSSERVAZIONE

In generale, preso $(P, \leq)$ insieme denso, ordinato, e privo di massimo e minimo, possiamo considerare l'insieme $\tilde{P}$ dei suoi tagli di Dedekind: $(\tilde{P}, \leq)$ risulta un insieme ordinato e completo, avente un sottoinsieme denso isomorfo a P mediante l'identificazione canonica.

Ricordiamo ora che, dati $X, Y \in \mathbb{R}$, si definisce la SOMMA:

$$X + Y = \{ q + q' \mid q \in X, \ q' \in Y \}$$

Vogliamo dimostrare che $X + Y \in \mathbb{R}$. Ciò seguirà immediatamente dal lemma seguente.

LEMMA

Siano $a, x, y \in \mathbb{Q}$, con $a < x + y$. Allora:

$\exists \ x' < x, \ y' < y \ \ni' \ a = x' + y' \quad (x', y' \in \mathbb{Q})$

Dim.

Si ha:

$$a < x + y \Rightarrow a - x < y$$

Per densità di $\mathbb{Q}$:

$\exists \ y' \in \mathbb{Q} \ \ni' \ a - x < y' < y$

A questo punto:

$$a - x < y' \Rightarrow a - y' < x,\ a - y' \in \mathbb{Q},$$

da cui $a - y' \in X_x$, ovvia $a - y' = x'$ per $x' \in \mathbb{Q}$, $x' < x$.
Dunque la tesi, c.v.d.

I seguenti fatti sono ora evidenti:

- $X + Y \in \mathbb{R}$;
- $\forall\ q, q' \in \mathbb{Q}:\ X_q + X_{q'} = X_{q+q'}$

In particolare, per quanto riguarda l'ultima dimostrazione:

- $\forall\ x \in X_q,\ y \in X_{q'}:\ x < q,\ x' < q \Rightarrow x + y < q + q'$;
- $\forall\ t < q + q':\ t \in X_q + X_{q'}$ per il lemma.

Allora $X_q + X_{q'} = X_{q+q'}$. L'operazione di somma, dunque è coerente con quella di $\mathbb{Q}$.

OSSERVAZIONE

È banale notare che la somma in $\mathbb{R}$ appena definita è COMMUTATIVA e ASSOCIATIVA.

Prima di continuare, alcune osservazioni. Vogliamo dimostrare che $(\mathbb{R}, +)$ è un gruppo Abeliano: per quanto visto finora, resta solo da dimostrare che esiste l'elemento neutro, e per ogni elemento $X \in \mathbb{R}$ esiste l'opposto.

Definiamo:

$$\mathbb{O} \overset{def}{=} X_0 = \{\ q \in \mathbb{Q}\ |\ q < 0\}$$

Allora:

$$\forall\ q \in \mathbb{Q}:\ X_q + \mathbb{O} = X_q + X_0 = X_{q+0} = X_q,$$

dunque $\mathbb{O}$ è un "buon candidato" ad essere elemento neutro.
In effetti:

- $\forall\ q \in \mathbb{O}:\ q < 0 \Rightarrow (X + \mathbb{O}) \subseteq X \quad \forall\ X \in \mathbb{R}$;
- $\forall\ q \in X\ \exists\ m \in \mathbb{N}$ t.c. $q + \frac{1}{m} \in X \Rightarrow q = \left(q + \frac{1}{m}\right) + \left(-\frac{1}{m}\right) \in (X + \mathbb{O}) \Rightarrow$
  $\Rightarrow (X + \mathbb{O}) \supseteq X \quad \forall\ X \in \mathbb{R}$.

Allora $\mathbb{O}$ è l'elemento neutro di $(\mathbb{R}, +)$.

Per concludere:

$\forall\ X \in \mathbb{R}: \quad X + (-X) = \{ q - q' \mid q \in X,\ q' \notin X \}$

Dato che X è segmento iniziale, $q - q' < 0$ in ogni caso.
Dunque $X + (-X) \subseteq \mathbb{O}$.

L'esercizio svolto precedentemente, però, ci assicura che $\mathbb{O} \subseteq X + (-X)$, da cui $X + (-X) = \mathbb{O}\ \forall\ X \in \mathbb{R}$.

$(\mathbb{R}, +)$ è dunque un gruppo Abeliano.

Abbiamo poi definito il prodotto tra reali positivi. Se $X, Y > \mathbb{O}$ si ha:

$$X^+ = \{ x \in X \mid x \geq 0 \} \neq \emptyset, \quad Y^+ = \{ y \in Y \mid y \geq 0 \} \neq \emptyset,$$

e si definisce:

$$X \cdot Y = \{ x \cdot y \mid x \in X^+,\ y \in Y^+ \} \cup \{ q \in \mathbb{Q} \mid q \leq 0 \}$$

Ex. Siano $a, x, y \in \mathbb{Q}^+$, con $a < x \cdot y$. Allora $a = x' \cdot y'$ per qualche $0 < x' < x$, $0 < y' < y$.

Consideriamo:

$$q = \frac{a}{xy} = \frac{m}{n} < 1$$

Si può decomporre q in questo modo:

$$q_1 = \frac{2n}{2m-1} \qquad q_2 = \frac{2m-1}{2n}$$

$$q = q_1 \, q_2$$

Siano $x' = x \cdot q_1$, $y' = y \cdot q_2$. Allora si ha quanto voluto:

$$a = x' \cdot y',$$

$$0 < x' < x, \quad 0 < y' < y$$

Appare ora evidente che:

- se $X, Y \in \mathbb{R}$, $X, Y > \mathbb{O}$, allora $X \cdot Y \in \mathbb{R}$, $X \cdot Y > \mathbb{O}$;
- $\forall\ q, q' \in \mathbb{Q}: \ X_q \cdot X_{q'} = X_{q \cdot q'}$.

L'operazione, inoltre, è ASSOCIATIVA e COMMUTATIVA.

Si estende poi in questa maniera l'operazione a $\mathbb{R}$, in modo che resti commutativa e associativa:

- $X = \mathbb{O} \vee Y = \mathbb{O} \Rightarrow X \cdot Y \overset{def}{=} Y \cdot X = \mathbb{O}$;
- $X > \mathbb{O} \wedge Y < \mathbb{O} \Rightarrow X \cdot Y \overset{def}{=} -(X \cdot (-Y))$;
- $X < \mathbb{O} \wedge Y > \mathbb{O} \Rightarrow X \cdot Y \overset{def}{=} -((-X) \cdot Y)$;
- $X < \mathbb{O} \wedge Y < \mathbb{O} \Rightarrow X \cdot Y \overset{def}{=} (-X) \cdot (-Y)$.

LEMMA

Vale la PROPRIETÀ DISTRIBUTIVA

$\forall X, Y, Z \in \mathbb{R} : X(Y+Z) = X \cdot Y + X \cdot Z$

Dim.

È elementare notare che:

- $\forall k \in Y+Z : k = h_1 + h_2,\ h_1 \in Y,\ h_2 \in Z \Rightarrow$
  $\Rightarrow \forall x \in X : x \cdot k = x(h_1 + h_2) = x \cdot h_1 + x \cdot h_2$;
- $\forall h_1 \in Y, \forall h_2 \in Z : \forall x \in X : x \cdot h_1 + x \cdot h_2 =$
  $= x \cdot (h_1 + h_2) = x \cdot k,\ |\ k \in Y+Z$.

Allora si ottiene

$$\begin{cases} X(Y+Z) \subseteq X \cdot Y + X \cdot Z \\ X(Y+Z) \supseteq X \cdot Y + X \cdot Z \end{cases} \Rightarrow X(Y+Z) = X \cdot Y + X \cdot Z, \text{ c.v.d.}$$

LEMMA

Le operazioni di somma e prodotto sono coerenti con l'ordinamento:

$\forall X \leq Y \in \mathbb{R}, \forall Z \in \mathbb{R}, Z \geq \mathbb{O} : X + Y \leq Y + Z,\ X \cdot Z \leq Y \cdot Z$

Dim

La prima affermazione discende banalmente dal fatto che $X \subseteq Y$. Idem così per la seconda affermazione, c.v.d.

Possiamo allora definire l'INVERSO di un taglio $X > \mathbb{O}$:

- se $X = X_q$, $q \in \mathbb{Q}$, $\frac{1}{X} \overset{def}{=} X_{\frac{1}{q}}$;
- in caso contrario, $X \overset{def}{=} \left\{ \frac{1}{q} \,\middle|\, q \notin X \right\}$.

Definiamo ora:

$$\mathbb{I} \overset{def}{=} X_1 = \{ q \in \mathbb{Q} \mid q < 1 \}$$

Dimostriamo ora che $(\mathbb{R}^*, \cdot)$ è un gruppo Abeliano rispetto al prodotto, ove $\mathbb{R}^* \overset{def}{=} \mathbb{R} \setminus \mathbb{O}$

Si ha (studiamo il caso $X > \mathbb{O}$, si generalizza facilmente):

$$\forall X > \mathbb{O} \in \mathbb{R}^* \quad X \cdot \mathbb{I} = \{ x \cdot y \mid x \in X^+, y \in \mathbb{I}^+ \} \cup \{ q \in \mathbb{Q} \mid q \leq 0 \}$$

Allora:

$\forall y \in \mathbb{I}^+ : y < 1 \Rightarrow \forall x \in X^+, \forall y \in \mathbb{I}^+ : x \cdot y < x$,

da cui $X \cdot \mathbb{I} \subseteq X$.

Il contenimento opposto si ha in questo modo:

$\forall x \in X^+ : \exists n \in \mathbb{N}$ t.c. $x + \frac{1}{n} \in X^+ \Rightarrow \frac{xn+1}{n} \in X^+, \frac{xn}{xn+1} \in \mathbb{I}^+$,

$x = \frac{xn+1}{n} \cdot \frac{xn}{xn+1} \in X \cdot \mathbb{I} \Rightarrow X \subseteq X \cdot \mathbb{I}$

Dunque $\mathbb{I}$ è elemento neutro per il prodotto.

Si ha allora:

- i prodotti dei tagli sono coerenti con i prodotti tra razionali, da cui:

  $\forall q \in \mathbb{Q}^* : X_q \cdot X_{\frac{1}{q}} = X_{q(\frac{1}{q})} = \mathbb{I}$;

- supponiamo $X > \mathbb{O}$. Siano $x \in X$, $y \notin X$. Allora $y > x$, ossia $xy < 1$. Dunque:

$$X \cdot \frac{1}{X} \subseteq \mathbb{I}$$

Sia ora $q \in \mathbb{I}$. Si hanno due casi:

- $q \leq 0$. Allora, preso $y \notin X$, si ha $q \cdot y \leq 0 \Rightarrow q \cdot y \in X \Rightarrow$
  $\Rightarrow q = \frac{q \cdot y}{y} \in X \left(\frac{1}{X} \right)$;

- $q > 0$ (più precisamente $0 < q < 1$). Sia $a \in X$, $a > 0$.

  Allora, considerato l'insieme illimitato:

$$A = \{ a \cdot q^{-n} \mid n \in \mathbb{N} \},$$

  detto $h = \min\{ n \in \mathbb{N} \mid a \cdot q^{-n} \notin X \} > 0$. Dunque:

$$x = \frac{a}{q^{h-1}} \in X, \quad \frac{x}{q} = \frac{a}{q^h} \notin X \Rightarrow q = \frac{q^h}{a} \cdot \frac{a}{q^{h-1}} \in X \left(\frac{1}{X} \right)$$

Se $X < \mathbb{O}$, si ha:

$$\mathbb{I} = (-X) \left(\frac{1}{(-X)} \right) = (-X) \left(-\frac{1}{X} \right) = X \cdot \frac{1}{X}.$$

Abbiamo dunque introdotto completamente i REALI:

$$(\mathbb{R}, \leq, \mathbb{O}, \mathbb{I}, +, \cdot),$$

ove:

- $\mathbb{R} = \{ X \subseteq \mathbb{Q} \mid X$ è un Taglio di Dedekind $\}$;
- $X \leq Y \Leftrightarrow X \subseteq Y$;
- $\mathbb{O} = X_0$, $\mathbb{I} = X_1$.

TEOREMA

Il sistema dei reali $(\mathbb{R}, \leq, \mathbb{O}, \mathbb{I}, +, \cdot)$ è un campo ordinato completo.

Dim.

Discende da tutto ciò che è stato visto finora, c.v.d.

Rimane da dimostrare che $\mathbb{R}$ è unico a meno di isomorfismi. Per dimostrare ciò, dimostriamo prima un lemma.

LEMMA

Sia F un campo ordinato completo. Allora F contiene una "copia" di $\mathbb{Q}$, ovvero esiste $T \subseteq F$, $T \cong \mathbb{Q}$.

Dim.

Consideriamo 0_F e 1_F. Sia $(-1)_F$ tale che $(-1)_F + 1_F = 1_F + (-1_F) = 0_F$.

Definiamo (necessariamente char $F = 0$):

$$N_F = \underbrace{1_F + \dots + 1_F}_{n \text{ volte}}, \quad (-N)_F = \underbrace{(-1)_F + \dots + (-1)_F}_{n \text{ volte}}$$

Allora:

$$\begin{aligned} \varphi : \mathbb{Q} &\to F \\ \frac{n}{m} &\to \frac{N_F}{M_F} \end{aligned}$$

è iniettiva, da cui:

$$\mathbb{Q} \cong \varphi(\mathbb{Q}) = T \subseteq F, \text{ c.v.d.}$$

UNICITÀ DI $\mathbb{R}$

TEOREMA

Ogni campo ordinato completo è isomorfo a $(\mathbb{R}, \leq, \mathbb{Q}, \mathbb{I}, +, \cdot)$.

Dim.

Sia $\mathbb{F}$ un qualunque campo ordinato completo: allora, a meno di isomorfismo, $\mathbb{Q} \subseteq \mathbb{F}$.

PREMESSA

Denoteremo con $\leq_{\mathbb{R}}$ e $\leq_{\mathbb{F}}$ le due relazioni d'ordine (per $q, q' \in \mathbb{Q}$ scriveremo semplicemente $q \leq q'$ perché l'isomorfismo costruito nel paragrafo precedente è ordinato); denoteremo con $\sup_{\mathbb{R}}$ e $\sup_{\mathbb{F}}$ gli estremi superiori calcolati in $\mathbb{R}$ e $\mathbb{F}$ rispettivamente.

Nella dimostrazione eviteremo di dire "a meno di isomorfismo" laddove la cosa è evidente.

Se $X \in \mathbb{R}$ è un taglio di Dedekind, allora è ben definito $\sup_{\mathbb{F}} X$. Possiamo dunque definire:

$$\psi : \mathbb{R} \longrightarrow \mathbb{F}$$
$$X \longrightarrow \sup_{\mathbb{F}} X$$

La funzione preserva l'ordine, dunque è iniettiva:

$X < Y \Rightarrow \exists\, q \in Y \setminus X \Rightarrow \psi(X) = \sup_{\mathbb{F}} X \leq q < \sup_{\mathbb{F}} Y$

Sia ora $x \in \mathbb{F}$. Allora $\mathbb{F}_x = \{ q \in \mathbb{Q} \mid q <_{\mathbb{F}} x \}$ è un taglio di Dedekind, tale che (per densità di $\mathbb{Q}$):

$$x = \sup_{\mathbb{F}} \mathbb{F}_x = \psi(\mathbb{F}_x)$$

ψ è dunque suriettiva.

Se dunque dimostriamo che ψ è omomorfismo di campi, allora la dimostrazione è conclusa. Notiamo che, dato $X \in \mathbb{R}$, $X > 0$, si ha:

$$\psi(-X) = \sup_{\mathbb{F}} \{ q \in \mathbb{Q} \mid -q \notin X \} = -\inf_{\mathbb{F}} \{ q \in \mathbb{Q} \mid q \notin X \} =$$
$$= -\sup_{\mathbb{F}} \{ q \in \mathbb{Q} \mid q \in X \} = -\psi(X),$$

dunque si può considerare solo il caso di $X, Y > 0$.

Dobbiamo dimostrare che, dati $X, Y > 0$:

$$\psi(X+Y) = \psi(X) + \psi(Y), \quad \psi(X \cdot Y) = \psi(X) \cdot \psi(Y)$$

Siano:

$$\xi = \psi(X) = \sup_F X \quad , \quad \eta = \psi(Y) = \sup_F Y$$

Allora, se $x \in X$, $y \in Y$:

$$x \leq_F \xi \, , \, y \leq_F \eta \quad \Rightarrow \quad x + y \leq_F \xi + \eta \quad \Rightarrow \quad \psi(X+Y) \leq_F \psi(X) + \psi(Y)$$

Sia ora $a <_F \xi + \eta$: sia $\lambda = \frac{1}{2}(\xi + \eta - a) >_F 0$. Allora:

$\exists \; x \in X, \; y \in Y \; \ni' \; x >_F \xi - \lambda \, , \, y >_F \eta - \lambda \; \Rightarrow \; x + y >_F \xi + \eta - 2\lambda = a$

Allora:

$$\psi(X+Y) \geq_F \psi(X) + \psi(Y),$$

da cui la prima uguaglianza (in effetti questa dimostrazione è già generale).

Supponiamo ora che $X, Y > 0$. Allora:

$$\psi(X \cdot Y) = \sup_F \{ x \cdot y \mid x \in X \, , \, y \in Y \} \leq_F \xi \cdot \eta$$

Viceversa, fissiamo $a <_F \xi \eta$, $a >_F 0$. Per densità di $\mathbb{Q}$:

$\exists \; q \in \mathbb{Q} \; \ni' \; \frac{a}{\xi \cdot \eta} <_F q < 1$

Per un esercizio precedente $q = q_1 q_2$, con $q_1 < 1$, $q_2 < 1$.

Dato che:

$$\xi \cdot q_1 < \xi \quad , \quad \eta \cdot q_2 < \eta$$

si ha che:

$\exists \; x \in X \, , \, y \in Y \; \ni' \; x > \xi \cdot q_1 \, , \, y > \eta \cdot q_2$

Dunque:

$$x \cdot y >_F \xi \cdot \eta \cdot q_1 q_2 >_F \xi \cdot \eta \cdot \frac{a}{\xi \cdot \eta} = a,$$

da cui:

$$\psi(X \cdot Y) \geq_F \xi \cdot \eta \, , \; \text{c.v.d.}$$

ARCHIMEDEITÀ DI $\mathbb{R}$

TEOREMA

Sia $\mathbb{F}$ un qualunque campo ordinato. Le condizioni seguenti sono equivalenti:

- $\mathbb{F}$ è ARCHIMEDEO:
  $\forall x > 0 : (\forall \varepsilon > 0 \ \exists n \in \mathbb{N} \ni' n \cdot \varepsilon > x)$
- $\mathbb{Q}$ è denso in $\mathbb{F}$;
- non esistono INFINITESIMI $\delta \neq 0$, ossia elementi $\delta \neq 0$ tali che per ogni $n \in \mathbb{N}^+$ valga $-\frac{1}{n} < \delta < \frac{1}{n}$;
- $\mathbb{N}$ è illimitato in $\mathbb{F}$:
  $\forall x \in \mathbb{F} \ \exists n \in \mathbb{N} \ni' x < n$

Dim.

Dimostriamo la sequenza di implicazioni seguente:

$$1) \Rightarrow 2) \Rightarrow 3) \Rightarrow 4) \Rightarrow 1)$$

Siano dunque $0 < x < y$, $x, y \in \mathbb{F}$. Allora:

$\exists m \in \mathbb{N} \ni' m \cdot 1 > \frac{1}{y-x} \Leftrightarrow \frac{1}{m} < y - x$

Consideriamo ora:

$$A = \left\{ n \in \mathbb{N} \mid n \cdot \frac{1}{m} > x \right\}$$

Per l'archimedeità di $\mathbb{F}$, $A \neq \emptyset$: sia $n = \min A$. Allora $(n-1) \notin A$, da cui:

$$x < \frac{n}{m} = (n-1)\frac{1}{m} + \frac{1}{m} \leq x + \frac{1}{m} < x + (y-x) = y,$$

da cui $x < \frac{n}{m} < y$, $\frac{n}{m} \in \mathbb{Q}$.

Se $y < x < 0$, allora $0 < -x < -y$: determinata $q \in \mathbb{Q}$, con $-x < q < -y$, si ha $y < -q < x$, $-q \in \mathbb{Q}$.

Infine, se $x < 0 < y$, banalmente $0 \in \mathbb{Q}$.

Dunque $\mathbb{Q}$ è denso in $\mathbb{F}$.

Per assurdo sia ora $\delta \neq 0$ un infinitesimo. Senza perdere di generalità, a meno di cambiare segno, $\delta > 0$. Allora:

$\forall m, n \in \mathbb{N}^+ : \ \delta < \frac{1}{m} \Rightarrow 0 < \delta < \frac{n}{m}$,

da cui $\mathbb{Q}$ non è de[illegible] in $\mathbb{F}$, e ciò è assurdo.

Se ora $\mathbb{N}$ fosse limitato, esisterebbe $x \in F$ con $x > n$ per ogni $n \in \mathbb{N}$, da cui avremmo $\frac{1}{x} < \frac{1}{n}$ $\forall n \in \mathbb{N}^+$, assurdo.

Considerati ora $x > 0$, $\varepsilon > 0$, consideriamo $\frac{x}{\varepsilon}$:

$\exists n \in \mathbb{N}$ t.c. $n > \frac{x}{\varepsilon} \Rightarrow n \cdot \varepsilon > x$, c.v.d.

COROLLARIO

Se F è completo, allora tutte le condizioni dette finora sono verificate.

Dim.

Basta dimostrare che, se una delle quattro non vale (ad esempio 4)), allora F non è completo.

Sia $\mathbb{N}$ limitato in F. Se $b \in F$ è un maggiorante di $\mathbb{N}$:

$\forall n \in \mathbb{N}: n \leq b$

Allora:

$\forall n \in \mathbb{N}: n+1 \leq b \Rightarrow n \leq b-1$,

da cui $(b-1)$ è un maggiorante di $\mathbb{N}$. In sostanza, $\sup_F \mathbb{N}$ non esiste, dunque F non è completo, c.v.d.

TEOREMA DI CANTOR
SUGLI INSIEMI ORDINATI NUMERABILI

TEOREMA (SOLO ENUNCIATO) (DI CANTOR)

Se $(A, <)$ è un insieme ordinato numerabile, allora:

$\exists\, B \in \mathbb{Q}$ t.c. $(A, <) \cong B$

Vediamo qualche esempio. Determiniamo $B, C \subseteq \mathbb{Q}$ tali che:

$$B \cong \omega \oplus \omega \quad , \quad C \cong \omega \otimes \omega$$

Dobbiamo ricercare due insiemi $B_1, B_2 \subseteq \mathbb{Q}$ isomorfi a ω, uno "maggiore" dell'altro, nel senso che:

$\forall\, b_1 \in B_1,\ b_2 \in B_2 : b_1 < b_2$

Possiamo considerare:

$$B_1 = \left\{ 1 - \frac{1}{n} \;\middle|\; n \in \mathbb{N}^+ \right\}$$

$$B_2 = \left\{ 2 - \frac{1}{n} \;\middle|\; n \in \mathbb{N}^+ \right\}$$

Si ha $B = B_1 \cup B_2 \cong \omega \oplus \omega$. A questo punto, si ha:

$$C = \bigcup_{k \in \mathbb{N}} \left\{ k - \frac{1}{n} \;\middle|\; n \in \mathbb{N}^+ \right\} \cong \omega \otimes \omega$$

Per generare un sottoinsieme di $\mathbb{R}$ numerabile e isomorfo a $\omega \otimes \omega \otimes \omega$, potremmo applicare a ogni punto di C la funzione:

$$\begin{aligned} \phi : C &\to [0, 1[\\ x &\mapsto \frac{2}{\pi} \operatorname{arctg} x \end{aligned}$$

Sia $C_0 = \phi(C)$, e sia $C_k = k + \phi(C)\ \forall\, k \in \mathbb{N}^+$.

Allora:

$$D = \bigcup_{k \in \mathbb{N}} C_k \cong \omega \otimes \omega \otimes \omega.$$

ORDINALI

Un elemento α si dice ORDINALE se:

- $(\alpha, \in)$ è un buon ordine;
- α è TRANSITIVO, ossia:
  $\forall x, \forall y : y \in x \in \alpha \Rightarrow y \in \alpha$

Ad esempio:

- $\{\emptyset, \{\emptyset\}\}$ è transitivo;
- $\{\{\emptyset\}\}$ non è transitivo: $\emptyset \notin \{\{\emptyset\}\}$.

Con la definizione data, ogni naturale, per costruzione, è un ordinale.

I numeri naturali, dunque, non sono solo i rappresentanti canonici dei cardinali finiti, ma sono anche i rappresentanti canonici dei buoni ordini finiti.
Anche ω è un ordinale: esso è il più piccolo, tra quelli infiniti, ossia ha il tipo d'ordine minimo tra gli ordinali infiniti: ciò segue dal fatto che ogni segmento iniziale di ω è finito.

Dimostreremo ora i seguenti fatti:

- due ordinali isomorfi sono uguali;
- ogni buon ordine è isomorfo ad un ordinale.

Un insieme T si dice INSIEMISTICAMENTE TRANSITIVO se $x \in y \in T \Rightarrow x \in T$ ossia se $x \in T \Rightarrow x \subseteq T$.
D'ora in poi, salvo avviso contrario, $\alpha, \beta, \gamma, \delta$ saranno ordinali.

PROPOSIZIONE
Vale quanto segue (sia α un ordinale)

- $\alpha \notin \alpha$;
- $x \in \alpha \Rightarrow x$ è un ordinale;
- $\alpha \cup \{\alpha\}$ è un ordinale.

Dim.

Se ciò fosse falso, ossia varrebbe $\alpha \in \alpha$, si avrebbe che α è minore di sé stesso in un insieme bene ordinato, e ciò è assurdo.

Dato che α è transitivo (insiemisticamente):

$$x \in \alpha \Rightarrow x \subseteq \alpha$$

Allora x è bene ordinato con la relazione indotta.

Vogliamo dimostrare che x è un insieme transitivo.

Sia $t \in s \in x$. Si ha:

$$s \in x \in \alpha \Rightarrow s \in \alpha$$

$$t \in s \in \alpha \Rightarrow t \in \alpha$$

Dunque $t, s, x \in \alpha$.

Per la transitività dell'ordine di $(\alpha, \in)$:

$$t \in s \in x \Rightarrow t \in x$$

Rimane ora da vedere l'ultima proprietà. In effetti, $\alpha \cup \{\alpha\}$ è un buon ordine, isomorfo a $\alpha \oplus \{*\}$.

Inoltre si verifica direttamente che $\alpha \cup \{\alpha\}$ è un insieme transitivo, c.v.d.

TEOREMA

Se $\alpha \simeq \beta$ sono ordinali isomorfi, allora $\alpha = \beta$.

Dim.

Vogliamo dimostrare che, se $\varphi: \alpha \to \beta$ è un isomorfismo, allora $\varphi \equiv \mathrm{Id}$.

Per assurdo, sia $\varphi \not\equiv \mathrm{Id}$. Sia:

$$\gamma = \min \{x \in \alpha \mid \varphi(x) \neq x\}$$

Consideriamo l'isomorfismo:

$$\varphi|_{\alpha_\gamma} : \alpha_\gamma \longrightarrow \beta_{\varphi(\gamma)}$$

OSSERVAZIONE

Dimostreremo più avanti che $(\alpha, \in)$ buon ordine è un ordinale se e solo se:

$$\forall a \in \alpha : \alpha_a = a$$

Dato che $\varphi|_{\alpha_\gamma}$ è l'identità, usando l'osservazione si ha

$$\alpha_\gamma = \gamma, \quad \beta_{\gamma(\psi)} = \psi(\gamma), \quad \alpha_\gamma = \beta_{\psi(\gamma)} \Rightarrow$$
$$\Rightarrow \gamma = \psi(\gamma),$$

una contraddizione, c.v.d.

Rimane da dimostrare il seguente lemma.

LEMMA

Sia $(\alpha, \in)$ un buon ordine. Allora esso è un ordinale se e solo se:

$\forall a \in \alpha : a = \alpha_a$

Dim.

