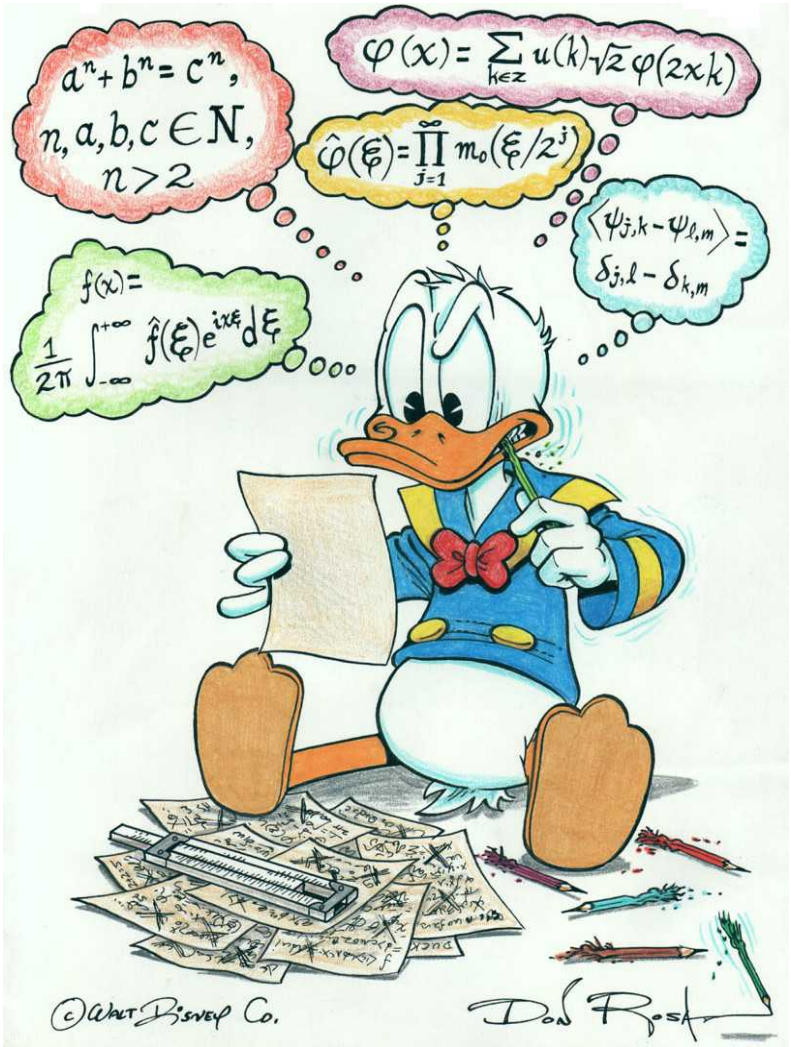
Marco Barlotti

Appunti di

Teoria degli insiemi

per l'insegnamento di "Complementi di Algebra"
per la laurea magistrale in Matematica

Vers. 1.7
Anno Accademico 2017-2018



In copertina un disegno originale (© Disney) di Keno Don Rosa.

PERCHE’ QUESTI APPUNTI, E COME USARLI

(Prefazione alla vers. 1.7)

Questi appunti vogliono costituire un supporto scritto alle lezioni di “Teoria degli insiemi” che tengo nell’insegnamento di “Complementi di algebra” per il corso di laurea magistrale in Matematica presso l’Università di Firenze.

Mi riprometto di rivedere al più presto questi appunti, per correggerli ed ampliarli con ulteriori esempi e qualche altro esercizio.

Al momento è inevitabile la presenza di errori materiali; inoltre, per quanto mi sia sforzato di conciliare il rigore con la chiarezza, alcuni brani del testo possono risultare poco comprensibili. Sarò grato a tutti coloro, e specialmente agli studenti, che vorranno segnalarmi qualunque problema, dai più banali errori di stompa alle oscurità nell’esposizione.

Firenze, 18.5.2018

Marco Barlotti

BIBLIOGRAFIA

[1] P. R. Halmos
Naive set theory
Van Nostrand, Princeton NJ (1966)

[2] G. Peano
Aritmetica generale e algebra elementare
Paravia, Torino (1902)

[3] M. Artin
Algebra
Prentice Hall, New Jersey (1991)

[4] M. Artin
Algebra
Bollati Boringhieri, Torino (1997)

SOMMARIO

3. - L’assioma della scelta

4. - Cardinalità

5. - Equisezionabilità nel piano

6. - Equiscomponibilità nello spazio: il teorema di Banach-Tarski

1.- GLI ASSIOMI DI ZERMELO E FRAENKEL

Aus dem paradies, das Cantor uns geshaffen,
solls uns niemand vertreiben können.
David Hilbert

1.1 - L'assioma di Leibniz.

$(\mathcal{A}_0)$
$A = B$ se e soltanto se A ha ogni proprietà che B ha e B ha ogni proprietà che A ha.

Teorema 1.1.1

(i) Per ogni A, $A = A$;

(ii) Per ogni A e B, se $A = B$ allora $B = A$;

(iii) Per ogni A, B e C, se $A = B$ e $B = C$ allora $A = C$.

1.2 - Le parole primitive.

Insieme, *appartiene*.

Notazione 1.2.1

Se A appartiene a B si dice anche che "A è un elemento di B" e si scrive

$$A \in B$$

Osservazione 1.2.2

Dunque "elemento" non è una parola primitiva, ma si può definire attraverso la parola primitiva "appartiene".

1.3 - L'assioma di estensione.

($\mathcal{A}_1$)
Per ogni A, B, C, se

$$C \in A \text{ se e soltanto se } C \in B$$

allora $A = B$.

Osservazione 1.3.1

Questo assioma si può riformulare in modo più semplice ma usando parole che non sono primitive:

Se gli insiemi A e B hanno gli stessi elementi, allora $A = B$.

Osservazione 1.3.2

L'assioma di estensione esprime il fatto che "avere gli stessi elementi" è condizione sufficiente per essere lo stesso insieme. Che sia condizione necessaria segue invece dall'assioma di Leibniz.

Notazione 1.3.3

Poiché un insieme resta completamente caratterizzato dai suoi elementi, se riusciamo a scriverli tutti possiamo indicarlo con il loro elenco; la convenzione è di scriverli fra parentesi graffe, separati da virgole. Ad esempio: $A = \{B, C, D\}$. Naturalmente, a questo punto dell'esposizione, non possiamo sapere né se esiste alcun insieme in assoluto né se, anche ammessa l'esistenza di B, C e D, esista l'insieme che ha come elementi esattamente B, C e D.

1.4 - L'assioma di separazione ("*Aussonderungsaxiom*").

($\mathcal{A}_s$)
Per ogni insieme A e per ogni proprietà Φ, esiste un insieme B tale che per ogni X

$$X \in B \text{ se e soltanto se } (X \in A \text{ e } X \text{ ha la proprietà } \Phi).$$

Osservazione 1.4.1

"proprietà" non è una parola primitiva: essa non appartiene al linguaggio degli insiemi, ma al (meta-)linguaggio col quale parliamo di insiemi. Di fatto, quello appena enunciato non è un assioma ma uno "schema" di assioma: per ogni proprietà ("predicato"?) Φ si ottiene un diverso assioma.

Poiché vogliamo un numero finito di assiomi alla base della nostra teoria, ci impegniamo ad usare questo schema di assioma soltanto un numero finito di volte (notiamo, di nuovo, che è improprio usare le parole "numero finito", che esprimono un concetto che definiremo più avanti nell'ambito della teoria degli insiemi; ma ciò non inficia la teoria stessa perché questa osservazione è "filosofica" e non fa parte di essa).

Notazione 1.4.2

Sia A un insieme A, e sia Φ una proprietà. L'insieme B tale che per ogni X

$$X \in B \text{ se e soltanto se } (X \in A \text{ e } X \text{ ha la proprietà } \Phi).$$

si indica con

$$\{X \in A \,/\, X \text{ ha la proprietà } \Phi\}.$$

(Tale insieme esiste per l'assioma di separazione, ed è unico per l'assioma di estensione).

Osservazione 1.4.3 (Il "paradosso di Russell")

L'assioma di separazione non afferma che

Per ogni proprietà Φ, esiste un insieme B tale che per ogni X

$$X \in B \text{ se e soltanto se } X \text{ ha la proprietà } \Phi.$$

Un tale assioma porterebbe a una contraddizione scegliendo (ad esempio) come proprietà Φ la seguente:

$$X \text{ ha la proprietà } \Phi \text{ se e soltanto se } X \notin X.$$

Ne seguirebbe l'esistenza di un insieme B tale che per ogni X

$$X \in B \text{ se e soltanto se } X \notin X.$$

Ma allora non potrebbe essere né $B \in B$ (perché ne seguirebbe la contraddizione $B \notin B$) né $B \notin B$ (perché ne seguirebbe la contraddizione $B \in B$); contro il principio aristotelico del "terzo escluso", che noi invece accettiamo nella nostra logica.

Osservazione 1.4.4

Non esiste alcun insieme di cui ogni insieme sia elemento. Più pittorescamente: *non esiste un universo*. Sia infatti per assurdo U un tale insieme; ragionando come nell'oss. 1.4.3 si potrebbe considerare

$$B := \{X \in U / X \notin X\}$$

e, di nuovo, non potrebbe essere né $B \in B$ né $B \notin B$.

1.5 - L'insieme vuoto.

Per poter applicare l'assioma di separazione, ci serve l'esistenza di almeno un insieme. La cosa più semplice è chiedere ciò con un apposito assioma:

$(\mathcal{A}_2)$
Esiste almeno un insieme.

Teorema 1.5.1

Esiste un insieme B (e uno solo) tale che

$$\text{per ogni } X, \quad X \notin B.$$

Dimostrazione — Per l'assioma $(\mathcal{A}_2)$ esiste un insieme A. Per l'assioma $(\mathcal{A}_s)$ esiste

$$B := \{X \in A / X \neq X\}.$$

Per ogni X, non è $X \neq X$ per la (i) del teorema 1.1.1; dunque, per ogni X, $X \notin B$.

In altre parole, l'insieme B non ha elementi. Infine, per l'assioma di estensione, esiste un solo insieme senza elementi.

Definizione 1.5.2

L'unico insieme B tale che

$$\text{per ogni } X, \quad X \notin B$$

(di cui al teorema 1.5.1) si chiama *insieme vuoto* e si indica con $\emptyset$.

Un insieme A tale che $A \neq \emptyset$ si dice *non vuoto*.

1.6 - L'assioma delle coppie.

($\mathcal{A}_3$)

Per ogni insieme A e per ogni insieme B, esiste un insieme C i cui elementi sono esattamente A e B.

Osservazione 1.6.1

A partire da questo assioma, diamo gli enunciati nella forma più "discorsiva", quella cioè che utilizza anche i termini definiti e non soltanto le parole primitive. È comunque sempre un utile esercizio rienunciare gli assiomi utilizzando soltanto le parole primitive; in questo caso:

Per ogni insieme A e per ogni insieme B, esiste un insieme C tale che, per ogni X,

$$X \in C \text{ se e soltanto se } (X = A \text{ oppure } X = B).$$

Osservazione 1.6.2

Si confrontino i due enunciati dell'assioma: nel primo la conclusione è "esattamente A e B", nel secondo la conclusione è "$X = A$ oppure $X = B$". Ma i due enunciati sono effettivamente equivalenti.

Notazione 1.6.3

Siano A, B insiemi. Coerentemente con quanto stabilito nella notazione 1.3.3, l'insieme C i cui elementi sono esattamente A e B si indica con

$$\{A, B\}.$$

Osservazione 1.6.4

Poiché nell'assioma delle coppie non si chiede che sia $A \neq B$, ne deduciamo che per ogni insieme A esiste un insieme che ha come unico elemento A. Tale insieme si indica con

$$\{A\}$$

e si dice "singoletto A" (in inglese: "singleton A").

Osservazione 1.6.5

Gli insiemi

$$\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \{\{\{\{\emptyset\}\}\}\}, \{\{\{\{\{\emptyset\}\}\}\}\}, \ldots$$

sono a due a due distinti fra loro (esercizio: spiegare perché).

1.7 - L'assioma di regolarità.

$(\mathcal{A}_4)$

Non esiste alcun insieme non vuoto A tale che ogni elemento di A ha un elemento che appartiene anche ad A.

Esercizio 1.7.1

Esprimere l'assioma di regolarità usando soltanto le parole primitive.

Teorema 1.7.2

Per ogni insieme A,

$$A \notin A .$$

Dimostrazione – Se fosse $A \in A$, l'insieme $B := \{A\}$ non rispetterebbe l'assioma di regolarità: infatti ogni elemento di B (cioè A, che è l'unico elemento di B) avrebbe un elemento (A) che appartiene anche a B.

Corollario 1.7.3

Per ogni insieme A,

$$A \neq \{A\} .$$

Dimostrazione – Poiché $\{A\}$ ha come unico elemento A, se fosse $A = \{A\}$ anche A dovrebbe avere come unico elemento A, e in particolare dovrebbe essere $A \in A$; ma ciò è assurdo per il teorema 1.7.2.

1.8 - L'assioma dell'unione.

$(\mathcal{A}_5)$

Per ogni insieme A, esiste un insieme i cui elementi sono esattamente gli elementi degli elementi di A.

Esercizio 1.8.1

Esprimere l'assioma dell'unione usando soltanto le parole primitive.

Notazione 1.8.2

Sia A un insieme. L'insieme i cui elementi sono esattamente gli elementi degli elementi di A si dice *unione degli elementi di* A e si indica con

$$\cup \mathrm{A}\,.$$

Osservazione 1.8.3

Sia A un insieme. Si ha

$$\cup \{\mathrm{A}\} = \mathrm{A}\,.$$

Notazione 1.8.4

Siano A, B insiemi. Si pone

$$\mathrm{A} \cup \mathrm{B} := \cup \{\mathrm{A}, \mathrm{B}\}\,.$$

L'insieme $\mathrm{A} \cup \mathrm{B}$ si dice *unione* di A e B .

Osservazione 1.8.5

Siano A, B insiemi. Si ha

(i) $\mathrm{A} \cup \mathrm{B} = \mathrm{B} \cup \mathrm{A}$;

(ii) $\mathrm{A} \cup \mathrm{B} = \mathrm{B}$ se e soltanto se ogni elemento di A è anche elemento di B .

Esercizio 1.8.6

Siano A, B, C insiemi. Si provi che

$$(\mathrm{A} \cup \mathrm{B}) \cup \mathrm{C} = \mathrm{A} \cup (\mathrm{B} \cup \mathrm{C}) = \cup \{\mathrm{A}, \mathrm{B}, \mathrm{C}\}\,.$$

Osservazione 1.8.7

$$\cup \emptyset = \emptyset$$

Esercizio 1.8.8

Sia A un insieme. Se

$$\cup \mathrm{A} = \emptyset$$

che cosa si può dire di A ?

1.9 - Intersezione di insiemi.

Notazione 1.9.1

Siano A, B insiemi. Si dice *intersezione* di A e B l'insieme

$$A \cap B := \{X \in A \,/\, X \in B\}.$$

Esercizio 1.9.2

Siano A, B, C insiemi. Si provi che

(i) $A \cap B = B \cap A$;

(ii) $A \cap B = A$ se e soltanto se ogni elemento di A è anche elemento di B.

(iii) $(A \cap B) \cap C = A \cap (B \cap C)$

(iv) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

(v) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

Notazione 1.9.3

Gli insiemi A, B si dicono *disgiunti* se $A \cap B = \emptyset$.

Notazione 1.9.4

Sia A un insieme. Gli elementi di A si dicono *a due a due disgiunti* se

$$\text{comunque presi } X, Y \in A, \quad \text{si ha} \quad (X = Y) \text{ oppure } (X \cap Y = \emptyset).$$

Teorema 1.9.5

Sia A un insieme non vuoto. Esiste uno e un solo insieme i cui elementi sono tutti e soli gli insiemi che appartengono a tutti gli elementi di A.

Dimostrazione — Poiché A non è vuoto, esiste $X_0 \in A$. L'insieme

$$\{X \in X_0 \,/\, \text{per ogni } B \in A,\ X \in B\}$$

esiste per l'assioma di separazione, e i suoi elementi sono proprio quelli dicharati nell'enunciato del teorema. Tale insieme è poi unico per l'assioma di estensione.

Notazione 1.9.6

Sia A un insieme non vuoto. L'insieme i cui elementi sono tutti e soli gli insiemi che appartengono a tutti gli elementi di A (che esiste ed è unico per il teorema 1.9.5) si indica con

$$\cap A .$$

Si noti che alla scrittura $\cap \emptyset$ non si dà alcun significato.

1.10 - L'assioma dei sottoinsiemi.

Notazione 1.10.1

Siano A, B insiemi. Si dice che A *è un sottoinsieme di* B (o, equivalentemente, che A *è contenuto in* B) e si scrive

$$A \subset B$$

se e soltanto se ogni elemento di A è anche elemento di B.

Esercizio 1.10.2

Esprimere la definizione di sottoinsieme usando soltanto le parole primitive.

Teorema 1.10.3

Per ogni insieme B, $\emptyset \subset B$.

Dimostrazione – Se il teorema non fosse vero, esisterebbe un insieme B_0 tale che $\emptyset \not\subset B_0$ e quindi esisterebbe X tale che $X \in \emptyset$ e $X \notin B_0$, assurdo perché $\emptyset$ non ha elementi.

$(\mathcal{A}_6)$

Per ogni insieme A, esiste un insieme i cui elementi sono esattamente i sottoinsiemi di A.

Esercizio 1.10.4

Esprimere l'assioma dei sottoinsiemi usando soltanto le parole primitive.

Notazione 1.10.5

Sia A un insieme. L'insieme i cui elementi sono esattamente i sottoinsiemi di A si indica con

$$\wp(A)$$

e si dice *insieme delle parti* di A .

1.11 - Complementare. Leggi di De Morgan.

Siano A, B insiemi,. Si dice *differenza tra* B *e* A e si indica con $B\backslash A$ l'insieme

$$\{X \in B \,/\, X \notin A\}\,.$$

Nel seguito di questa sezione supporremo fissato un insieme B .

Sia A un sottoinsieme di B . Si dice *complementare di* A (*in* B; ma se B è fissato di solito non c'è bisogno di questa precisazione) e si indica con A^c l'insieme $B\backslash A$. Dunque

$$A^c := \{X \in B \,/\, X \notin A\}\,.$$

Teorema 1.11.1 (le leggi di De Morgan)

Per ogni insieme A di sottoinsiemi di B,

(i) $\quad (\cup A)^c = \underset{X\in A}{\cap} X^c$;

(ii) $\quad (\cap A)^c = \underset{X\in A}{\cup} X^c$.