Sia α un ordinale. Sia $\alpha_a \subsetneq \alpha$ un segmento iniziale. Allora:

$\forall x \in \alpha_a : x \in a \Rightarrow \alpha_a \subseteq a$

D'altra parte, $a = \min(\alpha \setminus \alpha_a)$. Dunque:

$\forall x \in \alpha \setminus \alpha_a : x \notin a$,

da cui:

$\emptyset = (\alpha \setminus \alpha_a) \cap a = (\alpha \cap a) \setminus \alpha_a = a \setminus \alpha_a \Rightarrow a \subseteq \alpha_a$,

da cui $a = \alpha_a$.

Viceversa, se vale la condizione sopra esposta:

$\forall x \in \alpha : x = \alpha_x \subseteq \alpha$,

dunque α è transitivo, dunque un ordinale, c.v.d.

TRICOTOMIA DEGLI ORDINALI

TEOREMA (SOLO ENUNCIATO)

Se α, β sono ordinali, allora vale una e una sola delle seguenti proprietà:

- $\alpha = \beta$, ossia $\alpha \cong \beta$;
- $\alpha \in \beta$, ossia esiste $\gamma \in \beta$ t.c. $\alpha \cong \beta_\gamma = \gamma \Rightarrow \alpha = \gamma \in \beta$;
- $\beta \in \alpha$, ossia esiste $\delta \in \alpha$ t.c. $\beta \cong \alpha_\delta = \delta \Rightarrow \beta = \delta \in \alpha$.

Ex. Siano α, β ordinali.

Sono proprietà equivalenti:

- $\alpha \in \beta$;
- $\alpha \subsetneq \beta$;
- α è un segmento iniziale proprio di β.

Chiaramente 1) $\Rightarrow$ 3) per transitività degli ordinali, e per la tricotomia degli ordinali. Infatti:

$$\alpha \in \beta \Rightarrow \exists \gamma \in \beta \text{ t.c. } \alpha \cong \beta_\gamma = \gamma \Rightarrow \alpha = \gamma \in \beta,$$

e chiaramente $\alpha \neq \beta$ perché non può essere $\beta \cong \beta_\gamma$.

In particolare, 1) $\Rightarrow$ 2) e 3) $\Rightarrow$ 2).

Dimostriamo che 3) $\Rightarrow$ 1). Sia α un segmento iniziale proprio di β. Allora:

$\exists \gamma \in \beta$ t.c. $\alpha = \gamma \in \beta \Rightarrow \alpha \in \beta$,

ossia la 1)

Resta da dimostrare che 2) $\Rightarrow$ 1), ad esempio.

Sia $\alpha \subsetneq \beta$. Allora $\beta \setminus \alpha$ è non vuoto, dunque esiste $x = \min(\beta \setminus \alpha)$. Per definizione:

$\forall y \in \beta \setminus \alpha : y \notin x$

Dunque:

$$\emptyset = (\beta \setminus \alpha) \cap x = (\beta \cap x) \setminus \alpha = x \setminus \alpha \Rightarrow x \subseteq \alpha$$

Sia ora $z \in \alpha$: allora $z \in \beta$, e per ordine totale, si ha $z = x$, o $z \in x$, o $x \in z$. Dato che $x \notin \alpha$, necessariamente $z \in x$, da cui $\alpha \subseteq x$, da cui $\alpha = x \in \beta$.

COMPLEMENTI VARI

PROPOSIZIONE

Sia X un insieme di ordinali.
Allora X è un ordinale se e solo se X è un insieme transitivo.

Dim.
Un'implicazione è ovvia, e discende direttamente dalla definizione di ordinale.
Per l'altra implicazione, X è sicuramente un insieme totalmente ordinato; ciò discende dalla tricotomia degli ordinali.
Resta da vedere che ogni sottoinsieme non vuoto ha minimo.
A tal proposito, è utile il seguente esercizio.

OSSERVAZIONE

Sia $X \neq \emptyset$ un insieme di ordinali. Allora $\xi = \bigcap_{x \in X} x = \min X$ è un ordinale.

Sia $m \in n \in \xi$. Allora:
$\forall x \in X : m \in n \in x \Rightarrow m \in x$,
da cui $m \in \xi$. Dunque ξ è transitivo.

Che sia un buon ordine, è banale: chiaramente esso è totalmente ordinato, e in più, se $D \subseteq \xi$, $D \neq \emptyset$, allora $D \subseteq x \ \forall x \in X$, da cui esiste $\lambda = \min D \in \xi$.

Rimane da dimostrare che $\xi \in X$. Sia $\Xi = \xi \cup \{\xi\}$.
Dato che $\bigcap_{x \in X} x = \xi \in \Xi$, per la tricotomia dei buoni ordini:
$\exists\, \bar{x} \in X$ t.c. $\bar{x} \in \Xi$
I casi sono due:

$$\bar{x} \in \xi \quad \vee \quad \bar{x} = \xi$$

Se $\bar{x} \in \xi$, allora $\bar{x} \subsetneq \xi$, assurdo. Allora $\bar{x} = \xi \in X$.

OSSERVAZIONE

Dimostreremo che, se $X \neq \emptyset$ è un insieme di ordinali:

$$\eta = \bigcup_{x \in X} x = \sup X$$

La dimostrazione è conclusa, c.v.d.

Gli ordinali sono di tre tipi:

- 0;
- SUCCESSORI: ordinali del tipo $\beta \cup \{\beta\}$, con β ordinale;
- LIMITE, senza massimo.

LEMMA

Sia $\alpha \neq 0$ un ordinale avente massimo β. Allora:

$$\alpha = \beta \cup \{\beta\}$$

Dim.

Se β è il massimo di α, allora $\beta \in \alpha \Rightarrow \beta \subseteq \alpha$, da cui $\beta \cup \{\beta\} \subseteq \alpha$.

Se fosse $\beta \cup \{\beta\} \subsetneq \alpha$, sarebbe $\beta \cup \{\beta\} \in \alpha$, con $\beta \in \beta \cup \{\beta\}$. Dunque β non sarebbe il massimo.

Dunque $\alpha = \beta \cup \{\beta\}$, c.v.d.

OSSERVAZIONE

Se $X \neq \emptyset$ è un insieme di ordinali, allora $\eta = \bigcup_{x \in X} x = \sup X$ è un ordinale.

Che η sia ben ordinato, è ovvio. Che sia anche $\sup X = \eta$ è ovvio.

Resta da vedere la transitività. Si ha:

$$x \in \eta \Rightarrow \exists\, z \in X \ni' x \in z \Rightarrow \exists\, z \in X \ni' x \subseteq z \Rightarrow x \subseteq \eta,$$

e la dimostrazione è conclusa.

ESISTENZA DEGLI ORDINALI

TEOREMA

Sia $(A, <)$ un buon ordine. Allora esiste un ordinale γ tale che $(A, <) \cong (\gamma, \in)$.

Dim.

Siano:

$$X = \{a \in A \mid \exists\, \alpha \text{ ordinale} : A_a \cong \alpha\}$$
$$Y = \{\alpha \text{ ordinale} \mid \exists\, a \in A : A_a \cong \alpha\}$$

Sia $f : X \to Y$ una funzione tale che $f(a)$ è l'unico ordinale α tale che $A_a \cong \alpha$.

Prima di continuare, Y è un insieme? Per ora non lo giustifichiamo: dimostreremo che Y è un insieme, usando un assioma non ancora visto, l'ASSIOMA DI RIMPIAZZAMENTO.

f è per costruzione suriettiva.

Rimangono da verificare due proprietà che dimostreremo più avanti:

- $a' < a \in X \Rightarrow a' \in X \wedge f(a') \in f(a)$, ossia X è un segmento iniziale di A;
- $\beta \in f(a) \Rightarrow \exists\, a' \in X$ t.c. $f(a') = \beta$, ossia:
$$\beta \in f(a) \in Y \Rightarrow \beta \in Y,$$
ossia Y è transitivo.

Se queste valgono, allora:

- X è un segmento iniziale di A;
- Y è un ordinale, perché è un insieme transitivo di ordinali;
- f preserva l'ordine, dunque $f : X \to Y$ è un isomorfismo.

Infine $X = A$ (ossia la tesi) altrimenti, se esistesse $a \in A$ tale che $X = A_a$, ma dall'esistenza di $f : X \to Y$, con Y ordinale, avremmo $a \in X = A_a$, un assurdo.

Allora:

$$f : X \to A \to Y$$

è un isomorfismo tra A e l'ordinale Y.

Rimangono da dimostrare le due proprietà. Dunque:

- se $a \in X$, $A_a \cong \alpha$, con α ordinale. Se $a' < a$, allora $A_{a'}$ è segmento iniziale di A_a, da cui, se $\psi : A_a \to \alpha$ è isomorfismo, $\psi(A_{a'})$ è segmento iniziale di α, e dato che α è ordinale, si ha allora:

$$\alpha_{\psi(a')} = \psi(A_{a'}) = \psi(a') \in \alpha,$$

e un elemento di un ordinale è un ordinale, da cui $\psi(A_{a'})$ è un ordinale e dunque $a' \in X$.

Sia $f(a') = \beta$. Dobbiamo dimostrare che $\beta \in \alpha$.

Non può essere $\beta = \alpha$, altrimenti sarebbe $A_a \cong A_{a'}$, assurdo. Se $\alpha \in \beta$, allora A_a è segmento iniziale di $A_{a'}$, assurdo perché $a' \in A_a \setminus A_{a'}$. Dunque $f(a') \in f(a)$;

- per ipotesi $A_a \cong f(a)$, ossia esiste un isomorfismo ordinato:

$$\varphi : f(a) = \alpha \to A_a$$

Sia $a' = \varphi(\beta)$: allora $a' < a$.

Dato che l'isomorfismo è ordinato:

$$\varphi|_{\alpha_\beta} : \alpha_\beta = \beta \to A_{a'}$$

è un isomorfismo. Allora

$\exists\, a' \in X$ t.c. $A_{a'} \cong \beta \Rightarrow f(a') = \beta$, c.v.d.

PARADOSSO DI BURALI-FORTI

TEOREMA

Non esiste l'insieme di tutti gli ordinali:

$$Ord \overset{def}{=} \{ \alpha \mid \alpha \text{ è ordinale} \}$$

Dim

Se Ord fosse un insieme, sarebbe un ordinale.

Infatti:

- $\forall\ X \subseteq Ord,\ X \neq \emptyset :\ \xi = \bigcap_{x \in X} x = \min X \in Ord$, dunque Ord è ben ordinato (l'ordine totale deriva dalla tricotomia);
- elementi di ordinali sono ordinali, da cui Ord è transitivo.

Allora sarebbe $Ord \in Ord$, assurdo per un qualsiasi ordinale, c.v.d.

TEORIA DELLE CLASSI
(BERNAYS - VON NEUMANN)

Abbiamo già visto alcune collezioni di elementi che non possono essere insiemi:

- l'insieme di Russell
$$R = \{x \mid x \notin x\};$$
- l'insieme di tutti gli insiemi:
$$V = \{x \mid x = x\};$$
- l'insieme di tutti gli ordinali:
$$Ord = \{\alpha \mid \alpha \text{ è ordinale}\}$$

Dato che tali collezioni possono a volte essere utili, si dà loro il nome di CLASSI.
Intuitivamente, una CLASSE è una collezione di elementi del tipo:
$$C = \{x \mid \varphi(x)\}$$

Vi sono classi che sono anche insiemi (ogni insieme è, in particolare, una classe), ma vi sono anche classi che non sono insiemi (ad esempio quelle citate sopra), e che perciò sono dette CLASSI PROPRIE. Nelle formule, denoteremo le classi con lettere maiuscole, e gli insiemi con lettere minuscole.
Si può parlare allora di TEORIA DELLE CLASSI: in tale teoria, tutti gli oggetti matematici sono classi.
Per definizione, inoltre, gli elementi delle classi si dicono INSIEMI.

Per quanto riguarda gli assiomi, quelli sugli insiemi corrispondono a quelli già visti, senza nessuna modifica.
A questi vanno aggiunti alcuni ASSIOMI SULLE CLASSI:

- (ESTENSIONALITÀ)
  Due classi sono uguali se e solo se hanno gli stessi elementi;

• (COMPRENSIONE o ASTRAZIONE)
Per ogni formula φ dove si quantificano solo insiemi, e per ogni $i = 1, \dots, n$ A_i è una classe, esiste la seguente classe:

$$C = \{ x \mid \varphi(x, A_1, \dots, A_n) \}$$

(ove x è un insieme);

• (SOTTOINSIEME)
Se A è una classe e b è un insieme, allora $A \cap b$ è un insieme (equivalentemente, sottoclassi di insiemi sono insiemi).

OSSERVAZIONE
Se A e B sono classi, allora:

- $A \cup B = \{ x \mid x \in A \vee x \in B \}$ è una classe;
- $A \cap B = \{ x \mid x \in A \wedge x \in B \}$ è una classe;
- $A \setminus B = \{ x \mid x \in A \wedge \neg(x \in B) \}$ è una classe.

OSSERVAZIONE
Se $A = \{ x \mid \varphi(x) \}$ e b è un insieme, allora:

$$A \cap b = \{ x \in b \mid \varphi(x) \}$$

è un insieme.
Dunque l'assioma del sottoinsieme implica lo schema di separazione.

Facciamo ora un esempio. Sia $a \neq \emptyset$ un insieme.
Consideriamo:

$$\Lambda_a \overset{\text{def}}{=} \{ b \mid |a| = |b| \},$$

la CLASSE DI EQUIPOTENZA di A.
Essa è una CLASSE PROPRIA: se infatti fosse un insieme, per l'assioma dell'unione anche $\bigcup \Lambda_a$ sarebbe un insieme:

$$\bigcup \Lambda_a = \{ y \mid \exists x \in \Lambda_a \text{ t.c. } y \in x \} =$$
$$= \{ y \mid \exists |x| = |a| \text{ t.c. } y \in x \}$$

Si può dimostrare che si ha:

$$\bigcup A_a = V,$$

da cui l'insieme di tutti gli insiemi sarebbe un insieme, e ciò è assurdo.

Sia $a \neq \emptyset$ un insieme. Allora la seguente è una classe propria:

$$C_a = \{ x \mid a \in x \}$$

Anche la seguente è una classe propria:

$$OP = \{ x \mid \exists\, y, z \ni' x = (y, z) \}$$

Torniamo alla discussione precedente: vogliamo dimostrare che:

$$\bigcup A_a = V$$

Sia x un insieme. Sia $* \in a$ un elemento qualsiasi ($a \neq \emptyset$). Sia:

$$b = (a \setminus \{*\}) \cup \{x\}$$

Allora:

$$x \in b, \quad |b| = |a|$$

Allora $x \in \bigcup A_a$. Per l'arbitrarietà di x, $\bigcup A_a = V$.

RELAZIONE - CLASSE E FUNZIONE - CLASSE

Si dice RELAZIONE - CLASSE una classe i cui elementi sono coppie ordinate.

Se tale relazione - classe è univoca, essa è una FUNZIONE - CLASSE. Una FUNZIONE - CLASSE è una particolare classe F tale che i suoi elementi sono coppie ordinate, e inoltre:

$$(x, y), (x, y') \in F \Rightarrow y = y'$$

Si definisce allora:

$$\mathrm{Dom}\, F \overset{def}{=} \{ x \mid \exists\, y \ \ni' (x, y) \in F \}$$

Dom F è una classe. Per unicità, $F(x)$ denota l'unico elemento y tale che $(x, y) \in F$.

Alcuni esempi di funzioni - classe sono:

- $F_1(x) = \{x\}$;
- $F_2(x) = \mathcal{P}(x)$.
- $F_3 = \{ (x, y) \mid x = (A, <)$ è un buon ordine $\wedge$ $\wedge\ y$ è ordinale $\wedge\ x \simeq y \}$

  Questa è una funzione - classe il cui dominio è la classe degli insiemi bene ordinati.

Tutte queste sono classi proprie: un'altra classe propria è, ad esempio, $\mathrm{Fin} = \{ x \mid x$ è finito $\}$

Ex. Sia F una funzione - classe iniettiva, e sia C una classe propria inclusa in Dom F. Allora:

$$F[C] \overset{def}{=} \{ F(c) \mid c \in C \} = \{ x \mid \exists\, c \in C \ \ni' (c, x) \in F \}$$

è una classe (evidente), ma è una classe propria.

Supponiamo infatti che $F[C]$ non sia solamente una classe, ma anche un insieme.

Per ipotesi:

$$(x, y), (x, y') \in F \Rightarrow y = y'$$

Per iniettività di F:

$$(x, y), (x', y) \in F \Rightarrow x = x'$$

Allora la classe delle coppie ordinate "invertite" con secondo elemento in $\mathrm{Dom}\, F$ è una funzione-classe:

$$F^{-1} = \{ (y, x) \mid (x, y) \in F,\ x \in \mathrm{Dom}\, F \}$$

Chiaramente $\mathrm{Dom}\, F^{-1} = F[C]$ è un insieme. Inoltre:

$$C = F^{-1}[F[C]]$$

Allora, per l'ASSIOMA DI RIMPIAZZAMENTO (esposto al prossimo paragrafo), C è un insieme. Ciò è assurdo.

ASSIOMA DI RIMPIAZZAMENTO

ASSIOMA (DI RIMPIAZZAMENTO)
Sia F una funzione - classe, e sia $b \subseteq \mathrm{Dom}\, F$ un insieme. Allora anche
$$F[b] \stackrel{\text{def}}{=} \{ F(x) \mid x \in b \}$$
è un insieme.

Con questo assioma, possiamo completare una dimostrazione lasciata incompleta. Nel Teorema di esistenza degli ordinali, abbiamo supposto che:
$$Y = \{ \alpha \text{ ordinale} \mid \exists a \in A \ni' A_a \cong \alpha \}$$
fosse un insieme.
Ciò possiamo giustificarlo, considerando la funzione - classe F_3 enunciata nel precedente paragrafo, e l'insieme (per lo schema di separazione):
$$b = \{ A_a \in \mathcal{P}(A) \mid a \in A \}$$
(ricordando che A era un buon ordine).

ORDINALE NON NUMERABILE

Tutti gli ordinali visti finora avevano cardinalità al più numerabile. Vogliamo ora dimostrare che:

$$\omega_1 \overset{\text{def}}{=} \{ \alpha \text{ ordinale} \mid |\alpha| \leq |\omega| \}$$

è il più piccolo ordinale avente cardinalità non numerabile (più che numerabile).

Per dimostrarlo, iniziamo considerando l'insieme $T \subseteq P(\omega) \times P(\omega \times \omega)$ così definito:

$$T \overset{\text{def}}{=} \{ (A, <) \mid A \subseteq \omega \text{ , } (A, <) \text{ è buon ordine} \}$$

Consideriamo ancora una volta:

$$F_3 = \{ (x, y) \mid \text{"} x \text{ è buon ordine"} \wedge \text{"} y \text{ è ordinale"} \wedge x \cong y \}$$

Vogliamo dimostrare che

$$F_3 [T] = \omega_1$$

Il primo contenimento è banale: se $A \subseteq \omega$, e $\alpha \cong (A, <)$, allora necessariamente $|\alpha| \leq |\omega|$, da cui $F_3 [T] \subseteq \omega_1$.

L'altro contenimento è più delicato. Se $|\alpha| \leq |\omega|$, consideriamo:

$$\theta : \alpha \to \omega$$

iniettiva.

Definiamo $A \overset{\text{def}}{=} \operatorname{Im} \theta \subseteq \omega$, e:

$$\theta(\gamma) <_A \theta(\gamma') \overset{\text{def}}{\Leftrightarrow} \gamma \in \gamma'$$

Allora:

$$(A, <_A) \cong (\alpha, \in),$$

da cui $F_3 ((A, <_A)) = \alpha$.

Allora, per l'assioma del rimpiazzamento ω_1 è un insieme.

Dimostriamo ora che ω_1 è un ordinale.

In effetti, ω_1 è un insieme transitivo di ordinali.
Infatti, se

$$\beta \in \alpha \in \omega_1,$$

allora:

$$(\beta \in \alpha \Leftrightarrow \beta \subsetneq \alpha) \Rightarrow (|\beta| \leq |\alpha| \leq |\omega|),$$

da cui:

$$\beta \in \omega_1$$

Allora ω_1 è un ordinale.

Chiaramente $|\omega_1| \neq |\omega|$, altrimenti sarebbe, da definizione, $\omega_1 \in \omega_1$, assurdo per un qualsiasi ordinale. Per la tricotomia degli ordinali, allora:

$$|\omega_1| > |\omega|$$

Se ora β è un ordinale non numerabile, allora:
$\forall\ \alpha$ ordinale, $|\alpha| \leq |\omega| : \alpha \in \beta$,
da cui:

$$\omega_1 \subseteq \beta$$

La trattazione è ora completa.

FUNZIONE DI HARTOGS

Dato a insieme, si definisce:

$$H(a) = \{ \alpha \text{ è ordinale} \mid |\alpha| \leq |a| \}$$

Ad esempio:

$$\omega_1 = H(\omega)$$

Dato a insieme, si può dimostrare che:

- $H(a)$ è un insieme;
- $H(a)$ è un ordinale;
- $|H(a)| \not\leq |a|$, ossia non esiste $f : H(a) \to a$ iniettiva.

La dimostrazione ricalca quella del paragrafo precedente.

Definiamo:

$$T_a \subseteq \mathcal{P}(a) \times \mathcal{P}(a \times a)$$

$$T_a \overset{def}{=} \{ (A, <) \mid (A, <) \text{ è un buon ordine}, A \subseteq a \}$$

Consideriamo F_3 come prima. Si ha:

- se $A \subseteq a$, e $(\alpha, \in) \cong (A, <)$, allora $|\alpha| \leq |a|$. Allora: $F_3[T_a] \subseteq H(a)$;
- se $|\alpha| \leq |a|$, sia $\vartheta : \alpha \to a$ iniettiva. Sia $A = \operatorname{Im}\vartheta \subseteq a$, e definiamo:

$$\vartheta(\gamma) <_A \vartheta(\gamma') \overset{def}{\iff} \gamma \in \gamma'$$

Allora banalmente:

$$(\alpha, \in) \cong (A, <_A),$$

da cui $F_3[T_a] \supseteq H(a)$.

Allora:

$$H(a) = F_3[T_a],$$

e per l'assioma di rimpiazzamento, $H(a)$ è un insieme di ordinali, ed è transitivo:

$$\beta \in \alpha \in H(a) \Rightarrow \beta \subseteq \alpha \in H(a) \Rightarrow$$
$$\Rightarrow |\beta| \leq |\alpha| \leq |a| \Rightarrow |\beta| \leq |a| \Rightarrow \beta \in H(a)$$

Essendo transitivo, $H(a)$ è un ordinale.

A questo punto, se fosse $\|H(a)\| \leq |a|$, sarebbe:

$$H(a) \in H(a),$$

assurdo.

FORME EQUIVALENTI DELL'ASSIOMA DELLA SCELTA

Enunciamo subito alcune proposizioni.

LEMMA (DI ZORN) (SOLO ENUNCIATO)

Se $(P, \leq)$ è un insieme non vuoto su cui è definita una relazione d'ordine parziale tale che ogni sua catena (ossia ogni suo sottoinsieme totalmente ordinato in P) ammette un maggiorante p (ossia $\forall c \in C : c \leq p$), allora esistono elementi massimali (ossia $\exists \tilde{p} \in P$ tale che non esistono $q \in P$ con $q > \tilde{p}$).

TEOREMA (DI ZERMELO) (SOLO ENUNCIATO)

Ogni insieme X ammette un buon ordine.

TEOREMA

Sono equivalenti:

- l'assioma della scelta;
- il lemma di Zorn;
- il teorema di Zermelo;
- la confrontabilità delle cardinalità:
  $\forall A, B : |A| \leq |B| \vee |B| \leq |A|$
- la seguente uguaglianza, valida per ogni insieme infinito A:

$$|A \times A| = |A|.$$

Dim.

Dimostriamo che l'assioma della scelta implica il lemma di Zorn.

Sia dunque $(P, \leq)$ un insieme parzialmente ordinato, tale che ogni catena ascendente ammette maggioranti.

Fissiamo:

$$f : \mathcal{P}(P) \setminus \{\emptyset\} \to P$$
$$f(A) \in A \quad \forall A \in \mathcal{P}(P) \setminus \{\emptyset\}$$

funzione di scelta.

PREMESSA

Sia $p_0 = f(P)$: se p_0 è massimale abbiamo finito, altrimenti sia $p_1 = f(\{p \in P \mid p > p_0\})$ (ove $\{p \in P \mid p > p_0\} \neq \emptyset$). Chiaramente si ha $p_1 > p_0$. Se p_1 è massimale, abbiamo finito, altrimenti definiamo $p_2 = f(\{p \in P \mid p > p_1,\ p > p_0\})$, e così via.

Resta così definita una catena ascendente:

$$p_0 < p_1 < p_2 < \dots < p_n < \dots < p_\omega < \dots,$$

con:

$$p_\omega = f(\{p \in P \mid p > p_n \ \forall n \in \mathbb{N}\})$$

Sia $A = \{p_0 < p_1 < p_2 < \dots\}$. A si dice f-CATENA se:

- A è bene ordinato;
- per ogni $a \in A$, $a = f(\{p \in P \mid p > x \ \forall x \in A_a\})$.

OSSERVAZIONE

Notiamo che $A = \{a\}$ singoletto è una f-catena se e solo se $a = f(P)$.

Una freccia è banale; l'altra si ottiene dalla definizione:

$$a = f(\{p \in P \mid p > x \ \forall x \in A_a\}) = f(P),$$

perché A_a è vuoto, dunque ogni $p \in P$ soddisfa la disuguaglianza.

LEMMA

Se A, B sono due f-catene, allora $A \subseteq B$ o $B \subseteq A$.

Dim.

Dato che A, B sono buoni ordini, per la tricotomia dei buoni ordini esiste, ad esempio, $\psi: A \xrightarrow{\sim} B_b$ (negli altri casi la dimostrazione è analoga). Vogliamo dimostrare che $\psi = \mathrm{id}$, ossia $A = B_b$ (ossia $A \subseteq B$).

Supponiamo per assurdo che ciò non sia vero. Sia:

$$a = \min\{x \in A \mid \psi(x) \neq x\}$$

Allora $\psi(x) = x$ per ogni $x \in A_a$. Dunque:

$$\psi|_{A_a} = Id|_{A_a} : A_a \xrightarrow{\sim} A_a = B_{\psi(a)}$$

Siccome A e B sono f-catene:

$$a = f(\{p \in P \mid p > x \ \forall x \in A_a\})$$
$$\psi(a) = f(\{p \in P \mid p > y \ \forall y \in B_{\psi(a)}\}),$$

da cui è assurdo perché $\psi(a) = a$ per definizione, mentre avevamo supposto $\psi(a) \neq a$, c.v.d.

Allora:

$$\mathcal{F} = \{A \subseteq P \mid A \text{ è } f\text{-catena}\}$$

è una famiglia di buoni ordini che sono uno segmento iniziale dell'altro, dunque:

$$C = \bigcup_{A \in \mathcal{F}} A$$

è un buon ordine.
Si può verificare che C è una f-catena (lo faremo alla fine della dimostrazione): chiaramente C è la f-catena MASSIMA:
$\forall A \in \mathcal{F} : A \subseteq C$
Essa ammette un maggiorante $\tilde{p}$: si può dimostrare (e lo faremo) che $\tilde{p}$ è un elemento massimale per P.

Dimostriamo ora che il lemma di Zorn implica la proprietà espressa per ultima:
$$|A \times A| = |A|$$

LEMMA
Se A è infinito, allora $|\mathbb{N}| \leq |A|$.

Dim.
Sia:
$$P = \{f : S \to A \mid f \text{ è iniettiva}, S \subseteq \mathbb{N},\ S \text{ è segmento iniziale di } \mathbb{N}\}$$

LEMMA (SOLO ENUNCIATO)
$(P, \leq)$ soddisfa le ipotesi del lemma di Zorn.

Dunque esiste $\varphi : S \to A$, $\varphi \in P$ elemento massimale.

Ma allora $S = \mathbb{N}$ altrimenti, se fosse:

$$\varphi : [1, n] \to A,$$

per $n \in \mathbb{N}$, esisterebbe $\tilde{a} \notin \operatorname{Im} \varphi$ (perché $[1, n]$ è finito, A è infinito). Dunque sarebbe:

$$\tilde{\varphi} = \varphi \cup \{(n+1, \tilde{a})\} \supset \varphi,$$

assurdo per la massimalità di φ.

Di qui la tesi, c.v.d.

Sia ora:

$$Q = \{f : B \times B \to B \mid f \text{ è una bigezione}, B \subseteq A, |B| = +\infty\}$$

Q è parzialmente ordinato per inclusione.

Innanzitutto, dimostriamo che $Q \neq \emptyset$.

Per il lemma appena dimostrato, esiste $\varphi : \mathbb{N} \to A$ iniettiva. Sia $B = \varphi(\mathbb{N})$. Allora, dato che sappiamo che:

$$|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|,$$

si verifica facilmente che:

$$|B \times B| = |B|,$$

da cui $Q \neq \emptyset$.

La seconda cosa da dimostrare, ora, è che Q soddisfa le ipotesi del lemma di Zorn.

Se infatti $\mathcal{C}$ è una catena di elementi di Q allora:

$$\Lambda = \bigcup \mathcal{C}$$

è un maggiorante della catena (verificheremo ciò alla fine).

Allora, sia:

$$\varphi : B \times B \to B$$

Vogliamo dimostrare che $B = A$. Per assurdo, sia $a \in A \setminus B$. Allora esiste $\psi : (B \cup \{a\}) \times (B \cup \{a\}) \to (B \cup \{a\})$, contraddicendo la massimalità di φ.

Si ha infatti:

$$(B \cup \{a\})^2 = (B \times B) \cup (B \times \{a\}) \cup (\{a\} \times B) \cup (\{a, a\}),$$

con:

- $|B \times B| = |B|$ per ipotesi;
- $|\{a, a\}| = |1|$;
- $|B \times \{a\}| = |\{a\} \times B| = |B|$.

Allora:

$$|(B \cup \{a\})| \le |(B \cup \{a\})^2| = |B| + |B| + |B| + |1| \le$$
$$\le |B \times \{1, 2, 3, 4\}| \le |B \times B| = |B| \le |B \cup \{a\}|,$$

da cui:

$$|(B \cup \{a\})^2| = |B \cup \{a\}|,$$

assurdo. Allora $B = A$, e:

$$|A \times A| = |A|,$$

come si voleva.

Dimostriamo ora che il teorema di Zermelo implica l'assioma della scelta.
La verifica è immediata: dato A allora possiamo rendere A bene ordinato, e considerare dunque il buon ordine $(A, <)$.
Allora una funzione di scelta è data da:

$$f : P(A) - \{\emptyset\} \to X$$
$$f(X) = \min X$$

Dimostriamo ora che il teorema di Zermelo implica la confrontabilità delle cardinalità. Se abbiamo A e B, consideriamo i buoni ordini $(A, <)$ e $(B, \prec)$. Usando la tricotomia dei buoni ordini, si ha dunque $|A| < |B|$, $|A| = |B|$ o $|B| < |A|$, e in ogni caso si ottiene la tesi.

Dimostriamo ora che la confrontabilità delle cardinalità implica il teorema di Zermelo. Anche in questo caso la dimostrazione è molto semplice. Dato un insieme A, sia:

$$H(A) = \{\alpha \text{ ordinale} \mid |\alpha| \le |A|\}$$

il suo insieme di Hartogs. Abbiamo visto che $H(A)$ è un ordinale, e che vale $H(A) \not\le A$. Per ipotesi, allora, $A \le H(A)$, ossia:

$\exists\, \varphi : A \to H(A)$ iniettiva

Definiamo allora la seguente relazione d'ordine:

$$a < a' \overset{def}{\iff} \varphi(a) < \varphi(a')$$

Allora A è ordinatamente isomorfo ad un sottoinsieme del (buon ordine) $H(A)$, ed è dunque un buon ordine.

Per concludere, possiamo dimostrare che l'ultima proprietà implica il Teorema di Zermelo.

Se A è finito, banalmente A è bene ordinabile.
Sia dunque A infinito. Definiamo:

$$B \overset{def}{=} A \cup H(A),$$

ove, al solito, $H(A)$ è l'insieme di Hartogs di A.

OSSERVAZIONE

Senza perdere di generalità, possiamo supporre:

$$A \cup H(A) = \emptyset$$

Se così non fosse, infatti, potremmo considerare:

$$A' = A \times \{0\},$$

sulla scorta del fatto che, se α è un ordinale, allora $(\alpha, 0)$ non è un ordinale. Approfondiremo questo punto più avanti.

Per ipotesi:

$|B \times B| = |B| \iff \exists\, \varphi : B \times B \to B$ bigettiva

In particolare:

$$B \times B = (A \cup H(A))^2 = (A \times A) \cup (A \times H(A)) \cup (H(A) \times A) \cup$$
$$\cup\ (H(A) \times H(A)),$$

ove gli insiemi citati sono disgiunti.

In sostanza, è definizione ristretta:

$$\varphi|_{A \times H(A)} \overset{def}{\equiv} \psi : A \times H(A) \to B = A \cup H(A)$$

Essa è iniettiva.
È dunque definita, per ogni $a \in A$, la seguente applicazione iniettiva:

$$\psi_a : H(A) \to A \cup H(A)$$
$$\alpha \to \psi(a, \alpha)$$

Innanzitutto, dato che $|H(A)| \not\leq |A|$, vale:

$$\mathrm{Im}\,\psi_a \not\subseteq A \quad \forall a \in A$$

Dunque:

$\exists\ \gamma_a \stackrel{\text{def}}{=} \min\{\mathrm{Im}\,\psi_a \cap H(A)\} = \min\{\alpha \in H(A) \mid \alpha \in \mathrm{Im}\,\psi_a\}$

(ricordiamo che $H(A)$ è un ordinale, dunque un buon ordine).

Consideriamo allora:

$$\vartheta : A \longrightarrow H(A)$$
$$a \longrightarrow \gamma_a \in \mathrm{Im}\,\psi_a$$

Dunque, per l'iniettività di φ:

$\forall \alpha, \beta \in H(A) : (a, \alpha) \neq (a', \beta) \Rightarrow \varphi(a, \alpha) \neq \varphi(a, \beta)$,

da cui anche ϑ è iniettiva, perché:

$\forall a, a' \in A,\ a \neq a' : \varphi(a, H(A)) \cap \varphi(a', H(A)) = \emptyset$

Allora ϑ è iniettiva. Definiamo allora:

$$a < a' \stackrel{\text{def}}{\Leftrightarrow} \vartheta(\alpha) < \vartheta(\alpha')$$

quest'ordinamento rende A un buon ordine, da cui la tesi.

La tesi globale è stata dunque dimostrata, c.v.d.

FORME EQUIVALENTI DELL'ASSIOMA DELLA SCELTA: PUNTUALIZZAZIONI VARIE

Nel paragrafo precedente abbiamo lasciato indimostrate alcune affermazioni: vogliamo ora dimostrarle.

Sia $\mathcal{F} = \{ A \subseteq P \mid A \text{ è } f\text{-catena} \}$, dobbiamo dimostrare che:

$$C = \bigcup_{A \in \mathcal{F}} A$$

è una f-catena.

Sappiamo già che C è bene ordinato, da cui resta solo da dimostrare che:

$$\forall\, a \in C : a = f(\{ p \in P \mid p > x \ \forall\, x \in C_a \})$$

A priori sappiamo che:

$$\forall\, A \in \mathcal{F},\ a \in A : a = f(\{ p \in P \mid p > x \ \forall\, x \in A_a \})$$

Dunque, per la tricotomia dei buoni ordini:

$$\forall\, A \in \mathcal{F},\ a \in A : A \subseteq C \Rightarrow A_a = C_a$$

Allora:

$$\forall\, a \in C,\ \forall\, A \in \mathcal{F},\ a \in A : a = f(\{ p \in P \mid p > x \ \forall\, x \in A_a \}) =$$
$$= f(\{ p \in P \mid p > x \ \forall\, x \in C_a \}),$$

da cui C è una f-catena, chiaramente la f-catena massima.

Per ipotesi, tale catena ammette un maggiorante, sia esso $\tilde{p}$.

Allora:

$$\forall\, c \in C : \tilde{p} \geq c$$

D'altronde, non può essere $\tilde{p} > c \ \forall\, c \in C$, altrimenti potremmo estendere la catena C aggiungendoci $\tilde{p}$ in coda, e ciò è assurdo per la massimalità di C.

Allora $\tilde{p} = \max C$, e per l'osservazione appena fatta non possono esistere $q \in P$ con $q > \tilde{p}$, da cui $\tilde{p}$ è un elemento massimale per P.

Dimostriamo ora un lemma indimostrato.

LEMMA

$(P, \leq)$ soddisfa le ipotesi del lemma di Zorn.

Dim.

Sia $\mathcal{C}$ una catena ascendente di funzioni iniettive con $S = \mathbb{N}$ o S segmento iniziale di $\mathbb{N}$. Se vediamo queste funzioni come sottoinsiemi di $\mathbb{N} \times A$. Allora l'unione è un sottoinsieme di $\mathbb{N} \times A$, tale che, detto S il supporto di $g \overset{\text{def}}{=} \bigcup_{f \in \mathcal{C}} f$, e $T = \operatorname{Im} g$, si ha:

- $\forall\, x \in S \;\exists!\, y_x \in A \ni \forall\, f \in \mathcal{C},\ x \in \operatorname{Dom} f : (x, y_x) \in f$;
- $\forall\, y \in T \;\exists!\, x_y \in S \ni \forall\, f \in \mathcal{C},\ y \in \operatorname{Im} f : (x_y, x) \in f$.

Per la prima osservazione g è una funzione; per la seconda g è iniettiva. Allora g è un maggiorante della catena, c.v.d.

A questo punto, la dimostrazione del fatto che Q soddisfa anch'esso le ipotesi del lemma di Zorn è del tutto identica, perciò non la ripetiamo.

Come ultima puntualizzazione, dobbiamo mostrare che, se $\alpha \in \mathrm{Ord}$, allora $(\alpha, 0) \notin \mathrm{Ord}$ se interpretiamo $(\alpha, 0)$ come una coppia ordinata di Kuratowski:

$$(\alpha, 0) = \{\{\alpha\}, \{\alpha, 0\}\},$$

da cui, per un lemma relativo ai numeri naturali (con la definizione data da Von Neumann) non può essere $(\alpha, 0) \in \mathrm{Ord}$, in quanto, avendo $(\alpha, 0)$ due elementi, dovrebbe essere $(\alpha, 0) = \{\emptyset, \{\emptyset\}\}$, ma $\emptyset \notin (\alpha, 0)$.

OSSERVAZIONE SULLE CATENE

PROPOSIZIONE

Sia $(P, \leq)$ un insieme parzialmente ordinato. Sia:

$$Ch(P) = \{ S \subseteq P \mid S \text{ è una catena} \}$$

Allora, se $\mathscr{C}$ è una catena in $Ch(P)$:

$$\Lambda = \bigcup_{S \in \mathscr{C}} S \in Ch(P)$$

Dim.

Innanzitutto:

$(\forall S \in \mathscr{C} : S \in Ch(P) \Rightarrow \subseteq P) \Rightarrow (\Lambda \subseteq P)$

Siano ora $a, b \in \Lambda$. Allora:

- $\exists \alpha \in \mathscr{C} \ni' a \in \alpha$;
- $\exists \beta \in \mathscr{C} \ni' b \in \beta$.

Dato che $\mathscr{C}$ è una catena, $\alpha \leq \beta$ o $\beta \leq \alpha$ (o entrambi).
Supponiamo $\alpha \leq \beta$, l'altro caso è analogo: se $\alpha = \beta$, allora $a \in \beta$, $b \in \alpha$. Altrimenti, in ogni caso, $a \in \beta$.

Dunque, dato che β è una catena, $a \leq b$ o $b \leq a$.

Allora $\Lambda \subseteq P$ è totalmente ordinato, dunque $\Lambda \in Ch(P)$,
c.v.d.

INDUZIONE E INDUZIONE TRANSFINITA

Sia $(B, <)$ un buon ordine.

Sia $P(x)$ una proprietà, e assumiamo che:

$\forall b \in B : ([\forall x < b : P(x)] \Rightarrow [P(b)])$

Allora:

$\forall b \in B : P(b)$

Se così non fosse, sia:

$$\tilde{b} = \min \{ b \in B \mid \neg P(b) \}$$

Allora, per ogni $x < \tilde{b}$ $P(x)$, da cui $P(\tilde{b})$, assurdo.

OSSERVAZIONE

Si noti che questa è una generalizzazione dell'induzione sui naturali.

Si noti che, a meno di isomorfismo, $(B, <)$ è un ordinale: ciò giustifica la prossima definizione, che riguarda gli ordinali.

Negli ordinali, invece, si parla di INDUZIONE TRANSFINITA.

Sia $P(x)$ una proprietà, e assumiamo che:

$\forall \alpha \in \mathrm{Ord} : ([\forall \beta < \alpha : P(\beta)] \Rightarrow P(\alpha))$.

Allora:

$\forall \alpha \in \mathrm{Ord} : P(\alpha)$.

Se così non fosse, esisterebbe il minimo ordinale β tale che $\neg P(\beta)$. Ma allora:

$\forall \alpha < \beta : P(\alpha) \Rightarrow P(\beta)$,

assurdo.

Nella pratica gli ordinali si distinguono in 3 categorie:

- $\alpha = 0$
- $\alpha = \beta + 1$ (ordinale SUCCESSORE), aventi massimo;
- $\alpha = \lambda$ (ordinale LIMITE), non aventi massimo.

OSSERVAZIONE

Se λ è ordinale limite, allora vale:

$$\lambda = \bigcup_{\gamma < \lambda} \gamma$$

Se invece λ è ordinale successore, allora vale:

$$\lambda > \bigcup_{\gamma < \lambda} \gamma$$

Ad esempio:

- $\omega = \bigcup_{n < \omega} n$;
- $17 \neq \bigcup_{n < 17} n = 16$.

OSSERVAZIONE

In effetti Ord è una classe, per cui bisogna essere precisi quando si afferma che ogni sottoinsieme non vuoto di Ord ammette minimo.

Supponiamo allora che:

$$\{ \alpha \in \text{Ord} \mid \neg P(\alpha) \} \neq \emptyset$$

Per definizione, allora:

$\exists\, \gamma \in \text{Ord}$ t.c. $\neg P(\gamma)$

A questo punto, esiste:

$$\bar{\alpha} = \min \{ \beta \in \gamma \cup \{\gamma\} \mid \neg P(\beta) \},$$

dato che $\gamma \cup \{\gamma\}$ è un buon ordine.

OSSERVAZIONE

Non esistono catene discendenti di ordinali. Se per assurdo ce ne fosse una di queste, allora, detto $\alpha_0 \in \text{Ord}$ il primo termine, si avrebbe $\in \ni \alpha_0 \cup \{\alpha_0\}$, assurdo perché $\alpha_0 \cup \{\alpha_0\}$ è un ordinale.

INDUZIONE TRANSFINITA PER CASI

Sia $P(x)$ una proprietà, e assumiamo che:

- valga $P(0)$;
- $\forall \beta : P(\beta) \Rightarrow P(\beta+1)$
- se λ è limite: $\left[\forall \gamma < \lambda : P(\gamma) \Rightarrow P(\lambda) \right]$

Allora:

$\forall \alpha \in Ord : P(\alpha)$

TEOREMA (DI RICORSIONE TRANSFINITA) (SOLO ENUNCIATO)

Data una funzione-classe G definita su tutti gli insiemi. Allora esiste ed è unica la funzione-classe F definita nella classe Ord degli ordinali, tale che:

$$F(\alpha) = G(F|_\alpha)$$

OSSERVAZIONE

La funzione classe G può essere applicata solo a insiemi: occorre quindi accertarsi che $F|_\alpha$ sia un insieme. Ma ciò è vero. $\alpha \in Ord$ è un insieme, da cui $Dom\, F|_\alpha = \alpha$ è un insieme. Allora, per l'assioma di rimpiazzamento, $F(\alpha) = \beta$ è un insieme, e per lo schema di separazione:

$$F|_\alpha = \{ (x,y) \in \alpha \times \beta \mid (x,y) \in F \}$$

è un insieme.

Nella pratica, si usa una formulazione in cui si distinguono dei casi.

TEOREMA (SOLO ENUNCIATO)

Date due funzioni classe G e H e un insieme a esiste ed è unica una funzione classe F definita nella classe Ord degli ordinali tale che:

- $F(0) = a$;
- $F(\beta+1) = G(F(\beta))$, se $(\beta+1)$ è successore;
- $F(\lambda) = H(F|_\lambda)$ se λ è limite.

Si può dimostrare che la prima formulazione implica la seconda.

In effetti, basta definire la funzione-classe L così fatta:

$$L(x) = y \iff$$

$$\iff \begin{cases} x = \emptyset \;,\; y = a \,; \\ x \text{ è una funzione con dom } x = \alpha+1 \,,\; \alpha \in \mathrm{Ord}, \text{ e } \\ y = G\,(x(\alpha)) \,; \\ x \text{ è una funzione con dom } x = \lambda \,,\; \lambda \in \mathrm{Ord} \text{ limite}, \\ \text{e } y = H(x) \,; \\ x \text{ nessuno dei precedenti} \,,\; \text{con } y = \emptyset \end{cases}$$

Allora L è una funzione classe definita su tutti gli insiemi. Allora esiste ed è unica F tale che:

$\forall \; \alpha \in \mathrm{Ord} : \; F(\alpha) = L(F|_\alpha)$,

con:

- $L(F|_\alpha) = L(F|_0) = L(\emptyset) = a$;
- $L(F|_{\beta+1}) = G(F(\beta), \beta) \;\; \forall \; \beta+1$ ordinale successore;
- $L(F|_\lambda) = H(F|_\lambda) \;\; \forall \; \lambda$ ordinale limite.

Dunque, effettivamente, la prima formulazione implica la seconda.

SOMMA TRA ORDINALI

La SOMMA tra ordinali è definita in questo modo:

- $\alpha + 0 = \alpha \quad \forall \alpha \in Ord$;
- $\alpha + (\beta + 1) = (\alpha + \beta) + 1 \quad \forall \alpha, \beta \in Ord$, β successore;
- $\alpha + \lambda = \bigcup_{\gamma < \lambda} (\alpha + \gamma) \quad \forall \alpha, \lambda \in Ord$, λ limite.

Ad esempio:

$$\omega + \omega = \bigcup_{n < \omega} \omega + n$$

Fissato un α ordinale, per il teorema di ricorsione (seconda formulazione) esiste un'unica funzione - classe $S_\alpha : Ord \to Ord$ tale che:

- $S_\alpha(0) = \alpha \stackrel{def}{=} a$;
- $S_\alpha(\beta + 1) = S_\alpha(\beta) + 1 = G(S_\alpha(\beta), \beta)$;
- $S_\alpha(\lambda) = \bigcup_{\gamma < \lambda} S_\alpha(\gamma) = H(S_\alpha|_\lambda)$.

Definiamo allora:

$$\alpha + \beta \stackrel{def}{=} S_\alpha(\beta)$$

Ad esempio:

$$17 + \omega = \bigcup_{n < \omega} 17 + n = \bigcup_{16 < k < \omega} k = \omega$$

TEOREMA (SOLO ENUNCIATO)

Si ha:

$$\alpha + \beta \approx \alpha \oplus \beta$$

ESERCIZI VARI

1. Sia $\gamma \in \mathrm{Ord}$. Allora:

$$0 + \gamma = \gamma$$

Ragioniamo per induzione transfinita su γ.

Se $\gamma = 0$, allora $0 + 0 = S_0(0) \overset{\text{def}}{=} 0$.

Sia ora vera l'uguaglianza $0 + \beta = \beta$. Allora:

$$0 + (\beta + 1) \overset{\text{def}}{=} (0 + \beta) + 1 = \beta + 1.$$

Infine, supponendo che (per λ ordinale limite):
$\forall \delta < \lambda : 0 + \delta = \delta$,
allora:

$$0 + \lambda \overset{\text{def}}{=} \bigcup_{\delta < \lambda} (0 + \delta) = \bigcup_{\delta < \lambda} \delta = \lambda$$

(ricordando che λ è limite). Dunque la tesi.

2. Siano $\alpha, \beta, \gamma \in \mathrm{Ord}$. Allora:

$$\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$$

Ragioniamo per induzione transfinita su γ.

Se $\gamma = 0$, allora $\alpha + 0 = \alpha \leq \beta = \beta + 0$.

Se la disuguaglianza vale per γ, allora (assumendo vera l'associatività della somma):

$$\alpha + (\gamma + 1) = (\alpha + \gamma) + 1 \leq (\beta + \gamma) + 1 = \beta + (\gamma + 1)$$

Infine, supponendo che valga, per λ ordinale limite:
$\forall \delta < \lambda : (\alpha \leq \beta \Rightarrow \alpha + \delta \leq \beta + \delta)$,
allora:

$$\alpha + \lambda = \bigcup_{\delta < \lambda} (\alpha + \delta) \leq \bigcup_{\delta < \lambda} (\beta + \delta) = \beta + \lambda,$$

e l'induzione è conclusa.

In generale, l'implicazione opposta non vale:

$$2 + \omega = \bigcup_{n < \omega} (2 + n) = \bigcup_{n < \omega} n = \omega = 1 + \omega \not\Rightarrow 2 \leq 1$$

Inoltre è falso che:

$$\alpha < \beta \Rightarrow \alpha + \gamma < \alpha + \beta$$

Infatti:

$$1 < 2 \quad , \quad 1 + \omega = \omega = 2 + \omega$$

3. Siano $\alpha, \beta, \gamma \in \mathrm{Ord}$. Allora:

$$\alpha < \beta \iff \gamma + \alpha < \gamma + \beta$$

$$\alpha = \beta \iff \gamma + \alpha = \gamma + \beta$$

Ragioniamo per induzione transfinita su β.

Se $\beta = 0$, allora $\alpha < \beta \Rightarrow \gamma + \alpha < \gamma + \beta \ \forall \gamma \in \mathrm{Ord}$ è vera, perché l'ipotesi è falsa.

Sia allora vera l'implicazione nel caso β. Allora, considerando $\beta + 1$, si ha:

- se $\beta + 1 \leq \alpha$, l'implicazione è vera a vuoto;
- se $\alpha < \beta + 1$, allora $\alpha \leq \beta$:
  - se $\alpha = \beta$, allora $\gamma + \alpha = \gamma + \beta < \gamma + (\beta + 1)$;
  - se $\alpha < \beta$, allora $\gamma + \alpha < \gamma + \beta < \gamma + (\beta + 1)$.

Sia ora $\beta = \lambda$ un ordinale limite. Supponiamo che sia $\alpha < \lambda$, per non cadere in casi banali. Allora $\alpha + 1 < \lambda$, da cui:

$$\gamma + \alpha < (\gamma + \alpha) + 1 = \gamma + (\alpha + 1) \leq \bigcup_{\mu < \lambda} (\gamma + \mu) = \gamma + \lambda$$

Sia ora $\gamma + \alpha < \gamma + \beta$: non può essere né $\beta < \alpha$ (altrimenti sarebbe $\gamma + \beta < \gamma + \alpha$), né $\alpha = \beta$ (altrimenti sarebbe $\gamma + \alpha = \gamma + \beta$). Per la tricotomia de ,
$\alpha \leq \beta$.

Passiamo ora alla seconda proposizione: un'implicazione è ovvia. Viceversa, se $\gamma + \alpha = \gamma + \beta$, allora $\alpha = \beta$, se per assurdo fosse $\alpha \neq \beta$, allora sarebbe $\alpha < \beta$, ossia $\gamma + \alpha < \gamma + \beta$, oppure $\alpha > \beta$, da cui $\gamma + \alpha > \gamma + \beta$, contro l'ipotesi.

ASSOCIATIVITÀ DELLA SOMMA

Siano $\alpha, \beta, \gamma \in Ord$. Allora:

$$(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$$

Fissiamo $(\alpha+\beta)$, e ragioniamo per induzione transfinita su γ.

Se $\gamma = 0$, allora:

$$(\alpha+\beta)+0 = \alpha+\beta = 0+(\alpha+\beta),$$

usando la definizione, e un esercizio precedente.

Supponiamo l'uguaglianza vera per γ. Allora, considerando $(\gamma+1)$, si ha:

$$(\alpha+\beta)+(\gamma+1) = ((\alpha+\beta)+\gamma)+1 = (\alpha+(\beta+\gamma))+1 =$$
$$= \alpha+(\beta+(\gamma+1))$$

Sia ora $\gamma = \lambda$ un ordinale limite, e supponiamo che l'uguaglianza sussista per ogni $\delta < \lambda$. Allora:

$$(\alpha+\beta)+\lambda = \bigcup_{\delta<\lambda}((\alpha+\beta)+\delta) = \bigcup_{\delta<\lambda}(\alpha+(\beta+\delta))$$

Notiamo ora che, essendo λ un ordinale limite:

$$\bigcup_{\delta<\lambda}(\beta+\delta) = \beta+\lambda$$

OSSERVAZIONE

Se λ è limite, allora $\beta+\lambda$ è limite. Infatti, se $\xi < \beta+\lambda$, allora $\xi \leq \beta+\delta$ per un $\delta<\lambda$, da cui:

$$\xi+1 \leq (\beta+\delta)+1 = \beta+(\delta+1) < \beta+\lambda,$$

essendo λ limite.

Allora:

$$\bigcup_{\delta<\lambda}(\alpha+(\beta+\delta)) = \bigcup_{\xi<\beta+\lambda}(\alpha+\xi) = \alpha+(\beta+\lambda),$$

come si voleva. L'uguaglianza di sopra discende dal fatto, già dimostrato, che:

$$\delta<\lambda \Leftrightarrow \beta+\delta \stackrel{def}{=} \xi < \beta+\lambda$$

PRODOTTO TRA ORDINALI

Il PRODOTTO tra ordinali è definito in questo modo:

- $\alpha \cdot 0 = 0$
- $\alpha \cdot (\beta + 1) = \alpha \cdot \beta + \alpha$, se $(\beta+1)$ è successore;
- $\alpha \cdot \lambda = \bigcup_{\gamma < \lambda} \alpha \cdot \gamma$, se λ è limite.

Ad esempio:

$\gamma \cdot (1) = \gamma \cdot (0+1) = \gamma \cdot 0 + \gamma = 0 + \gamma = \gamma$

TEOREMA (SOLO ENUNCIATO)

Si ha:

$$\alpha \cdot \beta \simeq \alpha \otimes \beta$$

Si possono dimostrare i seguenti fatti:

- $1 \cdot \gamma = \gamma \quad \forall \gamma \in \mathrm{Ord}$;
- $\alpha \leq \beta \Rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma$ (l'implicazione opposta non sussiste);
- $\alpha \leq \beta \Leftrightarrow \gamma \cdot \alpha \leq \gamma \cdot \beta$, per $\gamma \neq 0$;
- $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$;
- $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

Dimostriamo la prima affermazione, per induzione transfinita su γ.

Se $\gamma = 0$, allora $1 \cdot 0 = 0$ per definizione.

Se la proprietà è vera per γ, allora:

$1 \cdot (\gamma + 1) = 1 \cdot \gamma + 1 = \gamma + 1$

Infine, se λ è limite, e la proprietà è vera per $\delta < \lambda$, allora:

$$1 \cdot \lambda = \bigcup_{\delta < \lambda} 1 \cdot \delta = \bigcup_{\delta < \lambda} \delta = \lambda,$$

e la dimostrazione è completa.

Dimostreremo le altre proprietà più avanti.