Precisiamo il significato dei simboli al secondo membro.

$$\underset{X\in A}{\cap} X^c := \cap \{Y \in \wp(B) \,/ Y = X^c \ \text{ con } \ X \in A\}$$

e analogamente

$$\underset{X\in A}{\cup} X^c := \cup \{Y \in \wp(B) \,/ Y = X^c \ \text{ con } \ X \in A\}\,.$$

Più in generale, tutte le volte che mediante una proprietà Φ si può caratterizzare un insieme Z come formato da tutti e soli gli X per i quali vale $\Phi(X)$ (e sappiamo che questo non è possibile in generale!), con le scritture $\underset{\Phi(X)}{\cap} X$ e $\underset{\Phi(X)}{\cup} X$ intenderemo rispettivamente

$$\underset{\Phi(X)}{\cap} X := \cap Z \qquad \text{e} \qquad \underset{\Phi(X)}{\cup} X := \cup Z\,.$$

Si veda anche quanto converremo nella sez. 1.13 .

1.12 - Coppie ordinate.

Siano A, B insiemi. Si dice *coppia ordinata individuata dagli elementi* A *e* B (in quest'ordine!) e si indica con (A, B) l'insieme

$$(A, B) := \{\{A\}, \{A, B\}\}\,.$$

Teorema 1.12.1

Siano A, B, C, D insiemi. Allora:

(i) $\quad \cup(\cap(A, B)) = A\,;$

(ii) se $A \neq B$, $\quad \cup((\cup(A, B))\setminus(\cap(A, B))) = B\,;$
se $A = B$, $\quad \cup((\cup(A, B))\setminus(\cap(A, B))) = \emptyset\,;$

(iii) $\quad (A, B) = (C, D)$ se e soltanto se $\quad (A = C \text{ e } B = D)\,;$

Dimostrazione – Osserviamo in primo luogo che

$$\cap(A, B) = \{A\} \cap \{A, B\} = \{A\} \qquad \text{e} \qquad \cup(A, B) = \{A\} \cup \{A, B\} = \{A, B\}\,.$$

Ne segue che $\cup(\cap(A, B)) = \cup\{A\} = A$ (cioè la (i)) e che

se $A \neq B$, $\cup((\cup(A, B))\setminus(\cap(A, B))) = \cup(\{A, B\}\setminus\{A\}) = \cup\{B\} = B$ mentre
se $A = B$, $\cup((\cup(A, B))\setminus(\cap(A, B))) = \cup(\{A\}\setminus\{A\}) = \cup\emptyset = \emptyset$ (cioè la (ii)).

Proviamo infine le (iii). Per l'assioma di Leibniz, dobbiamo soltanto dimostrare che

$$\text{se } (A, B) = (C, D) \quad \text{allora} \quad (A = C \text{ e } B = D).$$

Supponiamo dunque che sia $(A, B) = (C, D)$. Per la (i) si trova intanto che

$$A = \cup(\cap(A, B)) = \cup(\cap(C, D)) = C\,.$$

Se $A = B$,

$$\{A\} = \{A, B\} = \cup(A, B) = \cup(C, D) = \{C, D\}$$

quindi anche $C = D = A$ e non c'è altro da dimostrare. Analogamente, se $C = D$,

$$\{C\} = \{C, D\} = \cup(C, D) = \cup(A, B) = \{A, B\}$$

quindi anche $A = B = C$ e non c'è altro da dimostrare.

Se infine $A \neq B$ e $C \neq D$, per la (ii) si trova che

$$B = \cup((\cup(A, B))\setminus(\cap(A, B))) = \cup((\cup(C, D))\setminus(\cap(C, D))) = D\,.$$

Esercizio 1.12.2

"Estrarre" Z dall'insieme $\{\{X\}, \{X, Y\}, \{X, Y, Z\}\}$.

Esercizio 1.12.3

"Estrarre" X, Y, Z e W dall'insieme $\{\{X\}, \{X, Y\}, \{X, Y, Z\}, \{X, Y, Z, W\}\}$.

Osservazione 1.12.4

Come definiremo una terna ordinata (X, Y, Z)? E, più in là (quando sapremo che cos'è il numero naturale n), una $n-$pla ordinata $(X_1, X_2, \ldots, X_n)$?

Saltano all'occhio due strade "ovvie" per estendere alla terna ordinata il concetto di coppia ordinata. La prima consiste nel porre

$$(X, Y, Z) := ((X, Y), Z)$$

mentre la seconda suggerisce di definire

$$(X, Y, Z) := \{\{X\}, \{X, Y\}, \{X, Y, Z\}\} .$$

La seconda è preferibile, perché in tal modo una terna ordinata viene ad essere un insieme con tre elementi (e, se definita analogamente, una $n-$pla ordinata viene ad essere un insieme con n elementi). Ma si veda anche l'osservazione 1.13.1 .

Esercizio 1.12.5

Verificare che

$$((X, Y), Z) \neq \{\{X\}, \{X, Y\}, \{X, Y, Z\}\} .$$

Siano A, B insiemi. Si dice *prodotto cartesiano di* A *per* B e si indica con $A \times B$ l'insieme

$$\{Z \in \wp(\wp(A \cup B)) \,/\, Z = (X, Y) \quad \text{con} \quad X \in A \quad \text{e} \quad Y \in B\} .$$

Il prodotto cartesiano di due insiemi esiste per l'assioma di separazione.

A questo punto si può procedere con la teoria come è usuale, introducendo la nozione di relazione fra insiemi e poi in particolare trattare

– le funzioni, parlando di iniettività, suriettività, corrispondenza biunivoca, funzione inversa, ecc. ecc.;

– le relazioni di equivalenza, parlando in particolare di insieme quoziente;

– le relazioni di ordine, parlando in particolare di minorante, maggiorante, minimo, massimo, estremo inferiore, estremo superiore, intervalli ($[a, b]$ chiuso, (a, b) aperto, $[a, b)$ chiuso su a e aperto su b, $(a, b]$ aperto su a e chiuso su b), ecc. ecc. .

Osservazione 1.12.6

La funzione $(A \times B) \times C \to A \times (B \times C)$ che porta $((a, b), c)$ in $(a, (b, c))$ è una corrispondenza biunivoca.

1.13 - Famiglie di insiemi.

Siano A, X insiemi. Si dice *famiglia di* (*sotto*)*insiemi* (*di* X) *indiciata da* A una funzione

$$\mathbf{f} : \mathrm{A} \to \wp(\mathrm{X}) .$$

In questo contesto, per ogni $a \in \mathrm{A}$ l'immagine di a mediante **f** si indica con X_a. L'immagine di **f** si indica con

$$\{\mathrm{X}_a\}_{a\in\mathrm{A}}$$

e si scrive

$$\bigcup_{a\in\mathrm{A}} \mathrm{X}_a \quad \text{anziché} \quad \cup\{\mathrm{X}_a\}_{a\in\mathrm{A}} \qquad \text{e} \qquad \bigcap_{a\in\mathrm{A}} \mathrm{X}_a \quad \text{anziché} \quad \cap\{\mathrm{X}_a\}_{a\in\mathrm{A}} .$$

Si noti che l'insieme X (del quale gli X_a sono sottoinsiemi) non svolge in quanto sopra altro ruolo che quello di "ambiente". Spesso né X né la funzione **f** vengono esplicitati, e si scrive soltanto

«Sia $\{\mathrm{X}_a\}_{a\in\mathrm{A}}$ una famiglia di insiemi…»

facendo direttamente riferimento all'immagine di **f**.

Sia $\{\mathrm{X}_a\}_{a\in\mathrm{A}}$ una famiglia di insiemi. Si dice *prodotto cartesiano* degli X_a l'insieme delle funzioni $\varphi : \mathrm{A} \to \bigcup_{a\in\mathrm{A}} \mathrm{X}_a$ tali che $\varphi(a) \in \mathrm{X}_a$.

L'osservazione 1.13.1 e l'esercizio 1.13.2 utilizzano la nozione di numero naturale, quindi il fruitore di questi appunti è invitato a rimandarne la lettura a dopo quella del prossimo capitolo…

Osservazione 1.13.1

Se $\mathrm{X}, \mathrm{Y}, \mathrm{Z}$ sono insiemi, possiamo pensare a $\{\mathrm{X}, \mathrm{Y}, \mathrm{Z}\}$ come a una famiglia di insiemi indiciata da $\{1, 2, 3\}$. Se identifichiamo ogni elemento (x, y, z) di $\mathrm{X} \times \mathrm{Y} \times \mathrm{Z}$ con la funzione $\varphi : \mathrm{A} \to \mathrm{X} \cup \mathrm{Y} \cup \mathrm{Z}$ per la quale $\varphi(1) = x$, $\varphi(2) = y$ e $\varphi(3) = z$, vediamo come la definizione di prodotto cartesiano che abbiamo dato per una famiglia di insiemi generalizza quella della sez. 1.12.

Di fatto, spesso la definizione di prodotto cartesiano per un numero finito $n \geq 3$ di insiemi viene proprio data pensandoli come una famiglia di insiemi indiciati da $\{1, 2, \ldots, n\}$.

Esercizio 1.13.2

Si spieghi perché la definizione di prodotto cartesiano di n insiemi si può dare pensandoli come una famiglia di insiemi indiciati da $\{1, 2, \ldots, n\}$ soltanto se $n \geq 3$.

2.- I NUMERI NATURALI

Μονὰς ἔστιν, καθ' ἣν ὅ ἕκαστον τῶν ὄντων ἓν λέγεται
Ἀριθμὸς δε, τὸ ἐκ μονδάων συγκείμενον πλῆθος

Euclide, *Elementi*, VII libro

2.1 - L'assioma dell'infinito.

Sia A un insieme. L'insieme

$$A \cup \{A\}$$

si dice il *successivo* di A e si indica con A^+.

Osservazione 2.1.1

Per ogni insieme A, esiste l'insieme {A} (cfr. l'oss. 1.6.4) ed esiste l'insieme {A, {A}} (per l'assioma delle coppie), dunque esiste l'insieme A^+ (per l'assioma dell'unione).

Osservazione 2.1.2

Per ogni insieme A,

$$A \neq A^+ .$$

Infatti, per definizione, $A \in A^+$; e non può essere $A \in A$ per il teorema 1.7.2 .

($\mathcal{A}_7$)
Esiste un insieme A tale che: $\emptyset \in A$, e per ogni $x \in A$ anche $x^+ \in A$.

2.2 - L'insieme $\mathbb{N}$.

Per semplicità di notazione, farà comodo in questa sezione introdurre la seguente definizione: un insieme A si dice *chiuso rispetto al successivo* se per ogni $x \in \mathrm{A}$ è anche $x^+ \in \mathrm{A}$. L'assioma dell'infinito può essere così riformulato: esiste un insieme a cui appartiene $\emptyset$ e che è chiuso rispetto al successivo.

Lemma 2.2.1

Se A è un insieme non vuoto tale che ogni $\mathrm{Y} \in \mathrm{A}$ è chiuso rispetto al successivo, anche $\cap \mathrm{A}$ è chiuso rispetto al successivo.

Dimostrazione – Se $\cap \mathrm{A} = \emptyset$, esso è banalmente chiuso rispetto al successivo. Sia $x \in \cap \mathrm{A}$; allora $x \in \mathrm{Y}$ per ogni $\mathrm{Y} \in \mathrm{A}$, e pertanto $x^+ \in \mathrm{Y}$ (perché per ipotesi Y è chiuso rispetto al successivo) per ogni $\mathrm{Y} \in \mathrm{A}$. Dunque $x^+ \in \cap \mathrm{A}$, e per l'arbitrarietà di x in $\cap \mathrm{A}$ l'asserto è provato.

Teorema 2.2.2

Esiste uno e un solo insieme $\mathbb{N}$ tale che

(i) $\emptyset \in \mathbb{N}$, e inoltre $\mathbb{N}$ è chiuso rispetto al successivo;
(ii) per ogni insieme B chiuso rispetto al successivo tale che $\emptyset \in \mathrm{B}$, si ha $\mathbb{N} \subset \mathrm{B}$.

Dimostrazione – Sia A_0 uno degli insiemi la cui esistenza è prevista dall'assioma dell'infinito, e sia

$$\mathrm{S} := \{\mathrm{X} \in \wp(\mathrm{A}_0) \,/\, \emptyset \in \mathrm{X}, \text{ e X è chiuso rispetto al successivo}\}.$$

Poniamo

$$\mathbb{N} := \cap \mathrm{S}.$$

È chiaro che vale la (i) (per il lemma 2.2.1). Sia ora B un insieme chiuso rispetto al successivo tale che $\emptyset \in \mathrm{B}$; anche $\mathrm{A}_0 \cap \mathrm{B}$ è chiuso rispetto al successivo (sempre per il lemma 2.2.1), e inoltre $\emptyset \in \mathrm{A}_0 \cap \mathrm{B}$: dunque $\mathrm{A}_0 \cap \mathrm{B} \in \mathrm{S}$ e pertanto $\mathbb{N} \subset \mathrm{A}_0 \cap \mathrm{B} \subset \mathrm{B}$, ossia la ($ii$).
Supponiamo infine che $\mathbb{N}_1, \mathbb{N}_2$ entrambi verifichino la (i) e la (ii): deve essere

$$\mathbb{N}_1 \subset \mathbb{N}_2 \quad \text{e} \quad \mathbb{N}_2 \subset \mathbb{N}_1$$

ossia $\mathbb{N}_1 = \mathbb{N}_2$, dunque esiste un solo insieme che verifica sia la (i) che la (ii).

Notazione 2.2.3

L'insieme $\mathbb{N}$ di cui al teorema 2.2.2 si dice *insieme dei numeri naturali*. L'elemento $\emptyset$ si dice *zero* e si indica con "0"; l'elemento 0^+ (cioè: $\{0\}$, ossia $\{\emptyset\}$) si dice *uno* e si indica con "1"; l'elemento 1^+ (cioè $\{0, 1\}$, ossia $\{\emptyset, \{\emptyset\}\}$) si dice *due* e si indica con "2"; l'elemento 2^+ (cioè $\{0, 1, 2\}$, ossia $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$) si dice *tre* e si indica con "3"; e così via...

2.3 - Transitività.

Un insieme A si dice *transitivo* se per ogni insieme X e per ogni insieme Y da $X \in Y \in A$ segue $X \in A$.

Osservazione 2.3.1

Un insieme è transitivo se e soltanto se ogni suo elemento è anche suo sottoinsieme.

Teorema 2.3.2

Il successivo di un insieme transitivo è transitivo.

Dimostrazione – Sia A un insieme transitivo, e sia $A^+ = A \cup \{A\}$.
Sia $X \in A^+$, e proviamo che $X \subset A^+$. Se $X = A$, è immediato (per la definizione di A^+) che $X \subset A^+$; altrimenti $X \in A$, quindi (poiché per ipotesi A è transitivo) $X \subset A$; poiché $A \subset A^+$, anche in questo caso si conclude che $X \subset A^+$.

Teorema 2.3.3

Ogni numero naturale è transitivo.

Dimostrazione – Sia $B := \{n \in \mathbb{N} \,/\, n \text{ è transitivo}\}$.

È immediato che $\emptyset \in B$; inoltre (per il teorema 2.3.2) B è chiuso rispetto al successivo. Per la (ii) del teorema 2.2.2 si ha che $\mathbb{N} \subset B$ e dunque (poiché $B \subset \mathbb{N}$ per definizione di B) che $B = \mathbb{N}$, cioè l'asserto.

Osservazione 2.3.4

Esistono altri insiemi transitivi oltre ai numeri naturali. Ad esempio, col teorema 2.3.5 proveremo che $\mathbb{N}$ è transitivo; ma $\mathbb{N}$ non è un numero naturale (altrimenti sarebbe $\mathbb{N} \in \mathbb{N}$ contro il teorema 1.7.2).

Teorema 2.3.5

Ogni elemento di un numero naturale è un numero naturale.

Dimostrazione – Sia $B := \{n \in \mathbb{N} \,/\, \text{ogni elemento di } n \text{ è un numero naturale}\}$.

È immediato che $\emptyset \in B$; se proviamo che B è chiuso rispetto al successivo, per la (ii) del teorema 2.2.2 si ha che $\mathbb{N} \subset B$ e dunque (poiché $B \subset \mathbb{N}$ per definizione di B) che $B = \mathbb{N}$, cioè l'asserto.
Sia allora $n \in B$, e sia $m \in n^+ = n \cup \{n\}$. Deve essere $m = n$ (e quindi m è un numero naturale) oppure $m \in n$ (e quindi m è un numero naturale, perché $n \in B$).

Questo risultato sarà precisato più avanti (osservazione 2.8.1).

Esercizi

2.3.6 Si trovi un insieme transitivo che non sia un sottoinsieme di $\mathbb{N}$.

2.3.7 Si trovi un sottoinsieme di $\mathbb{N}$ che non è un insieme transitivo.

2.4 - Gli assiomi di Peano.

Come è noto, il matematico italiano Giuseppe Peano (1858-1932) aveva proposto di introdurre i numeri naturali con un sistema di cinque assiomi.

Due delle parole primitive di Peano ("*insieme*", "*appartiene*") sono parole primitive anche nella teoria di Zermelo e Frankel; in tale teoria, però, le altre si possono definire (lo abbiamo fatto nelle sezioni 2.1 e 2.2), e il contenuto degli assiomi si può dimostrare. È quel che ci accingiamo a fare, provando così che i "numeri naturali" da noi costruiti sono "gli stessi" introdotti da Peano. A questo punto potremo "dimenticare" la nostra definizione di $\mathbb{N}$ e per tutte le considerazioni successive utilizzare la teoria sviluppata da Peano.

$$\cdot 1 \quad 0 \in \mathrm{N}_0$$

$$\cdot 2 \quad a \in \mathrm{N}_0 \,.\supset.\, a+ \in \mathrm{N}_0$$

$$\cdot 3 \quad s \in \mathrm{Cls} \,.\, 0 \in s : x \in \mathrm{N}_0 \cap s \,.\supset x.\, x+ \in s :\supset.\, \mathrm{N}_0 \supset s$$

$$\cdot 4 \quad a,b \in \mathrm{N}_0 \,.\, a+ = b+ \,.\supset.\, a = b$$

$$\cdot 5 \quad a \in \mathrm{N}_0 \,.\supset.\, a+ \neq 0$$

Fig. 1 - Gli assiomi di Peano, nella formulazione di [2].

Facciamo riferimento, con qualche irrilevante aggiornamento nei termini [1], alla formulazione di [2], esplicitandone con termini discorsivi il pesante formalismo simbolico; la prima esposizione del sistema di assiomi è in un lavoro scientifico pubblicato nel 1891.

Le parole primitive di Peano sono: "*insieme*", "*appartiene*" (queste due sono parole primitive anche nella nostra costruzione), "*numero naturale*", "*zero*", "*successivo*" (queste, come si è già detto, le abbiamo definite nelle sezioni 2.1 e 2.2 . Gli assiomi corrispondono al contenuto dei seguenti cinque teoremi.

[1] Ad esempio, Peano scrive "classe" anziché "insieme", "successore" invece di "successivo" e "numero" *tout-court* anziché "numero naturale".

Teorema 2.4.1

Zero è un numero naturale.

Dimostrazione – Ovvio, per definizione di $\mathbb{N}$.

Teorema 2.4.2

Ogni numero naturale ha un successivo, che è anch'esso un numero naturale.