ASSOCIATIVITÀ DEL PRODOTTO

Siano $\alpha, \beta, \gamma \in Ord$. Allora:

$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

Fissiamo $\alpha \cdot \beta$, e ragioniamo per induzione su γ. Se $\gamma = 0$:

$$(\alpha \cdot \beta) \cdot \gamma = 0 = \alpha \cdot 0 = \alpha \cdot (\beta \cdot \gamma)$$

Supponiamo che la proposizione valga per γ. Allora:

$$(\alpha \cdot \beta) \cdot (\gamma + 1) = (\alpha \cdot \beta) \cdot \gamma + \alpha \cdot \beta =$$
$$\alpha \cdot (\beta \cdot \gamma) + \alpha \cdot \beta = \alpha \cdot (\beta \cdot \gamma + \beta) =$$
$$= \alpha \cdot (\beta \cdot (\gamma + 1))$$

Notiamo che abbiamo assunto vera la distributività a sinistra del prodotto rispetto alla somma. Dimostreremo in seguito tale proprietà, senza fare uso della associatività del prodotto.

Sia ora λ un ordinale limite, e supponiamo che l'uguaglianza valga per $\delta < \lambda$. Allora:

$$(\alpha \cdot \beta) \cdot \lambda = \bigcup_{\delta < \lambda} (\alpha \cdot \beta) \cdot \delta = \bigcup_{\delta < \lambda} \alpha \cdot (\beta \cdot \delta) =$$
$$= \bigcup_{\xi < \beta \cdot \lambda} \alpha \cdot \xi = \alpha \cdot (\beta \cdot \lambda)$$

Dobbiamo giustificare i passaggi:

- per una proposizione che dimostreremo, si ha:
$$\delta < \lambda \iff \beta \cdot \delta < \beta \cdot \lambda,$$
da cui:
$$\bigcup_{\delta < \lambda} \alpha \cdot (\beta \cdot \delta) = \bigcup_{\xi < \beta \cdot \lambda} \alpha \cdot \xi ;$$

- se λ è limite, e $\beta \neq 0$, $\beta \cdot \lambda$ è limite. Se $\xi < \beta \cdot \lambda$, allora $\xi \leq \beta \cdot \delta$, con $\delta < \lambda$. Allora:
$$\xi + 1 \leq \beta \cdot \delta + 1 \leq \beta \cdot \delta + \beta = \beta \cdot (\delta + 1) < \beta \cdot \lambda,$$
da cui $\beta \cdot \lambda$ è limite. Allora:
$$\bigcup_{\xi < \beta \cdot \lambda} \alpha \cdot \xi = \alpha \cdot (\beta \cdot \lambda)$$

La dimostrazione è ora completa.

ESPONENZIAZIONE TRA ORDINALI

Sia $\alpha \geq 1$ un ordinale. Allora:

- $\alpha^0 = 1$;
- $\alpha^{\beta+1} = \alpha^\beta \alpha$, se $(\beta+1)$ è successore;
- $\alpha^\lambda = \bigcup_{\gamma<\lambda} \alpha^\gamma$, se λ è limite.

Alcuni esercizi sono i seguenti:

- $\alpha^\beta \cdot \alpha^\gamma = \alpha^{\beta+\gamma}$;
- $(\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}$.

OSSERVAZIONE

Esistono ordinali ε tali che, ad esempio:

$$\omega^\varepsilon = \varepsilon$$

Dimostriamo ora che:

$$\alpha^\beta \cdot \alpha^\gamma = \alpha^{\beta+\gamma},$$

procedendo per induzione transfinita su γ.

Se $\gamma = 0$:

$$\alpha^\beta \cdot \alpha^0 = \alpha^\beta \cdot 1 = \alpha^\beta = \alpha^{\beta+0}$$

Se la proprietà è vera per γ, allora:

$$\alpha^\beta \cdot \alpha^{\gamma+1} = \alpha^\beta \cdot (\alpha^\gamma \cdot \alpha) = (\alpha^\beta + \alpha^\gamma) \cdot \alpha =$$
$$= \alpha^{\beta+\gamma} \cdot \alpha = \alpha^{(\beta+\gamma)+1} = \alpha^{\beta+(\gamma+1)}$$

Sia λ limite, ora, sia la proprietà vera per ogni $\delta < \lambda$. Allora:

$$\alpha^\beta \cdot \alpha^\lambda = \alpha^\beta \cdot \left(\bigcup_{\delta<\lambda} \alpha^\delta\right) = \bigcup_{\delta<\lambda} \alpha^\beta \cdot \alpha^\delta = \bigcup_{\delta<\lambda} \alpha^{\beta+\delta} =$$
$$= \bigcup_{\xi<\beta+\lambda} \alpha^\xi = \alpha^{\beta+\lambda},$$

dato che $\beta+\lambda$ è limite.

Dimostriamo ora la seconda la seconda proposizione, procedendo per induzione transfinita su γ:

$$(\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}$$

Se $\gamma = 0$:

$$(\alpha^\beta)^0 = 1 = \alpha^0 = \alpha^{\beta\cdot 0}$$

Se la proprietà è vera per γ:

$$(\alpha^\beta)^{(\gamma+1)} = (\alpha^\beta)^\gamma\cdot(\alpha^\beta) = \alpha^{\beta\cdot\gamma}\cdot\alpha^\beta =$$
$$= \alpha^{\beta\cdot\gamma+\beta} = \alpha^{\beta(\gamma+1)}$$

Sia ora λ limite, e supponiamo che la proprietà valga per tutti i $\delta < \lambda$. Allora:

$$(\alpha^\beta)^\lambda = \bigcup_{\delta<\lambda}(\alpha^\beta)^\delta = \bigcup_{\delta<\lambda}\alpha^{\beta\cdot\delta} = \bigcup_{\xi<\beta\cdot\lambda}\alpha^\xi = \alpha^{\beta\cdot\lambda},$$

dato che $\beta\cdot\lambda$ è limite.

ESERCIZIO

Determiniamo:

$$(\omega+1)^{\omega}$$

In base alla definizione:

$$(\omega+1)^{\omega} = \bigcup_{n<\omega} (\omega+1)^{n}$$

Calcoliamo ad esempio:

$$(\omega+1)^2$$

Si ha:

$$(\omega+1)^2 = (\omega+1)(\omega+1) = (\omega+1)\cdot\omega + (\omega+1),$$

ora:

$$(\omega+1)\cdot\omega = \bigcup_{n<\omega} (\omega+1)\cdot n,$$

con:

- $(\omega+1)\cdot 2 = (\omega+1)+(\omega+1) = \omega + (1+\omega) + 1 =$
  $= \omega + \omega + 1 = \omega\cdot 2 + 1;$
- in generale:
  $(\omega+1)\cdot n = \omega\cdot n + 1.$

Allora:

$$(\omega+1)\cdot\omega = \bigcup_{n<\omega} (\omega+1)\cdot n = \bigcup_{n<\omega} (\omega\cdot n)+1 =$$

$$= \bigcup_{k<\omega} \omega\cdot k \overset{\text{def}}{=} \omega\,\omega = \omega^2,$$

da cui:

$$(\omega+1)^2 = \omega^2 + \omega + 1$$

Ora:

$$(\omega+1)^3 = (\omega+1)^2(\omega+1) =$$

$$=(\omega^2+\omega+1)(\omega+1) =$$

$$=(\omega^2+\omega+1)\cdot\omega + (\omega^2+\omega+1),$$

con:

$$(\omega^2+\omega+1)\cdot\omega = \bigcup_{n<\omega} (\omega^2+\omega+1)\cdot n,$$

con:

- $(\omega^2+\omega+1)\cdot 2 = \omega^2+\omega+1+\omega^2+\omega+1 = \omega^2 + (\omega+1+\omega^2) +$
  $+ \omega + 1 = \omega^2 + \omega^2 + \omega + 1 = \omega^2\cdot 2 + \omega + 1;$
- in generale, $(\omega^2+\omega+1)\cdot n = \omega^2\cdot n + \omega + 1.$

Allora:

$$(\omega^2+\omega+1)\cdot\omega = \bigcup_{n<\omega} \omega^2\cdot n+\omega+1 =$$
$$= \bigcup_{k<\omega} \omega^2\cdot k = \omega^3,$$

da cui:

$$(\omega+1)^3 = \omega^3+\omega^2+\omega+1$$

In generale, allora:

$$(\omega+1)^n = \omega^n+\omega^{n-1}+\ldots+\omega+1$$

Allora:

$$(\omega+1)^\omega = \bigcup_{n<\omega}(\omega^n+\omega^{n-1}+\ldots+\omega+1) = \bigcup_{k<\omega}\omega^k = \omega^\omega$$

DISTRIBUTIVITÀ A SINISTRA DEL PRODOTTO RISPETTO ALLA SOMMA

Siano $\alpha, \beta, \gamma \in Ord$. Allora:

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

Ragioniamo per induzione transfinita su γ

Se $\gamma = 0$, allora:

$$\alpha \cdot (\beta + 0) = \alpha \cdot \beta = \alpha \cdot \beta + 0 = \alpha \cdot \beta + \alpha \cdot 0$$

Se la proprietà è vera per γ:

$$\alpha \cdot (\beta + (\gamma + 1)) = \alpha \cdot ((\beta + \gamma) + 1) = \alpha \cdot (\beta + \gamma) + \alpha =$$
$$= (\alpha \cdot \beta + \alpha \cdot \gamma) + \alpha = \alpha \cdot \beta + (\alpha \cdot \gamma + \alpha) =$$
$$= \alpha \cdot \beta + \alpha \cdot (\gamma + 1)$$

Sia ora λ limite, e supponiamo che la proprietà sussista per $\delta > \lambda$. Allora:

$$\alpha \cdot (\beta + \lambda) = \alpha \cdot \bigcup_{\delta > \lambda} (\beta + \delta) = \bigcup_{\delta < \lambda} \alpha \cdot (\beta + \delta) =$$
$$= \bigcup_{\delta < \lambda} (\alpha \cdot \beta + \alpha \cdot \delta) = \bigcup_{\xi < \alpha \cdot \beta + \alpha \cdot \lambda} \xi$$

Ora λ è limite, dunque $\alpha \cdot \lambda$ è limite, dunque $(\alpha \cdot \beta + \alpha \cdot \lambda)$ è limite. Allora si ha la tesi:

$$\alpha \cdot (\beta + \lambda) = \bigcup_{\xi < \alpha \cdot \beta + \alpha \cdot \lambda} \xi = \alpha \cdot \beta + \alpha \cdot \lambda$$

ESERCIZI VARI

Svolgiamo ora alcuni esercizi lasciati in sospeso.

Dimostriamo ora che:

$$\alpha \leq \beta \Rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma \quad \forall \alpha, \beta, \gamma \in Ord$$

Ragioniamo per induzione transfinita su γ.

Se $\gamma = 0$, $\alpha \cdot 0 = \beta \cdot 0 = 0$ in ogni caso, da cui la tesi è vera.

Supponendo vera la tesi per γ, si ha, considerando $(\gamma + 1)$:

$$\alpha \leq \beta \Rightarrow \alpha \cdot (\gamma + 1) = \alpha \cdot \gamma + \alpha \leq \beta \cdot \gamma + \beta = \beta \cdot (\gamma + 1)$$

Infine, se λ è un ordinale limite, allora, supponendo vera la tesi per $\delta < \lambda$:

$$\alpha \leq \beta \Rightarrow \alpha \cdot \lambda = \bigcup_{\delta < \lambda} \alpha \cdot \delta \leq \bigcup_{\delta < \lambda} \beta \cdot \delta = \beta \cdot \lambda,$$

e l'induzione è completa.

Notiamo che l'implicazione opposta non vale:

$$2 \cdot \omega = \bigcup_{n < \omega} 2 \cdot n = \bigcup_{k < \omega} k = \omega, \quad 2 \nleq 1$$

Inoltre, non vale:

$$\alpha < \beta \Rightarrow \alpha \cdot \gamma < \beta \cdot \gamma$$

Infatti:

$$1 < 2, \quad 1 \cdot \omega = \omega = 2 \cdot \omega$$

Dimostriamo ora che:

$$\alpha < \beta \Leftrightarrow \gamma \cdot \alpha < \gamma \cdot \beta$$
$$\alpha = \beta \Leftrightarrow \gamma \cdot \alpha = \gamma \cdot \beta$$

Supponiamo di aver dimostrato la prima affermazione: allora la seconda affermazione è facile da dimostrare: un'implicazione, immediatamente, è banale. Riguardo l'implicazione opposta, supponiamo:

$$\gamma \cdot \alpha = \gamma \cdot \beta$$

Se fosse $\alpha \neq \beta$, allora sarebbe:

- $\alpha < \beta$, da cui $\gamma \cdot \alpha < \gamma \cdot \beta$;
- $\alpha > \beta$, da cui $\gamma \cdot \alpha > \gamma \cdot \beta$.

Dunque, per tricotomia, $\alpha = \beta$.

Dimostriamo ora la prima affermazione, procedendo per induzione transfinita su β.

Se $\beta = 0$, $\alpha < 0$ è sempre falsa, da cui la tesi è vera.

Supponiamo la tesi vera per β, e dimostriamola per $\beta+1$.
Supponiamo, senza perdere di generalità, $(\beta+1) > \alpha$.
Allora:

- $\alpha = \beta \Rightarrow \gamma \cdot \alpha = \gamma \cdot \beta < \gamma \cdot \beta + \gamma = \gamma(\beta+1)$
- $\alpha < \beta \Rightarrow \gamma \cdot \alpha < \gamma \cdot \beta < \gamma(\beta+1)$,

avendo usato:

$$0 < \gamma \Rightarrow \gamma \cdot \beta + 0 = \gamma \cdot \beta < \gamma \cdot \beta + \gamma$$

Se infine λ è limite, supponendo vera la tesi per $\delta < \lambda$, si ha:

$$\alpha < \lambda \Rightarrow \alpha + 1 < \lambda, \quad \gamma \cdot \alpha < \gamma(\alpha+1) \leq$$

$$\leq \bigcup_{\delta < \lambda} \gamma \cdot (\delta + 1) \quad \bigcup_{\eta < \gamma \cdot \lambda} \alpha \cdot \eta = \gamma \cdot \lambda,$$

perché $\gamma \cdot \lambda$ è limite.

Viceversa, se $\gamma \cdot \alpha < \gamma \cdot \beta$, non può essere $\beta < \alpha$ (altrimenti sarebbe $\gamma \cdot \beta < \gamma \cdot \alpha$), né $\beta = \alpha$ (altrimenti sarebbe $\gamma \cdot \alpha = \gamma \cdot \beta$), da cui, per tricotomia, $\alpha < \beta$.

Dunque la tesi.

DIFFERENZA A DESTRA E DIVISIONE EUCLIDEA

Se α, β sono ordinali, e $\alpha \leq \beta$, allora esiste un unico ordinale γ con $\alpha + \gamma = \beta$.

Procediamo per induzione transfinita su β. Se $\beta < \alpha$, non c'è nulla da dimostrare, e se $\beta = \alpha$ allora esiste ed è unico $\gamma = 0$ tale che $\alpha + \gamma = \alpha + 0 = \alpha = \beta$.

Supponiamo allora $\alpha < \beta$. Allora $\alpha < \beta + 1$. Si ha:

$\exists! \ \gamma \in \mathrm{Ord} \ \ni' \ \alpha + \gamma = \beta \Rightarrow \exists! \ \gamma \in \mathrm{Ord} \ \ni' \ (\alpha + \gamma) + 1 = \alpha + (\gamma + 1) = \beta + 1$,

da cui:

$\exists! \ (\gamma + 1) \in \mathrm{Ord} \ \ni' \ \alpha + (\gamma + 1) = \beta + 1$

Se invece λ è ordinale limite, $\alpha < \lambda$. Per ipotesi induttiva:

$\forall \ \delta < \lambda \ \exists! \ \gamma_\delta \in \mathrm{Ord} \ \ni' \ \alpha + \gamma_\delta = \delta$

(chiaramente si intende $\alpha \leq \delta$).

Allora, definendo:

$$\tilde{\gamma} = \bigcup_{\delta < \lambda} \gamma_\delta ,$$

si ha (notiamo che non può essere $\tilde{\gamma}$ successore, perché λ è limite):

$$\alpha + \tilde{\gamma} = \bigcup_{\delta < \lambda} (\alpha + \gamma_\delta) = \bigcup_{\delta < \lambda} \delta = \lambda,$$

da cui la tesi, dato che $\tilde{\gamma}$ è unico.

Abbiamo dimostrato la DIFFERENZA A DESTRA. Notiamo che la differenza a sinistra non sempre esiste: se infatti α è successore e λ è limite, allora $\gamma + \alpha$ è successore per ogni $\gamma \in \mathrm{Ord}$, da cui $\gamma + \alpha \neq \lambda$ per ogni $\gamma \in \mathrm{Ord}$.

Dimostriamo ora la DIVISIONE EUCLIDEA.

Se α, β sono ordinali, con $\beta \neq 0$, allora esistono e sono unici due ordinali ξ e ρ tali che $\alpha = \beta\xi + \rho$, con $\rho < \beta$.

Supponiamo che esista unico:

$$\xi \overset{\text{def}}{=} \max \{ \delta \in \mathrm{Ord} \mid \beta \cdot \delta \leq \alpha \}$$

Allora, considerando l'unico $\rho \in \mathrm{Ord}$ tale che:

$$\beta \cdot \xi + \rho = \alpha,$$

e supponendo $\rho < \beta$, si avrebbe la Tesi.

Dimostriamo dunque che ξ esiste ed è unico.

Dato che $\beta \neq 0$, si ha:

$$\beta \cdot (\alpha + 1) \geq \alpha + 1 > \alpha,$$

da cui l'insieme degli ordinali γ tali che $\beta \cdot \gamma > \alpha$ è non vuoto, e ammette perciò un minimo δ. Tale ordinale non può essere un ordinale limite, in quanto, se fosse:

$$\delta = \bigcup_{\nu < \delta} \nu,$$

allora avremmo:

$$\beta \cdot \delta = \bigcup_{\nu < \delta} \beta \cdot \nu > \alpha \Rightarrow \exists\, \nu < \delta \ni' \beta \cdot \nu > \alpha,$$

contro la minimalità di δ. Allora $\delta = \xi + 1$ è un successore. Allora ξ esiste (ed è unico), ed è il massimo per cui $\beta \cdot \xi \leq \alpha$.

Per concludere, notiamo che, se dimostriamo l'unicità di ξ, allora si ha l'unicità di ρ, in quanto $\beta \cdot \xi \leq \alpha$, e ρ è l'unico ordinale tale che $\beta \cdot \xi + \rho = \alpha$. Tale ordinale soddisfa $\rho < \beta$. Se così non fosse, ossia se fosse $\beta \leq \rho$, allora accadrebbe $\rho = \beta + \mu$, da cui avremmo:

$$\alpha = \beta \cdot \xi + \rho = \beta \cdot \xi + \beta + \mu = \beta \cdot (\xi + 1) + \mu =$$
$$= \beta \cdot \delta + \mu,$$

ossia $\beta \cdot \delta \leq \alpha$, assurdo.

Resta dunque da provare l'unicità di ξ. Sia:

$$\alpha = \beta \cdot \xi_1 + \rho_1 = \beta \cdot \xi_2 + \rho_2,$$

con $\rho_1, \rho_2 < \alpha$. Supponiamo $\xi_1 < \xi_2$. Allora $\xi_1 + 1 \leq \xi_2$, da cui:

$$\alpha \cdot \beta_1 + \rho_1 = \alpha \cdot \beta_2 + \rho_2 \geq \alpha \cdot (\beta_1 + 1) + \rho_2 =$$
$$= \alpha \cdot \beta_1 + (\alpha + \rho_2),$$

da cui:

$$\rho_1 \geq \alpha + \rho_2 \geq \alpha,$$

assurdo. Per simmetria, non può essere $\xi_2 < \xi_1$, da cui $\xi_1 = \xi_2$ e $\rho_1 = \rho_2$, come si voleva.

DUE TEOREMI

Vogliamo ora dimostrare due teoremi lasciati indimostrati.

TEOREMA

Siano $\alpha, \beta \in Ord$. Allora:

$$\alpha + \beta \simeq \alpha \oplus \beta$$

Dim.

Consideriamo la funzione seguente:

$$\Phi : \alpha + \beta \to \alpha \oplus \beta$$

Tale che:

- $\forall \gamma \in \alpha + \beta,\ \gamma < \alpha : \Phi(\gamma) = (\gamma, 0)$;
- $\forall \gamma \in \alpha + \beta,\ \gamma \geq \alpha : \gamma = \alpha + \mu,\ \mu \in Ord \Rightarrow$
  $\Rightarrow \Phi(\gamma) = (\mu, 1)$

E' evidente che Φ sia un isomorfismo, c.v.d.

TEOREMA

Siano $\alpha, \beta \in Ord$. Allora:

$$\alpha \cdot \beta \simeq \alpha \otimes \beta$$

Dim.

Consideriamo:

$$\varphi : \alpha \otimes \beta \to \alpha \cdot \beta$$

$$(\eta, \xi) \mapsto \eta \cdot \alpha + \xi$$

E' evidente che φ sia un isomorfismo, c.v.d.

ALTRI ESERCIZI

Osserviamo preliminarmente:

$\forall\ n < \omega$: $n + \omega = \bigcup_{m<\omega} (n+m) = \bigcup_{k<\omega} k = \omega$

Vogliamo dimostrare che

$$\omega + 1 + \omega^2 = \omega^2$$

Innanzitutto:

$$1 < \omega \Rightarrow 1 + \omega^2 \leq \omega + \omega^2 \Rightarrow$$

$$\Rightarrow \omega + 1 + \omega^2 \leq \omega + \omega + \omega^2 = \omega \cdot 2 + \omega^2,$$

e inoltre:

$$0 < \omega + 1 \Rightarrow 0 + \omega^2 = \omega^2 \leq \omega + 1 + \omega^2,$$

da cui:

$$\omega^2 \leq \omega + 1 + \omega^2 \leq \omega \cdot 2 + \omega^2$$

Usando la distributività a sinistra:

$$\omega \cdot 2 + \omega^2 = \omega(2+\omega) = \omega \cdot \omega,$$

perché $2 + \omega = \omega$. Allora $\omega + 1 + \omega^2 = \omega^2$.

Dimostriamo ora che:

$\forall\ \alpha < \omega^2$: $\alpha + \omega^2 = \omega^2$

Si ha:

$$\omega^2 = \bigcup_{n<\omega} \omega \cdot n,$$

da cui, se $\alpha < \omega^2$:

$\exists\ n < \omega$ t.c. $\alpha \leq \omega \cdot n$,

da cui:

$$\omega^2 \leq \alpha + \omega^2 \leq \omega \cdot n + \omega^2 = \omega(n + \omega) =$$

$$= \omega \cdot \omega = \omega^2,$$

da cui:

$$\alpha + \omega^2 = \omega^2$$

CARDINALITÀ DEI BORELIANI DI $\mathbb{R}$

Consideriamo $\mathcal{B}(\mathbb{R})$, la σ-algebra dei BORELIANI di $\mathbb{R}$.
Essa è generata, ad esempio, dagli aperti di $\mathbb{R}$.

Intendiamo calcolare $|\mathcal{B}(\mathbb{R})|$.

Definiamo, per ricorsione transfinita:

$$\begin{cases} B_0 = \{ A \subseteq \mathbb{R} \mid A \text{ è aperto} \} \\ B_{n+1} = B_n \cup \{ D \subseteq \mathbb{R} \mid D^c \in B_n \} \cup \{ \bigcup_{k \in \mathbb{N}} D_k \mid D_k \in B_n \} \cup \\ \quad \cup \{ \bigcap_{k \in \mathbb{N}} D_k \mid D_k \in B_n \} \end{cases}$$

Non è $\mathcal{B}(\mathbb{R}) = \bigcup_{n \in \mathbb{N}} B_n$, altrimenti $\mathcal{B}(\mathbb{R})$ non sarebbe chiuso per unioni e intersezioni numerabili.

Definiamo allora per ricorsione transfinita:

$$\begin{cases} B_0 \text{ come prima} \\ B_{\alpha+1} \text{ come prima} \\ B_\lambda = \bigcup_{\alpha < \lambda} B_\alpha \text{, se } \lambda \text{ è limite} \end{cases}$$

Osserviamo che, questa volta, si ha:

$$\mathcal{B}(\mathbb{R}) = \bigcup_{\alpha < \omega_1} B_\alpha ,$$

ove (lo ricordiamo):

$$\omega_1 = \min \{ \alpha \in \mathrm{Ord} \mid |\omega| < |\alpha| \}$$

è il più piccolo ordinale non numerabile.

Un contenimento deriva da quest'osservazione:

$$\forall \alpha < \omega_1 : B_\alpha \subseteq \mathcal{B}(\mathbb{R}) \Rightarrow B_{\omega_1} = \bigcup_{\alpha < \omega_1} B_\alpha \subseteq \mathcal{B}(\mathbb{R})$$

Per l'altro contenimento possiamo dimostrare che $\bigcup_{\alpha < \omega_1} B_\alpha$ è una σ-algebra che contiene gli aperti di $\mathbb{R}$, dunque contiene $\mathcal{B}(\mathbb{R})$.

A tal scopo useremo un'induzione transfinita non sull'insieme di tutti gli ordinali (non sarebbe neppure corretto), ma su ω_1, che è un buon ordine.

Per $\alpha = 0$, $B_0 \subseteq \mathcal{B}(\mathbb{R})$ per definizione.

Per $\alpha = \beta+1$, se per ipotesi induttiva $B_\beta \subseteq \mathcal{B}(\mathbb{R})$, allora, dato che $\mathcal{B}(\mathbb{R})$ è una σ-algebra:

- $B_\beta \subseteq \mathcal{B}(\mathbb{R})$
- $\{ D^c \subseteq \mathbb{R} \mid D \in B_\beta \} \subseteq \mathcal{B}(\mathbb{R})$;
- $\{ \bigcup_{k\in\mathbb{N}} D_k \mid D_k \in B_\beta \} \subseteq \mathcal{B}(\mathbb{R})$;
- $\{ \bigcap_{k\in\mathbb{N}} D_k \mid D_k \in B_\beta \} \subseteq \mathcal{B}(\mathbb{R})$,

da cui $B_{\beta+1} = B_\alpha \subseteq \mathcal{B}(\mathbb{R})$.

Infine, se λ è limite, allora:

$\forall \alpha < \lambda : B_\alpha \subseteq \mathcal{B}(\mathbb{R}) \Rightarrow B_\lambda \overset{\text{def}}{=} \bigcup_{\alpha<\lambda} B_\alpha \subseteq \mathcal{B}(\mathbb{R})$.

Vediamo ora l'altro contenimento. Sia $D \in \bigcup_{\alpha<\omega_1} B_\alpha$.

Allora:

$\exists\, \alpha < \omega_1$ t.c. $D \in B_\alpha$,

dunque, poiché $\alpha < \omega_1 \Rightarrow \alpha+1 < \omega_1$ (perché ω_1 è limite)

$$D \in B_\alpha \Rightarrow D^c \in B_{\alpha+1} \subseteq \bigcup_{\alpha<\omega_1} B_\alpha$$

Sia ora $(D_n)_{n\in\mathbb{N}} \subseteq \bigcup_{\alpha<\omega_1} B_\alpha$.

Per ogni $n \in \mathbb{N}$, sia $\alpha_n < \omega_1$ il più piccolo ordinale tale che $D_n \in B_{\alpha_n}$. Sia poi:

$$\tilde{\alpha} \overset{\text{def}}{=} \bigcup_{n\in\mathbb{N}} \alpha_n = \sup_{n\in\mathbb{N}} \alpha_n$$

Si ha:

$$\tilde{\alpha} < \omega_1,$$

dato che è un'unione numerabile di ordinali numerabili.

Allora tutte le successioni numerabili di ω_1 sono limitate.

Si usa dunque parlare di COFINALITÀ. In questo caso, si ha:

$$\operatorname{Cof}(\omega_1) = \omega_1,$$

mentre ad esempio:

$$\operatorname{Cof}(\omega_1+\omega) = \omega$$

Analizzeremo la questione in seguito; diciamo che la cofinalità rende l'idea della cardinalità che una successione deve avere perché sia illimitata.

Torniamo alla dimostrazione. Si ha che:

$$\forall n \in \mathbb{N} : D_n \in \mathcal{B}_{\alpha_n} \subseteq \mathcal{B}_{\tilde{\alpha}},$$

dato che $\alpha_n \leq \tilde{\alpha}$. Dunque:

$$(D_n)_{n\in\mathbb{N}} \subseteq \mathcal{B}_{\tilde{\alpha}} \Rightarrow \bigcup_{n\in\mathbb{N}} D_n \subseteq \mathcal{B}_{\tilde{\alpha}+1} \subseteq \mathcal{B}_{\omega_1}$$

$$\bigcap_{n\in\mathbb{N}} D_n \subseteq \mathcal{B}_{\tilde{\alpha}+1} \subseteq \mathcal{B}_{\omega_1}$$

Allora $\mathcal{B}_{\omega_1} = \bigcup_{\alpha<\omega_1} \mathcal{B}_\alpha$ è una σ-algebra contenente gli aperti di $\mathbb{R}$, perché è chiusa per complementare, unione numerabile e intersezione numerabile.

In conclusione:

$$\mathcal{B}(\mathbb{R}) = \mathcal{B}_{\omega_1}$$

Passiamo ora allo studio della cardinalità: vogliamo dimostrare per induzione transfinita che $|\mathcal{B}(\mathbb{R})| = \mathfrak{c}$.
È sufficiente dimostrare che $|\mathcal{B}_\alpha| = \mathfrak{c}$ per ogni $\alpha < \omega_1$.
Infatti $|\omega_1| \leq \mathfrak{c}$, e si può allora usare la proprietà seguente già dimostrata:

$$|I| \leq \mathfrak{c}, \ |A_i| \leq \mathfrak{c} \ \forall i \in I \Rightarrow$$
$$\Rightarrow \left| \bigcup_{i\in I} A_i \right| \leq \mathfrak{c}.$$

Sia $\alpha = 0$. Dobbiamo dimostrare che $|\mathcal{B}_0| = \mathfrak{c}$.
Sicuramente $|\mathcal{B}_0| \geq \mathfrak{c}$, dato che la funzione seguente:

$$\theta : \mathbb{R} \to \mathcal{B}_0, \quad \theta(x) = \mathbb{R} \setminus \{x\}$$

è iniettiva. Dato ora $A \in \mathcal{B}_0$, sia $\Psi(A) = \{(q_1, q_2) \in \mathbb{Q}\times\mathbb{Q} \mid B(q_1, q_2) \subseteq A\} \in \mathcal{P}(\mathbb{Q}^2)$.
Si può dimostrare che Ψ è iniettiva: dato che $|\mathcal{P}(\mathbb{Q}^2)| = \mathfrak{c}$, si ha, in conclusione, $|\mathcal{B}_0| = \mathfrak{c}$.

Sia ora $\alpha = \beta + 1$. Sia, per ipotesi, $|\mathcal{B}_\beta| = \mathfrak{c}$. Si ha ora:

$$\mathcal{B}_{\beta+1} = \mathcal{B}_\beta \cup \mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3,$$

con:

- $|\mathcal{B}_\beta| = \mathfrak{c}$ per ipotesi induttiva;
- $\mathcal{A}_1 = \{D^c \mid D \in \mathcal{B}_\beta\} \Rightarrow |\mathcal{A}_1| = |\mathcal{B}_\beta| = \mathfrak{c}$, perché $\phi : D \to D^c$ è una bigezione;

- $\Delta_2 = \left\{ \bigcup_{k\in\mathbb{N}} D_k \mid D_k \in B_\beta \right\} \Rightarrow |\Delta_2| = |B_\beta \times \mathbb{N}| = |\mathbb{R} \times \mathbb{N}| = |\mathbb{R}| = c$;
- $\Delta_3 = \left\{ \bigcap_{k\in\mathbb{N}} D_k \mid D_k \in B_\beta \right\} \Rightarrow |\Delta_3| = |B_\beta \times \mathbb{N}| = |\mathbb{R} \times \mathbb{N}| = |\mathbb{R}| = c$.

Allora:

$$|B_{\beta+1}| = c$$

Per concludere, sia λ un ordinale limite, con $\lambda < \omega_1$. Allora:

$$B_\lambda = \bigcup_{\alpha<\lambda} B_\alpha$$

Per ipotesi induttiva, $|B_\alpha| = c$ per ogni $\alpha < \lambda$. In più $\lambda < \omega_1$, da cui $|\lambda| \leq |\omega| = \aleph_0$. Allora, per quanto ricordato prima:

$$\left| B_\lambda = \bigcup_{\alpha<\lambda} B_\alpha \right| = c$$

Per concludere, osserviamo che $|\omega_1| \leq |\mathbb{R}|$. Usando l'assioma della scelta, ossia il Teorema di Zermelo, possiamo bene ordinare $\mathbb{R}$. Allora esiste un ordinale γ con $|\gamma| = |\mathbb{R}|$, da cui, per minimalità di ω_1, si ha:

$$|\omega_1| \leq |\gamma| = |\mathbb{R}|$$

La cardinalità di $\mathcal{L}(\mathbb{R})$, invece, è 2^c: per dimostrarlo, consideriamo l'insieme di Cantor $C_{[0,1]}$, ossia l'insieme dei numeri che in base 3 hanno una scrittura decimale che contiene solo 0 e 2.

Si può dimostrare che:

- $|C_{[0,1]}| = c$;
- $m(C_{[0,1]}) = 0$.

Allora $\mathcal{P}(C_{[0,1]}) \subseteq \mathcal{L}(\mathbb{R})$, da cui:

$$2^c = |\mathcal{P}(C_{[0,1]})| \leq |\mathcal{L}(\mathbb{R})| \leq |\mathcal{P}(\mathbb{R})| = 2^c$$

OSSERVAZIONI SUGLI ORDINALI

Siano α, β ordinali maggiori strettamente di 1.

Consideriamo la seguente tabella:

α	S	S	L	L
β	S	L	S	L
$\alpha+\beta$	?	?	?	?
$\alpha\cdot\beta$	?	?	?	?
α^β	?	?	?	?

Completiamo la tabella.

Per quanto riguarda la somma, tutto dipende esclusivamente da β. Dunque:

$\alpha+\beta$	S	L	S	L

Studiamo ora $\alpha\cdot\beta$.

Se $\beta = \gamma+1$, allora $\alpha\beta = \alpha\gamma + \alpha$, da cui:

- $\alpha\beta$ è successore se α è successore;
- $\alpha\beta$ è limite se α è limite.

Se invece β è limite, allora $\alpha\cdot\beta = \bigcup_{\gamma<\beta} \alpha\cdot\gamma$ non può avere massimo perché β non ha massimo. Allora $\alpha\beta$ è limite in ogni caso. Si ha dunque:

$\alpha\cdot\beta$	S	L	L	L

Per concludere, trattiamo il caso α^β.

Se $\beta = \lambda$ è limite, $\alpha^\lambda = \bigcup_{\gamma<\lambda} \alpha^\gamma$. Infatti α^λ non ha massimo: se $\delta \in \alpha^\lambda$, allora esiste $\gamma < \lambda$ tale che $\delta < \alpha^\gamma$. Dunque:

$$\delta < \alpha^\gamma < \alpha^\gamma\cdot 2 \leq \alpha^\gamma\cdot\alpha = \alpha^{\gamma+1} < \alpha^\lambda$$

$$\delta + 1 \leq \alpha^\gamma < \alpha^{\gamma+1} < \alpha^\lambda$$

Se β è successore e α è limite, allora:

$$\alpha^\beta = \alpha^{\gamma+1} = \alpha^\gamma\cdot\alpha$$

è limite perché lo è α.

Rimane da studiare il caso in cui α, β sono entrambi successori.

In questo caso, si ha:

$$\alpha = \delta + 1 \qquad \beta = \gamma + 1$$

$$\alpha^{\beta} = (\delta+1)^{\gamma+1} = (\delta+1)^{\gamma}(\delta+1) =$$

$$= (\delta+1)^{\gamma}\delta + (\delta+1)^{\gamma},$$

da cui si ha che, se γ è limite, α^{β} è limite.

Se invece $\gamma = \tilde{\gamma} + 1$ è un successore, allora:

$$(\delta+1)^{\gamma} = (\delta+1)^{\tilde{\gamma}}\delta + (\delta+1)^{\tilde{\gamma}},$$

da cui si ritorna nel caso precedente.

Facciamo qualche esempio:

- $(\omega+1)^3 = (\omega+1)^2(\omega+1) = (\omega^2+\omega+1)(\omega+1) =$
  $= \omega^3 + \omega^2 + \omega + 1$ è successore;
- $(\omega+1)^{\omega+1} = (\omega+1)^{\omega}(\omega+1) = \omega^{\omega}(\omega+1) = \omega^{\omega}\cdot\omega +$
  $+ \omega^{\omega}$ è limite.

Gli ordinali sono bene ordinati, dunque ogni catena discendente diventa stazionaria, dunque si ferma dopo un numero finito di passi. Dunque ogni ordinale è la somma di un ordinale limite e di un ordinale finito (in ω_1, si intende).

I casi sono due:

- $\beta = k$, $k < \omega$;
- $\beta = \lambda + k$, $k < \omega$, λ ordinale limite.

PROPOSIZIONE

Se β è un ordinale successore allora esiste un ordinale λ limite (eventualmente $\lambda = 0$) e un ordinale $k < \omega$ tale che $\beta = \lambda + k$ ($k \neq 0$).

Dim.

LEMMA

Sia α un ordinale limite. Allora:

$\exists\, \delta \in \mathrm{Ord}$ t.c. $\alpha = \omega \cdot \delta$

Dim.

Operando la divisione euclidea, si ha:

$$\alpha = \omega \cdot \gamma + \rho \quad , \rho < \omega,$$

da cui:

$$\omega \cdot \gamma \leq \alpha < \omega \cdot (\gamma + 1)$$

Se fosse $\omega \cdot \gamma < \alpha$ sarebbe $\alpha = \omega \cdot \gamma + n$, con $n < \omega$, $n \geq 1$. Allora sarebbe $\alpha = \beta + 1$, con $\beta = \omega \cdot \gamma + (n-1)$, e ciò è assurdo. Dunque $\omega \cdot \gamma = \alpha$, c.v.d.

Se α è successore, allora:

$$\alpha = \omega \cdot \gamma + \rho \quad , \rho < \omega,$$

con $\rho > 0$ per il lemma, dato che α è successore. Considerando $\lambda = \omega \cdot \gamma$, si ha allora:

$$\alpha = \lambda + \rho \quad , \rho < \omega, \text{ c.v.d.}$$

Dunque, se β è della forma $\beta = \lambda + k$, $\lambda \neq 0$, allora α^β è limite. Se α e β sono entrambi ordinali finiti, allora α^β è finito, dunque (a meno di casi estremi) è successore.

Anche nel caso in cui $\alpha = \lambda + k$, $\lambda \neq 0$, e $\beta = n < \omega$, α^β è successore. Procediamo per induzione (semplice) su β.

Se $\beta = 0$ la tesi è banale: $\alpha^0 = 1$ è successore.

Ora, supponendo che $\alpha^\beta = (\lambda + k)^\beta = (\mu + \rho)$ è successore

$$\alpha^{\beta+1} = \alpha^\beta \cdot \alpha = (\lambda + k)^\beta (\lambda + k) = (\mu + \rho)(\lambda + k) =$$
$$= (\mu + \rho)\lambda + (\mu + \rho)k =$$
$$= (\mu + \rho)\lambda + \mu k + \rho k$$

è successore.

ESERCIZIO

Effettuiamo la seguente divisione tra ordinali:

$$\omega^2 + \omega\cdot 3 + 2 \;\underline{|\,\omega + 4}$$

Si ha ovviamente:

$$\omega + 4 < \omega^2 + \omega\cdot 3 + 2$$

Ora:

- $(\omega+4)\cdot\omega \overset{\text{def}}{=} \bigcup_{n<\omega} (\omega+4)\, n = \bigcup_{n<\omega} \omega\cdot n + 4 = \omega^2$;
- $(\omega+4)\cdot(\omega+1) = \omega^2 + \omega + 4$;
- $(\omega+4)\cdot(\omega+2) = \omega^2 + \omega + 4 + \omega + 4 = \omega^2 + \omega\cdot 2 + 4$;
- $(\omega+4)\cdot(\omega+2) = \omega^2 + \omega + 4 + \omega + 4 + \omega + 4 =$
  $= \omega^2 + \omega\cdot 3 + 4.$

Allora:

$$\omega^2 + \omega\cdot 3 + 2 = (\omega+4)(\omega+2) + \rho,$$

con $\rho = \omega + 2 < \omega + 4$. Infatti:

$$(\omega+4)(\omega+2) + \omega + 2 =$$
$$= \omega + 4 + \omega\cdot 2 + 4 + \omega + 2 =$$
$$= \omega^2 + \omega\cdot 3 + 2$$

COMPLEMENTI VARI E OSSERVAZIONI

PROPOSIZIONE

Sia $\alpha > 0$. Sono fatti equivalenti:

- $\forall \beta < \alpha : \beta + \alpha = \alpha$;
- $\forall \beta, \gamma < \alpha : \beta + \gamma < \alpha$;
- $\alpha = \omega^\delta$, $\delta \in Ord$.

Dim.

Che la prima affermazione implichi la seconda, è ovvio:

$\forall \beta, \gamma < \alpha : \beta + \gamma < \beta + \alpha = \alpha$.

Dimostriamo ora che la seconda affermazione implica la terza.

La classe $\Lambda = \{\xi \in Ord \mid \omega^\xi > \alpha\}$ è non vuota, perché contiene almeno $\alpha+1$. Consideriamo allora:

$$\Lambda_1 = \{\xi \in \alpha+1 \mid \omega^\xi > \alpha\}$$

In generale, infatti, si ha $\omega^\delta \geq \delta$, e la cosa si dimostra per induzione transfinita. Infatti:

- $\alpha = 0 \Rightarrow \omega^0 = 1 > 0$;
- $\alpha = \beta + 1 \Rightarrow \omega^\alpha = \omega^{\beta+1} = \omega^\beta \cdot \omega$,

  da cui:

  - se $\beta = 0$, $\omega^\alpha = \omega > \alpha = 1$;
  - se $\beta \neq 0$, $\omega^\beta \cdot \omega \geq \beta \cdot \omega \geq \beta + 1 = \alpha$;
- $\alpha = \lambda$ limite $\Rightarrow \omega^\lambda = \bigcup_{\delta<\lambda} \omega^\delta \geq \bigcup_{\delta<\lambda} \delta = \lambda$.

Definiamo dunque $\bar{\xi} = \min \Lambda_1$.

Si ha che:

- $\bar{\xi} \neq 0$, altrimenti si avrebbe $\omega^{\bar{\xi}} = \omega^0 = 1 > \alpha \Rightarrow \alpha = 0$, contro l'ipotesi che $\alpha \neq 0$;
- $\bar{\xi}$ non è limite, altrimenti:

  $\alpha < \omega^{\bar{\xi}} = \bigcup_{\eta < \bar{\xi}} \omega^\eta \Rightarrow \exists\, \eta < \bar{\xi} : \alpha < \omega^\eta$,

  contro l'ipotesi che $\bar{\xi} = \min \Lambda_1$.

Allora $\bar{\xi} = \delta + 1$ è successore. Si ha dunque $\omega^\delta \leq \alpha < \omega^{\delta+1}$

Ora:

$\alpha < \omega^{\delta+1} = \omega^\delta \cdot \omega = \bigcup_{n<\omega} \omega^\delta \cdot n \Rightarrow \exists\, n \geq 1$ t.c. $\omega^\delta n \leq \alpha \leq \omega^\delta(n+1)$,
e ciò è vero in generale.

Sfruttiamo ora l'ipotesi: la tesi è $\alpha = \omega^\delta$.

A priori, si ha $\omega^\delta \cdot n \leq \alpha < \omega^\delta(n+1)$, ossia:

$$\alpha = \omega^\delta \cdot n + \beta, \quad \beta < \omega^\delta$$

Ora, se per assurdo $\omega^\delta < \alpha$, si ha:

- se $\beta = 0$, $\alpha = \omega^\delta \cdot n$, $n \geq 2 \Rightarrow \omega^\delta, \omega^\delta(n-1) < \alpha$, $\omega^\delta + \omega^\delta(n-1) = \omega^\delta n = \alpha$, assurdo;
- se $\beta > 0$, $\alpha > \omega^\delta \cdot n \Rightarrow \omega^\delta, \omega^\delta \cdot n < \alpha$, $\omega^\delta + \omega^\delta n = \omega^\delta(n+1) > \alpha$, assurdo.

Allora necessariamente $\omega^\delta = \alpha$, ossia la tesi.

Dimostriamo ora che l'ultima affermazione implica la prima.
Sia dunque $\alpha = \omega^\delta$, e sia $\beta < \alpha$. Si ha allora:

- se $\delta = 0$, allora:
  $\forall \beta < \alpha = \omega^0 = 1 : \beta = 0 \Rightarrow \beta + \alpha = 0 + \alpha = \alpha$;
- se $\delta = \gamma + 1$, allora:
  $\forall \beta < \alpha = \omega^{\gamma+1} = \omega^\gamma \cdot \omega = \bigcup_{m<\omega} \omega^\gamma \cdot m : \exists\, m < \omega$ t.c.
  $\beta < \omega^\gamma \cdot m \Rightarrow \alpha \leq \beta + \alpha \leq \omega^\gamma \cdot m + \omega^{\gamma+1} = \omega^\gamma(m+\omega) =$
  $= \omega^\gamma(\omega) = \omega^{\gamma+1} = \alpha$;
- se $\delta = \lambda$ è limite, allora:
  $\forall \beta < \alpha = \omega^\lambda = \bigcup_{\delta<\lambda} \omega^\delta : \exists\, \delta < \lambda$ t.c. $\beta < \omega^\delta$,
  da cui:
  $\beta + \alpha \leq \omega^\delta + \omega^\lambda = \bigcup_{\gamma<\lambda}\left[\omega^\delta + \omega^\gamma\right] = \bigcup_{\gamma<\lambda} \omega^\gamma = \omega^\lambda$.

Dunque la tesi, c.v.d.

ESERCIZI VARI

1. Siano $\alpha, \beta < \omega_1$. Allora (posto $\alpha \neq 0$) si ha $\alpha^\beta < \omega_1$.

Consideriamo:

$$\mu = \min\{\gamma \in \omega_1 \mid \alpha^\gamma \geq \omega_1\}$$

Tale ordinale μ:

- non è 0 perché $\alpha^0 = 1 < \omega_1$;
- non è limite, perché è unione numerabile di insiemi numerabili è numerabile:

$$\alpha^\mu = \bigcup_{\delta < \mu} \alpha^\delta < \omega_1;$$

- non è successore, perché altrimenti sarebbe:

$$\alpha^\delta < \omega_1, \quad \alpha^{\delta+1} = \alpha^\delta \cdot \alpha = \alpha^\mu \geq \omega_1,$$

CARDINALI

Consideriamo gli ordinali ω e ω_1. Essi sono particolari, in quanto hanno due proprietà:

- $n < \omega \Rightarrow |n| < |\omega|$;
- $\alpha < \omega_1 \Rightarrow |\alpha| < |\omega_1|$.

Un ordinale k si dice CARDINALE se è un "ordinale iniziale", ossia se:

$$\alpha < k \Rightarrow |\alpha| < |k|$$

Ad esempio $n \in \omega$ è un cardinale finito. Chiaramente, se k cardinale è infinito allora esso è un ordinale limite. Infatti, se β è infinito, allora $|\beta| = |\beta + 1|$, da cui k cardinale infinito non può essere successore.

Tuttavia, non è vero che ogni ordinale limite è cardinale: $\omega_1 + \omega$ ad esempio, non è cardinale; stessa cosa per $\omega + \omega$, ad esempio.

Il nostro obiettivo, ora, sarà quello di dimostrare che ogni insieme è equipotente ad un unico cardinale. Notiamo subito che l'assioma di scelta è necessario.

TEOREMA (DI PINCUS) (SOLO ENUNCIATO)
Senza usare l'assioma di scelta, non esistono funzioni-classe F tali che:

- $|F(A)| = |A|$;
- $|A| = |B| \Rightarrow F(A) = F(B)$

Un passo "intermedio", che si può dimostrare senza l'assioma di scelta consiste nel dimostrare che ogni insieme bene ordinabile è equipotente ad un unico cardinale.
Dopodiché useremo l'assioma di scelta, ossia il Teorema di Zermelo, per concludere che ogni insieme è equipotente ad un unico ordinale.

In particolare, se un insieme A è bene ordinabile, allora $\exists!\ \alpha \in Ord$ t.c. $(A, <) \cong (\alpha, \in)$,

e quindi $|\alpha| = |A|$.

Ogni ordinale α è equipotente ad un unico cardinale. Infatti, considerando un ordinale α, si può considerare:

$$\kappa = \min\{\beta \leq \alpha \mid |\beta| = |\alpha|\},$$

non vuoto perché α appartiene all'insieme. È ovvio che κ sia un cardinale, tale che $|\kappa| = |\alpha|$.

Se A è bene ordinabile, in conclusione, è equipotente ad un unico cardinale: l'unicità deriva dal fatto che due cardinali diversi non sono equipotenti ($\kappa_1 < \kappa_2 \Rightarrow |\kappa_1| \neq |\kappa_2|$).

A questo punto, si conclude utilizzando l'assioma di scelta.

Finora abbiamo visto solamente i cardinali finiti, ω e ω_1. Nel prossimo paragrafo, definiremo tutti i cardinali.

FUNZIONE - CLASSE "ALEPH"

Si definisce, per ricorsione transfinita:

- $\aleph_0 = \omega$;
- $\aleph_{\alpha+1} = H(\aleph_\alpha)$;
- $\aleph_\lambda = \bigcup_{\delta<\lambda} \aleph_\delta$, se λ è limite.

Ad esempio:

- $\aleph_1 = H(\aleph_0) = H(\omega) \overset{def}{=} \{ \alpha \in Ord \mid |\alpha| \leq |\omega| \} = \omega_1$;
- $\aleph_2 = H(\aleph_1) = H(\omega_1) \overset{def}{=} \{ \alpha \in Ord \mid |\alpha| \leq |\omega_1| \} = \omega_2$.

OSSERVAZIONE

Si noti che:

$$\aleph_1^{\aleph_0} = c$$

Si ha in particolare:

- $\omega_1^{\omega_0} > \omega_1$;
- $|\omega_1^{\omega_0}| = |\omega_1|$.

Non bisogna dunque confondere i cardinali con gli ordinali.

Si ha inoltre, ad esempio:

$$\aleph_\omega = \bigcup_{n<\omega} \aleph_n$$

COMPLEMENTI VARI

PROPOSIZIONE

Sia $\alpha \geq \omega$. Sono equivalenti:

- $\forall \beta < \alpha : \beta \cdot \alpha = \alpha$
- $\forall \beta, \gamma < \alpha : \beta \cdot \gamma < \alpha$
- $\exists \delta \in \mathrm{Ord} \ni' \alpha = \omega^{\omega^\delta}$

Dim

Che la prima affermazione implichi la seconda, è ovvio:

$\forall \beta, \gamma < \alpha : \beta \cdot \gamma < \beta \cdot \alpha = \alpha$

Dimostriamo ora che la seconda affermazione implica la terza.

> OSSERVAZIONE
>
> Si ha:
>
> $\forall \delta \in \mathrm{Ord} : \omega^{\omega^\delta} \geq \omega^\delta \geq \delta$.

Consideriamo allora:

$$\Lambda = \{\delta \in \alpha + 1 \mid \omega^{\omega^\delta} > \alpha\}$$

Sia $\xi = \min \Lambda$.

Allora:

- $\xi \neq 0$. Infatti $\omega^{\omega^0} = \omega^1 = \omega$ non è strettamente maggiore di α;
- ξ non è limite, se infatti fosse $\alpha < \omega^{\omega^\xi} = \bigcup_{\delta < \xi} \omega^{\omega^\delta}$, esisterebbe $\delta < \xi$ con $\alpha < \omega^{\omega^\delta}$, contro la minimalità di ξ.

Allora $\xi = \beta + 1$ è successore. Dunque:

$$\omega^{\omega^\beta} \leq \alpha < \omega^{\omega^{\beta+1}}$$

In generale:

$$\alpha < \omega^{\omega^{\beta+1}} = \omega^{\omega^\beta \omega} = \bigcup_{n<\omega} \omega^{\omega^\beta n} \Rightarrow \exists n < \omega \ni' \omega^{\omega^\beta n} \leq \alpha \leq \omega^{\omega^\beta (n+1)}$$

Sosteniamo che $\omega^{\omega^\beta} = \alpha$. Se così non fosse, effettuando la divisione euclidea otterremmo:

$$\alpha = \omega^{\omega^\beta n} + \rho, \quad \rho < \omega^{\omega^\beta}$$

Supponiamo che $\omega^{\omega^\beta} < \alpha$. Allora:

- se $\rho = 0$, $\omega^{\omega^\beta n} = \alpha$, $n \geq 2$. Allora si ha un assurdo:

$$\omega^{\omega^\beta}, \omega^{\omega^\beta (n-1)} < \alpha, \quad \omega^{\omega^\beta} \cdot \omega^{\omega^\beta (n-1)} = \omega^{\omega^\beta n} = \alpha;$$

- se $\beta > 0$, allora si ha di nuovo un assurdo:

$$\omega^{\omega^\beta},\ \omega^{\omega^\beta \cdot n} < \alpha,\quad \omega^{\omega^\beta} \cdot \omega^{\omega^\beta \cdot n} = \omega^{\omega^{\beta}(n+1)} > \alpha$$

Dunque necessariamente $\alpha = \omega^{\omega^\beta}$, ossia la tesi.

Dimostriamo ora che l'ultima affermazione implica la prima.
Sia dunque $\omega^{\omega^\beta} = \alpha$:

- se $\beta = 0$, allora:
  $\forall \gamma < \omega^{\omega^0} = \omega^1 = \omega : \gamma \cdot \omega = n \cdot \omega = \omega = \omega^{\omega^0}$;
- se $\beta = \phi + 1$, allora:
  $\forall \gamma < \omega^{\omega^{\phi+1}} = \omega^{\omega^\phi \omega} = \bigcup_{n<\omega} \omega^{\omega^\phi n} : \exists\, n < \omega \ni' \gamma < \omega^{\omega^\phi n}$,
  da cui:
  $\alpha \leq \gamma \cdot \alpha \leq \omega^{\omega^\phi n} \cdot \omega^{\omega^\phi \omega} = \omega^{\omega^\phi (n+\omega)} = \omega^{\omega^\phi \omega} = \alpha$,
- se $\beta = \lambda$ è limite, allora:
  $\forall \gamma < \alpha = \omega^{\omega^\lambda} = \bigcup_{\phi<\lambda} \omega^{\omega^\phi} : \exists\, \phi < \lambda \ni' \gamma < \omega^{\omega^\phi} \Rightarrow$
  $\Rightarrow \gamma \cdot \alpha \leq \omega^{\omega^\phi} \cdot \omega^{\omega^\lambda} = \omega^{\omega^{(\phi+\lambda)}} = \omega^{\omega^\lambda} = \alpha$,

e con ciò la dimostrazione è conclusa, c.v.d.

FORMA NORMALE DI CANTOR (BASE ω)

TEOREMA (FORMA NORMALE DI CANTOR, BASE ω)

Sia $\alpha > 0$ un qualsiasi ordinale non nullo. Allora:

$\exists!\ \gamma_1 > \dots > \gamma_k$, $\exists!\ m_i \in \omega$, $m_i \neq 0$ $\ni'$

$$\alpha = \omega^{\gamma_1} m_1 + \dots + \omega^{\gamma_k} m_k$$

Dim.

PREMESSA

Se il teorema è vero, sarà, ad esempio:

$\alpha < \omega^4 \Rightarrow \alpha = \omega^3 \cdot n + \omega^2 \cdot m + \omega \cdot p + q$, $m, n, p, q < \omega$

Dimostriamo l'esistenza procedendo per induzione transfinita: dato $\alpha \in \mathrm{Ord}$, supponiamo per ipotesi induttiva che la forma normale esista per tutti gli ordinali $\beta < \alpha$.