Dimostrazione – Per ogni insieme X esiste il successivo di X (cfr. l'oss. 2.1.1), dunque in particolare ogni elemento di $\mathbb{N}$ ha un successivo; che tale successivo appartenga ad esso a $\mathbb{N}$ equivale al fatto che $\mathbb{N}$ è chiuso rispetto al successivo (cfr. la (i) del teorema 2.2.2).

Teorema 2.4.3 ("*Principio di induzione*")

Sia A un insieme. Supponiamo che zero appartenga ad A e che per ogni numero naturale che appartiene ad A anche il suo successivo appartenga ad A; allora ogni numero naturale appartiene ad A.

Dimostrazione – Le ipotesi ci dicono che $\emptyset \in \mathrm{A}$ e che A è chiuso rispetto al successivo; ma allora $\mathbb{N} \subset \mathrm{A}$ per la (ii) del teorema 2.2.2.

Teorema 2.4.4

Se due numeri naturali hanno lo stesso successivo, essi sono lo stesso numero.

Dimostrazione – Siano $m, n \in \mathbb{N}$ tali che $m^+ = n^+$.
Poiché $m^+ = m \cup \{m\}$ e $n^+ = n \cup \{n\}$, per l'assioma di estensione deve essere $m = n$ (e in questo caso l'asserto è provato) oppure $m \in n$ e $n \in m$. Ma questo non è possibile, perché i numeri naturali sono transitivi (teorema 2.3.3) e ne seguirebbe che $m \in m$ (e che $n \in n$), assurdo per il teorema 1.7.2.

Teorema 2.4.5

Zero non è il successivo di alcun numero naturale.

Dimostrazione – Per ogni insieme A, $\mathrm{A} \in \mathrm{A}^+$ e dunque $\mathrm{A}^+ \neq \emptyset = 0$.

Fin qui le proprietà espresse dagli assiomi di Peano. Ne segnaliamo un'altra che potrà esserci utile.

Teorema 2.4.6

Ogni numero naturale, tranne 0, è il successivo di un numero naturale.

Dimostrazione – Supponiamo che $n_0 \in \mathbb{N}$ non sia il successivo di alcun numero naturale e proviamo che $n_0 = 0$.

L'insieme $\mathbb{N}\backslash\{n_0\}$ è chiuso rispetto al successivo (perché $\mathbb{N}$ lo è, e sopprimendo n_0 non abbiamo eliminato il successivo di alcun numero). Se fosse $n_0 \neq 0$, per la (ii) del teorema 2.2.2 dovrebbe essere $\mathbb{N} \subset \mathbb{N}\backslash\{n_0\}$, ma questo è assurdo (perché $n_0 \in \mathbb{N}$ ma $n_0 \notin \mathbb{N}\backslash\{n_0\}$). Dunque $n_0 = 0$, come si voleva.

Terminiamo questa sezione formalizzando il classico algoritmo delle "dimostrazioni per induzione".

Teorema 2.4.7

Sia **P**(n) una proposizione aperta con variabile libera n su $\mathbb{N}$. Se

– **P**(0) è vera

e

– $(\forall n \in \mathbb{N})($**P**$(n) \Rightarrow$ **P**$(n^+))$ è vera

allora è vero che

$$(\forall n \in \mathbb{N})(\textbf{P}(n)) \, .$$

Dimostrazione – Sia

$$\mathrm{A} = \{n \in \mathbb{N} \,/\, \textbf{P}(n)\}.$$

Le ipotesi del teorema ci dicono che $0 \in$ A e che per ogni numero naturale che appartiene ad A anche il suo successivo appartiene ad A. Allora, per il teorema 2.4.3, A $= \mathbb{N}$, e dunque **P**(n) è vera per ogni $n \in \mathbb{N}$, come si voleva dimostrare.

2.5 - Funzioni definite induttivamente.

Altra classica applicazione del principio di induzione è la possibilità di definire una funzione

$$\mathbf{f} : \mathbb{N} \rightarrow \mathrm{A}$$

(dove A è un insieme qualsiasi) precisando come **f** opera su 0 e poi dicendo come si ricava il valore di **f** sul successivo di n a partire da n e dal valore di **f** su n, per ogni $n \in \mathbb{N}$.

Che queste informazioni definiscano effettivamente una funzione $\mathbb{N} \rightarrow$A può forse essere intuitivo ma va certamente dimostrato.

Teorema 2.5.1 ("di recursione")

Siano A un insieme, $a_0 \in \mathrm{A}$ e **w** una funzione $\mathbb{N} \times \mathrm{A} \to \mathrm{A}$. Esiste una e una sola funzione $\mathbf{f} : \mathbb{N} \to \mathrm{A}$ tale che

$$\mathbf{f}(0) = a_0$$

e inoltre

$$\mathbf{f}(n^+) = \mathbf{w}(n, \mathbf{f}(n)) \qquad \text{per ogni } n \in \mathbb{N}\,.$$

Dimostrazione – Ricordiamo che un funzione $\mathbb{N} \to \mathrm{A}$ è un particolare sottoinsieme di $\mathbb{N} \times \mathrm{A}$. Costruiamo esplicitamente **f** come insieme di coppie ordinate (che **f**, se esiste, sia unica è immediata conseguenza della definizione di funzione e dell'assioma di estensione). Sia

$$\mathrm{C} \coloneqq \{\mathrm{X} \in \wp(\mathbb{N} \times \mathrm{A}) \,/\, (0, a_0) \in \mathrm{X} \text{ e inoltre se } (n, a) \in \mathrm{X} \text{ anche } (n^+, \mathbf{w}(n, a)) \in \mathrm{X}\}\,.$$

L'insieme C non è vuoto, perché $\mathbb{N} \times \mathrm{A} \in \mathrm{C}$. Poniamo

$$\mathbf{f} \coloneqq \cap\, \mathrm{C}\,.$$

È immediato verificare che $\mathbf{f} \in \mathrm{C}$, cioè che **f** (se è una funzione) si comporta come richiesto. Ma **f** è una funzione? Resta da dimostrare che per ogni $n \in \mathbb{N}$ c'è uno e un solo $a \in \mathrm{A}$ tale che $(n, a) \in \mathbf{f}$. Sia

$$\mathrm{S} \coloneqq \{n \in \mathbb{N} \,/\, \text{esiste uno e un solo } a \in \mathrm{A} \text{ tale che } (n, a) \in \mathbf{f}\}\,.$$

Dobbiamo provare che $\mathrm{S} = \mathbb{N}$, e lo facciamo applicando il principio di induzione.

In primo luogo, $0 \in \mathrm{S}$. Se così non fosse, esisterebbe $\overline{a} \neq a_0$ tale che $(0, \overline{a}) \in \mathbf{f}$ (infatti certamente $(0, a_0) \in \mathbf{f}$ per come abbiamo definito C e poi **f**). Ma allora $\mathbf{f} \setminus \{(0, \overline{a})\}$ sarebbe un elemento di C incluso propriamente in **f**, assurdo per come abbiamo definito **f**. Si noti che se $(n, a) \in \mathbf{f} \setminus \{(0, \overline{a})\}$ anche $(n^+, \mathbf{w}(n, a)) \in \mathbf{f} \setminus \{(0, \overline{a})\}$ perché 0 non è il successivo di alcun numero naturale (teorema 2.4.5).

Ora supponiamo che sia $n \in \mathrm{S}$, cioè che esista uno e un solo $a \in \mathrm{A}$ tale che $(n, a) \in \mathbf{f}$, e proviamo che $n^+ \in \mathrm{S}$ (cioè che esiste uno e un solo $b \in \mathrm{A}$ tale che $(n^+, b) \in \mathbf{f}$). Certamente $(n^+, \mathbf{w}(n, a)) \in \mathbf{f}$ (per come abbiamo definito C e poi **f**). Supponiamo per assurdo che esista $b_0 \neq \mathbf{w}(n, a)$ tale che $(n^+, b_0) \in \mathbf{f}$, e consideriamo $\mathbf{f} \setminus \{(n^+, b_0)\}$: se dimostriamo che

$$\mathbf{f} \setminus \{(n^+, b_0)\} \in \mathrm{C}$$

vuol dire che abbiamo trovato un elemento di C incluso propriamente in **f** e quindi (per come è stata definita **f**) il desiderato assurdo.

In effetti, $(0, a_0) \in \mathbf{f} \setminus \{(n^+, b_0)\}$ (perché $(0, a_0) \in \mathbf{f}$ e certamente $n^+ \neq 0$, ancora per il teorema 2.4.5). Resta da provare che

$$\text{se} \quad (m, c) \in \mathbf{f} \setminus \{(n^+, b_0)\} \quad \text{anche} \quad (m^+, \mathbf{w}(m, c)) \in \mathbf{f} \setminus \{(n^+, b_0)\}\,.$$

Se $m \neq n$, per il teor. 2.4.4 è anche $m^+ \neq n^+$ e dunque certamente $(m^+, \mathbf{w}(m, c)) \neq (n^+, b_0)$, pertanto $(m^+, \mathbf{w}(c)) \in \mathbf{f} \setminus \{(n^+, b_0)\}$ (dato che $(m^+, \mathbf{w}(c)) \in \mathbf{f}$ essendo $(m, c) \in \mathbf{f}$). Se invece $m = n$, deve essere $c = a$ (poiché $n \in \mathrm{S}$) e quindi $(n^+, \mathbf{w}(a)) \in \mathbf{f} \setminus \{(n^+, b_0)\}$ perché $\mathbf{w}(a) \neq b_0$. L'asserto è così completamente provato.

2.6 - La somma in $\mathbb{N}$.

Sia $m \in \mathbb{N}$. Per il teorema 2.5.1, esiste una e una sola funzione $\boldsymbol{s}_m$:$\mathbb{N}\to\mathbb{N}$ tale che

$$\boldsymbol{s}_m(0) = m \qquad \text{e} \qquad \boldsymbol{s}_m(n^+) = (\boldsymbol{s}_m(n))^+.$$

Siano $m, n \in \mathbb{N}$. Il numero naturale $\boldsymbol{s}_m(n)$ si dice *somma* di m e n e si indica con

$$m + n\,.$$

Lemma 2.6.1

Per ogni $n \in \mathbb{N}$ si ha

$$0 + n = n + 0 = n\,.$$

Dimostrazione – Si ha $n + 0 = \boldsymbol{s}_n(0) = n$ per definizione di somma, dunque c'è solo da provare che $0 + n = n$, e lo facciamo per induzione su n.

L'asserto è vero per $n = 0$: infatti $0 + 0 = \boldsymbol{s}_0(0) = 0$ per definizione. Supponiamo di aver provato l'asserto per n; allora

$$0 + n^+ = \boldsymbol{s}_0(n^+) = (\boldsymbol{s}_0(n))^+ = (0 + n)^+ = n^+$$

come si voleva.

Lemma 2.6.2

Per ogni $m, n \in \mathbb{N}$ si ha

$$m + n^+ = (m + n)^+$$

e

$$m^+ + n = (m + n)^+\,.$$

Dimostrazione – La prima uguaglianza segue immediatamente dalla definizione di somma; proviamo la seconda per induzione su n. Per il lemma 2.6.1 si ha subito che

$$m^+ + 0 = m^+ = (m + 0)^+\,.$$

Sia allora

$$m^+ + n = (m + n)^+$$

e proviamo che

$$m^+ + n^+ = (m + n^+)^+\,.$$

Si ha

$$m^+ + n^+ = (m^+ + n)^+ = \big((m + n)^+\big)^+ = (m + n^+)^+$$

come si voleva.

Teorema 2.6.3

Per ogni $m, n \in \mathbb{N}$ si ha

$$m + n = n + m\,.$$

Dimostrazione – Per induzione su m. Se $m = 0$, segue dal lemma 2.6.1; supponiamo dunque che sia $m + n = n + m$ per ogni $n \in \mathbb{N}$, e proviamo che

$$m^+ + n = n + m^+\,.$$

Si ha

$$m^+ + n \overset{\text{(lemma 2.6.2)}}{=} (m + n)^+ = (n + m)^+ \overset{\text{(lemma 2.6.2)}}{=} n + m^+$$

cosicché l'asserto è completamente provato.

Teorema 2.6.4

Per ogni $n \in \mathbb{N}$ si ha

$$1 + n = n + 1 = n^+\,.$$

Dimostrazione – Per il teorema 2.6.3 basterà dimostrare che per ogni $n \in \mathbb{N}$ si ha

$$1 + n = n^+$$

e lo facciamo procedendo per induzione su n. Poiché

$$1 + 0 = \boldsymbol{s}_1(0) = 1 = 0^+$$

l'asserto è vero per $n = 0$. Supponiamo adesso che l'asserto sia vero per n; allora

$$1 + n^+ = \boldsymbol{s}_1(n^+) = (\boldsymbol{s}_1(n))^+ = (1 + n)^+ = (n^+)^+$$

come si voleva.

Esercizio 2.6.5

Si provi che per ogni $\ell, m, n \in \mathbb{N}$ si ha

$$(\ell + m) + n = \ell + (m + n)\,.$$

Suggerimento: Si proceda per induzione su n.

Esercizio 2.6.7

Si provi che, per ogni $\ell, m, n \in \mathbb{N}$,

se $\ell + n = m + n$ oppure $n + \ell = n + m$, allora $\ell = m$ ("legge di cancellazione per la somma")

Suggerimento: Si proceda per induzione su n.

Teorema 2.6.7 ("Legge di annullamento della somma")

Per ogni $x, y \in \mathbb{N}$ si ha

$$x + y = 0 \quad \text{se e soltanto se} \quad x = y = 0.$$

Dimostrazione – Per definizione $0 + 0 = 0$, quindi dobbiamo soltanto dimostrare che se $x \neq 0$ oppure $y \neq 0$ allora $x + y \neq 0$. Poiché la somma è commutativa (teor. 2.6.3) basterà considerare il caso $x \neq 0$: proviamo dunque che se $x \neq 0$ allora $x + y \neq 0$.

Sia $x \neq 0$. Se $y = 0$, $x + 0 = x \neq 0$; se $y \neq 0$, per il teor. 2.4.6 è $y = y_0^+$ per un opportuno $y_0 \in \mathbb{N}$; allora

$$x + y = x + y_0^+ \overset{\text{(lemma 2.6.2)}}{=} (x + y_0)^+$$

e quindi $x + y \neq 0$ per il teor. 2.4.5.

2.7 - Il prodotto in $\mathbb{N}$.

Sia $m \in \mathbb{N}$. Per il teorema 2.5.1, esiste una e una sola funzione $\boldsymbol{p}_m$:$\mathbb{N}\to\mathbb{N}$ tale che

$$\boldsymbol{p}_m(0) = 0 \qquad \text{e} \qquad \boldsymbol{p}_m(n^+) = \boldsymbol{p}_m(n) + m\,.$$

Siano $m, n \in \mathbb{N}$. Il numero naturale $\boldsymbol{p}_m(n)$ si dice *prodotto* di m e n e si indica con mn

Esercizio 2.7.1

Si provi che per ogni $\ell, m, n \in \mathbb{N}$ si ha:

(i) $n0 = 0n = 0$;
(ii) $n1 = 1n = n$;
(iii) $(\ell m)n = \ell(mn)$;
(iv) $mn = nm$;
(v) $(\ell + m)n = \ell n + mn$;
(vi) se $\ell n = mn$ e $n \neq 0$, allora $\ell = m$ ("legge di cancellazione a destra per il prodotto").

Teorema 2.7.2 ("Legge di annullamento del prodotto")

Per ogni $x, y \in \mathbb{N}$ si ha

$$xy = 0 \quad \text{se e soltanto se} \quad x = 0 \text{ oppure } y = 0.$$

Dimostrazione – Per definizione di prodotto $x0 = 0$ per ogni $x \in \mathbb{N}$, e si prova senza difficoltà per induzione su y che $0y = 0$ per ogni $y \in \mathbb{N}$; quindi dobbiamo soltanto dimostrare che se $x \neq 0$ e $y \neq 0$ allora $xy \neq 0$.

Supponiamo allora che sia $x \neq 0$ e $y \neq 0$. Per il teor. 2.4.6, y è il successivo di un numero naturale y_0, e si ha

$$xy = \boldsymbol{p}_x(y) = \boldsymbol{p}_x(y_0^+) = \boldsymbol{p}_x(y_0) + x$$

e quest'ultimo numero è certamente diverso da zero per il teor. 2.6.7 poiché per ipotesi $x \neq 0$.

2.8 - Ordine in $\mathbb{N}$.

Per comodità, introduciamo la classica relazione di ordine in $\mathbb{N}$ utilizzando la definizione di $\mathbb{N}$ (cfr. sez. 2.2) e non gli assiomi di Peano. Il collegamento con la costruzione di Peano è dato dal teorema 2.8.10.

Siano $x, y \in \mathbb{N}$. Si dice che x è (strettamente) *minore* di y, e si scrive $x < y$ se $x \in y$. Si dice che x è *minore o uguale* a y, e si scrive $x \leq y$ se $x \in y$ oppure $x = y$.

Osservazione 2.8.1

Per ogni $n \in \mathbb{N}$,

$$n = \{x \in \mathbb{N} \,/\, x < n\}.$$

Dimostrazione – Sappiamo dal teorema 2.3.5 che tutti gli elementi di n sono numeri naturali. Che siano tutti e soli quelli che precedono strettamente n è banale immediata conseguenza della definizione di " $<$ ".

Lemma 2.8.2

Per ogni $n \in \mathbb{N}$ si ha $n = 0$ oppure $0 \in n$.

Dimostrazione – Per induzione su n. L'asserto è ovvio se $n = 0$. Supponiamo di sapere che

$$n = 0 \quad \text{oppure} \quad 0 \in n$$

per un certo n, e dimostriamo che lo stesso vale per n^+. Per definizione, $n^+ = n \cup \{n\}$, quindi sia nel caso in cui $n = 0$ sia nel caso in cui $0 \in n$ si può concludere che $0 \in n^+$ e l'asserto è completamente provato.

Teorema 2.8.3

La relazione $\leq$ è una relazione di ordine totale in $\mathbb{N}$.

Dimostrazione – Per ogni $x \in \mathbb{N}$ si ha $x = x$ (per la (i) del teorema 1.1.1), dunque $\leq$ è riflessiva.

Siano $x, y \in \mathbb{N}$ tali che $x \leq y$ e $y \leq x$. Se fosse $x \neq y$, sarebbe $x \in y$ e $y \in x$, da cui $x \in x$ (per la transitività dei numeri naturali, cfr. teorema 2.3.3) contro il teorema 1.7.2. Dunque necessariamente $x = y$, quindi $\leq$ è antisimmetrica.

Siano $x, y, z \in \mathbb{N}$ tali che $x \leq y$ e $y \leq z$. Se $x = y$ oppure $y = z$ è chiaro che $x \leq z$. Se invece $x \neq y$ e $y \neq z$, deve essere $x \in y$ e $y \in z$, da cui $x \in z$ (e quindi $x \leq z$) per la già citata transitività dei numeri naturali.

Resta da provare che $\leq$ è una relazione di ordine *totale*, cioè che due numeri naturali comunque presi sono sempre confrontabili. A tale scopo, per ogni numero naturale n indichiamo con S(n) l'insieme dei numeri naturali confrontabili con n, cioè

$$\mathrm{S}(n) := \{x \in \mathbb{N} \,/\, x = n \text{ oppure } x \in n \text{ oppure } n \in x\}\,.$$

Poniamo poi

$$\mathrm{S} := \{n \in \mathbb{N} \,/\, \mathrm{S}(n) = \mathbb{N}\}$$

e dimostriamo che $\mathrm{S} = \mathbb{N}$.

In primo luogo, sia ha che $0 \in \mathrm{S}$; infatti $\mathrm{S}(0) = \mathbb{N}$ per il lemma 2.8.2 . Supponiamo ora che sia $n \in \mathrm{S}$, e proviamo che $n^+ \in \mathrm{S}$, cioè che $\mathrm{S}(n^+) = \mathbb{N}$. Di nuovo ragioniamo per induzione: $0 \in \mathrm{S}(n^+)$ (ancora per il lemma 2.8.2); ora supponiamo che sia $x \in \mathrm{S}(n^+)$ e dimostriamo che $x^+ \in \mathrm{S}(n^+)$. Dobbiamo distinguere tre casi. Se $x = n^+$, è $n^+ = x \in x \cup \{x\} = x^+$ e quindi $x^+ \in \mathrm{S}(n^+)$; se $n^+ \in x$, poiché $x \in x^+$ si ha $n^+ \in x^+$ (e quindi $x^+ \in \mathrm{S}(n^+)$) per la già citata transitività dei numeri naturali; se infine $x \in n^+ (= n \cup \{n\})$ dobbiamo ancora distinguere due casi: $x = n$ (e quindi $x^+ = n^+$, cosicché $x^+ \in \mathrm{S}(n^+)$) oppure $x \in n$.

In quest'ultimo caso, ricordiamo che $\mathrm{S}(n) = \mathbb{N}$, cosicché deve essere $x^+ \in n$, oppure $x^+ = n$, oppure $n \in x^+$. Nei primi due casi, $x^+ \in n \cup \{n\} = n^+$, cosicché $x^+ \in \mathrm{S}(n^+)$ come si voleva; resta da provare che non può essere $n \in x^+ (= x \cup \{x\})$: infatti dovrebbe essere $n \in x$ oppure $n = x$; ricordando che $x \in n$, in entrambi i casi si otterrebbe che $x \in x$, contro il teorema 1.7.2.

Nel seguito, ci farà comodo la seguente osservazione.

Osservazione 2.8.4

Siano $x, y \in \mathbb{N}$. Si ha

(i) $\quad x < y \quad$ se e soltanto se $\quad x^+ < y^+$;

(ii) $\quad x \leq y \quad$ se e soltanto se $\quad x^+ \leq y^+$.

Dimostrazione – Proviamo la (i). Se $x^+ \in y^+ = y \cup \{y\}$, deve essere $x^+ \in y$ oppure $x^+ = y$; poiché $x \in x^+$, si può concludere che $x \in y$ (nel primo caso applicando il teorema 2.3.3). Viceversa, se $x \in y$ non può essere $x^+ = y^+$ (altrimenti per il teorema 2.4.4 ne seguirebbe che $x = y$ e quindi $x \in x$ contro il teorema 1.7.2); se fosse $y^+ < x^+$ ne seguirebbe (per quanto appena dimostrato) che $y \in x$ e quindi infine che $x \in x$, ancora contro il teorema 1.7.2. Poiché $\leq$ è una relazione di ordine totale in $\mathbb{N}$ (cfr. teorema 2.8.3), deve essere $x \leq y$, e quindi $x < y$ (altrimenti avremmo di nuovo che $x \in y = x$ contro il teorema 1.7.2).

Adesso proviamo la (ii). Se $x = y$ è chiaro che $x^+ = y^+$; se $x^+ = y^+$ deve essere $x = y$ per il teorema 2.4.4. Negli altri casi, basta applicare la (i).

Teorema 2.8.5

Per ogni $x \in \mathbb{N}$,

$$x < x^+ \quad \text{e non esiste alcun } y \in \mathbb{N} \text{ tale che } \quad x < y < x^+ .$$

Dimostrazione — Per definizione di successivo si ha $x \in x^+$ (cioè, appunto, $x < x^+$). Se esistesse $y \in \mathbb{N}$ tale che $x \in y \in x^+ = x \cup \{ x\}$ dovrebbe essere $y \in x$ oppure $y = x$ da cui in ogni caso $x \in x$ contro il teorema 1.7.2 .

Teorema 2.8.6

Siano $x, y \in \mathbb{N}$. Si ha

$$x \leq y \quad \text{se e soltanto se} \quad x \subset y .$$

Dimostrazione — Sia $x \leq y$; allora $x = y$ oppure $x \in y$. Se $x = y$, è in particolare $x \subset y$ (per l'assioma di estensione), se invece $x \in y$ si ha $x \subset y$ per la transitività dei numeri naturali (teorema 2.3.3).

Viceversa, sia $x \subset y$; non può essere $y \in x$ (altrimenti sarebbe anche $y \in y$, contro il teorema 1.7.2), dunque per il teorema 2.8.3 deve essere $x \leq y$.

Osservazione 2.8.7

Si faccia attenzione a non fraintendere il teorema 2.8.6: esso **non** afferma che ogni sottoinsieme di un numero naturale y è un numero naturale $\leq y$.

Ad esempio, se $y := 3 = \{0, 1, 2\}$, allora $\{ 1\}$, $\{2\}$, $\{1, 2\}$ e $\{0, 2\}$ sono sottoinsiemi di 3 ma non sono numeri naturali!

Lemma 2.8.8

Siano $x, y \in \mathbb{N}$. Si ha

$$x < y \quad \text{se e soltanto se} \quad x^+ \leq y .$$

Dimostrazione — Sia in primo luogo $x < y$, e supponiamo per assurdo che non sia $x^+ \leq y$; poiché $\leq$ è una relazione di ordine totale in $\mathbb{N}$ (cfr. teorema 2.8.3), deve essere $y < x^+$, cosicché $x < y < x^+$ contro il teorema 2.8.5 .

Viceversa, sia $x^+ \leq y$. Se fosse $y \leq x$, dall'oss. 2.8.4 seguirebbe che $y^+ \leq x^+$ e quindi $y^+ \leq y$, da cui infine (ricordando il teorema 2.8.5) $y = y^+$ contro l'oss. 2.1.2.

Lemma 2.8.9

Sia $x \in \mathbb{N}$. Si ha

$$x \leq x + n \quad \text{per ogni } n \in \mathbb{N}.$$

Dimostrazione – Procediamo per induzione su n. Se $n = 0$, si ha $x + 0 = x$ (cfr. lemma 2.6.1) e quindi $x \leq x + 0$.

Supponiamo di aver provato che $x \leq x + n$ e mostriamo che $x \leq x + (n^+)$. Per il teorema 2.8.5 e per il lemma 2.6.2,

$$x + n \leq (x + n)^+ = x + (n^+)$$

e dunque, per la proprietà transitiva della relazione $\leq$, $x \leq x + (n^+)$ come si voleva.

Il prossimo teorema mostra che la nostra relazione di ordine in $\mathbb{N}$ è esattamente quella considerata da Peano.

Teorema 2.8.10

Siano $x, y \in \mathbb{N}$. Si ha

$$x \leq y \quad \text{se e soltanto se esiste } n \in \mathbb{N} \text{ tale che } x + n = y.$$

Dimostrazione – Per il lemma 2.8.9, se esiste $n \in \mathbb{N}$ tale che $x + n = y$ deve essere $x \leq y$.

Viceversa, proviamo per induzione su y che

(*) per ogni $x \in \mathbb{N}$, se $x \leq y$ allora esiste $n \in \mathbb{N}$ tale che $x + n = y$.

Sia in primo luogo $y = 0$. Se $x \leq y$ deve essere $x = 0$, quindi basta prendere $n := 0$. Supponiamo ora di aver provato la (*) per y e dimostriamola per y^+. Sia $x \leq y^+$ e distinguiamo due casi: se $x = 0$, per il lemma 2.6.1 possiamo prendere $n := y^+$; altrimenti (per il teorema 2.4.6) deve essere $x = x_0^+$ per un opportuno $x_0 \in \mathbb{N}$ e si ha che

$$x_0^+ \leq y^+$$

da cui per l'oss. 2.8.4

$$x_0 \leq y$$

e quindi per l'ipotesi di induzione esiste $n \in \mathbb{N}$ tale che

$$x_0 + n = y.$$

Dunque

$$x + n = x_0^+ + n \overset{\text{(lemma 2.6.2)}}{=} (x_0 + n)^+ = y^+$$

come si voleva.

Osserviamo infine che la relazione di ordine introdotta in $\mathbb{N}$ è "compatibile" (nel senso che ci aspettiamo) con le operazioni di somma e di prodotto definite in $\mathbb{N}$.

Teorema 2.8.11

Siano $x, y, k \in \mathbb{N}$. Si ha

(i) $x \leq y$ se e soltanto se $x + k \leq y + k$;

(ii) se $k \neq 0$, $x \leq y$ se e soltanto se $xk \leq yk$.

Dimostrazione — Proviamo la (i).

Se $x \leq y$, per il teorema 2.8.10 esiste $n \in \mathbb{N}$ tale che $x + n = y$. Sommando k ad ambo i membri si ottiene che $(x + n) + k = y + k$; ma applicando ripetutamente la proprietà associativa (esercizio 2.6.5) e la proprietà commutativa (teor. 2.6.3) della somma si vede che $(x + n) + k = (x + k) + n$ e dunque si ottiene che $(x + k) + n = y + k$ ossia (ancora per il teor. 2.8.10) che $x + k \leq y + k$.

Viceversa, sia $x + k \leq y + k$ e dunque (per il teor. 2.8.10) esista $n \in \mathbb{N}$ tale che $(x + k) + n = y + k$: come si è già osservato, $(x + k) + n = (x + n) + k$ e dunque abbiamo che $(x + n) + k = y + k$. Per la legge di cancellazione (esercizio 2.6.7) si può concludere che $x + n = y$ ossia (ancora per il teor. 2.8.10) che $x \leq y$.

Proviamo ora la (ii).

Se $x \leq y$, per il teorema 2.8.10 esiste $n \in \mathbb{N}$ tale che $x + n = y$. Moltiplicando per k ambo i membri (e applicando la proprietà distributiva del prodotto rispetto alla somma (esercizio 2.7.1, (v)), si ottiene che $xk + nk = yk$ e dunque (per il teor. 2.8.10) che $xk \leq yk$.

Viceversa, sia $xk \leq yk$ e dunque (per il teor. 2.8.10) esista $\overline{n} \in \mathbb{N}$ tale che $xk + \overline{n} = yk$. Se $\overline{n} = 0$, è $xk = yk$ da cui (per la legge di cancellazione, esercizio 2.7.1, (vi)) $x = y$ e quindi in particolare $x \leq y$; se $\overline{n} \neq 0$ (e quindi $xk \neq yk$), supponiamo per assurdo che sia $y \leq x$: allora (per la parte già dimostrata della (ii)) $yk \leq xk$ e quindi $yk = xk$, assurdo perché stiamo considerando il caso in cui $\overline{n} \neq 0$, dunque $x < y$ e in particolare $x \leq y$ come si voleva dimostrare.

2.9 - La divisione euclidea in ℕ.

Teorema 2.9.1

Ogni insieme non vuoto superiormente limitato di numeri naturali ha massimo.

Dimostrazione — Proviamo (per induzione su n) che:

se $\emptyset \neq \mathrm{A} \subset \mathbb{N}$ e $a \leq n$ per ogni $a \in \mathrm{A}$, allora A ha massimo.

Se $n = 0$, deve essere $\mathrm{A} = \{0\}$ e quindi A ha per massimo lo zero. Supponiamo dunque che l'asserto sia vero per n.

Sia $\emptyset \neq \mathrm{A} \subset \mathbb{N}$ tale che $a \leq n^+$ per ogni $a \in \mathrm{A}$, e proviamo che A ha massimo. Distinguiamo due casi:

(i) se è addirittura $a \leq n$ per ogni $a \in \mathrm{A}$, A ha massimo per l'ipotesi di induzione;

(ii) se esiste $a_0 \in \mathrm{A}$ tale che $n < a_0$, per il lemma 2.8.8 deve essere $n^+ \leq a_0$; d'altro lato, per ipotesi $a_0 \leq n^+$ (perché $a_0 \in \mathrm{A}$), dunque $n^+ = a_0 \in \mathrm{A}$ e possiamo concludere che n^+ è il massimo di A .

Teorema 2.9.2

Ogni insieme non vuoto di numeri naturali ha minimo.

Dimostrazione — Sia $\emptyset \neq \mathrm{A} \subset \mathbb{N}$. Se $0 \in \mathrm{A}$, 0 è il minimo di A (infatti $0 \leq x$ per ogni $x \in \mathbb{N}$, dunque in particolare $0 \leq x$ per ogni $x \in \mathrm{A}$). Se $0 \notin \mathrm{A}$, poniamo

$$\mathrm{S} := \{n \in \mathbb{N} \,/\, n \notin \mathrm{A} \text{ e } (n \leq a \text{ per ogni } a \in \mathrm{A})\} .$$

L'insieme S non è vuoto (infatti $0 \in \mathrm{S}$) e (per come è definito) è superiormente limitato (da ogni $a \in \mathrm{A}$): per il teorema 2.9.1, S ha un massimo m. Poiché $m \in \mathrm{S}$,

(*) $$m \notin \mathrm{A} \quad \text{e} \quad m \leq a \text{ per ogni } a \in \mathrm{A} .$$

Consideriamo il successivo m^+ di m e dimostriamo che

(°) $$m^+ \leq a \text{ per ogni } a \in \mathrm{A} .$$

Ne seguirà che $m^+ \in \mathrm{A}$, e quindi che m^+ è il minimo di A. In effetti, se fosse $m^+ \notin \mathrm{A}$, per la (°) sarebbe $m^+ \in \mathrm{S}$ e quindi $m^+ \leq m$ (assurdo, perché per definizione di successivo è $m \in m^+$, cioè $m < m^+$).

Resta da provare la (°). Se esistesse $\overline{a} \in \mathrm{A}$ tale che $\overline{a} < m^+$, sarebbe

$$\overline{a} \in m^+ = m \cup \{m\}$$

e dunque necessariamente $\overline{a} \in m$ (ossia $\overline{a} < m$, contro la (*)) oppure $\overline{a} = m$ (e quindi $m \in \mathrm{A}$, di nuovo contro la (*)). Resta così provata la (°), e con essa la dimostrazione è completa.

Teorema 2.9.3

Comunque presi $a, b \in \mathbb{N}$ con $b \neq 0$ esiste un'unica coppia ordinata (q, r) di numeri interi tale che

(i) $a = bq + r$;

e

(ii) $0 \leq r < b$.

Dimostrazione — Sia

$$\mathrm{S} := \{x \in \mathbb{N} \,/\, x = bn \text{ con } n \in \mathbb{N} \text{ e } x \leq a\} .$$

L'insieme S non è vuoto (perché $0 \in$ S, essendo $0 = b \cdot 0$ e $0 \leq a$), dunque per il teorema 2.9.1 ha massimo x_0 (che, per definizione di S, è della forma bq con $q \in \mathbb{N}$). Poiché $bq \leq a$, per il teorema 2.8.10 esiste un numero naturale r per il quale vale la (i). Se fosse $r \geq b$, ancora per il teorema 2.8.10 potremmo scrivere $r = b + r_1$ con $r_1 \in \mathbb{N}$, da cui

$$a = bq + r = bq + b + r_1 = b(q+1) + r_1$$

assurdo perché $b(q+1)$ sarebbe un elemento di S strettamente maggiore di x_0.

Dunque per ogni scelta di a e b in $\mathbb{N}$ (con $b \neq 0$) esiste una coppia ordinata (q, r) di numeri interi che verifica sia la (i) che la (ii). Resta da provare che tale coppia è unica.

Supponiamo che sia

$$a = bq_1 + r_1 = bq_2 + r_2$$

(con $0 \leq r_1 < b$, $0 \leq r_2 < b$) e proviamo che $q_1 = q_2$ e $r_1 = r_2$. Poniamo, per fissare le idee, $q_1 \geq q_2$ (altrimenti nel ragionamento che segue si scambia il ruolo di q_1 con quello di q_2 e il ruolo di r_1 con quello di r_2). Per il teorema 2.8.10, esiste $n \in \mathbb{N}$ tale che

$$q_1 = q_2 + n\,.$$

Dall'uguaglianza

$$bq_2 + r_2 = bq_1 + r_1 = b(q_2 + n) + r_1 = bq_2 + bn + r_1$$

segue che

$$r_2 = bn + r_1\,.$$

Se fosse $n \neq 0$, cioè $n > 0$, sarebbe $n \geq 1$ (cfr. lemma 2.8.8) e quindi $n = 1 + n_0$ per un opportuno $n_0 \in \mathbb{N}$, cosicché

$$r_2 = bn + r_1 = b(1 + n_0) + r_1 = b + bn_0 + r_1$$

e quindi (per il teorema 2.8.10) $r_2 \geq b$ contro l'ipotesi che sia $0 \leq r_2 < b$. Pertanto $n = 0$, cosicché $q_1 = q_2$ e $r_2 = r_1$ proprio come si voleva dimostrare.

Siano $a, b \in \mathbb{N}$, con $b \neq 0$. I due numeri interi q e r di cui al teorema 2.9.3 si dicono rispettivamente *quoziente* e *resto* della *divisione euclidea di a per b*.

2.10 - I numeri interi.

Nel prodotto cartesiano $\mathbb{N} \times \mathbb{N}$ definiamo

$$(a, b) \sim (c, d) \quad \text{se e soltanto se} \quad a + d = b + c\,.$$

È facile verificare che la $\sim$ è una relazione di equivalenza in $\mathbb{N} \times \mathbb{N}$.

L'insieme quoziente $\frac{\mathbb{N}}{\sim}$ si dice *insieme dei numeri interi* e si indica con $\mathbb{Z}$.

Osservazione 2.10.1

La funzione f: $\mathbb{N}\to\mathbb{Z}$ che al numero naturale n associa la classe di equivalenza $[(n,0)]$ è iniettiva, e si ha

$$[(n,0)] = \{(a,b) \in \mathbb{N}\times\mathbb{N} \,/\, a = n+b\}\,.$$

Osservazione 2.10.2

Ogni elemento di $\mathbb{Z}$ è una classe di equivalenza della forma $[(n,0)]$ oppure $[(0,n)]$.

Si definisce in $\mathbb{Z}$ un'operazione di somma come segue:

$$[(a,b)] + [(c,d)] \coloneqq [(a+c, b+d)]\,.$$

Bisogna verificare che la definizione è ben posta, cioè non dipende dai rappresentanti scelti per le classi di equivalenza. Si trova poi che:

(i) $[(0,0)]$ è l'elemento neutro per la somma in $\mathbb{Z}$;

(ii) $[(b,a)]$ è l'opposto di $[(a,b)]$;

(iii) la somma in $\mathbb{Z}$ è associativa e commutativa;

(iv) $[(a,0)] + [(b,0)] = [(a+b,0)]$.