Come visto in una dimostrazione precedente:

$\exists\ \gamma_1 \in \mathrm{Ord}$ $\ni'$ $\omega^{\gamma_1} \leq \alpha < \omega^{\gamma_1 + 1}$

Operando la divisione euclidea, si ottiene:

$$\alpha = \omega^{\gamma_1} \cdot m_1 + \rho, \quad \rho < \omega^{\gamma_1}, \quad m_1 \neq 0, \quad m_1 < \omega$$

(se infatti fosse $m_1 \geq \omega$ si avrebbe $\alpha \geq \omega^{\gamma_1} \cdot \omega = \omega^{\gamma_1+1}$, un assurdo).

Per ipotesi induttiva, $\rho < \omega^{\gamma_1} \leq \alpha$ ha la seguente forma normale:

$$\rho = \omega^{\beta_1} m_1 + \dots + \omega^{\beta_k} m_k,$$

ove:

- $\beta_1 > \dots > \beta_k$;
- $m_i \neq 0$, $m_i < \omega$ $\forall\, i = 1 \dots k$.

Per concludere, dimostriamo che $\gamma_1 > \beta_1$. In effetti:

$$\rho < \omega^{\gamma_1} \Rightarrow \omega^{\beta_1} \leq \rho < \omega^{\gamma_1} \Rightarrow \beta_1 < \gamma_1$$

La dimostrazione dell'esistenza è conclusa. Notiamo tuttavia che, se vale $\gamma_1 > \dots > \gamma_k$, allora:

$$\omega^{\gamma_1} m_1 + \dots + \omega^{\gamma_k} m_k \leq \omega^{\gamma_1} m_1 + \dots + \omega^{\gamma_1} m_k =$$
$$= \omega^{\gamma_1}(m_1 + \dots + m_k) < \omega^{\gamma_1} \cdot \omega = \omega^{\gamma_1 + 1}$$

In conclusione, dunque:

$$\alpha = \omega^{\gamma_1} m_1 + \omega^{\beta_1} m_1 + \dots + \omega^{\beta_k} m_k$$

Dimostriamo ora l'unicità: procediamo anche in questo caso per induzione transfinita. Sia:

$$\alpha = \omega^{\gamma_1} m_1 + \dots + \omega^{\gamma_k} m_k = \omega^{\beta_1} m_1 + \dots + \omega^{\beta_h} m_h$$

Innanzitutto, $\gamma_1 = \beta_1$. Se così non fosse, avremmo, ad esempio $\gamma_1 < \beta_1$, da cui:

$$\alpha < \omega^{\gamma_1 + 1} \leq \omega^{\beta_1} \leq \alpha,$$

palesemente assurdo.
A questo punto, effettuando la divisione euclidea, e poi procedendo per ipotesi induttiva nel resto ρ, si conclude la dimostrazione.

Se $\omega^\alpha = \alpha$, quella è la sua forma normale di Cantor.
Ordinali di questo genere esistono. Definiamo ad esempio:

$$\begin{cases} \beta_0 = \gamma \\ \beta_{n+1} = \omega^{\beta_n} \end{cases}$$

Si ha, in generale:

$$\beta_0 \leq \beta_1 \leq \dots \leq \beta_k \leq \dots$$

I casi sono due:

- esiste $k < \omega$ per cui $\beta_k = \omega^{\beta_k}$. Allora:

$$\beta_0 \leq \dots \leq \beta_k = \beta_{k+1} = \dots = \dots,$$

da cui:

$$\beta_k = \omega^{\beta_k};$$

- la catena ascendente non è stazionaria:

$$\beta_0 < \dots < \beta_k < \dots < \dots$$

Allora, considerando:

$$\beta \overset{def}{=} \bigcup_{k<\omega} \beta_k$$

si ha:

- β è limite:

$$\forall \xi < \beta \Rightarrow \exists\, n < \omega \ni \xi < \beta_n \Rightarrow \xi + 1 < \beta_{n+1} < \beta;$$

- $\beta = \omega^\beta$. Infatti:

$$\omega^\beta = \bigcup_{\xi < \beta} \omega^\xi = \bigcup_{n < \omega} \omega^{\beta_n} = \bigcup_{n < \omega} \beta_{n+1} = \beta.$$

CARDINALITÀ

La CARDINALITÀ di un insieme A è quell'unico cardinale k (ordinale iniziale) tale che $|A| = |k|$. In tal caso, si scrive direttamente $|A| = k$.

Ad esempio:

- $|\mathbb{N}| = \aleph_0$;
- $|\mathbb{N}^{\mathbb{N}}| = c$.

L'ipotesi del continuo afferma che:

$$\aleph_1 = c$$

LEMMA

Sia $\alpha \in \mathrm{Ord}$. Allora:

$$\alpha \leq \aleph_\alpha$$

Dim.

Procediamo per induzione transfinita su α:

- se $\alpha = 0$, $0 \leq \aleph_0 = \omega$;
- se $\alpha = \beta + 1$ è successore, allora:

$$\beta + 1 \leq \aleph_\beta + 1 \leq \aleph_{\beta+1} \Rightarrow \beta + 1 \leq \aleph_{\beta+1},$$

dato che, per cardinali infiniti,

$$|\aleph_\beta + 1| = |\aleph_\beta| < |\aleph_{\beta+1}|$$

- se $\alpha = \lambda$ è limite, allora:

$$\aleph_\lambda = \bigcup_{\delta < \lambda} \aleph_\delta \geq \bigcup_{\delta < \lambda} \delta = \lambda \Rightarrow \lambda \leq \aleph_\lambda,$$

e la dimostrazione è conclusa, c.v.d.

PROPOSIZIONE

L'unione di un insieme di cardinali è un cardinale.

Dim.

Sia X l'insieme di cardinali considerato, e sia $\alpha = \bigcup X$. Innanzitutto α è un ordinale. Sia ora $\beta < \alpha = \bigcup X$: allora $\beta \in \bigcup X$, $\beta \in \bigcup X$, ossia esiste $\gamma \in X$ tale che $\beta \in \gamma$. Dato che $\gamma \in X$, ossia è un cardinale, si ha:

$$|\beta| < |\gamma| \leq |\alpha|,$$

da cui α è un cardinale, c.v.d.

TEOREMA

κ è un cardinale infinito se e solo se è un Aleph: $\exists\, \alpha \in Ord$ t.c. $\kappa = \aleph_\alpha$

Dim.

Dimostriamo la seconda implicazione, procedendo per induzione transfinita su α.

Per $\alpha = 0$, $\aleph_0 = \omega$ è un cardinale infinito.

Per $\alpha = \beta + 1$ successore, si ha:

$$\aleph_{\beta+1} \overset{def}{=} H(\aleph_\beta)$$

Esso è un ordinale. Infatti:

$$\gamma < H(\aleph_\beta) \overset{def}{\Leftrightarrow} |\gamma| \leq |\aleph_\beta|$$

A questo punto si conclude, ricordando che $|\aleph_\beta| < |H(\aleph_\beta)| = |\aleph_{\beta+1}|$. Allora:

$$\gamma < \aleph_{\beta+1} \Rightarrow |\gamma| < |\aleph_{\beta+1}|,$$

e $\aleph_{\beta+1}$ è un cardinale.

Per $\alpha = \lambda$ limite, si ha:

$$\aleph_\lambda = \bigcup_{\gamma < \lambda} \aleph_\gamma$$

Per la proposizione precedente, $\aleph_\lambda$ è un cardinale.

Dimostriamo ora la prima implicazione: preso un cardinale, sia:

$$\xi = \min A_\kappa = \min \{\beta \in \kappa+1 \mid \kappa < \aleph_\beta\}$$

Allora:

- $\xi \neq 0$, in quanto $\kappa < \aleph_0 = \omega$ è falso;
- ξ non è limite, altrimenti sarebbe violata la minimalità di ξ:

$$\gamma < \aleph_\xi = \bigcup_{\phi < \xi} \aleph_\phi \Rightarrow \exists\, \phi < \xi \text{ t.c. } \gamma < \aleph_\phi$$

Allora $\xi = \psi + 1$ è un successore. Allora:

$$\aleph_\psi \leq \kappa < \aleph_\xi = H(\aleph_\psi)$$

$$|\kappa| \leq |\aleph_\psi|,$$

e per il Teorema di Cantor-Bernstein, unito al fatto che due cardinali equipotenti sono uguali, si ha la tesi:

$$|\kappa| = |\aleph_\psi| \Rightarrow \kappa = \aleph_\psi, \text{ c.v.d.}$$

OPERAZIONI TRA CARDINALI

Siano A e B insiemi tali che $|A| = \kappa$, $|B| = \mu$, con $A \cap B = \emptyset$. Allora si definisce la SOMMA:

$$\kappa + \mu \overset{def}{=} |A \cup B|$$

Ad esempio:

- $\aleph_0 + \aleph_0 = \aleph_0$;
- $\aleph_0 + c = c$;
- $c + c = c$.

La definizione è ovviamente ben posta, e la dimostrazione è semplice, e fa uso di bigezioni. Dunque:

$$\begin{cases} |A| = |A'| \\ |B| = |B'| \end{cases}, \quad A \cap B = \emptyset = A' \cap B' \Rightarrow |A \cup B| = |A' \cup B'|$$

Siano ora A e B insiemi, con $|A| = \kappa$, $|B| = \mu$. Allora si definisce il PRODOTTO:

$$\kappa \cdot \mu \overset{def}{=} |A \times B|$$

Ad esempio:

- $\aleph_0 \cdot n = \aleph_0$;
- $\aleph_0 \cdot \aleph_0 = \aleph_0$;
- $c \cdot \aleph_0 = c$;
- $c \cdot c = c$.

La definizione è ben posta anche in questo caso.

PROPOSIZIONE

Se κ, μ sono cardinali infiniti, allora:

$$\kappa \cdot \mu = \kappa + \mu = \max\{\kappa, \mu\}$$

Dim.

Sia $\nu = \max\{\kappa, \mu\}$. Allora, usando l'assioma della scelta:

- $\nu \leq \kappa + \mu \leq \nu + \nu = \nu \cdot 2 \leq \nu \cdot \nu = \nu$;
- $\nu \leq \kappa \cdot \mu \leq \nu \cdot \nu = \nu$, c.v.d.

Definiamo infine l' ESPONENZIAZIONE di cardinali. Dati A e B insiemi, con $|A| = k$, $|B| = \mu$, si definisce:

$$k^{\mu} \overset{def}{=} \left| \{ f : B \to A \} \right| = |A^B|$$

Anche in questo caso la definizione è ben posta.

Si ha ad esempio:

- $2^{\aleph_0} = c$;
- $c = 2^{\aleph_0} \leq \aleph_1^{\aleph_0} \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \times \aleph_0} = 2^{\aleph_0} = c \Rightarrow$
  $\Rightarrow \aleph_1^{\aleph_0} = c$, per il teorema di Cantor-Bernstein.

PROPOSIZIONE

Siano k, μ cardinali infiniti, con $k \leq 2^{\mu}$. Allora:

$$k^{\mu} = 2^{\mu}$$

In particolare $k^{k} = 2^{k}$.

Dim.

PREMESSA

La disuguaglianza $\aleph_1^{\aleph_0} \leq c$ può essere provata con questa proposizione:

$$\aleph_1 \leq 2^{\aleph_0} \Rightarrow \aleph_1^{\aleph_0} \leq 2^{\aleph_0} = c$$

Usando l'assioma della scelta e il teorema di Cantor-Bernstein:

$$2^{\mu} \leq k^{\mu} \leq (2^{\mu})^{\mu} = 2^{\mu \times \mu} = 2^{\mu}, \text{ c.v.d.}$$

Ex. I cardinali sono particolari ordinali. Dunque, se $k_1 \leq k_2$ e $\mu_1 \leq \mu_2$:

- $k_1 + \mu_1 \leq k_1 + \mu_2 \leq k_2 + \mu_2$;
- $k_1 \cdot \mu_1 \leq k_1 \cdot \mu_2 \leq k_2 \cdot \mu_2$.

Più complicato è senz'altro dimostrare che:

$$k_1^{\mu_1} \leq k_2^{\mu_2}$$

Dalla definizione, si ha $k_2^{\mu_2} = |A_2^{B_2}|$. Siano ora $A_1 \subseteq A_2$ e $B_1 \subseteq B_2$, tali che $|A_1| = k_1$, $|B_1| = \mu_1$.

Allora:

$$A_1 \leq A_2 \,,\ B_1 \leq B_2 \Rightarrow$$
$$\Rightarrow A_1^{B_2} \leq A_2^{B_2}$$

Inoltre una funzione $f: B_1 \to A_1$ può essere facilmente estesa ad una funzione $f_*: B_2 \to A_2$. Allora:

$$|A_1^{B_1}| \leq |A_2^{B_2}|$$
$$K_1^{\mu_1} \leq \mu_2^{K_2}.$$

OSSERVAZIONE

Se dunque K è un cardinale infinito:

$$2^K \leq K^K \leq 2^K$$
$$2^K = K^K.$$

Ex. Siano α, β ordinali infiniti. Allora:

$$|\alpha+\beta| = |\alpha\cdot\beta| = |\alpha^\beta| = \max\{|\alpha|,|\beta|\}$$

Infatti:

- $|\alpha+\beta| = |\alpha \oplus \beta| = |\alpha \times \{0\} \cup \beta \times \{1\}| = |\alpha \times \{0\}| + |\beta \times \{1\}| = |\alpha| + |\beta| = \max\{|\alpha|,|\beta|\}$;
- $|\alpha\cdot\beta| = |\alpha \otimes \beta| = |\alpha \times \beta| = |\alpha|\cdot|\beta| = \max\{|\alpha|,|\beta|\}$
- Ragioniamo per induzione transfinita su β.

Se $\beta = \omega$ e α è infinito, ossia $|\omega| \leq |\alpha|$:

$$|\alpha^\omega| = \left|\bigcup_{n<\omega} \alpha^n\right| \leq \sum_{n<\omega} |\alpha^n| = \sum_{n<\omega} |\alpha| = |\alpha|\cdot|\omega| = |\alpha| =$$
$$= \max\{|\alpha|,|\omega|\}$$

(notiamo che per affermare che $|\alpha^n| = |\alpha|$ per ogni $n \in \mathbb{N}$, è necessario l'assioma di scelta). D'altra parte:

$$|\omega| \leq |\alpha| \leq |\alpha^\omega|$$

Se invece $|\alpha| < |\omega|$:

$$|\alpha^\omega| = \left|\bigcup_{n<\omega} \alpha^n\right| \leq \sum_{n<\omega} |\alpha^n| = \sum_{k<\omega} |k| = |\omega| = \max\{|\alpha|,|\omega|\},$$

e d'altra parte α^ω è infinito, dunque $|\omega| \leq |\alpha^\omega|$.

Se $\beta = \gamma + 1$, allora per ipotesi induttiva:
$$|\alpha^\gamma| = \max\{|\alpha|, |\gamma|\}$$
si ha allora:
$$|\alpha^\beta| = |\alpha^{\gamma+1}| = |\alpha^\gamma \cdot \alpha| = |\alpha^\gamma| \cdot |\alpha| = \max\{|\alpha^\gamma|, |\alpha|\} =$$
$$= \max\{|\gamma|, |\alpha|\} =$$
$$= \max\{|\gamma+1|, |\alpha|\} = \max\{|\beta|, |\alpha|\},$$
dato che (per γ infinito), vale evidentemente $|\gamma| = |\gamma+1|$.

Se infine $\beta = \lambda$ è limite, per ipotesi induttiva:
$\forall \gamma < \lambda : |\alpha^\gamma| = \max\{|\gamma|, |\alpha|\}$
Allora:
$$|\alpha^\lambda| = \left|\bigcup_{\gamma<\lambda} \alpha^\gamma\right| \leq \sum_{\gamma<\lambda} |\alpha^\gamma| = \sum_{\gamma<\lambda} \max\{|\gamma|, |\alpha|\} \leq$$
$$\leq \sum_{\gamma<\lambda} \max\{|\lambda|, |\alpha|\} = \max\{|\lambda|, |\alpha|\} \cdot |\lambda| =$$
$$= \max\{\max\{|\lambda|, |\alpha|\}, |\lambda|\} = \max\{|\alpha|, |\lambda|\},$$
e d'altro canto:

- $|\alpha| \leq |\alpha^\lambda|$;
- $|\lambda| \leq |2^\lambda| \leq |\alpha^\lambda|$,

da cui $\max\{|\alpha|, |\gamma|\} \leq |\alpha^\lambda|$, da cui l'uguaglianza, per il teorema di Cantor-Bernstein.

Ex. Si ha, in effetti:

- $|2^\omega| = \left|\bigcup_{i<\omega} 2^i\right| \leq \sum_{i<\omega} |2^i| = \sum_{k<\omega} k = \omega \leq |2^\omega|$;
- $|\omega| \leq |\omega^\omega| = \left|\bigcup_{n<\omega} \omega^n\right| \leq \sum_{n<\omega} |\omega^n| = \sum_{n<\omega} |\omega| = |\omega| \cdot |\omega| =$
  $= |\omega|$.

Allora $|2^\omega| = |\omega^\omega| = \aleph_0$.

OSSERVAZIONE
Non bisogna confondere l'esponenziazione tra ordinali con quella tra cardinali. Ad esempio $\omega = \aleph_0$, ma:
$$|2^\omega| = |\omega| = \aleph_0 < c = 2^{\aleph_0}$$

PUNTI FISSI

Chiamiamo PUNTI FISSI:

- gli ordinali α tali che $\omega^\alpha = \alpha$;
- gli ordinali α tali che $\aleph_\alpha = \alpha$.

Abbiamo visto che esistono ordinali di questo tipo.

Considerando le funzioni - classe:

$$F: \mathrm{Ord} \to \mathrm{Ord} \qquad\qquad G: \mathrm{Ord} \to \mathrm{Ord}$$
$$\alpha \to \omega^\alpha \qquad\qquad \alpha \to \aleph_\alpha,$$

il nome di punto fisso è pienamente giustificato.

PROPOSIZIONE

Sia $F: \mathrm{Ord} \to \mathrm{Ord}$ una funzione tale che:

- $\alpha < \beta \Rightarrow F(\alpha) < F(\beta)$,
- F è "continua", ossia, se λ è limite:

$$F\left(\bigcup_{\delta<\lambda} \delta\right) = \bigcup_{\delta<\lambda} F(\delta)$$

Allora F ammette punti fissi.

Infine, se F è strettamente crescente, allora F ammette frequentemente punti fissi:
$\forall \beta\ \exists \alpha > \beta$ t.c. $F(\alpha) = \alpha$

Dim.

Dimostriamo la proposizione nel caso in cui F è strettamente crescente.

LEMMA

Si ha, per ogni $\beta \in \mathrm{Ord}$:

$$\beta \leq F(\beta)$$

Dim.

Procediamo per induzione transfinita su β:

- $0 \leq F(0)$ è ovvio;
- se $\beta \leq F(\beta)$, usando l'ipotesi induttiva e la stretta monotonia di F:

$$\beta \leq F(\beta) < F(\beta+1) \Rightarrow$$
$$\Rightarrow \beta+1 \leq F(\beta+1)$$

- se λ è limite, allora:

$$\lambda = \bigcup_{\beta<\lambda} \beta = \bigcup_{\beta<\lambda} F(\beta) = F(\lambda) \text{, c.v.d.}$$

Consideriamo:

$$\begin{cases} \alpha_0 = \beta \\ \alpha_{n+1} = F(\alpha_n) \end{cases}$$

Sia:

$$\alpha \overset{def}{=} \bigcup_{n\in\omega} F(\alpha_n)$$

Se esiste $k < \omega$ t.c. $\alpha_k = F(\alpha_k)$, la catena è definitivamente stazionaria, e in ogni caso $\alpha_k \geq \beta$ è punto fisso.

Altrimenti, se:

$$\alpha_0 < \alpha_1 < \dots < \alpha_k < \dots,$$

allora α è limite perché è evidente che non abbia massimo. Dato che α è limite, si ha:

$$F(\alpha) = F\left(\bigcup_{n\in\omega} \alpha_n\right) = \bigcup_{n\in\omega} F(\alpha_n) = F(\alpha),$$

e banalmente $\alpha > \beta$.

Dunque si ha la tesi, c.v.d.

ESERCIZI CON I CARDINALI

Calcoliamo alcune cardinalità ($n \geq 2$):

- $\aleph_0 + n$, $n < \omega$. Si ha:

$$\aleph_0 \leq \aleph_0 + n \leq \aleph_0 + \aleph_0 = \aleph_0,$$

da cui $\aleph_0 + n = \aleph_0$;

- $\aleph_0 \cdot \aleph_0 = \aleph_0$;

- $\aleph_0 \cdot n = \aleph_0$. Infatti:

$$\aleph_0 \leq \aleph_0 \cdot n \leq \aleph_0 \cdot \aleph_0 = \aleph_0;$$

- $\aleph_0^n = \aleph_0$. Infatti, per induzione su n:
  - $\aleph_0^2 = \aleph_0 \cdot \aleph_0 = \aleph_0$;
  - $\aleph_0^{n+1} = \aleph_0^n \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0$;

- $\aleph_0^{\aleph_0} = c$. Infatti:

$$c = 2^{\aleph_0} \leq \aleph_0^{\aleph_0} \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0},$$

avendo usato:

$$\aleph_0 \leq 2^{\aleph_0};$$

- $n^{\aleph_0} = c$. Infatti:

$$c = 2^{\aleph_0} \leq n^{\aleph_0} \leq \aleph_0^{\aleph_0} = c.$$

- $\aleph_1^{\aleph_0} = c$. Infatti:

$$c = 2^{\aleph_0} \leq \aleph_1^{\aleph_0} \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0};$$

- $c^n = c$, banalmente (per induzione);

- $c^c = 2^c$. Allora, dato che:

$$2^c \leq n^c \leq \aleph_0^c \leq \aleph_1^c \leq c^c = 2^c,$$

allora:

- $n^c = 2^c$;
- $\aleph_0^c = 2^c$;
- $\aleph_1^c = 2^c$;

- $\aleph_1^{\aleph_1} = 2^{\aleph_1}$;
- $\aleph_0^{\aleph_1} = 2^{\aleph_1}$. Infatti:

$$2^{\aleph_1} \leq \aleph_0^{\aleph_1} \leq \aleph_1^{\aleph_1} = 2^{\aleph_1};$$

- $c^{\aleph_0} = c$. Infatti:

$$c^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = c$$

- $c^{\aleph_1} = (2^{\aleph_0})^{\aleph_1} = 2^{\aleph_0 \cdot \aleph_1} = 2^{\aleph_1}$.

SOMME E PRODOTTI INFINITI DI CARDINALI

Sia $\langle k_i \mid i \in I \rangle$ una I-sequenza di cardinali.
Definiamo la somma infinita:

$$\sum_{i \in I} k_i \overset{def}{=} \left| \bigcup_{i \in I} A_i \right|,$$

con:

- $\forall\, i \in I : |A_i| = k_i$;
- $\forall\, i \neq j : A_i \cap A_j = \emptyset$.

Si definisce poi il prodotto infinito:

$$\prod_{i \in I} k_i \overset{def}{=} \left| \prod_{i \in I} A_i \right|,$$

ove:

$\forall\, i \in I : |A_i| = k_i$.

La definizione è ben posta; inoltre, se I è finito, le definizioni date coincidono con quelle di somma e prodotto finiti.

Inoltre:

$$(\forall\, i \in I : k_i \leq \mu_i) \Rightarrow \sum_{i \in I} k_i \leq \sum_{i \in I} \mu_i \,,\ \prod_{i \in I} k_i \leq \prod_{i \in I} \mu_i$$

Dimostreremo più avanti quanto segue:

- $\sum_{i \in I} k = k \cdot |I|$;
- $\prod_{i \in I} k = k^{|I|}$;
- $\prod_{i \in I} k^{\mu_i} = k^{\sum_{i \in I} \mu_i}$;
- $\left(\prod_{i \in I} k_i \right)^{\nu} = \prod_{i \in I} k_i^{\nu}$.

Si ha, ad esempio:

- $\sum_{n \in \omega} n = \aleph_0$. Infatti:

$$\aleph_0 = \sum_{n \geq 1} 1 \leq \sum_{n \in \omega} n \leq \sum_{n \in \omega} \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0 \,;$$

- $\prod_{n \geq 1} n = c$. Infatti:

$$c = 2^{\aleph_0} = \prod_{n \geq 1} 2 \leq \prod_{n \geq 1} n \leq \prod_{n \geq 1} \aleph_0 = \aleph_0^{\aleph_0} = c.$$

PROPOSIZIONE

Siano I e k_i infiniti (per ogni $i \in I$). Allora:

$$\sum_{i \in I} k_i = \max \{ |I|, \sup_{i \in I} k_i \}$$

Dim.

Definiamo:

$$\lambda \overset{def}{=} \sup_{i \in I} k_i$$

Allora:

$$\sum_{i \in I} k_i \leq \sum_{i \in I} \lambda = \lambda \cdot |I| = \max \{ \lambda, |I| \}$$

D'altra parte:

- $\sum_{i \in I} k_i \geq \sum_{i \in I} 1 = |I|$;
- $\sum_{i \in I} k_i \geq \lambda$,

da cui:

$$\sum_{i \in I} k_i \geq \max \{ |I|, \lambda \}$$

da cui la tesi, c.v.d.

Ad esempio:

$$\sum_{n < \omega} \aleph_n = \max \{ \aleph_0, \aleph_\omega \} = \aleph_\omega$$

Studiare la cardinalità del prodotto è più complicato.

In particolare, ad esempio:

$$\prod_{n < \omega} \aleph_n \leq \prod_{n < \omega} \aleph_\omega = \aleph_\omega^{\aleph_0}$$

Ottenere l'altra disuguaglianza non è semplice.

PREMESSA

Si può dimostrare che, considerata una sequenza:

$$\langle k_{ij} \mid i \in I, j \in J \rangle$$

Allora:

- $\sum_{i \in I} \left(\sum_{j \in J} k_{ij} \right) = \sum_{j \in J} \left(\sum_{i \in I} k_{ij} \right)$;
- $\prod_{i \in I} \left(\prod_{j \in J} k_{ij} \right) = \prod_{j \in J} \left(\prod_{i \in I} k_{ij} \right)$.

Allora ad esempio:

$$\prod_{n<\omega} \aleph_n \geq \prod_{p \text{ primo}} \left(\prod \aleph_{p^n} \right) \geq \prod_{p \text{ primo}} \aleph_\omega = \aleph_\omega^{\aleph_0},$$

da cui:

$$\prod_{n<\omega} \aleph_n = \aleph_\omega^{\aleph_0}.$$

Infatti:

$$\prod_{n<\omega} \aleph_{p^n} \geq \sup_{n<\omega} \aleph_{p^n} = \aleph_\omega$$

PROPOSIZIONE

Sia I un insieme infinito. Allora esiste una famiglia di insiemi $\{A_i \mid i \in I\}$ a due a due disgiunti, tale che:

$$|A_i| = |I|, \quad \bigcup_{i \in I} A_i = I$$

Dim.

Sappiamo che $|I \times I| = |I|$, da cui esiste $\psi : I \times I \to I$ biunivoca. Definiamo:

$\forall i \in I : A_i \stackrel{\text{def}}{=} \{ \psi(i, j) \mid j \in I \}$

Si ha:

- $\bigcup_{i \in I} A_i = \operatorname{Im} \psi = I$;
- $|A_i| = |I| \ \forall i \in I$, perché $\psi(i, \cdot) : A_i \to I$ è biunivoca.

Infine $i \neq j \Rightarrow A_i \cap A_j = \emptyset$, perché:
$\forall h, k \in I : \psi(i, h) \neq \psi(j, k)$, c.v.d.