Osservazione 2.10.3

In $\mathbb{Z}$ non vale un analogo del teorema 2.6.7 (perché $[(1,0)] + [(0,1)] = [(1,1)] = [(0,0)]$ ma $[(1,0)] \neq [(0,0)]$ e $[(0,1)] \neq [(0,0)]$).

Si definisce in $\mathbb{Z}$ un'operazione di prodotto come segue:

$$[(a,b)] \cdot [(c,d)] \coloneqq [(ac+bd, ad+bc)]\,.$$

Bisogna verificare che la definizione è ben posta, cioè non dipende dai rappresentanti scelti per le classi di equivalenza. Si trova poi che:

(i) $[(1,0)]$ è l'elemento neutro per il prodotto in $\mathbb{Z}$;

(ii) $[(a,b)] \cdot [(0,1)] = [(b,a)]$;

(iii) il prodotto in $\mathbb{Z}$ è associativo, commutativo e distributivo rispetto alla somma.

(iv) $[(a,0)] \cdot [(b,0)] = [(ab,0)]$.

Osservazione 2.10.4

In $\mathbb{Z}$ vale l'analogo del teorema 2.7.2. Infatti se $[(a,b)] = [(0,0)]$ (cioè $a = b$) si ha

$$[(a,a)] \cdot [(c,d)] \coloneqq [(ac + ad, ad + ac)] = [(0,0)]\,;$$

se $[(c,d)] = [(0,0)]$ (cioè $c = d$) si ha

$$[(a,b)] \cdot [(c,c)] \coloneqq [(ac + bc, ac + bc)] = [(0,0)]\,.$$

Viceversa, se $[(0,0)] = [(a,b)] \cdot [(c,d)] \coloneqq [(ac + bd, ad + bc)]$ deve essere

$$ac + bd = ad + bc\,.$$

Se $c = d$ è $[(c,d)] = [(0,0)]$; in caso contrario, supponiamo (per fissare le idee) che sia $c > d$, cioè $c = d + n$ con $n \neq 0$. Allora

$$a(d+n) + bd = ad + b(d+n)$$

da cui, per la proprietà distributiva (in $\mathbb{N}$) del prodotto rispetto alla somma

$$ad + an + bd = ad + bd + bn$$

e per la proprietà commutativa della somma

$$ad + bd + an = ad + bd + bn$$

e per la legge di cancellazione rispetto alla somma

$$an = bn$$

e infine per la legge di cancellazione rispetto al prodotto (esercizio 2.7.1, (vi))

$$a = b$$

cioè $[(a,b)] = [(0,0)]$.

Osservazione 2.10.5

Nell'accennare al percorso che dai numeri naturali conduce ai reali e poi ai complessi stiamo seguendo la via suggerita dall'odierna classificazione delle strutture algebriche: abbiamo quindi introdotto subito i numeri negativi perché la struttura $(\mathbb{Z}, +, \cdot)$ così costruita è "ricca" (è un anello!). La struttura successiva sarà quella dei numeri razionali, ancora più ricca (infatti $(\mathbb{Q}, +, \cdot)$ è un campo!); poi, attraverso i numeri reali (ancora un campo, ma con una interazione più profonda con la geometria perché finalmente adatto a misurare tutti i segmenti!) si può arrivare all'apoteosi dei numeri complessi (infatti $(\mathbb{C}, +, \cdot)$ è un campo algebricamente chiuso! Ma qualcosa è stato perso per strada...).

Questa via di successivi ampliamenti degli insiemi numerici non ripercorre però la storia effettiva del pensiero matematico: furono infatti molto forti le obiezioni all'uso dei numeri negativi, la cui esistenza pareva sconvolgere con paradossi alcuni saldi princìpi. Ad esempio, l'uguaglianza

$$\frac{-1}{+1} = \frac{+1}{-1}$$

esprime il fatto ("contro natura") che il rapporto fra una grandezza maggiore e una minore è uguale al rapporto fra una grandezza minore e una maggiore (si noti che non è in questo momento in discussione se -1 sia minore o maggiore di $+1$: per creare il "paradosso" basta che i due numeri siano diversi e che la relazione di ordine sia totale in $\mathbb{Z}$!).

In effetti, la compatibilità fra le operazioni di somma e prodotto e il modo in cui la relazione " $\leq$ " si estende a $\mathbb{Z}$ è più "debole" di quella espressa dal teorema 2.8.11.

La relazione $\preceq$ definita in $\mathbb{Z}$ ponendo

$$[(a,b)] \preceq [(c,d)] \quad \text{se e soltanto se} \quad a+d \leq b+c$$

è ben posta (cioè dipende soltanto dalle classi di equivalenza $[(a,b)]$ e $[(c,d)]$ e non dai particolari rappresentanti a, b, c, d scelti per esse) ed è una relazione di ordine totale in $\mathbb{Z}$.

È immediato che

$$[(a,b)] \prec [(0,0)] \quad \text{se e soltanto se} \quad a < b$$

e che

$$[(0,0)] \prec [(a,b)] \quad \text{se e soltanto se} \quad b < a\,;$$

in particolare, i numeri interi della forma $[(0,b)]$ (con $b \neq 0$) precedono tutti $[(0,0)]$, e viceversa $[(0,0)]$ precede ogni numero intero della forma $[(a,0)]$: si pone

$$\mathbb{Z}^- := \{x \in \mathbb{Z} \,/\, x \prec [(0,0)]\} \quad \text{e} \quad \mathbb{Z}^+ := \{x \in \mathbb{Z} \,/\, [(0,0)] \prec x\}\,.$$

È altrettanto immediato verificare che

$$[(a,0)] \preceq [(c,0)] \quad \text{se e soltanto se} \quad a \leq c,$$

cosicché (se identifichiamo i numeri interi della forma $[(a,0)]$ con i numeri naturali) la relazione $\preceq$ "estende" la relazione $\leq$ già definita in $\mathbb{N}$.

Teorema 2.10.6

Siano $[(a,b)], [(c,d)], [(h,k)] \in \mathbb{Z}$. Si ha

(i) $\quad [(a,b)] \preceq [(c,d)] \quad$ se e soltanto se $\quad [(a,b)] + [(h,k)] \preceq [(c,d)] + [(h,k)]\,;$

(ii) $\quad$ se $[(0,1)] \prec [(h,k)]$,

$$[(a,b)] \preceq [(c,d)] \quad \text{se e soltanto se} \quad [(a,b)] \cdot [(h,k)] \preceq [(c,d)] \cdot [(h,k)]\,.$$

Dimostrazione — Poiché

$$[(a,b)] + [(h,k)] = [(a+h, b+k)] \quad \text{e} \quad [(c,d)] + [(h,k)] = [(c+h, d+k)],$$

la (i) si può esprimere scrivendo che

$$a+d \leq b+c \quad \text{se e soltanto se} \quad (a+h)+(d+k) \leq (b+k)+(c+h)$$

ma la seconda disuguaglianza, tenendo conto delle proprietà associativa e commutativa della somma in $\mathbb{N}$, equivale a

$$(a+d)+(h+k) \leq (b+c)+(h+k)$$

e quindi la (i) segue dalla (i) del teorema 2.8.11.

Ora supponiamo che sia $0 \prec [(h,k)]$; per quanto fin qui osservato, esiste $h_0 \in \mathbb{N}\backslash\{0\}$ tale che $[(h,k)] = [(h_0,0)]$. La (ii) esprime allora il fatto che

$$[(a,b)] \preceq [(c,d)] \quad \text{se e soltanto se} \quad [(a,b)] \cdot [(h_0,0)] \preceq [(c,d)] \cdot [(h_0,0)] .$$

D'altro lato, per definizione di prodotto in $\mathbb{Z}$ si ha che

$$[(a,b)] \cdot [(h_0,0)] = [(ah_0, bh_0)] \qquad \text{e} \qquad [(c,d)] \cdot [(h_0,0)] = [(ch_0, dh_0)]$$

cosicchè

$$[(a,b)] \cdot [(h_0,0)] \preceq [(c,d)] \cdot [(h_0,0)] \qquad \text{sse } (^2) \qquad ah_0 + dh_0 \leq bh_0 + ch_0$$

ossia se e solo se

$$(a+d)h_0 \leq (b+c)h_0$$

ma per la (ii) del teorema 2.8.11 quest'ultima disuguaglianza equivale appunto alla

$$a + d \leq b + c$$

cioè alla

$$[(a,b)] \preceq [(c,d)]$$

come si voleva dimostrare.

Esercizio 2.10.7

Siano $[(a,b)], [(c,d)], [(h,k)] \in \mathbb{Z}$ con $[(h,k)] \prec [(0,0)]$. Si dimostri che

$$[(a,b)] \preceq [(c,d)] \qquad \text{sse} \qquad [(c,d)] \cdot [(h,k)] \preceq [(a,b)] \cdot [(h,k)] .$$

e se ne deduca che, per ogni $z \in \mathbb{Z}$, si ha $0 \leq z^2$; inoltre, $z^2 = 0$ sse $z = 0$.

2.11 - I numeri razionali.

Si dice *insieme delle frazioni* e si indica con $\mathbb{F}$ il prodotto cartesiano $\mathbb{Z} \times \mathbb{Z}^+$. Definiamo in $\mathbb{F}$

$$(a,b) \sim (c,d) \quad \text{se e soltanto se} \quad ad = bc .$$

È facile verificare che la $\sim$ è una relazione di equivalenza in $\mathbb{F}$. L'insieme quoziente $\frac{\mathbb{F}}{\sim}$ si dice *insieme dei numeri razionali* e si indica con $\mathbb{Q}$.

[2] Useremo talvolta l'abbreviazione "sse" per sostituire la locuzione "se e solo se".

Osservazione 2.11.1

La funzione f: $\mathbb{Z}\to\mathbb{Q}$ che al numero intero z associa la classe di equivalenza $[(z,1)]$ è iniettiva, e si ha

$$[(z,1)] = \{(a,b) \in \mathbb{F} \ / \ a = bz\}\,.$$

Si definisce in $\mathbb{Q}$ un'operazione di somma come segue:

$$[(a,b)] + [(c,d)] \coloneqq [(ad+bc, bd)]\,.$$

Bisogna verificare che la definizione è ben posta, cioè non dipende dai rappresentanti scelti per le classi di equivalenza. Si trova poi che:

(i) $[(0,1)]$ è l'elemento neutro per la somma in $\mathbb{Q}$;

(ii) $[(-a,b)]$ è l'opposto di $[(a,b)]$;

(iii) la somma in $\mathbb{Q}$ è associativa e commutativa;

(iv) $[(a,1)] + [(b,1)] = [(a+b,1)]$.

Si definisce in $\mathbb{Q}$ un'operazione di prodotto come segue:

$$[(a,b)] \cdot [(c,d)] \coloneqq [(ac, bd)]\,.$$

Bisogna verificare che la definizione è ben posta, cioè non dipende dai rappresentanti scelti per le classi di equivalenza. Si trova poi che:

(i) $[(1,1)]$ è l'elemento neutro per il prodotto in $\mathbb{Q}$;

(ii) se $a \in \mathbb{Z}^+$, l'inverso di $[(a,b)]$ è $[(b,a)]$; se invece $a \in \mathbb{Z}^-$, l'inverso di $[(a,b)]$ è $[(-b,\,-a)]$;

(iii) il prodotto in $\mathbb{Q}$ è associativo, commutativo e distributivo rispetto alla somma.

(iv) $[(a,1)] \cdot [(b,1)] = [(ab,1)]$.

Osservazione 2.11.2

Anche in $\mathbb{Q}$ vale l'analogo del teorema 2.7.2. Infatti, se

$$[(a,b)] = [(0,1)] \quad (\text{cioè } a = 0) \quad \text{oppure} \quad [(c,d)] = [(0,1)] \quad (\text{cioè } c = 0)$$

si ha

$$[(a,b)] \cdot [(c,d)] = [(0,bd)] = [(0,1)]$$

e viceversa se

$$[(0,1)] = [(a,b)] \cdot [(c,d)] = [(ac,bd)]$$

deve essere $0 = ac$ e quindi, per l'osservazione 2.10.4,

$a = 0$ (ossia $[(a,b)] = [(0,b)] = [(0,1)]$) oppure $c = 0$ (ossia $[(c,d)] = [(0,d)] = [(0,1)]$) .

La relazione $\preceq$ definita in $\mathbb{Q}$ ponendo

$$[(a,b)] \preceq [(c,d)] \quad \text{se e soltanto se} \quad ad \leq bc$$

è ben posta (cioè dipende soltanto dalle classi di equivalenza $[(a,b)]$ e $[(c,d)]$ e non dai particolari rappresentanti a, b, c, d scelti per esse) ed è una relazione di ordine totale in $\mathbb{Q}$.

È immediato che

$$[(a,b)] \prec [(0,1)] \quad \text{se e soltanto se} \quad a < 0 \quad (\text{cioè sse } a \in \mathbb{Z}^-);$$

che

$$[(0,1)] \prec [(a,b)] \quad \text{se e soltanto se} \quad 0 < a \quad (\text{cioè sse } a \in \mathbb{Z}^+);$$

e che

$$[(a,b)] \prec [(1,1)] \quad \text{se e soltanto se} \quad a < b\,.$$

È altrettanto immediato verificare che

$$[(a,1)] \preceq [(c,1)] \quad \text{se e soltanto se} \quad a \leq c,$$

cosicché (se identifichiamo i numeri razionali della forma $[(a,1)]$ con i numeri interi) la relazione $\preceq$ "estende" la relazione $\leq$ già definita in $\mathbb{Z}$.

Teorema 2.11.3

Siano $[(a,b)], [(c,d)], [(h,k)] \in \mathbb{Q}$. Si ha

(i) $[(a,b)] \preceq [(c,d)]$ se e soltanto se $[(a,b)] + [(h,k)] \preceq [(c,d)] + [(h,k)]$;

(ii) se $[(0,1)] \prec [(h,k)]$,

$[(a,b)] \preceq [(c,d)]$ se e soltanto se $[(a,b)] \cdot [(h,k)] \preceq [(c,d)] \cdot [(h,k)]$.

Dimostrazione — Proviamo intanto la (i).

Poiché

$$[(a,b)]+[(h,k)]=[(ak+bh,bk)] \quad \text{e} \quad [(c,d)]+[(h,k)]=[(ck+dh,dk)],$$

la disuguaglianza

$$[(a,b)]+[(h,k)] \preceq [(c,d)]+[(h,k)]$$

equivale al fatto che si abbia

$$(ak+bh)dk \leq bk(ck+dh)$$

ossia

$$adk^2+bdhk \leq bck^2+bdhk$$

che a sua volta (per la (i) del teorema 2.10.6) equivale al fatto che si abbia

$$adk^2 \leq bck^2$$

ossia (applicando due volte la (ii) del teorema 2.10.6, poiché $k>0$ per definizione di $\mathbb{F}$)

$ad \leq bc$, cioè $[(a,b)] \preceq [(c,d)]$ come si voleva dimostrare.

Proviamo infine la (ii), ricordando che la condizione $0 \prec [(h,k)]$ equivale al fatto che sia $0<h$ in $\mathbb{Z}$. Poiché

$$[(a,b)]\cdot[(h,k)]=[(ah,bk)] \quad \text{e} \quad [(c,d)]\cdot[(h,k)]=[(ch,dk)],$$

la disuguaglianza

$$[(a,b)]\cdot[(h,k)] \preceq [(c,d)]\cdot[(h,k)]$$

equivale al fatto che si abbia

$$(ah)(dk) \leq (bk)(ch)$$

ossia

$$(ad)(hk) \leq (bc)(hk)$$

ossia (applicando due volte la (ii) del teorema 2.10.6, poiché $k>0$ per definizione di $\mathbb{F}$ e $h>0$ per ipotesi)

$ad \leq bc$, cioè $[(a,b)] \preceq [(c,d)]$ come si voleva dimostrare.

Esercizio 2.11.4

Siano $[(a,b)],[(c,d)],[(h,k)] \in \mathbb{Q}$ con $[(h,k)] \prec [(0,1)]$. Si dimostri che

$$[(a,b)] \preceq [(c,d)] \quad \text{se e soltanto se} \quad [(c,d)]\cdot[(h,k)] \preceq [(a,b)]\cdot[(h,k)].$$

e se ne deduca che, per ogni $z \in \mathbb{Q}$, si ha $0 \leq z^2$; inoltre, $z^2=0$ se e soltanto se $z=0$.

2.12 - Verso i numeri reali: l'incommensurabilità fra lato e diagonale del quadrato.

Non rientra negli scopi di questo insegnamento proseguire nella costruzione degli insiemi numerici (quella di $\mathbb{R}$, con significative possibilità di scelta fra il metodo delle sezioni di Dedekind, il metodo delle successioni di Cauchy e il prodiano tentativo di sintesi fra i due costituito dalle "scatole cinesi" o meno informalmente "intervalli annidati"; e poi la costruzione della chiusura algebrica di $\mathbb{R}$, cioè $\mathbb{C}$). Come è noto, il principale motivo che giustifica il passaggio da $\mathbb{Q}$ a $\mathbb{R}$ è l'inadeguatezza dei numeri razionali ad esprimere le misure dei segmenti, cioè l'esistenza nella geometria euclidea di coppie di segmenti incommensurabili. Diamo qui una dimostrazione puramente geometrica del fatto che in qualsiasi quadrato lato e diagonale sono incommensurabili: è probabilmente lo stesso ragionamento dei primi geometri greci che fecero questa scoperta.

Supponiamo per assurdo che esista un quadrato $\mathcal{Q}$ nel quale il lato e la diagonale hanno un sottomultiplo comune σ; dimostriamo che si può trovare un altro quadrato $\mathcal{Q}'$ tale che

(i) il lato di $\mathcal{Q}'$ è minore della metà del lato di $\mathcal{Q}$;

(ii) lo stesso segmento σ che era sottomultiplo comune del lato e della diagonale di $\mathcal{Q}$ è sottomultiplo comune anche del lato e della diagonale di $\mathcal{Q}'$.

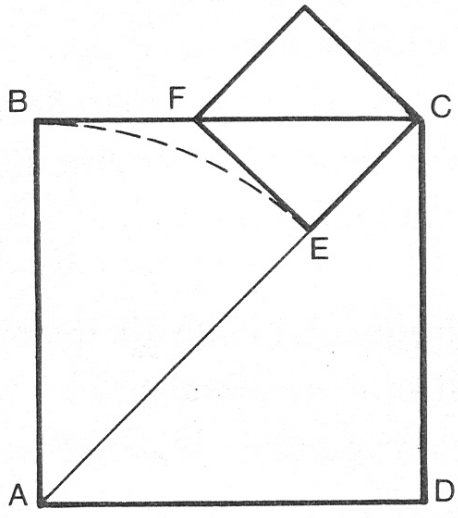
Allora, iterando il procedimento, dopo un numero finito di passi si arriverebbe a trovare un quadrato $\mathcal{Q}^*$ tale che

(a) il lato di $\mathcal{Q}^*$ è minore di σ;

(b) σ è sottomultiplo comune del lato e della diagonale di $\mathcal{Q}^*$.