Siano ora k_i $(i \in \nu)$ e ν cardinali infiniti. Se $\langle k_i \mid i \in \nu \rangle$ è una sequenza debolmente crescente di cardinali, allora:

$$\prod_{i \in \nu} k_i = \left(\sup_{i \in \nu} k_i \right)^\nu$$

Per dimostrarlo, sia $k = \sup_{i \in \nu} k_i$.
Allora:

$$\prod_{i \in \nu} k_i \leq \prod_{i \in \nu} k = k^\nu$$

Viceversa, per la proposizione precedente, esistono $A_j \subseteq \nu$ (con $j \in \nu$), a due a due disgiunti, tali che:

$$|A_j| = \nu \quad \forall\, j \in \nu \quad , \quad \bigcup_{j \in \nu} A_j = \nu$$

Si ha ora:

$$\prod_{i \in \nu} k_i = \prod_{j \in \nu} \left(\prod_{i \in A_j} k_i \right),$$

e inoltre:

$\forall\, j \in \nu$: $\prod_{i \in A_j} k_i \geq \sup_{i \in A_j} k_i$

Osserviamo che $A_j \subseteq \nu$, con $|A_j| = \nu$. Allora A_j deve essere illimitato in ν, perché altrimenti esisterebbe $\beta < \nu$ tale che $A_j \subseteq \beta$, da cui l'assurdo (ν è cardinale):

$$|A_j| \leq |\beta| < \nu$$

Visto che $\langle k_i \mid i \in I \rangle$ è debolmente crescente, e inoltre $A_j \subseteq \nu$ è illimitato per ogni $j \in \nu$. Allora:

$$\sup_{i \in A_j} k_i = k$$

Infatti, per ogni $i_0 \in \nu$, esiste $i \in A_j$ con $i > i_0$, da cui:

$$k_i \geq k_{i_0} \Rightarrow \sup_{i \in A_j} k_i \geq k_{i_0}$$

Ciò vale per ogni $i_0 \in I$, da cui:

$$k = \sup_{i \in \nu} k_i \geq \sup_{i \in A_j} k_i \geq \sup_{i \in A_j} k_{i_0} = k,$$

da cui:

$$\prod_{i \in \nu} k_i = \prod_{j \in \nu} \left(\prod_{i \in A_j} k_i \right) \geq \prod_{j \in \nu} k = k^{\nu}, \text{ c.v.d.}$$

PUNTUALIZZAZIONI

Dimostriamo che:

$$\sum_{i \in I} k = k \cdot |I|$$

In effetti (sia $|A| = k$):

$$\sum_{i \in I} k = \left| \bigcup_{i \in I} A \right| = \left| \bigcup_{i \in I} A \times \{i\} \right| = \left| A \times I \right| \stackrel{def}{=} k \cdot |I|$$

Dimostriamo ora che:

$$\prod_{i \in I} k = k^{|I|}$$

In effetti (sia $|A| = k$):

$$\prod_{i \in I} k = \left| \prod_{i \in I} A \right| = \left| A^I \right| \stackrel{def}{=} k^{|I|}$$

Dimostriamo ora che:

$$\prod_{i \in I} k^{\mu_i} = k^{\sum_{i \in I} \mu_i}$$

In effetti:

- se $f : \bigcup_{i \in I} A_i \to A$ ($|A_i| = \mu_i$, $|A| = k$), allora:

  $\forall i \in I \;\exists f_i : A_i \to A$,

  e tutto è ben definito perché $A_i \cap A_j = \emptyset$ sempre.

  Allora $F = \langle f_i \mid i \in I \rangle \in \prod_{i \in I} A^{A_i}$;

- data $F = \langle f_i \mid i \in I \rangle \in \prod_{i \in I} A^{A_i}$, si può considerare la funzione globale:

  $$f : \bigcup_{i \in I} A_i \to A,$$

  ben definita perché $A_i \cap A_j = \emptyset$ sempre. In particolare, se $f \in A^{\bigcup_{i \in I} A_i}$.

Dunque si ha la tesi:

$$\prod_{i \in I} k^{\mu_i} = k^{\sum_{i \in I} \mu_i}$$

Dimostriamo ora che:

$$\left(\prod_{i\in I} k_i\right)^{\nu} = \prod_{i\in I} k_i^{\nu}$$

In effetti (siano $|A_i| = k_i$, $|A| = \nu$):

- se $f : A \to \prod_{i\in I} A_i$, a ogni elemento $a \in A$ corrisponde una I-sequenza g_a tale che $g_a(i) \in A_i \ \forall i \in I$.
  Possiamo allora definire, per $i \in I$, $h_i : A \to A_i$ in questo modo:
  $$h_i(a) \stackrel{\text{def}}{=} g_a(i)$$
  Si ha allora $H = \langle h_i \mid i \in I \rangle \in \prod_{i\in I} A_i^A$;
- È chiaro che si può eseguire la costruzione inversa.

Dunque:

$$\left(\prod_{i\in I} k_i\right)^{\nu} = \prod_{i\in I} k_i^{\nu}$$

Sia ora:

$$\langle k_{ij} \mid i \in I, j \in J \rangle$$

una sequenza.
Vogliamo dimostrare che:

- $\displaystyle\sum_{i\in I}\left(\sum_{j\in J} k_{ij}\right) = \sum_{j\in J}\left(\sum_{i\in I} k_{ij}\right)$;
- $\displaystyle\prod_{i\in I}\left(\prod_{j\in J} k_{ij}\right) = \prod_{j\in J}\left(\prod_{i\in I} k_{ij}\right)$.

Dunque (sia $|A_{ij}| = k_{ij}$):

$$\bigcup_{i\in I}\left(\bigcup_{j\in J} A_{ij}\right) = \left\{ x \mid \exists\, i \in I \ni x \in \bigcup_{j\in J} A_{ij} \right\} =$$
$$= \{ x \mid \exists\, i \in I, \exists\, j \in J \ni' x \in A_{ij} \} =$$
$$= \left\{ x \mid \exists\, j \in J \ni' x \in \bigcup_{i\in I} A_{ij} \right\} = \bigcup_{j\in J}\left(\bigcup_{i\in I} A_{ij}\right)$$

In maniera analoga, dimostreremo l'altra uguaglianza.
Si ha:

$$\prod_{i\in I}\left(\prod_{j\in J} A_{ij}\right) = \{ f \mid f \text{ è una } i\text{-sequenza tale che}$$
$$\forall\, i \in I : f(i) \in \prod_{j\in J} A_{ij} \} =$$

$= \{ f \mid f$ è una i-sequenza tale che $\forall i \in I$
$f(i)$ è una j-sequenza tale che $f(i)(j) \in A_{ij}$
$\forall j \in J \} \approx$

$\approx \{ g \mid g$ è una j-sequenza tale che $\forall j \in J$
$g(j)$ è una i-sequenza tale che $g(j)(i) \in A_{ij}$
$\forall i \in I \} =$

$= \{ g \mid g$ è una j-sequenza tale che $\forall j \in J$:
$g(j) \in \prod_{i \in I} A_{ij} \} = \prod_{j \in J} \left(\prod_{i \in I} A_{ij} \right)$

Di qui la tesi:

$$\prod_{i \in I} \left(\prod_{j \in J} K_{ij} \right) = \prod_{j \in J} \left(\prod_{i \in I} K_{ij} \right)$$

TEOREMA DI KÖNIG

TEOREMA (DI KÖNIG)
Siano, per ogni $i \in I$ (I insieme infinito) $\kappa_i < \mu_i$ cardinali infiniti. Allora:

$$\sum_{i \in I} \kappa_i < \prod_{i \in I} \mu_i$$

Dim.
Dimostrare che $\sum_{i \in I} \kappa_i \leq \prod_{i \in I} \mu_i$ è semplice: la tralasciamo, per ora.
Supponiamo ora, per assurdo, che esista una bigezione:

$$\varphi : \bigcup_{i \in I} A_i \longrightarrow \prod_{i \in I} B_i ,$$

ove:

- $\forall\, i \in I : |A_i| = \kappa_i$, $|B_i| = \mu_i$;
- $\forall\, i \neq j : A_i \cap A_j = \emptyset$

Consideriamo il seguente diagramma:

$$\begin{tikzcd}
A_{i_0} \arrow[r, dashed, "\theta_{i_0}"'] \arrow[d, hook, "\nu_{i_0}"'] & B_{i_0} \\
\bigcup_{i \in I} A_i \arrow[r, "\varphi"'] & \prod_{i \in I} B_i \arrow[u, "\pi_{i_0}"']
\end{tikzcd} ,$$

ove:

- ν_{i_0} è l'inclusione;
- π_{i_0} è la proiezione sull' i_0-esima componente.

Sia dunque:

$$\theta_{i_0} = \pi_{i_0} \circ \varphi \circ \nu_{i_0}$$

Visto che $|A_{i_0}| < |B_{i_0}|$, θ_{i_0} non è suriettiva.
Utilizzando l'assioma della scelta, possiamo determinare una I-upla $\vec{b} = \langle b_{i_0} \mid i_0 \in I \rangle$, ove $b_{i_0} \notin \operatorname{Im} \theta_{i_0}$ per ogni $i_0 \in I$.
Allora $\vec{b} \notin \operatorname{Im} \varphi$.

Se infatti esistesse $a \in \bigcup_{i \in I} A_i$ tale che $\varphi(a) = \vec{b}$, considerato A_{i_0} tale che $a \in A_{i_0}$, si avrebbe un assurdo:

$$\theta_{i_0}(a) = \pi_{i_0}(\varphi((\nu_{i_0}(a))) = \pi_{i_0}(\vec{b}) = b_{i_0},$$

dato che $b_{i_0} \notin \operatorname{Im} \theta_{i_0}$.

Dunque φ non è suriettiva, un assurdo.

Per completare la dimostrazione, dobbiamo dimostrare che:

$$\sum_{i \in I} k_i \leq \sum_{i \in I} \mu_i$$

Per ipotesi:

$\forall i \in f_i : A_i \to B_i$ iniettiva

Essendo gli A_i disgiunti, utilizzando l'assioma della scelta:

$\exists F : \bigcup_{i \in I} A_i \to \bigcup_{i \in I} B_i \ni' \forall i \in I, \forall a \in A_i : F(a) = f_i(a) \in B_i$

Le funzioni f_i non sono suriettive, da cui:

$\forall i \in I \ \exists x_i \notin \operatorname{Im} f_i$

Utilizzando l'assioma della scelta:

$\exists < x_i \mid i \in I > \in \prod_{i \in I} B_i \ni' \forall i \in I : x_i \notin \operatorname{Im} f_i$

Definiamo allora:

$$\Phi : \bigcup_{i \in I} A_i \to \prod_{i \in I} B_i$$

$$\Phi((i, a))(j) = \begin{cases} f_i(a), & i = j \\ x_j, & i \neq j \end{cases}$$

Tale funzione è palesemente iniettiva. Allora

$$\sum_{i \in I} k_i \leq \prod_{i \in I} \mu_i, \text{ c.v.d.}$$

COFINALITÀ

Sia $(A, <)$ un insieme totalmente ordinato. Si definisce COFINALITÀ di A:

$$\mathrm{Cof}(A) = \min \{ |X| \mid X \subseteq A \text{ è illimitato} \}$$

Facciamo un paio di osservazioni:

- se A ha massimo, allora $\mathrm{Cof}(A) = 1$;
- se A non ha massimo, allora $\mathrm{Cof}(A)$ è un cardinale infinito.

Alcuni esempi:

- $\mathrm{Cof}(\mathbb{N}, <) = \aleph_0$;
- $\mathrm{Cof}(\mathbb{R}, <) = \aleph_0$;
- $\mathrm{Cof}(\omega_1 + \omega_2) = \mathrm{Cof}(\omega^2) = \aleph_0$;

Si ha in generale:

$$\mathrm{Cof}(\alpha + \beta) = \mathrm{Cof}(\beta)$$

Studiamo ora:

$$\mathrm{Cof}(\omega_1)$$

Si ha banalmente:

$$\mathrm{Cof}(\omega_1) \leq \aleph_1$$

La diseguaglianza stretta non è possibile. Se infatti $X \subseteq \omega_1$ con $|X| < \aleph_1$, ossia $|X| \leq \aleph_0$, allora:

$$\sup X = \bigcup_{\gamma \in X} \gamma = \xi < \omega_1,$$

perché ξ è al più numerabile, essendo un unione al più numerabile di ordinali al più numerabili. Dunque X non è illimitato.

Diremo che un cardinale k è:

- REGOLARE, se $\mathrm{Cof}\, k = k$ (ad esempio, ω_1 è regolare);
- SINGOLARE, se $\mathrm{Cof}\, k < k$ (ad esempio, $\omega_1 + \omega^2$ è singolare).

A priori, infatti, è banale che sia $\mathrm{Cof}\, k \leq k$.

PROPOSIZIONE

Sia $(A, <)$ ordinato. Allora sono uguali:

- $\mathrm{Cof}(A)$;
- $\mathrm{Cof}_1(A) \overset{\text{def}}{=} \min\{\alpha \in \mathrm{Ord} \mid \exists f : \alpha \to A \text{ illimitata}\}$;
- $\mathrm{Cof}_2(A) \overset{\text{def}}{=} \min\{\alpha \in \mathrm{Ord} \mid \exists g : \alpha \to A \text{ illimitata e crescente}\}$.

Dim.

Sia $k = \mathrm{Cof}(A)$. Allora esiste $\exists X \subseteq A$ illimitato con $|X| = k$. Consideriamo $f : k \to X \subseteq A$ bigettiva; tale funzione è illimitata. Allora:

$$\mathrm{Cof}_1(A) \leq \mathrm{Cof}(A) = k$$

Sia ora $\mu = \mathrm{Cof}_1(A)$, e sia $f : \mu \to A$ illimitata. Allora $X = \mathrm{Im}\, f$ è illimitato, e $|X| \leq \mu$, da cui:

$$\mathrm{Cof}(A) \leq |X| \leq \mathrm{Cof}_1(A)$$

Dunque:

$$\mathrm{Cof}(A) = \mathrm{Cof}_1(A)$$

OSSERVAZIONE

$\mathrm{Cof}_1(A)$ è un cardinale. Se non fosse così, esisterebbe $\gamma < \mathrm{Cof}_1(A)$ con $|\gamma| = |\mathrm{Cof}_1(A)|$. Allora, se $\sigma : \gamma \to \mathrm{Cof}_1(A)$ è una bigezione, e se $f : \mathrm{Cof}_1(A) \to A$ è illimitata, allora $f \circ \sigma : \gamma \to A$ è illimitata, e ciò è assurdo.

Banalmente, ora, si ha $\mathrm{Cof}_1(A) \leq \mathrm{Cof}_2(A)$. È sufficiente allora dimostrare che:

$$\mathrm{Cof}_2(A) \leq \mathrm{Cof}(A)$$

Consideriamo $X \subseteq A$ illimitato, con $|X| = k = \mathrm{Cof}(A)$: fissiamo $\sigma : k \to X \subseteq A$ bigettiva.

Per ricorsione transfinita su k, definiamo

$$\begin{cases} f(0) = \sigma(0) \\ f(\beta) = \sigma(\beta') \end{cases}$$

con:

$$\beta' = \min\{\delta \in \mathrm{Ord} \mid \sigma(\delta) \geq \sigma(\beta) \wedge \sigma(\delta) > f(\gamma)\ \forall \gamma < \beta\} < k$$

Notiamo che, se $\beta < k$, allora:

$$|\{\delta(\beta)\} \cup \{f(\gamma) \mid \gamma < \beta\}| = |\beta + 1| < k,$$

da cui l'insieme è limitato. Dunque $\beta < k$ è ben definito.

La funzione $f: k \to X$ è illimitata, perché:
$\forall \beta < k: f(\beta) \geq \delta(\beta)$,
e δ è illimitata.

Dunque $Cof_2(A) \leq Cof(A)$, dunque la tesi, c.v.d.

PROPOSIZIONE
Si ha, per $\alpha, \beta \in Ord$:

$$Cof(\alpha + \beta) = Cof(\beta)$$

Dim.
Sia $g: Cof(\beta) \to \beta$ illimitata. Consideriamo allora:

$$G: Cof(\beta) \to \alpha + \beta$$
$$\gamma \longrightarrow \alpha + g(\gamma)$$

Tale G è illimitata. Se $\gamma \in \alpha + \beta$, i casi sono due:

- $\gamma < \alpha$, e allora $\gamma < \alpha \leq G(\xi)$ $\forall \xi \in Cof(\beta)$;
- $\gamma \geq \alpha \Rightarrow \gamma = \alpha + \gamma_1$, $\gamma_1 < \beta$. In questo caso:
  $\exists \xi \in Cof(\beta)$ t.c. $g(\xi) > \gamma_1 \Rightarrow G(\xi) = \alpha + g(\xi) >$
  $> \alpha + \gamma_1 = \gamma$.

Dunque $Cof(\alpha + \beta) \leq Cof(\beta)$.

Viceversa, sia $G: Cof(\alpha + \beta) \to \alpha + \beta$ illimitata.
Consideriamo:

$$g: Cof(\alpha + \beta) \to \beta$$
$$\xi \to \min\{\gamma < \beta \mid G(\xi) < \alpha + \gamma\}$$

g è illimitata. Per ogni $\gamma < \beta$:
$\exists \xi \in Cof(\alpha + \beta)$ t.c. $G(\xi) > \alpha + \gamma$

Dato che $G(\xi) < \alpha + g(\xi)$, si ha $\gamma < g(\xi)$.
Dunque $Cof(\beta) \leq Cof(\alpha + \beta)$, c.v.d.

CARDINALI REGOLARI E SINGOLARI

PROPOSIZIONE

Dato un cardinale κ, il suo successore si indica con κ^+.

Ogni cardinale successore $\kappa^+ = \aleph_{\alpha+1}$ è regolare.

Dim.

Sia $A \subseteq \aleph_{\alpha+1}$ con $|A| < \aleph_{\alpha+1}$: dimostriamo che A è limitato. Si ha:

$$\sup A = \bigcup_{\gamma \in A} \gamma \ , \quad \left| \bigcup_{\gamma \in A} \gamma \right| \leq \sum_{\gamma \in A} |\gamma| = \max \left\{ \sup_{\gamma \in A} |\gamma| , |A| \right\}$$

Ora:

- $\forall \gamma \in \aleph_{\alpha+1} : |\gamma| \leq \aleph_\alpha \Rightarrow \sup_{\gamma \in A} |\gamma| \leq \aleph_\alpha$;
- $|A| < \aleph_{\alpha+1} \Rightarrow |A| \leq \aleph_\alpha$.

Allora $|\sup A| \leq \max \left\{ \sup_{\gamma \in A} |\gamma| , |A| \right\} \leq \aleph_\alpha$.

Allora A è limitato, c.v.d.

PROPOSIZIONE

Sia λ un cardinale limite. Allora $Cof(\aleph_\lambda) = Cof(\lambda)$.

Dim.

Dimostriamo che $Cof(\aleph_\alpha) \leq Cof(\lambda)$. Sia $f : Cof(\lambda) \to \lambda$ una funzione illimitata. Definiamo:

$$F : Cof(\lambda) \to \aleph_\lambda$$
$$\xi \mapsto \aleph_{f(\xi)}$$

Sia $\beta \in \aleph_\lambda$: allora esiste γ tale che $\beta \in \aleph_\gamma$. Dato che f è illimitata, esiste μ con $f(\mu) > \gamma$, da cui $F(\mu) = \aleph_{f(\mu)} > \aleph_\gamma > \beta$. Dunque F è illimitata, e $Cof(\aleph_\lambda) = Cof(\lambda)$.

Viceversa, sia $F : Cof(\aleph_\lambda) \to \aleph_\lambda$ illimitata. Consideriamo:

$$f : Cof(\aleph_\lambda) \to \lambda$$
$$\xi \mapsto \min \{ \beta < \lambda \mid F(\xi) \in \aleph_\beta \}$$

Sia $\gamma < \lambda$. Allora, considerando ξ tale che $F(\xi) > \aleph_\gamma$ e $F(\xi) < \aleph_{f(\xi)}$ (per definizione), allora $\gamma < f(\xi)$, e f è illimitata, da cui $Cof(\lambda) \leq Cof(\aleph_\alpha)$, c.v.d.

TEOREMA (SOLO ENUNCIATO)

Cof $k = \nu$ se e solo se ν è il minimo cardinale tale che:

$$k = \sum_{i \in \nu} k_i \quad , \quad k_i < k$$

Vediamo ora alcune applicazioni di tale teorema:

- $k^{\mathrm{Cof}\, k} > k$ (ad esempio $\aleph_\omega^{\aleph_0} > \aleph_\omega$).

  Se $\nu = \mathrm{Cof}\, k$, allora $k = \sum_{i \in \nu} k_i$, $k_i < k \ \forall i \in \nu$.

  Per il teorema di König, si ha:

  $$k = \sum_{i \in \nu} k_i < \prod_{k \in \nu} k = k^{\nu} = k^{\mathrm{Cof}\, k} ;$$

- $\mathrm{Cof}\, 2^k > k$

  Per assurdo sia $\mathrm{Cof}\, 2^k \leq k$. Si avrebbe allora, per la proprietà precedente:

  $$2^k < (2^k)^{\mathrm{Cof}\, 2^k} \leq (2^k)^k = 2^{k \cdot k} = 2^k ,$$

  assurdo.

OSSERVAZIONE

Dato che $c = 2^{\aleph_0}$, allora:

$$\mathrm{Cof}(c) > \aleph_0 ,$$

da cui ricaviamo che:

$$c \neq \aleph_\omega \quad , \quad c \neq \aleph_{\omega+\omega} \quad , \quad c \neq \aleph_{\omega_1 + \omega^2} ,$$

ad esempio.

TEOREMA DI HAUSDORFF

TEOREMA (DI HAUSDORFF)

Si ha:

$$(\kappa^+)^\nu = \max\{\kappa^\nu, \kappa^+\} = \kappa^\nu \cdot \kappa^+ = \kappa^\nu + \kappa^+$$

Dim.

La disuguaglianza:

$$(\kappa^+)^\nu \geq \max\{\kappa^\nu, \kappa^+\}$$

è banale.

Dimostriamo dunque l'altra disuguaglianza.

Supponiamo che sia $\kappa^+ \leq \nu$. Allora:

- $\kappa^+ \leq \nu < 2^\nu$;
- $2^\nu = \kappa^\nu$; $\kappa^\nu \leq (\kappa^+)^\nu \leq \nu^\nu \leq (2^\nu)^\nu = 2^{\nu\cdot\nu} = 2^\nu$, perché $\kappa < 2^\nu$;
- $\max\{\kappa^\nu, \kappa^+\} = \max\{2^\nu, \kappa^+\} = 2^\nu$, perché $\kappa^+ < 2^\nu$.

Supponiamo ora che sia $\nu < \kappa^+$. Si ha:

$$(\kappa^+)^\nu = |\mathrm{Fun}(\nu, \kappa^+)|$$

Notiamo che ogni funzione $f : \nu \to \kappa^+$ è limitata, perché:

$$\mathrm{Cof}\ \kappa^+ = \kappa^+ > \nu$$

Allora:

$\exists\ \gamma < \kappa^+ \ni' f : \nu \to \gamma$

Allora:

$$|\mathrm{Fun}(\nu, \kappa^+)| = \left|\bigcup_{\gamma<\kappa^+} \mathrm{Fun}(\nu, \gamma)\right| \leq \sum_{\gamma<\kappa^+} |\mathrm{Fun}(\nu, \gamma)| =$$

$$= \sum_{\gamma<\kappa^+} |\gamma|^\nu = \max\left\{\sup_{\gamma<\kappa^+} |\gamma|^\nu, \kappa^+\right\} \leq$$

$$\leq \max\{\kappa^\nu, \kappa^+\}, \text{ c.v.d.}$$

PUNTUALIZZAZIONI VARIE

TEOREMA

Sia κ un cardinale infinito. Allora $\text{Cof}\,\kappa = \nu$ se e solo se ν è il minimo cardinale tale che:

$$\sum_{i \in \nu} \kappa_i = \kappa \quad , \kappa_i < \kappa$$

(Supponiamo $\kappa > \aleph_0$).

Dim.

Se κ è regolare, allora:

$$\kappa = \sum_{i \in \kappa} \aleph_0$$

Se κ è singolare, allora κ è limite, ossia $\kappa = \aleph_\lambda$, con λ limite. In questo caso:

$$\text{Cof}\ \aleph_\lambda = \text{Cof}\ \lambda ,$$

dunque esiste $f : \nu \to \lambda$ illimitata. Allora:

$$\kappa = \aleph_\lambda = \sum_{i \in \nu} \aleph_{f(i)}$$

Infatti:

$$\sum_{i \in \nu} \aleph_{f(i)} = \max \left\{ \sup_{i \in \nu} \aleph_{f(i)} , \nu \right\} = \kappa$$

$\nu = \text{Cof}\ \kappa$ è il più piccolo cardinale con quella proprietà. Infatti se $\mu < \nu$ e $\kappa_i < \kappa$:

$$\sum_{i < \mu} \kappa_i = \max \left\{ \sup_{i < \mu} \kappa_i , \mu \right\}$$

Se poniamo $\max \left\{ \sup_{i < \mu} \kappa_i , \mu \right\} = \kappa$, allora:

$$\sup_{i < \mu} \kappa_i = \kappa ,$$

da cui esisterebbe $f : \mu \to \kappa$, con $i \to \kappa_i$ illimitata perché $\sup_{i < \mu} f(i) = \kappa$. Ma ciò è assurdo, perché $\text{Cof}\ (\kappa) = \nu > \mu$.

Viceversa, sia ν il minimo cardinale tale che:

$$\sum_{i \in \nu} \kappa_i = \kappa \quad , \kappa_i < \kappa$$

A priori $\nu \leq \kappa$. Sia, per ora, $\nu < \kappa$.

Allora la funzione:

$$f : \nu \to \kappa$$
$$i \to \kappa_i$$

è illimitata in κ, da cui $\operatorname{Cof} \kappa \leq \nu$. Infatti, dato che i κ_i sono cardinali:

$$\kappa = \sum_{i \in \nu} \kappa_i = \max\{\nu, \sup_{i \in \nu} \kappa_i\}$$

da cui $\sup_{i \in \nu} \kappa_i = \kappa$.

D'altra parte non può essere $\operatorname{Cof} \kappa = \mu < \nu$ altrimenti (per quanto già dimostrato) ν non sarebbe il minimo cardinale valido per la proprietà (esso sarebbe μ): dunque $\operatorname{Cof} \kappa = \nu$.

Se $\nu = \kappa$, allora

$$\mathrm{Id} : \kappa \to \kappa$$
$$i \to i$$

è illimitata. Dunque, anche in questo caso, $\operatorname{Cof} \kappa \leq \kappa$, e l'uguaglianza deriva dalla minimalità di κ, c.v.d.

ESERCIZI VARI

1. Calcolare:

$$\aleph_\omega^{\aleph_1}$$

Si ha:

$$\prod_{n<\omega} \aleph_n^{\aleph_1} = \left(\prod_{n<\omega} \aleph_n\right)^{\aleph_1} = \left(\aleph_\omega^{\aleph_0}\right)^{\aleph_1} = \aleph_\omega^{\aleph_1}$$

Per il Teorema di Hausdorff:

$$\aleph_n^{\aleph_1} = \aleph_{n-1}^{\aleph_1} \cdot \aleph_n = \dots = \aleph_0^{\aleph_1} \cdot \aleph_1 \cdot \ldots \cdot \aleph_n =$$

$$= 2^{\aleph_1} \cdot \aleph_n$$

Ora:

$$\prod_{n<\omega} \aleph_n^{\aleph_1} = \prod_{n<\omega} 2^{\aleph_1} \cdot \aleph_n = \sup_{n<\omega} \left(2^{\aleph_1} \aleph_n\right)^{\aleph_0} =$$

$$= \left(2^{\aleph_1} \cdot \aleph_\omega\right)^{\aleph_0} = 2^{\aleph_1 \cdot \aleph_0} \cdot \aleph_\omega^{\aleph_0} = 2^{\aleph_1} \aleph_\omega^{\aleph_0}$$

Dunque:

$$\aleph_\omega^{\aleph_1} = 2^{\aleph_1} \cdot \aleph_\omega^{\aleph_0}$$

2. Sia κ un cardinale limite, e sia $\mathrm{Cof}\,\kappa \leq \nu$. Allora:

$$\kappa^\nu = \left(\sup_{\mu<\kappa} \mu^\nu\right)^{\mathrm{Cof}\,\kappa}$$

Sia $\langle \kappa_i \mid i < \mathrm{Cof}\,\kappa \rangle$ una successione crescente (strettamente) di cardinali $\kappa_i < \kappa$, illimitata in κ: ciò è possibile perché κ è limite. Consideriamo:

$$\prod_{i \in \mathrm{Cof}\,\kappa} \kappa_i^\nu$$

Si ha:

$$\prod_{i \in \mathrm{Cof}\,\kappa} \kappa_i^\nu = \left(\sup_{i \in \mathrm{Cof}\,\kappa} \kappa_i^\nu\right)^{\mathrm{Cof}\,\kappa} = \left(\sup_{\mu<\kappa} \mu^\nu\right)^{\mathrm{Cof}\,\kappa}$$

D'altra parte:

$$\prod_{i \in \mathrm{Cof}\,\kappa} \kappa_i^\nu = \left(\prod_{i \in \mathrm{Cof}\,\kappa} \kappa_i\right)^\nu = \left[\left(\sup_{i \in \mathrm{Cof}\,\kappa} \kappa_i\right)^{\mathrm{Cof}\,\kappa}\right]^\nu =$$

$$= \left(\kappa^{\mathrm{Cof}\,\kappa}\right)^\nu = \kappa^{\mathrm{Cof}\,\kappa \cdot \nu} = \kappa^\nu,$$

da cui la tesi.

3. Sia ν un cardinale, e sia κ tale che:

$$\mu^\nu < \kappa \quad \forall \mu < \kappa$$

Allora:

- se $\nu < \mathrm{Cof}\,\kappa \Rightarrow \kappa^\nu = \kappa$;
- se $\nu \geq \mathrm{Cof}\,\kappa \Rightarrow \kappa^\nu = \kappa^{\mathrm{Cof}\,\kappa} > \kappa$.

PREMESSA

Supponiamo vera l'ipotesi generalizzata del continuo.

Siano $\kappa = \aleph_\omega$, $\nu = \aleph_{17}$.

Allora, per ogni $\mu < \aleph_\omega$ (ossia $\mu = \aleph_m$ per qualche $m < \omega$), si ha:

$$\aleph_m^{\aleph_{17}} = 2^{\aleph_{17}} \cdot \aleph_m = \aleph_{18} \cdot \aleph_m =$$

$$= \max\{\aleph_{18}, \aleph_m\} = \aleph_{\max\{18, m\}} < \aleph_\omega = \kappa$$

Sempre assumendo l'ipotesi generalizzata del continuo:

$$\kappa < \kappa^{\mathrm{cof}\,\kappa} \leq \kappa^\kappa = 2^\kappa = \kappa^+,$$

da cui:

$$\kappa^{\mathrm{Cof}\,\kappa} = \kappa^+$$

Trattiamo il caso in cui $\nu < \mathrm{Cof}\,\kappa$. Allora, dato che ogni $f : \nu \longrightarrow \kappa$ è limitata:

$$\kappa^\nu = |\mathrm{Fun}(\nu, \kappa)| = |\bigcup_{\gamma < \kappa} \mathrm{Fun}(\nu, \gamma)| \leq$$

$$\leq \sum_{\gamma < \kappa} |\mathrm{Fun}(\nu, \gamma)| = \sum_{\gamma < \kappa} |\gamma|^\nu =$$

$$= \max\{\sup_{\gamma \in \kappa} |\gamma|^\nu, \kappa\} = \kappa \leq \kappa^\nu,$$

ove i γ sono ordinali.

Trattiamo ora il caso in cui $\mathrm{Cof}\,\kappa \leq \nu < 2^\nu < \kappa$. Allora κ è singolare, dunque limite.

Per un esercizio precedente:

$$\kappa^\nu = \left(\sup_{\mu < \kappa} \mu^\nu\right)^{\mathrm{Cof}\,\kappa} \leq \kappa^{\mathrm{Cof}\,\kappa} \leq \kappa^\nu.$$

SEQUENZA DI BETHS

La sequenza di BETHS è così definita:

- $\beth_0 \overset{\text{def}}{=} \aleph_0$;
- $\beth_{\alpha+1} \overset{\text{def}}{=} 2^{\beth_\alpha}$;
- $\beth_\lambda \overset{\text{def}}{=} \bigcup_{\gamma<\lambda} \beth_\gamma$.

Si può dimostrare che:
$\forall \alpha \in \mathrm{ORD} : \aleph_\alpha \leq \beth_\alpha$

La funzione aleph è crescente e continua ai limiti, dunque ha punti fissi.

Procediamo per induzione transfinita.

Se $\alpha = 0$, la proposizione è vera perché $\beth_0 = \aleph_0$.

Se $\alpha = \beta+1$ per ipotesi induttiva:

$$\aleph_\beta \leq \beth_\beta$$

Allora:

$$\aleph_{\beta+1} \leq 2^{\aleph_\beta} \leq 2^{\beth_\beta} = \beth_{\beta+1}$$

Se infine $\alpha = \lambda$ è limite:

$$\aleph_\lambda = \bigcup_{\gamma<\lambda} \aleph_\gamma \leq \bigcup_{\gamma<\lambda} \beth_\gamma = \beth_\lambda.$$

GERARCHIA DI VON NEUMANN

La GERARCHIA DI VON NEUMANN è così definita:

- $V_0 \overset{def}{=} \emptyset$
- $V_{\alpha+1} \overset{def}{=} \mathcal{P}(V_\alpha)$
- $V_\lambda \overset{def}{=} \bigcup_{\alpha<\lambda} V_\alpha$

Si definisce poi la classe propria:

$$VN = \bigcup_{\alpha \in Ord} V_\alpha$$

Ricordiamo che un insieme T si dice TRANSITIVO se (sono equivalenti):

- $\forall x \in y \in T : x \in T$;
- $T \subseteq \mathcal{P}(T)$.

Valgono le seguenti proprietà:

- $\forall x \in y \in V_\alpha : \exists \beta < \alpha \ni' x \in V_\beta$;
- $\beta \leq \alpha \Rightarrow V_\beta \subseteq V_\alpha$;
- $\forall \alpha : V_\alpha$ è transitivo.

In effetti:

- Ragionando per induzione transfinita:
  - per $\alpha = 0$ la proprietà è vera a vuoto;
  - per $\alpha = \beta+1$:

    $x \in y \in V_{\beta+1} = \mathcal{P}(V_\beta) \Rightarrow x \in y \subseteq V_\beta \Rightarrow x \in V_\beta \Rightarrow$
    $\Rightarrow x \in V_{\beta+1}$;
  - per $\alpha = \lambda$ limite:

    $x \in y \in V_\lambda = \bigcup_{\gamma<\lambda} V_\gamma \Rightarrow \exists \gamma < \lambda \ni' x \in y \in V_\gamma \Rightarrow$
    $\Rightarrow \exists \beta < \gamma \ni' x \in V_\beta \Rightarrow x \in V_\lambda$;
- Ragionando per induzione transfinita:
  - per $\alpha = 0$ la tesi è banale;
  - per $\alpha = \lambda$ limite, allora:

    $$\beta < \alpha \Rightarrow V_\beta \subseteq V_\lambda = \bigcup_{\gamma<\lambda} V_\gamma ;$$

- se $\alpha = \beta+1$. Basta vedere che $V_\beta \subseteq V_{\beta+1}$. Infatti, per ipotesi induttiva, se $\gamma \leq \beta$, allora $V_\gamma \subseteq V_\beta$ (a sua volta incluso in $V_{\beta+1}$).
  Per dimostrarlo sia $x \in V_\beta$. Per la prima proprietà:
  $\forall\, y \in x \;\; \exists\, \gamma < \beta$ t.c. $y \in V_\gamma$.
  Per ipotesi induttiva, $V_\gamma \subseteq V_\beta$, da cui $y \in V_\beta$.
  Allora $x \subseteq V_\beta$, ossia $x \in \mathcal{P}(V_\beta) = V_{\beta+1}$.

- Usando le prime due proprietà:
  $x \in y \in V_\alpha \Rightarrow \exists\, \beta < \alpha$ t.c. $x \in V_\beta \subseteq V_\alpha \Rightarrow x \in V_\alpha$,
  da cui la tesi.

PROPOSIZIONE

Sia $\alpha \in \mathrm{Ord}$. Allora:

- $\alpha \subseteq V_\alpha$ (ossia $\alpha \in V_{\alpha+1}$);
- $\alpha \notin V_\alpha$.

Dim.

Ragioniamo per induzione transfinita su α:

- $\alpha = 0$. In tal caso è vero che $\emptyset \subseteq V_0 = \emptyset$, ma $\emptyset \notin \emptyset$;
- $\alpha = \beta+1$. Allora, per ipotesi induttiva:
  $\beta \subseteq V_\beta \subseteq V_{\beta+1} \Rightarrow \beta \in V_{\beta+1} \Rightarrow \{\beta\} \subseteq V_{\beta+1} \Rightarrow \beta+1 = \beta \cup \{\beta\} \subseteq V_{\beta+1}$.
  D'altra parte, se per assurdo $\beta+1 \in V_{\beta+1} = \mathcal{P}(V_\beta)$, allora $\beta \cup \{\beta\} \subseteq V_\beta$, da cui $\beta \in V_\beta$, contro l'ipotesi induttiva;
- $\alpha = \lambda$ limite. Per ogni $\beta < \lambda$, per ipotesi induttiva:
  $$\beta \subseteq V_\beta \Rightarrow \beta \in V_{\beta+1}$$
  Allora $\lambda \subseteq \bigcup_{\beta<\lambda} V_{\beta+1} = V_\lambda$
  D'altra parte, se per assurdo $\lambda \in V_\lambda = \bigcup_{\gamma<\lambda} V_\gamma$, allora:
  $\exists\, \beta < \lambda$ t.c. $\lambda \in V_\beta$. Allora:
  $$\beta \in \lambda \in V_\beta \Rightarrow \beta \in V_\beta,$$
  contro l'ipotesi induttiva, c.v.d.

ASSIOMA DI FONDAZIONE

ASSIOMA (DI FONDAZIONE)
Sia $X \neq \emptyset$ un insieme. Allora:
$\exists\, y \in X$ t.c. $y \cap X = \emptyset$

Equivalentemente, $X \neq \emptyset$ ha elementi $\in$-MINIMALI.

TEOREMA
L'assioma di fondazione è valido se e solo se non esistono catene $\in$-discendenti.

Dim.
Supponiamo l'esistenza di una catena discendente:
$$x_1 \ni x_2 \ni x_3 \ni \dots$$
Allora $X = \{x_n \mid n \in \mathbb{N}\}$ contraddice l'assioma di fondazione.

Viceversa, se $X \neq \emptyset$ non ha elementi $\in$-minimali in X, allora, preso $x_1 \in X$, x_1 non è $\in$-minimale in X, ossia $x_1 \cap X \neq \emptyset$, ossia esiste $x_2 \in x_1 \cap X$.
Di nuovo $x_2 \in X \Rightarrow x_2 \cap X \neq \emptyset$, ed esiste $x_3 \in x_2 \cap X$.
Iterando il procedimento (usando l'assioma di scelta, l'assioma di rimpiazzamento e la ricorsione numerabile), si ottiene l'esistenza di una catena discendente:
$$X \ni x_1 \ni x_2 \ni x_3 \ni \dots \quad \text{, c.v.d.}$$

Prima di continuare, diamo le seguenti definizioni:
$$\mathbb{V} = \{x \mid x \text{ è un insieme}\}$$
$$\mathbb{WN} = \bigcup_{\alpha \in \mathrm{Ord}} V_\alpha$$

LEMMA
Se $A \in \mathbb{V}$ e $A \subseteq \mathbb{WN}$, allora $A \in \mathbb{WN}$.

Dim.
Per ogni $a \in A$, l'insieme di ordinali seguente è non vuoto:
$$\square_a \overset{\text{def}}{=} \{\alpha \in \mathrm{Ord} \mid a \in V_\alpha\}$$

Sia dunque, per ogni $a \in A$:
$$\alpha_a = \min \Xi_a$$
La corrispondenza $a \to \alpha_a$ è funzionale, dunque:
$$\mathbb{F} : A \to Ord$$
$$a \to \alpha_a$$
è una funzione classe, e per l'assioma di rimpiazzamento, il seguente è un insieme:
$$X = \mathbb{F}(A) \overset{def}{=} \{ \alpha_a \mid a \in A, \alpha_a = \mathbb{F}(a) \}$$
$\mathbb{F}(A)$, in particolare, è un insieme di ordinali. Sia:
$$\gamma = \bigcup X = \sup_{\alpha \in X} \alpha = \sup_{a \in A} \alpha_a$$
Per un esercizio precedente:
$$\alpha_a \leq \gamma \Rightarrow V_{\alpha_a} \subseteq V_\gamma,$$
da cui:
$$\forall a \in A : a \in V_{\alpha_a} \subseteq V_\gamma \Rightarrow \forall a \in A : a \in V_\gamma$$
Dunque $A \subseteq V_\gamma$, da cui $A \in \mathcal{P}(V_\gamma) = V_{\gamma+1}$. Allora, in conclusione, $A \in \mathbb{WN}$, c.v.d.

TEOREMA

L'assioma di fondazione equivale all'uguaglianza:
$$\mathbb{V} = \mathbb{WN}$$

Dim.

Supponiamo che valga l'assioma di fondazione: sia, per assurdo, $A \in \mathbb{V} \setminus \mathbb{WN}$.

Per il lemma $A \notin \mathbb{WN} \Rightarrow A \nsubseteq \mathbb{WN}$, da cui:

$\exists\, a_1 \in A \setminus \mathbb{WN}$.

Dato che $a_1 \notin \mathbb{WN}$:
$$a_1 \nsubseteq \mathbb{WN} \Rightarrow \exists\, a_2 \in a_1 \setminus \mathbb{WN}$$
Iterando il procedimento, si ottiene dunque una catena discendente:
$$a_1 \ni a_2 \ni a_3 \ni \dots,$$
e ciò è assurdo.

Dimostriamo ora l'implicazione opposta: sia dunque $\mathbb{V} = \mathbb{VN}$.

Innanzitutto, dato $x \in \mathbb{VN}$, definiamo:

$$\rho(x) = \min\{\alpha \in Ord \mid x \in V_\alpha\}$$

LEMMA

Si ha:

$$x \in y \Rightarrow \rho(x) < \rho(y)$$

Dim.

Se $\alpha = \rho(y)$, allora $y \in V_\alpha$. Se $x \in y \in V_\alpha$, allora:

$\exists\ \beta < \alpha$ t.c. $x \in V_\beta \Rightarrow \rho(x) < \rho(y)$, c.v.d.

Sotto queste ipotesi, vale necessariamente il principio di fondazione. Se così non fosse, infatti (per il lemma) dall'esistenza di una catena discendente si proverebbe l'esistenza di una catena discendente di ordinali, e ciò è assurdo:

$$x_1 \ni x_2 \ni x_3 \ni \dots \Rightarrow$$
$$\Rightarrow \rho(x_1) > \rho(x_2) > \rho(x_3) > \dots, \text{ c.v.d.}$$

INTERPRETAZIONE GEOMETRICA DELL'ESPONENZIAZIONE TRA ORDINALI

Abbiamo già dimostrato, in precedenza che:

- $\alpha + \beta \cong \alpha \oplus \beta$;
- $\alpha \cdot \beta \cong \alpha \otimes \beta$.

Vogliamo dare interpretare α^β.

Si ha:

$$(\alpha^\beta, \in) \cong \left(\{ f : \beta \to \alpha \mid |\operatorname{Supp} f| < \aleph_0 \}, < \right),$$

ove:

$$\operatorname{Supp} f = \{ \gamma \in \beta \mid f(\gamma) \neq 0 \}$$

Le funzioni in quell'insieme hanno dunque supporto finito. Dato dunque f, è definito il massimo elemento di β tale che $f(\cdot) \neq 0$.

Facciamo un esempio, considerando ω^ω:

$$\begin{array}{ccccc}
0 & \longrightarrow & 0 & & 2 \\
1 & \longrightarrow & 1 & & 0 \\
2 & \longrightarrow & 2 & & 0 \\
3 & \longrightarrow & 4 & & 3 \\
4 & \longrightarrow & 0 & & 0 \\
\vdots & & \vdots & & \vdots
\end{array}$$

Siano f e g le due successione. Definiamo il seguente ordine, detto DELLA MASSIMA DIFFERENZA: $f < g$ se e solo se, detto $i \in \beta$ il massimo elemento tale che $f(i) \neq g(i)$, si ha $f(i) < g(i)$.

Nell'esempio (supponendo che le restanti immagini siano tutte nulle) si ha $g < f$, in quanto $3 < 4$.

Per dimostrare l'isomorfismo, si può notare che:

$$\Phi : (\{\ldots\}, <) \longrightarrow (\alpha^\beta, \in)$$

$$f \longrightarrow \sum_{i = \max \operatorname{Supp} f}^{\min \operatorname{Supp} f} \alpha^i f(i) < \alpha^\beta$$

ove gli addendi sono considerati in ordine decrescente, è biunivoca.

Si sfrutta allora la forma normale di Cantor in base α.
È facile notare che:

$$f < g \Leftrightarrow \Phi(f) < \Phi(g)$$

Nel caso precedente, in particolare, si ha:

$$\Phi(f) = \omega^3 \cdot 4 + \omega^2 \cdot 2 + \omega \cdot 1 < \omega^\omega$$

$$\Phi(g) = \omega^3 \cdot 3 + 2 < \omega^\omega$$

In particolare:

- $\forall i \in \beta : f(i) < \alpha$;
- $i < \beta$,

da cui:

$\forall f \in (\{\ldots\}, <) : \Phi(f) < \alpha^\beta$.

CHIUSURA TRANSITIVA

Sia X un insieme.

Definiamo per ricorsione numerabile:

$$\begin{cases} X_0 = X \\ X_{n+1} = X_n \cup \{a \mid \exists\, b \in X_n \ \text{t.c.}\ a \in b\} = \\ \quad = X_n \cup \bigcup X_n \end{cases}$$

Sia ora $Y = \bigcup_{n<\omega} X_n$. Si ha che Y è transitivo:

$$a \in b \in Y = \bigcup_{n<\omega} X_n \Rightarrow \exists\, n < \omega \ \text{t.c.}\ a \in b \in X_n \Rightarrow$$

$$\Rightarrow a \in X_{n+1} \Rightarrow a \in Y$$

PROPOSIZIONE

Supponiamo che $Z \supseteq X$ sia transitivo. Allora $Z \supseteq Y$. Y è dunque il più piccolo insieme transitivo contenente X.

Dim.

Basta dimostrare che $Z \supseteq X_n \ \forall\, n < \omega$. Procediamo per induzione su n:

- $n = 0$. Per ipotesi $Z \supseteq X = X_0$;
- $n \Rightarrow n+1$.

  Per ipotesi induttiva, $Z \supseteq X_n$. Sia $a \in X_{n+1}$. Le alternative sono due:

  - $a \in X_n$. In tal caso, per ipotesi induttiva, $a \in Z$;
  - $a \notin X_n \Rightarrow \exists\, b \in X_n$ t.c. $a \in b \in X_n$. Dato che $X_n \subseteq Z$, si ha $a \in b \in Z$. Ma Z è transitivo dunque $a \in Z$.

  Allora $X_{n+1} \subseteq Z$, c.v.d.

L'insieme Y, per tale ragione, è detto CHIUSURA TRANSITIVA di X, e si indica con $TC(X)$.

ESERCIZI VARI

1. Sia α un ordinale limite. Allora:

- $a, b \in V_\alpha \Rightarrow \{a, b\} \in V_\alpha$;
- $a \in V_\alpha \Rightarrow \mathcal{P}(a) \in V_\alpha$.

Siano $a, b \in V_\alpha$. Allora:

- $\exists\ i < \alpha$ t.c. $a \in V_i$;
- $\exists\ j < \alpha$ t.c. $b \in V_j$.

Allora:

$\exists\ k = \max\{i, j\}$ t.c. $a, b \in V_k$.

Allora $\{a, b\} \in \mathcal{P}(V_k) = V_{k+1}$, e dato che $k+1 < \alpha$, si ha $\{a, b\} \in V_\alpha$.

Sia ora $a \in V_\alpha$. Allora:

$\exists\ i < \alpha$ t.c. $a \in V_i$,

e per transitività, $a \subseteq V_i$, da cui $\mathcal{P}(a) \subseteq \mathcal{P}(V_i) = V_{i+1}$, da cui $\mathcal{P}(a) \in \mathcal{P}(V_{i+1}) = V_{i+2}$, da cui $\mathcal{P}(a) \in V_\alpha$ perché $i + 2 < \alpha$.

2. Sia:

$$Y = \bigcup_{\alpha < \omega_1} X_\alpha,$$

con:

- $\forall\ \alpha < \omega_1 : |X_\alpha| < \aleph_1$;
- $\forall\ \alpha, \beta \in \omega_1 : \alpha < \beta \Rightarrow X_\alpha \subsetneq X_\beta$;
- se $\lambda < \omega_1$, allora:

$$X_\lambda = \bigcup_{\gamma < \lambda} X_\gamma$$

Dimostrare che:

- $|Y| = \aleph_1$;
- se $Y = \bigcup_{\alpha < \omega_1} X_\alpha = \bigcup_{\beta < \omega_1} X'_\beta$, con le stesse ipotesi di sopra, allora:

$$\{\alpha < \omega_1 \mid X_\alpha = X'_\alpha\}$$

è illimitato in ω_1.

Innanzitutto:

$$|Y| = \Big|\bigcup_{\alpha<\omega_1} X_\alpha\Big| \le \sum_{\alpha<\omega_1} |X_\alpha| \le \sum_{\alpha<\omega_1} \aleph_0 = \aleph_0 \cdot |\omega_1| =$$
$$= \aleph_0 \cdot \aleph_1 = \aleph_1$$

Possiamo concludere determinando $f : \aleph_1 \to Y$ iniettiva.
Per ipotesi, si ha:

$$\forall \alpha < \omega_1 : X_{\alpha+1} \setminus X_\alpha \neq \emptyset \Rightarrow \exists y_\alpha \in X_{\alpha+1} \setminus X_\alpha \subseteq Y$$

Usando allora l'assioma della scelta, definiamo:

$$f(\alpha) = y_\alpha \quad \forall \alpha < \omega_1$$

Notiamo ora che, se $\alpha \neq \beta$ (supponiamo $\alpha < \beta$, l'altro caso è analogo), allora $\alpha + 1 \le \beta$, da cui:

$$(X_{\alpha+1} \setminus X_\alpha) \cap (X_{\beta+1} \setminus X_\beta) = \emptyset,$$

da cui necessariamente $f(\alpha) \neq f(\beta)$, ossia f è iniettiva.
Per il teorema di Cantor-Bernstein, dunque:

$$|Y| = \aleph_1$$

Per affrontare il secondo punto dell'esercizio, ricordiamo che, se $F : Ord \to Ord$ è una funzione classe tale che:

- $\alpha < \beta \Rightarrow F(\alpha) < F(\beta)$;
- F è "continua", ossia, per λ limite:

$$F\Big(\bigcup_{\delta<\lambda} \delta\Big) = \bigcup_{\delta<\lambda} F(\delta),$$

allora F ammette frequentemente punti fissi:
$\forall \beta \in Ord \ \exists \alpha > \beta$ s.t. $F(\alpha) = \alpha$.

Cerchiamo di usare questo teorema nel nostro caso.

Dato $\alpha < \omega_1$, definiamo

$$f(\alpha) \overset{def}{=} \min\{\beta < \omega_1 \mid X_\alpha \subseteq X'_\beta\}$$

Analogamente:

$$g(\beta) = \min\{\alpha < \omega_1 \mid X'_\beta \subseteq X_\alpha\}$$

Dobbiamo far vedere che tali funzioni sono ben definite: dato che la dimostrazione è analoga nei due casi, dimostriamolo solo per f.

Se $|X_\alpha| \leq \aleph_0$, allora $X_\alpha = \{a_{\alpha,n}\}_{n\in\mathbb{N}}$. Allora:

$$\forall\, a_{\alpha,n} \in X_\alpha \ \exists\, \beta_n < \omega_1 \ \text{t.c.} \ a_{\alpha,n} \in X'_{\beta_n}$$

Allora, se $\beta = \sup_{n\in\omega} \beta_n$, si ha $X_\alpha \subseteq X'_\beta$.

Dato che:

- $\forall n \in \omega : |\beta_n| \leq \aleph_0$;
- $|\omega| = \aleph_0$;
- $\mathrm{Cof}(\aleph_1) = \aleph_1 > \aleph_0$,

la successione $\langle \beta_n \mid n \in \omega \rangle$ è limitata, e dunque $\beta < \omega_1$.

Dunque f (e anche g) è ben definita. Sia allora:

$$h = g \circ f$$

Sia $x \leq y$: vogliamo dimostrare che $h(x) \leq h(y)$. Ma ciò è evidente:

$$x \leq y \Rightarrow f(x) \leq f(y) \Rightarrow$$
$$\Rightarrow g(f(x)) \leq g(f(y))$$

Questa è una variante del teorema enunciato prima, ma non è un problema. Infatti, se comunque dimostriamo la continuità di h, allora sappiamo che esiste almeno un punto fisso.

A quel punto, però, dato $\gamma < \omega_1$, e dato $\delta < \omega_1$ tale che $\gamma < \delta$, definendo:

$$\begin{cases} x_0 = \delta \\ x_{n+1} = h(x_n), \end{cases}$$

si ha che:

$$x = \sup_{n<\omega} x_n = \sup_{n<\omega} x_{n+1} = h(x),$$

(nell'ultimo passaggio si usa la continuità di h, e si è usato anche il fatto (banale) che $h(x_n) \geq x_n$), da cui $x > \delta$ è punto fisso, e l'insieme dei punti fissi è dunque illimitato in ω_1.

Dimostriamo dunque la continuità. Vogliamo che:

$$h\left(\sup_{i\in I} X_{\alpha_i}\right) = \sup_{i\in I}\left(h(X_{\alpha_i})\right)$$

È sufficiente dimostrare la continuità per f. Siano:

$$\alpha = \sup_{i\in I}\alpha_i \qquad \beta = \sup_{i\in I} f(\alpha_i) = \sup_{i\in I}\beta_i,$$

ove $X_{\beta_i} \overset{def}{=} f(X_{\alpha_i})\ \forall i \in I$. Allora sicuramente:

$$X_\alpha \leq X'_\beta,$$

ma:

$\forall \gamma < \beta : X_\alpha \not\leq X'_\gamma$, dato che:

dato che:

$\gamma < \beta \Rightarrow \exists \beta_i \ni' \gamma < \beta_i \Rightarrow X_{\alpha_i} \not\leq X^{+}_{\gamma}$.

Dunque f (quindi h) è continua, e l'esercizio è concluso.

3. Per quali $\alpha, \beta < \omega^2$ si ha $\alpha+\beta = \beta+\alpha$?

Usando la divisione euclidea con base ω:

$\exists\, m, n, h, k < \omega \ni' \alpha = \omega\cdot m + h,\ \beta = \omega\cdot n + k$

Dunque:

- $\alpha+\beta = \omega\cdot m + h + \omega\cdot n + k$;
- $\beta+\alpha = \omega\cdot n + k + \omega\cdot m + h$.

Ci sono allora vari casi:

- $n = 0$. Allora $\alpha+\beta = \omega\cdot m + h + k$. Se fosse $m \neq 0$ sarebbe $\beta+\alpha = \omega\cdot m + h$, e si avrebbe l'uguaglianza se e solo se $k = 0$ (ossia $\beta = 0$, dunque banalmente $\alpha + 0 = 0 + \alpha = \alpha$). A parte questo caso banale bisogna porre $m = 0$, e in questo caso si ha:
$$\alpha+\beta = h+k = k+h = \beta+\alpha,$$
qualunque siano h e k;
- $n \neq 0$. Se $m = 0$, si "ricade" il caso precedente, a parti invertite, e si giunge alla conclusione che

solo $\alpha = 0$ commuta con β. Negli altri casi, anche $m \neq 0$.

Dunque:

$$\alpha + \beta = \omega \cdot (m + n) + k$$
$$\beta + \alpha = \omega \cdot (n + m) + h,$$

da cui la condizione da imporre è $h = k$.

Ricapitolando,

- 0 commuta con tutti gli ordinali;
- se $\alpha \neq 0$, $\beta \neq 0$, allora α e β commutano se e solo se sono entrambi finiti, oppure sono entrambi infiniti, con $h = k$.