Poiché ciò è impossibile, si deve concludere che il quadrato $\mathcal{Q}$ da cui siamo partiti non può esistere.

Sia allora ABCD il quadrato $\mathcal{Q}$, e sia E il punto in cui la circonferenza di centro A e raggio uguale al lato di $\mathcal{Q}$ incontra la diagonale AC. Sia F il punto in cui la retta per E ortogonale alla diagonale AC incontra il lato BC.



Il segmento AE è congruente al lato ℓ di $\mathcal{Q}$, dunque σ è sottomultiplo di AE; poiché per ipotesi σ è sottomultiplo anche della diagonale AC, σ è sottomultiplo di EC.

Per costruzione, FE è ortogonale alla retta AE e dunque è tangente in E alla circonferenza $\mathcal{C}$ di centro A e raggio AE; analogamente, poiché BF è ortogonale alla retta AB (essendo AB e BC lati consecutivi del quadrato $\mathcal{Q}$), BF è tangente in B alla stessa circonferenza $\mathcal{C}$. In particolare, BF e FE sono congruenti perché segmenti di tangente alla circonferenza $\mathcal{C}$ tracciati dallo stesso punto F.

Adesso consideriamo il triangolo FEC. Esso è retto in E per costruzione; inoltre l'angolo in C è la metà di un angolo retto (perché il triangolo ABC è rettangolo con ipotenusa AC e isoscele perché AB e BC sono lati del quadrato $\mathcal{Q}$), quindi anche l'angolo in F è la metà di un angolo retto. Dunque il triangolo FEC è un triangolo rettangolo isoscele, ed è la metà di un quadrato $\mathcal{Q}$' di lato EC e diagonale FC.

Abbiamo già osservato che σ è sottomultiplo di EC; ma, poiché il triangolo FEC è isoscele con base FC e quindi EF ed EC sono congruenti, σ è sottomultiplo anche di EF (che a sua volta abbiamo visto essere congruente a BF). Poiché σ è sottomultiplo sia di BC (lato di $\mathcal{Q}$) che di BF, σ è sottomultiplo di FC. Dunque σ è sottomultiplo sia del lato che della diagonale del quadrato $\mathcal{Q}$'.

Resta da dimostrare che il lato EC di $\mathcal{Q}$' è meno della metà del lato BC di $\mathcal{Q}$. Ma se fosse $\boldsymbol{d}(\mathrm{E},\mathrm{C}) \geq \frac{1}{2}\boldsymbol{d}(\mathrm{B},\mathrm{C})$ si avrebbe l'assurdo che

$$\boldsymbol{d}(\mathrm{B},\mathrm{C}) = \boldsymbol{d}(\mathrm{B},\mathrm{F}) + \boldsymbol{d}(\mathrm{F},\mathrm{C}) > \boldsymbol{d}(\mathrm{E},\mathrm{C}) + \boldsymbol{d}(\mathrm{E},\mathrm{C}) \geq \tfrac{1}{2}\boldsymbol{d}(\mathrm{B},\mathrm{C}) + \tfrac{1}{2}\boldsymbol{d}(\mathrm{B},\mathrm{C}) = \boldsymbol{d}(\mathrm{B},\mathrm{C})$$

essendo $\boldsymbol{d}(\mathrm{B},\mathrm{F}) = \boldsymbol{d}(\mathrm{E},\mathrm{C})$ come già visto, ed essendo $\boldsymbol{d}(\mathrm{F},\mathrm{C}) > \boldsymbol{d}(\mathrm{E},\mathrm{C})$ perché nel triangolo EFC l'angolo opposto al lato FC (cioè l'angolo retto) è maggiore dell'angolo opposto al lato EC.

2.13 - L'irrazionalità di π.

Concludiamo questo capitolo con una dimostrazione dell'irrazionalità di π ([3]).

Supponiamo che, per assurdo, esistano dei numeri interi $p, q \in \mathbb{Z}^+$ tali che $\pi = \frac{p}{q}$. In funzione del parametro $k \in \mathbb{Z}^+$, definiamo come segue le funzioni $f_k : \mathbb{R} \to \mathbb{R}$ e $g_k : \mathbb{R} \to \mathbb{R}$:

$$f_k(x) := \frac{x^k \cdot (p - qx)^k}{k!}$$

(per cui, ad esempio: $f_1(x) := px - qx^2$; $f_2(x) := \frac{1}{2}x^2(p - qx)^2$) e

$$g_k(x) := f_k(x) - f_k^{(2)}(x) + f_k^{(4)}(x) - \ldots + (-1)^k f_k^{(2k)}(x) .$$

[3] Che π sia non solo irrazionale ma addirittura trascendente è stato provato nel 1882 da Carl Louis Ferdinand von Lindemann con una linea di ragionamento piuttosto complicata che è stata poi generalizzata (in modo da fornire un'ampia classe di risultati sulla trascendenza di certi numeri) ma non molto semplificata.

Poiché le $f_k(x)$ sono funzioni polinomiali di grado $2k$, è

(1) $$f_k^{(n)}(x) = 0 \quad \text{per} \quad n > 2k+1\,.$$

Si ha poi

$$f_k'(x) = \frac{kx^{k-1}\cdot(p-qx)^k + kx^k\cdot(p-qx)^{k-1}(-q)}{k!} = (p-2qx)\frac{x^{k-1}\cdot(p-qx)^{k-1}}{(k-1)!} = (p-2qx)f_{k-1}(x)$$

(e in particolare: $f_1'(x) = p - 2qx\,,$ da cui $f_1^{(2)}(x) = -2q$).

Induttivamente se ne ricava che:

$f_k^{(n)}(0)$ e $f_k^{(n)}(\pi)$ sono numeri interi per ogni scelta di $n \in \mathbb{N}$ e di $k \in \mathbb{Z}^+$

e quindi che

(2) $g_k(0)$ e $g_k(\pi)$ sono numeri interi per ogni $k \in \mathbb{Z}^+$.

Adesso calcoliamo le prime due derivate delle $g_k(x)$. Si ha

$$g_k'(x) = f_k'(x) - f_k^{(3)}(x) + f_k^{(5)}(x) - \ldots + (-1)^k f_k^{(2k+1)}(x)\,;$$

e

$$g_k^{(2)}(x) = f_k^{(2)}(x) - f_k^{(4)}(x) + f_k^{(6)}(x) - \ldots + (-1)^k f_k^{(2k+2)}(x)\,;$$

ma in effetti, ricordando la (1),

$$g_k^{(2)}(x) = f_k^{(2)}(x) - f_k^{(4)}(x) + f_k^{(6)}(x) - \ldots + (-1)^{k-1} f_k^{(2k)}(x)\,.$$

Allora

$$g_k(x) + g_k^{(2)}(x) = f_k(x)$$

e quindi, posto $H_k(x) := g_k'(x)\mathbf{sin}(x) - g_k(x)\mathbf{cos}(x)\,,$ si trova che

$$H_k'(x) = g_k^{(2)}(x)\mathbf{sin}(x) + g_k'(x)\mathbf{cos}(x) - g_k'(x)\mathbf{cos}(x) + g_k(x)\mathbf{sin}(x) =$$
$$= \big(g_k^{(2)}(x) + g_k(x)\big)\mathbf{sin}(x) = f_k(x)\mathbf{sin}(x)$$

da cui

$$\int_0^\pi f_k(x)\mathbf{sin}(x)\,\mathrm{d}x = \big[H_k(x)\big]_0^\pi = g_k(\pi) + g_k(0)\,.$$

Per la (2), $g_k(\pi)$ e $g_k(0)$ sono numeri interi. D'altro lato, per ogni $x \in (0,\pi)$ si ha

$$f_k(x)\mathbf{sin}(x) > 0$$

e quindi anche l'integrale fra 0 e π deve essere maggiore di zero; trattandosi di un numero intero, possiamo concludere che

$$\int_0^\pi f_k(x)\mathbf{sin}(x)\,\mathrm{d}x \geq 1\,.$$

Ma ora osserviamo che

$$0 < f_k(x)\mathbf{sin}(x) < \tfrac{\pi^k \cdot p^k}{k!}$$

e quindi

$$\int_0^\pi f_k(x)\mathbf{sin}(x)\,\mathrm{d}x < \pi\,\tfrac{\pi^k \cdot p^k}{k!}$$

assurdo perché per ogni $\alpha \in \mathbb{R}^+$ si ha

$$\lim_{k\to+\infty} \frac{\alpha^k}{k!} = 0$$

e quindi $\pi\,\frac{\pi^k \cdot p^k}{k!}$ può essere reso piccolo a piacere scegliendo k sufficientemente grande.

Esercizio 2.11.4

Col risultato di Lindemann fu stabilito, dopo qualche millennio dal loro enunciato, che i classici problemi della rettificazione della circonferenza e della quadratura del cerchio non sono risolubili con riga e compasso. Per arrivare a tale conclusione non è sufficiente, come vedremo, provare che π è irrazionale: dovremmo dimostrare che non esiste una catena di ampliamenti di campi, ciascuno di grado due, da $\mathbb{Q}$ a un campo $\mathbb{F}$ tale che $\pi \in \mathbb{F}$; risultato, questo, che in teoria è molto più debole della trascendenza di π ma che nessuno è finora riuscito a stabilire con mezzi elementari.

3.- L'ASSIOMA DELLA SCELTA

The Axiom of Choice is obviously true,
the Well-ordering theorem is obviously false,
and who can tell about Zorn's lemma?
Jerry L. Bona

– Che cos'è marroncino, pelosetto,
corre verso il mare
ed è equivalente all'Assioma della Scelta?
– Un lemming di Zorn
citata da Bruno Winckler

3.1 - L'assioma della scelta.

$(\mathcal{A}_c)$

Per ogni insieme A i cui elementi sono a due a due disgiunti, esiste un insieme B tale che ogni elemento di B appartiene a un elemento di A, e in ogni elemento non vuoto di A c'è uno e un solo elemento che appartiene a B.

Osservazione 3.1.1

Vale la pena di enunciare esplicitamente l'assioma della scelta usando soltanto le parole primitive:

Sia A un insieme tale che, comunque presi $Y, Z \in A$, se esiste $X \in Y$ tale che $X \in Z$ allora $Y = Z$; esiste un insieme B tale che: per ogni $X \in B$ esiste $Y \in A$ tale che $X \in Y$, e inoltre per ogni $X \in A$ se esiste $Y \in X$ allora esiste $Z \in X$ tale che: $Z \in B$, e per ogni $T \in X$ se $T \in B$ allora $T = Z$.

Osservazione 3.1.2

L'assioma della scelta non appartiene alla famiglia degli assiomi "fondamentali" enunciati da Zermelo e Fraenkel. Molta matematica può essere sviluppata anche senza tale assioma: ad esempio (come si è visto nel capitolo precedente) tutta l'aritmetica in $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ (e in $\mathbb{R}$, e in $\mathbb{C}$). Col teorema 3.2.2, nella sez. 3.9 e nel capitolo 4 vedremo diversi risultati per i quali risulta irrinunciabile l'uso dell'assioma della scelta in una delle tante forme equivalenti.

Sia X un insieme. Si dice *funzione di scelta su* X una funzione $\mathbf{f}_s : X\backslash\{\emptyset\} \to \cup X$ tale che

$$\mathbf{f}_s(Y) \in Y \quad \text{per ogni } Y \in X\backslash\{\emptyset\} .$$

($\mathcal{A}_c$ – enunciato (2))

Per ogni insieme A, esiste (almeno) una funzione di scelta su $\wp(A)$.

Teorema 3.1.3

($\mathcal{A}_c$ – enunciato (2)) è conseguenza di **($\mathcal{A}_c$)**.

Dimostrazione – Sia A un insieme, e costruiamo una funzione di scelta su $\wp(A)$. Se $\wp(A) = \{\emptyset\}$ (e quindi in particolare se $A = \emptyset$) la funzione vuota è una funzione di scelta su $\wp(A)$, quindi possiamo supporre ($A \neq \emptyset$ e) $\wp(A) \neq \{\emptyset\}$.

Una funzione di scelta su $\wp(A)$ è un insieme di coppie ordinate (X, x) con $x \in X$ al variare di X in $\wp(A)$. Per ogni sottoinsieme X di A, sia

$$\overline{X} := \{(X, x) \in \wp(A) \times A \,/\, x \in X\} .$$

Ogni $\overline{X}$ è un sottoinsieme del prodotto cartesiano $\wp(A) \times A$, quindi per l'assioma di separazione esiste

$$\mathfrak{X} := \{\overline{X} \in \wp(\wp(A) \times A) \,/\, \text{esiste } X \subset A \text{ tale che } \overline{X} = \{(X, x) \in \wp(A) \times A \,/\, x \in X\}\} .$$

Se dimostro che gli elementi di $\mathfrak{X}$ sono a due a due disgiunti, posso applicare l'enunciato **($\mathcal{A}_c$)** dell'assioma della scelta per estrarre una coppia ordinata (X, x) da ogni $\overline{X}$ e ottenere così una funzione di scelta su $\wp(A)$.

In effetti, sia $(W, w) \in \overline{X} \cap \overline{Y}$; allora $W = X$ e $W = Y$, quindi $X = Y$ e pertanto $\overline{X} = \overline{Y}$, come si voleva.

Teorema 3.1.4

$(\mathcal{A}_c$ – **enunciato (2)**$)$ è equivalente ad $(\mathcal{A}_c)$.

Dimostrazione – Per il teorema 3.1.3, basterà provare che $(\mathcal{A}_c)$ è conseguenza di $(\mathcal{A}_c$ – **enunciato (2)**$)$.

Sia A un insieme i cui elementi sono a due a due disgiunti, e sia $A_0 := \cup A$; allora

$$A \subset \wp(A_0).$$

Sia **f** la restrizione ad A di una funzione di scelta su $\wp(A_0)$ (che esiste per $(\mathcal{A}_c$ – **enunciato (2)**$)$). L'immagine B di **f** verifica le condizioni di $(\mathcal{A}_c)$: ogni elemento di B appartiene a un elemento di A; e in ogni elemento non vuoto di A c'è un elemento di B (e uno solo, perché se $x, y \in B$ essi provengono mediante **f** da due elementi di A che per ipotesi sono disgiunti e quindi non possono appartenere a uno stesso elemento di A)

$(\mathcal{A}_c$ – **enunciato (3)**$)$

Per ogni famiglia di insiemi tutti non vuoti $\{X_a\}_{a\in A}$ indiciata da A, esiste (almeno) una funzione $\hat{\mathbf{f}}_s : A \to \bigcup_{a\in A} X_a$ tale che $\hat{\mathbf{f}}_s(a) \in X_a$ per ogni $a \in A$; cioè (cfr. sez. 1.13) il prodotto cartesiano di una famiglia di insiemi tutti non vuoti non è vuoto.

Teorema 3.1.5

$(\mathcal{A}_c$ – **enunciato (3)**$)$ è equivalente ad $(\mathcal{A}_c$ – **enunciato (2)**$)$.

Dimostrazione – Supponiamo che valga $(\mathcal{A}_c$ – **enunciato (2)**$)$.

Sia $\{X_a\}_{a\in A}$ una famiglia di insiemi indiciata dall'insieme A, attraverso la funzione **f** (cioè sia $\mathbf{f}(a) = X_a$ per ogni $a \in A$). Detta $\mathbf{f}_s$ una funzione di scelta sull'insieme $\wp\left(\bigcup_{a\in A} X_a\right)$, la funzione composta

$$\hat{\mathbf{f}}_s := \mathbf{f}_s \circ \mathbf{f}$$

è una funzione $\hat{\mathbf{f}}_s : A \to \bigcup_{a\in A} X_a$ tale che $\hat{\mathbf{f}}_s(a) \in X_a$ per ogni $a \in A$.

Ora supponiamo che valga $(\mathcal{A}_c$ – **enunciato (3)**$)$.

Gli elementi non vuoti di $\wp(A)$ si possono pensare come una famiglia di insiemi indiciata da $\wp(A)\backslash\{\emptyset\}$ attraverso la funzione identità $\mathbf{id}_{\wp(A)\backslash\{\emptyset\}}$. La funzione $\hat{\mathbf{f}}_s$ la cui esistenza è garantita da $(\mathcal{A}_c$ – **enunciato (3)**$)$ è allora una funzione di scelta su $\wp(A)$.

Scopo di questo capitolo è provare l'equivalenza fra l'assioma della scelta, il "lemma di Zorn" e il "principio del buon ordine". Nella sez. 3.2 dimostreremo il "lemma di Zorn" utilizzando l'assioma della scelta; nella sez. 3.3 dimostreremo il "principio del buon ordine" utilizzando il "lemma di Zorn"; e nella sez. 3.4 osserveremo che l'assioma della scelta si può dedurre dal "principio del buon ordine".

3.2 - Il "lemma di Zorn".

Sia (A, $\leq$) un insieme ordinato. Ricordiamo alcune definizioni.

Si dice *catena* di A un sottoinsieme di A totalmente ordinato.

Se B $\subset$ A, si dice *limitazione superiore* per B in A (o anche *maggiorante* di B in A) un $s \in$ A tale che $b \leq s$ per ogni $b \in$ B; si dice *massimo* di B una limitazione superiore per B in B: si dimostra facilmente che il massimo di B, se esiste, è unico. Analogamente, si dice *limitazione inferiore* per B in A (o anche *minorante* di B in A) un $i \in$ A tale che $i \leq b$ per ogni $b \in$ B; si dice *minimo* di B una limitazione inferiore per B in B: si dimostra facilmente che il minimo di B, se esiste, è unico.

Un elemento m_0 di B di dice *massimale* (in B) se per ogni $b \in$ B dalla relazione $m_0 \leq b$ segue che $b = m_0$. Se B ha massimo, questo è anche l'unico elemento massimale di B; se però B non ha massimo, in B ci può essere un numero qualsiasi di elementi massimali, da zero a infiniti.

Teorema 3.2.1 ("lemma di Zorn")

Sia (A, $\leq$) un insieme ordinato. Se in A ogni catena è superiormente limitata, allora in A esiste almeno un elemento massimale.

Dimostrazione – Sia ($\mathcal{C}$, $\subset$) l'insieme di tutte le catene di A (compresa la catena vuota $\emptyset$) ordinate rispetto all'inclusione. Ci basterà provare che in $\mathcal{C}$ c'è un elemento massimale $\overline{\mathrm{C}}$: infatti per ipotesi $\overline{\mathrm{C}}$ è superiormente limitata da un elemento $\overline{a}$ di A; si vede subito che $\overline{a}$ deve essere massimale in (A, $\leq$). Sia infatti $b \in$ A tale che $\overline{a} \leq b$; se fosse $\overline{a} < b$, l'insieme $\overline{\mathrm{C}} \cup \{b\}$ sarebbe ancora una catena (perché $a \leq \overline{a} < b$ per ogni $a \in \overline{\mathrm{C}}$) e conterrebbe propriamente $\overline{\mathrm{C}}$, assurdo per la supposta massimalità di $\overline{\mathrm{C}}$.

Possiamo in sostanza riformulare il nostro asserto (originariamente riferito all'insieme A con una generica relazione di ordine $\leq$) riferendolo all'insieme ($\mathcal{C}$, $\subset$): se proviamo che in $\mathcal{C}$ c'è un elemento massimale (rispetto all'inclusione), il teorema è dimostrato.

L'insieme ordinato $(\mathcal{C},\ \subset)$ è comodo da trattare non solo perché l'inclusione ci è familiare ma perché (come è immediato verificare) valgono in esso le seguenti due condizioni:

(i) $\emptyset \in \mathcal{C}$;

(ii) se $\mathcal{K}$ è una catena di $(\mathcal{C},\ \subset)$ (ebbene sì: $\mathcal{K}$ è dunque una catena di catene, ordinate rispetto all'inclusione), $\cup \mathcal{K} \in \mathcal{C}$.

Di fatto, nel seguito di questa dimostrazione non ci interesserà più la particolare natura dei sottoinsiemi di A che appartengono a $\mathcal{C}$ (cioè il fatto che sono catene), ma utilizzeremo soltanto le condizioni (i) e (ii).

Vogliamo dunque dimostrare che in $(\mathcal{C},\ \subset)$ c'è almeno un elemento massimale.

Per ogni $\mathrm{C} \in \mathcal{C}$, poniamo

$$\mathrm{C}^* := \{x \in \mathrm{A}\backslash\mathrm{C} \ / \ \mathrm{C} \cup \{x\} \in \mathcal{C}\}$$

(cioè: C^* è l'insieme di tutti gli elementi di A non appartenenti a C che, se aggiunti a C, danno luogo ancora a un insieme appartenente a $\mathcal{C}$).

Sia $\mathbf{f_s}$ una funzione di scelta su $\wp(\mathrm{A})$, e sia $\mathbf{g}$ la funzione $\mathcal{C} \to \mathcal{C}$ così definita:

$$\mathbf{g}(\mathrm{C}) := \begin{cases} \mathrm{C} & \text{se } \mathrm{C}^* = \emptyset \\ \mathrm{C} \cup \{\mathbf{f_s}(\mathrm{C}^*)\} & \text{se } \mathrm{C}^* \neq \emptyset \end{cases}$$

È chiaro che C è massimale in $(\mathcal{C},\ \subset)$ se e soltanto se $\mathbf{g}(\mathrm{C}) = \mathrm{C}$, ossia (poiché certamente $\mathrm{C} \subset \mathbf{g}(\mathrm{C})$ per definizione di $\mathbf{g}$) se e soltanto se $\mathbf{g}(\mathrm{C}) \subset \mathrm{C}$. Dobbiamo dunque dimostrare che esiste $\mathrm{C} \in \mathcal{C}$ tale che $\mathbf{g}(\mathrm{C}) \subset \mathrm{C}$.

Introduciamo una definizione "tecnica". Un sottoinsieme $\mathcal{T}$ di $\mathcal{C}$ si dice *una torre* se

(a) $\emptyset \in \mathcal{T}$;

(b) se $\mathcal{K}$ è una catena di $(\mathcal{T},\ \subset)$, $\cup \mathcal{K} \in \mathcal{T}$.

(c) se $\mathrm{C} \in \mathcal{T}$, allora $\mathbf{g}(\mathrm{C}) \in \mathcal{T}$;

È immediato osservare che

- esistono torri (infatti $\mathcal{C}$ è una torre);
- l'intersezione di torri è una torre.

Dunque l'intersezione $\mathcal{T}_0$ di tutte le torri è una torre, contenuta in ogni torre. Vogliamo dimostrare che $\mathcal{T}_0$ è anche una catena rispetto all'inclusione. Posto $\mathrm{C} := \cup \mathcal{T}_0$, ne seguirà che $\mathrm{C} \in \mathcal{T}_0$ (per la (b)) e quindi anche $\mathbf{g}(\mathrm{C}) \in \mathcal{T}_0$ (per la (c)); in particolare si avrà che $\mathbf{g}(\mathrm{C}) \subset \cup \mathcal{T}_0 = \mathrm{C}$ come si voleva dimostrare.

Diciamo che un elemento X di $\mathcal{T}_0$ è *confrontabile* (tout court) se è confrontabile con ogni elemento di $\mathcal{T}_0$, cioè se per ogni $Y \in \mathcal{T}_0$ si ha $X \subset Y$ oppure $Y \subset X$. Noi vogliamo dimostrare che $\mathcal{T}_0$ è una catena, cioè che ogni elemento di $\mathcal{T}_0$ è confrontabile. Faremo vedere che gli elementi confrontabili di $\mathcal{T}_0$ costituiscono una torre: poiché $\mathcal{T}_0$ è contenuta in ogni torre, ne seguirà che l'insieme degli elementi confrontabili di $\mathcal{T}_0$ coincide con $\mathcal{T}_0$, come si voleva.

(a) $\emptyset$ è confrontabile; questo è ovvio, perché $\emptyset \subset X$ per ogni insieme X;

(b) se $\mathcal{K}$ è una catena di elementi confrontabili, $\cup\mathcal{K}$ è confrontabile. Sia infatti $Y \in \mathcal{T}_0$; se esiste $X \in \mathcal{K}$ tale che $Y \subset X$, certamente $Y \subset \cup\mathcal{K}$; altrimenti è $X \subset Y$ per ogni $X \in \mathcal{K}$, e quindi $\cup\mathcal{K} \subset Y$.

Resta da dimostrare che se un elemento $\overline{C}$ è confrontabile anche $\mathbf{g}(\overline{C})$ è confrontabile. Poniamo

$$\mathcal{U}_{\overline{C}} := \{X \in \mathcal{T}_0 \,/\, X \subset \overline{C} \text{ oppure } \mathbf{g}(\overline{C}) \subset X\}.$$

Basterà provare che $\mathcal{U}_{\overline{C}}$ è una torre: infatti per definizione $\mathcal{U}_{\overline{C}} \subset \mathcal{T}_0$, e poiché $\mathcal{T}_0$ è la minima torre ne seguirà che $\mathcal{U}_{\overline{C}} = \mathcal{T}_0$; sia allora $X \in \mathcal{T}_0$: deve essere $X \subset \overline{C}$ ($\subset \mathbf{g}(\overline{C})$ per definizione di **g**) oppure $\mathbf{g}(\overline{C}) \subset X$, e in ogni caso $\mathbf{g}(\overline{C})$ è confrontabile con X.

Proviamo allora, infine, che $\mathcal{U}_{\overline{C}}$ è una torre. È immediato che $\emptyset \in \mathcal{U}_{\overline{C}}$. Se $\mathcal{K}$ è una catena di elementi di $\mathcal{U}_{\overline{C}}$, distinguiamo due casi: se esiste $K \in \mathcal{K}$ tale che $\mathbf{g}(\overline{C}) \subset K$, certamente $\mathbf{g}(\overline{C}) \subset \cup\mathcal{K}$; in caso contrario, $K \subset \overline{C}$ per ogni $K \in \mathcal{K}$, e quindi $\cup\mathcal{K} \subset \overline{C}$. In ogni caso, $\cup\mathcal{K} \in \mathcal{U}_{\overline{C}}$.

Sia infine $X \in \mathcal{U}_{\overline{C}}$, e proviamo che $\mathbf{g}(X) \in \mathcal{U}_{\overline{C}}$. Distinguiamo tre casi:

$$\mathbf{g}(\overline{C}) \subset X; \qquad X = \overline{C}; \qquad X \subsetneq \overline{C}.$$

Se $\mathbf{g}(\overline{C}) \subset X$($\subset \mathbf{g}(X)$ per definizione di **g**), è $\mathbf{g}(\overline{C}) \subset \mathbf{g}(X)$ e quindi $\mathbf{g}(X) \in \mathcal{U}_{\overline{C}}$.

Se $X = \overline{C}$, $\mathbf{g}(X) = \mathbf{g}(\overline{C})$ e quindi in particolare $\mathbf{g}(\overline{C}) \subset \mathbf{g}(X)$ cosicché ancora $\mathbf{g}(X) \in \mathcal{U}_{\overline{C}}$.

Infine, se X è un sottoinsieme proprio di $\overline{C}$ deve essere $\mathbf{g}(X) \subset \overline{C}$ (e quindi $\mathbf{g}(X) \in \mathcal{U}_{\overline{C}}$); infatti in caso contrario, poiché $\overline{C}$ è confrontabile, $\overline{C}$ sarebbe un sottoinsieme proprio di $\mathbf{g}(X)$ e quindi X sarebbe un sottoinsieme proprio di un sottoinsieme proprio di $\mathbf{g}(X)$: assurdo perché alla differenza $\mathbf{g}(X)\backslash X$ appartiene al massimo un elemento (per definizione di **g**).

Il teorema è così completamente dimostrato.

Come esempio di applicazione del lemma di Zorn dimostriamo che ogni spazio vettoriale ha (almeno) una base. Per un altro esempio, si veda il teorema 4.4.3 .

Teorema 3.2.2

Sia V uno spazio vettoriale. In V esiste almeno una base.

Dimostrazione – Siano V uno spazio vettoriale e X un sottoinsieme di V. Ricordiamo che X si dice *libero* se comunque presi in X un numero finito di elementi l'unica loro combinazione lineare che dia il vettore nullo è quella con i coefficienti tutti uguali a zero; inoltre si dice che X *genera* V se ogni elemento di V è combinazione lineare di elementi di X. Una *base* per V è un sottoinsieme libero di V che genera V.

Sia $$\mathcal{L} \coloneqq \{X \in \wp(V) \,/\, X \text{ è libero}\}$$

l'insieme di tutti i sottoinsiemi liberi di V. Se ordiniamo $\mathcal{L}$ rispetto all'inclusione, ogni catena di $\mathcal{L}$ è superiormente limitata (se $\mathcal{C}$ è una catena di $\mathcal{L}$, $\cup\mathcal{C}$ è una limitazione superiore per $\mathcal{C}$). Dunque, per il lemma di Zorn, in $\mathcal{L}$ esistono elementi massimali.

Sia X_0 un sottoinsieme libero massimale di V e dimostriamo che X_0 genera V (e quindi è una base per V), cioè che ogni $y \in V$ è combinazione lineare di elementi di X_0. Sia dunque $y \in V$: se $y \in X_0$, non c'è niente da dimostrare; se $y \notin X_0$, $X_0 \cup \{y\}$ non è libero (per la massimalità di X_0). Dunque esistono $x_1, x_2, \dots x_n \in X_0$ e $\lambda_0, \lambda_1, \lambda_2, \dots \lambda_n \in \mathbb{R}$ tali che

$$\lambda_0 y + \lambda_1 x_1 + \lambda_2 x_2 + \dots + \lambda_n x_n = 0_{\mathbf{V}} \quad \text{con i } \lambda_i \text{ non tutti nulli.}$$

Se fosse $\lambda_0 = 0$, avremmo una combinazione lineare di elementi di X_0 che dà il vettore nullo senza che i coefficienti siano tutti nulli, assurdo perché X_0 è libero; dunque $\lambda_0 \neq 0$ e si è trovato che

$$y = -\tfrac{\lambda_1}{\lambda_0} x_1 - \tfrac{\lambda_2}{\lambda_0} x_2 + \dots - \tfrac{\lambda_n}{\lambda_0} x_n$$

cioè y è combinazione lineare di elementi di X_0, come si voleva dimostrare.

Esercizio 3.2.3

Si dimostri che in ogni insieme ordinato ci sono catene massimali (rispetto all'inclusione).

Suggerimento – Sia $(\mathcal{C}, \subset)$ l'insieme (ordinato rispetto all'inclusione) di tutte le catene dell'insieme ordinato che si sta considerando. Si dimostri che ogni catena di $(\mathcal{C}, \subset)$ è superiormente limitata rispetto all'inclusione, e si applichi il lemma di Zorn.

3.3 - Il "principio del buon ordine".

Sia A un insieme, e sia $\preceq$ una relazione di ordine in A. Si dice che $\preceq$ è un *buon ordine* per A, oppure (equivalentemente) che $(A, \preceq)$ è un *insieme bene ordinato* se ogni sottoinsieme non vuoto di A ha minimo (rispetto alla restrizione ad esso di $\preceq$).

Osservazione 3.3.1

Ogni buon ordine è una relazione di ordine totale.

Dimostrazione – Sia A un insieme, e sia $\preceq$ un buon ordine per A. Siano $x, y \in$ A. Per ipotesi, $\{x, y\}$ ha minimo: se tale minimo è x, si ha che $x \preceq y$; se tale minimo è y, si ha che $y \preceq x$. In ogni caso x, y sono confrontabili e dunque $\preceq$ è una relazione di ordine totale in A.

Esempio 3.3.2

La relazione di ordine $\leq$ in $\mathbb{N}$ definita nella sez. 2.8 è un buon ordine per $\mathbb{N}$ (lo si è provato col teorema 2.9.2).

Osservazione 3.3.3

L'usuale relazione di ordine $\leq$ definita in $\mathbb{Q}$ non è un buon ordine per $\mathbb{Q}$ (l'insieme dei numeri razionali rappresentati dalle frazioni della forma $\frac{1}{n}$ con $n \in \mathbb{N}$ non ha minimo; e del resto lo stesso insieme $\mathbb{Q}$ non ha minimo).

L'usuale relazione di ordine $\leq$ definita in $\mathbb{R}$ non è un buon ordine per $\mathbb{R}$ (valgono in sostanza gli esempi appena visti per $\mathbb{Q}$).

Esempio 3.3.4

Si pone

$$\mathbb{N} + \mathbb{N} := \{x \in \mathbb{N} \times \mathbb{N} \,/\, x = (n, h) \text{ con } h \in \{0, 1\}\}$$

e si definisce in $\mathbb{N} + \mathbb{N}$ la seguente relazione $\preceq$:

$(n, h) \preceq (m, k)$ se e soltanto se $(h = 0 \text{ e } k = 1)$ oppure $(h = k \text{ e } n \leq m \text{ in } \mathbb{N})$.

La relazione $\preceq$ così definita è un buon ordine in $\mathbb{N} + \mathbb{N}$.

Teorema 3.3.5 ("del buon ordine")

Qualunque sia l'insieme A, esiste un buon ordine per A.

Dimostrazione – Sia A un insieme. Se $A = \emptyset$, non c'è niente da dimostrare (la relazione vuota, che è l'unica relazione su A, è un buon ordine per A). Possiamo dunque supporre $A \neq \emptyset$.

Sia $\mathcal{B}$ l'insieme ([4]) delle coppie ordinate $(B, \leq_B)$ tali che $B \subset A$ e $\leq_B$ è un buon ordine per B. Poiché $A \neq \emptyset$, anche $\mathcal{B} \neq \emptyset$ (se B è un qualsiasi sottoinsieme finito di A, c'è sicuramente almeno un ordine in B con la proprietà richiesta).

Definiamo in $\mathcal{B}$ la seguente relazione (di "continuazione"):

$(X, \leq_X) \preceq (Y, \leq_Y)$ (e si dice che $(X, \leq_X)$ *trova continuazione in* $(Y, \leq_Y)$ ([5])) sse

(i) $X \subset Y$
(ii) $\leq_X$ è la restrizione a X di $\leq_Y$
(iii) $x \leq_Y y$ per ogni $x \in X$ e per ogni $y \in Y \backslash X$.

Si verifica senza problemi che $\preceq$ è una relazione di ordine su $\mathcal{B}$. Osserviamo ora che ogni catena $\mathcal{C}$ di $\mathcal{B}$ ha una limitazione superiore in $\mathcal{B}$.

Sia $B_{\mathcal{C}}$ l'unione degli insiemi B che compaiono come primo elemento nelle coppie di $\mathcal{C}$, e sia $\leq_{\mathcal{C}}$ l'unione ([6]) delle relazioni che compaiono come secondo elemento nelle coppie di $\mathcal{C}$: è immediato verificare che

$$(B, \leq_B) \preceq (B_{\mathcal{C}}, \leq_{\mathcal{C}}) \quad \text{per ogni } (B, \leq_B) \in \mathcal{C}.$$

Per dimostrare che $(B_{\mathcal{C}}, \leq_{\mathcal{C}})$ è una limitazione superiore per $\mathcal{C}$ in $\mathcal{B}$ resta da provare che $(B_{\mathcal{C}}, \leq_{\mathcal{C}}) \in \mathcal{B}$, cioè che $\leq_{\mathcal{C}}$ è un buon ordine per $B_{\mathcal{C}}$.

Sia X un sottoinsieme non vuoto di $B_{\mathcal{C}}$ e sia $\overline{x} \in X$; allora esiste $\overline{B}$ tale che $(\overline{B}, \leq_{\overline{B}}) \in \mathcal{C}$ e $\overline{x} \in \overline{B}$, cosicché $X \cap \overline{B} \neq \emptyset$ e (poiché $\leq_{\overline{B}}$ è un buon ordine per $\overline{B}$) $X \cap \overline{B}$ ha minimo m (rispetto all'ordine $\leq_{\overline{B}}$).

Poiché $(\overline{B}, \leq_{\overline{B}}) \preceq (B_{\mathcal{C}}, \leq_{\mathcal{C}})$, in base alla condizione (iii) per ogni $y \in X \backslash \left(X \cap \overline{B}\right)$ è

$$m \leq_{\mathcal{C}} y$$

e dunque m è anche minimo per X rispetto a $\leq_{\mathcal{C}}$. Si è così provato che $\leq_{\mathcal{C}}$ è un buon ordine per $B_{\mathcal{C}}$, come si voleva.

Dunque ogni catena di $\mathcal{B}$ ha una limitazione superiore in $\mathcal{B}$. Possiamo applicare il "lemma di Zorn" (teorema 3.2.1) e concludere che esistono un sottoinsieme B_0 di A e una relazione di ordine $\leq_{B_0}$ in B_0 tali che $(B_0, \leq_{B_0})$ è massimale rispetto a $\preceq$.

Vogliamo provare che $B_0 = A$ (da cui immediatamente il nostro asserto). Ma se così non fosse esisterebbe $a_0 \in A \backslash B_0$; si potrebbe allora porre $B_* := B_0 \cup \{a_0\}$ ed estendere $\leq_{B_0}$ ad una relazione $\leq_{B_*}$ in B_* per la quale ogni elemento di B_0 precede a_0: la coppia $(B_*, \leq_{B_*})$ apparterrebbe a $\mathcal{B}$ e si avrebbe $(B_0, \leq_{B_0}) \prec (B_*, \leq_{B_*})$ assurdo per la massimalità di $(B_0, \leq_{B_0})$ in $\mathcal{B}$ rispetto a $\preceq$.

---

[4] Si osservi che $\mathcal{B}$ può essere definito mediante l'assioma-schema di separazione, essendo un sottoinsieme di $\wp(A) \times \wp(A \times A)$.

[5] si dice anche che $(X, \leq_X)$ *è segmento iniziale di* $(Y, \leq_Y)$.

[6] ricordiamo che ogni relazione è un insieme di coppie ordinate!

3.4 - Dal "buon ordine" all'assioma della scelta.

Deduciamo infine $(\mathcal{A}_c)$ dal "principio del buon ordine".

Sia A un insieme i cui elementi sono a due a due disgiunti, e sia $\leq$ un buon ordine per $\cup$ A . Posto

$$B := \{x \in \cup A \,/\, x \in X \text{ con } X \in A, \text{ e } x = \min(X, \leq)\}$$

(un tale insieme B esiste per l'assioma di separazione), è immediato verificare che ogni elemento di B appartiene a un elemento di A, e in ogni elemento non vuoto di A c'è uno e un solo elemento che appartiene a B .

Esercizio 3.4.1

Si commenti la seguente affermazione, attribuita a Bertrand Russell: "Per scegliere, tra infinite paia di calzini, un calzino per ogni paio serve l'assioma della scelta; mentre per scegliere, tra infinite paia di scarpe, una scarpa per ogni paio non c'è bisogno dell'assioma della scelta".

Un insieme bene ordinato ha significativi punti in comune con l'insieme $(\mathbb{N}, \leq)$ che abbiamo studiato nel capitolo 2 : in esso, ad esempio, si può procedere induttivamente (sia per le dimostrazioni che per le definizioni). Nella prossima sezione studieremo il principio generalizzato di induzione in un contesto leggermente più generale (quello degli "insiemi ben fondati"); poi ne vedremo qualche applicazione agli insiemi bene ordinati, nei quali infine (sez. 3.7) generalizzeremo la nozione di "successivo" incontrata nei numeri naturali, usando un termine simile ma diverso ("successore") per evitare confusione col concetto insiemistico di "successivo di un insieme".

3.5 - Insiemi ben fondati.

Sia A un insieme, e sia $\preceq$ una relazione di ordine in A. Si dice che (A, $\preceq$) è un *insieme ben fondato* se ogni sottoinsieme non vuoto di A ha almeno un elemento minimale (rispetto alla restrizione ad esso di $\preceq$). È chiaro che ogni insieme bene ordinato è ben fondato; e che un insieme ben fondato è bene ordinato se e soltanto se la relazione di ordine considerata è totale.

Esempio 3.5.1

Sia "|" la relazione "divide" in $\mathbb{N}$ (cioè: comunque presi $x, y \in \mathbb{N}$, $x|y$ se e soltanto se esiste $n \in \mathbb{N}$ tale che $y = nx$). Allora $(\mathbb{N}, |)$ è un insieme ben fondato ma non bene ordinato (infatti la relazione | non è una relazione di ordine totale).

Teorema 3.5.2

Sia (A, $\preceq$) un insieme ordinato. Sono fatti equivalenti:

(i) (A, $\preceq$) è ben fondato;

(ii) in (A, $\preceq$) vale il principio generalizzato di induzione:

(*) se P(a) è una proprietà tale che
per ogni $x \in$ A, se P(y) è vera per ogni $y \prec x$ allora anche P(x) è vera
allora P(a) è vera per ogni $a \in$ A.

Dimostrazione — (i) $\Rightarrow$ (ii).
Supponiamo che valga la (*) e dimostriamo che P(a) è vera per ogni $a \in$ A. Sia

$$\mathrm{F} := \{x \in \mathrm{A} \,/\, \mathrm{P}(x) \text{ è falsa}\}$$

e supponiamo per assurdo che F non sia vuoto; per la (i) esiste in F un elemento minimale m. Allora per ogni $y \prec m$ non può essere $y \in$ F, cioè P(y) è vera: per la (*) allora anche P(m) è vera, e questo è assurdo perché $m \in$ F. Dunque F è vuoto, cioè P(a) è vera per ogni $a \in$ A, come si voleva dimostrare.

(ii) $\Rightarrow$ (i).
Dobbiamo provare che ogni sottoinsieme di A ha almeno un elemento minimale. Sia B un sottoinsieme di A senza elementi minimali, e dimostriamo che B è vuoto: utilizziamo il principio generalizzato di induzione per dimostrare che la proprietà

$$\mathrm{P}(x) := x \notin \mathrm{B}$$

è vera per ogni $x \in$ A. Dobbiamo dimostrare che per ogni $x \in$ A

se P(y) è vera per ogni $y \prec x$ allora anche P(x) è vera

cioè che per ogni $x \in$ A

se $y \notin$ B per ogni $y \prec x$ allora nemmeno $x \in$ B;

ma in effetti se esistesse $x_0 \in$ B tale che $y \notin$ B per ogni $y \prec x$, tale x sarebbe un elemento minimale di B, contro l'ipotesi che B sia un sottoinsieme di A privo di elementi minimali.

Sia A un insieme. Ricordiamo che si dice *successione a valori in* A, o anche semplicemente *successione in* A, una funzione $\mathbf{f} : \mathbb{N} \to \mathrm{A}$. Se $\mathbf{f}$ è una successione in A, si scrive spesso $\mathbf{f}_n$ anziché $\mathbf{f}(n)$, e la stessa $\mathbf{f}$ si indica con la notazione $(\mathbf{f}_n)$.

Una successione $(\mathbf{f}_n)$ si dice *stazionaria* se esiste $n_0 \in \mathbb{N}$ tale che

$$\mathbf{f}_n = \mathbf{f}_{n_0} \text{ per ogni } n \geq n_0 .$$

Sia (A, $\preceq$) un insieme ordinato. Una successione $(\mathbf{f}_n)$ in A si dice *decrescente* se comunque presi $n_1, n_2 \in \mathbb{N}$ si ha

$$n_1 \leq n_2 \quad \Rightarrow \quad \mathbf{f}_{n_2} \preceq \mathbf{f}_{n_1} .$$

Teorema 3.5.3

Sia (A, $\preceq$) un insieme ordinato. Sono fatti equivalenti:

(i) (A, $\preceq$) è ben fondato;

(ii) ogni successione decrescente in A è stazionaria.

Dimostrazione – (i) $\Rightarrow$ (ii).
Sia ($\mathbf{f}_n$) una successione decrescente in A, e sia B la sua immagine: per la (i) in B c'è un elemento minimale m_0 che è l'immagine di un certo $n_0 \in \mathbb{N}$. Per ogni $n \geq n_0$, deve essere $\mathbf{f}_n \preceq \mathbf{f}_{n_0} = m_0$ (perché la successione è decrescente) da cui $\mathbf{f}_n = m_0$ (per la minimalità di m_0 in B) come si voleva dimostrare.

(ii) $\Rightarrow$ (i). Sia B un sottoinsieme di A, e supponiamo per assurdo che in B non ci siano elementi minimali; in particolare, per ogni $b \in$ B l'insieme

$$\mu(b) \coloneqq \{x \in \mathrm{B} \,/\, x \prec b\}$$

non è vuoto. Sia $b_0 \in$ B, e sia **f** una funzione di scelta su $\wp$(B); definiamo induttivamente come segue una successione σ a valori in B:

$$\sigma(0) \coloneqq b_0\,; \qquad \sigma(n^+) \coloneqq \mathbf{f}(\mu(\sigma(n)))\,.$$

La successione σ è decrescente ma non è stazionaria (infatti $\sigma(n^+) \in \mu(\sigma(n))$ e ogni elemento di $\mu(\sigma(n))$ precede strettamente $\sigma(n)$ per come si è definito $\mu(\sigma(n))$), contro la (ii). Poiché ciò è assurdo, in B ci devono essere elementi minimali.

3.6 - Applicazioni del principio generalizzato di induzione agli insiemi bene ordinati.

Sia (A, $\preceq$) un insieme ordinato.

Una funzione $\mathbf{f}: \mathrm{A} \to \mathrm{A}$ si dice *strettamente crescente* se comunque presi $a_1, a_2 \in$ A

$$a_1 < a_2 \qquad \Rightarrow \qquad \mathbf{f}(a_1) \prec \mathbf{f}(a_2)\,.$$

Teorema 3.6.1

Sia (A, $\preceq$) un insieme bene ordinato. Per ogni funzione $\mathbf{f}: \mathrm{A} \to \mathrm{A}$ strettamente crescente si ha

$$a \preceq \mathbf{f}(a)\,.$$

Dimostrazione – Applicando il principio generalizzato di induzione, possiamo supporre che sia $x \preceq \mathbf{f}(x)$ per ogni $x \prec a$. Se non fosse $a \preceq \mathbf{f}(a)$, poiché $\preceq$ è una relazione di ordine totale (oss. 3.3.1) sarebbe $\mathbf{f}(a) \prec a$; allora si avrebbe

$\mathbf{f}(a) \preceq \mathbf{f}(\mathbf{f}(a))$ (per l'ipotesi di induzione, applicabile a $\mathbf{f}(a)$ perché $\mathbf{f}(a) \prec a$)

e

$\mathbf{f}(\mathbf{f}(a)) \prec \mathbf{f}(a)$ (perché $\mathbf{f}(a) \prec a$ e **f** è strettamente crescente)

da cui $\mathbf{f}(a) \prec \mathbf{f}(a)$, assurdo.

Osservazione 3.6.2

Il teorema 3.6.1 non vale in generale se la relazione di ordine in A è (soltanto) una relazione di ordine totale. Ad esempio, sia $A := \mathbb{R}$ l'insieme dei numeri reali con l'usuale relazione di ordine totale $\leq$; la funzione $x^3 - 1$ è una funzione $\mathbb{R} \to \mathbb{R}$ strettamente crescente ma

$$1 > 1^3 - 1 = 0\,.$$

Teorema 3.6.3 ("di recursione transfinita")

Sia (A, $\preceq$) un insieme bene ordinato. Indichiamo con 0 il minimo di A .

Siano B un insieme, $b_0 \in$ B e **w** una funzione $A \times B^A \to B$ ([7]). Esiste una e una sola funzione $\mathbf{f}: A \to B$ tale che

$$\mathbf{f}(0) = b_0$$

e inoltre

$$\mathbf{f}(a) = \mathbf{w}(a, \mathbf{f}|_{[0,\,a)}) \qquad \text{per ogni } a \in A$$

(indicando con $\mathbf{f}|_{[0,\,a)}$ la restrizione di **f** all'intervallo $[0, a)$).

Dimostrazione – Lasciamo al lettore volenteroso il (non banale) compito di sviluppare la dimostrazione, adattando al prinipio generalizzato di induzione le tecniche utilizzate nella dimostrazione del teorema 2.5.1 .

3.7 - Ancora sugli insiemi bene ordinati.

Sia (A, $\preceq$) un insieme bene ordinato. Se $a \in$ A, (a diverso dall'eventuale massimo di A) si dice *successore* di a l'elemento

$$a + 1 := \mathit{min}\{x \in A \,/\, a \prec x \quad \text{(cioè, } a \preceq x \text{ e } a \neq x)\}.$$

Teorema 3.7.1

Sia (A, $\preceq$) un insieme bene ordinato, e siano $a, b \in$ A . Se a e b hanno lo stesso successore, allora $a = b$.

Dimostrazione – Per l'oss. 3.3.1, $\preceq$ è una relazione di ordine totale in A. Supponiamo che sia $a \prec b$; allora

$$a + 1 \preceq b \prec b + 1$$

da cui $a + 1 \prec b + 1$, contro l'ipotesi che sia $a + 1 = b + 1$. Analogamente si raggiunge un assurdo supponendo che sia $b \prec a$, dunque non può che essere $a = b$.

[7] indichiamo con B^A l'insieme di tutte le funzioni $A \to B$.

Sia (A, $\preceq$) un insieme bene ordinato. Ovviamente il minimo di (A, $\preceq$) non è successore di alcun elemento di A; ma non è necessariamente l'unico elemento di A con tale proprietà. Un elemento di A che non è successore di alcun elemento di A si dice un *elemento limite* di A.

Per ogni elemento limite ℓ di A, definiamo induttivamente per $n \in \mathbb{N}$ (cfr. teorema 2.5.1)

$\ell + 0 := \ell$;
$\ell + n^+ := (\ell + n) + 1$ purché $\ell + n$ sia diverso dall'eventuale massimo di A.

Teorema 3.7.2

Sia (A, $\preceq$) un insieme bene ordinato, e sia L l'insieme degli elementi limite di A. Ogni elemento di A si può scrivere in uno e un solo modo nella forma $\ell + n$ con $\ell \in$ L e $n \in \mathbb{N}$.

Dimostrazione – Sia $a \in$ A. Applicando il principio generalizzato di induzione, possiamo supporre che ogni elemento di A che precede a sia della forma $\ell + n$ con $\ell \in$ L e $n \in \mathbb{N}$. Se a è un elemento limite, $a = a + 0$ e non c'è altro da dimostrare; altrimenti a è il successore di un elemento $\overline{a}$ della forma $\overline{\ell} + n$ con $\overline{\ell} \in$ L e $n \in \mathbb{N}$ e dunque

$$a = \overline{a} + 1 = (\overline{\ell} + n) + 1 = \overline{\ell} + n^+$$

con $\overline{\ell} \in$ L e $n^+ \in \mathbb{N}$, come si voleva dimostrare.

Resta da provare che l'espressione di a nella forma $\ell + n$ con $\ell \in$ L e $n \in \mathbb{N}$ è unica. Sia

$$\ell_1 + n_1 = \ell_2 + n_2 \qquad \text{con} \quad \ell_1, \ell_2 \in \text{L e } n_1, n_2 \in \mathbb{N}$$

e supponiamo, senza perdere in generalità, che sia $n_1 \leq n_2$, cioè (teor. 2.8.10) $n_2 = n_1 + k$ con $k \in \mathbb{N}$. Per induzione su n_1, grazie al teorema 3.7.1 si dimostra facilmente che deve essere

$$\ell_1 = \ell_2 + k$$

e quindi, per definizione di L, $k = 0$ (da cui $n_1 = n_2$) e $\ell_1 = \ell_2$.

Teorema 3.7.3

Per ogni insieme A che non sia in corrispondenza biunivoca con alcun numero naturale ([8]) esiste un buon ordine tale che, detto L l'insieme degli elementi limite di A, esiste una corrispondenza biunivoca tra A e L $\times \mathbb{N}$.

Dimostrazione – Sia $\preceq$ un buon ordine in A. La funzione $\mathbf{f}$: A $\to$ L $\times \mathbb{N}$ definita da

$$\mathbf{f}(\ell + n) := (\ell, n)$$

è iniettiva per il teorema 3.7.2.

[8] nella sez. 4.2 esprimeremo questo fatto dicendo che A è un insieme *infinito*.

Se non è suriettiva, esistono $\ell_0 \in$ L e $n_0 \in \mathbb{N}$ tali che $(\ell_0, n_0) \notin$ **f**(A), ossia non si può definire l'elemento $\ell_0 + n_0$ di A; ciò avviene se e soltanto se $n_0 = n_*^+$ e $\ell_0 + n_*$ è il massimodi A. Poiché per ipotesi A non è in corrispondenza biunivoca con alcun numero naturale, deve essere in particolare $\ell_0 \neq 0$.

Detto a_0 il minimo di A, possiamo allora definire un nuovo ordine $\preceq_*$ in A ponendo

$a_1 \preceq_* a_2$ sse $a_1 \preceq a_2$ quando $a_0 \preceq a_1, a_2 \prec \ell_0$ oppure $\ell_0 \preceq a_1, a_2 \prec \ell_0 + n_*$;

$a_1 \prec_* a_2$ quando $\ell_0 \preceq a_1 \preceq \ell_0 + n_*$ e $a_0 \preceq a_2 \prec \ell_0$.

L'ordine $\preceq_*$ così definito è un buon ordine rispetto al quale il minimo è ℓ_0, l'insieme degli elementi limite è L\{0} e non c'è massimo, cosicché la funzione

$$(\ell + n) \to (\ell, n)$$

è anche suriettiva.

Osservazione 3.7.4

Sia (A, $\preceq$) un insieme bene ordinato. Accenniamo, per una volta senza preoccuparci troppo delle formalità ([9]), a come si possono indicare gli elementi di A.

Poiché A ha minimo, indichiamo con "0" tale minimo; indichiamo poi con "1" il successore di 0, con "2" il successore di 1 e così via. Se, raggiunto un numero naturale n, si sono esauriti gli elementi di A, il nostro compito è finito; altrimenti, indichiamo con "ω" il minimo degli elementi che non si possono indicare con alcun numero naturale, con "$\omega + 1$" il suo successore, con "$\omega + 2$" il successore di $\omega + 1$ e così via. Se ci sono elementi di A che non si possono indicare né con alcun numero naturale n né con alcuna scrittura della forma $\omega + n$, indichiamo con $\omega 2$ il minimo di tal elementi.

Proseguendo allo stesso modo, avremo in A elementi che si indicano con $\omega 2 + 1$, $\omega 2 + 2$, $\omega 2 + 3$, …, $\omega 3$, …, ωn, … . Se ancora non sono esauriti gli elementi di A, il minimo di quelli che rimangono sarà indicato con ω^2. Poi, naturalmente, potremo avere $\omega^2 + 1$, $\omega^2 + 2$, …, $\omega^2 + \omega$, …, $\omega^2 n + \omega h + k$, …, ω^3, …, $\omega^n m + \omega^{n-1} m_1 + \ldots$, …, ω^ω, …, $\omega^{\omega^{\omega^{\cdots^{\omega}}}}$, … .

Teorema 3.7.5

Sia (A, $\preceq$) un insieme bene ordinato. Ogni sottoinsieme non vuoto B di A che sia superiormente limitato ha estremo superiore.

Dimostrazione – Infatti se l'insieme L delle limitazioni superiori di B non è vuoto deve esistere il minimo di L che appunto, per definizione, è l'estremo superiore di B.

[9] per le quali sarebbe comunque necessario utilizzare l'assioma della scelta; torneremo in parte sulla questione con il teorema 4.2.6.

3.8 - Un altro principio equivalente all'assioma della scelta.

Siano X, Y insiemi non vuoti e sia $\mathbf{f}: \mathrm{X} \to \mathrm{Y}$ una funzione.

Si dice *inversa sinistra* di **f** una funzione $\mathbf{s}: \mathrm{Y} \to \mathrm{X}$ tale che

$$\mathbf{s} \circ \mathbf{f} = \mathbf{id}_{\mathbf{X}}, \qquad \text{ossia tale che} \qquad \mathbf{s}(\mathbf{f}(x)) = x \text{ per ogni } x \in \mathrm{X};$$

si dice *inversa destra* di **f** una funzione $\mathbf{d}: \mathrm{Y} \to \mathrm{X}$ tale che

$$\mathbf{f} \circ \mathbf{d} = \mathbf{id}_{\mathbf{Y}}, \qquad \text{ossia tale che} \qquad \mathbf{f}(\mathbf{d}(y)) = y \text{ per ogni } y \in \mathrm{Y}.$$

Osservazione 3.8.1

Siano X, Y insiemi non vuoti e $\mathbf{f}: \mathrm{X} \to \mathrm{Y}$ una funzione. Se **f** ha una inversa sinistra, **f** è iniettiva.

Dimostrazione — Sia **s** una inversa sinistra per **f**. Se $x, y \in \mathrm{X}$,

$$\text{da} \quad \mathbf{f}(x) = \mathbf{f}(y) \quad \text{segue} \quad \mathbf{s}(\mathbf{f}(x)) = \mathbf{s}(\mathbf{f}(y)) \quad \text{cioè} \quad x = y$$

e quindi **f** è iniettiva.

Teorema 3.8.2

Siano X, Y insiemi non vuoti e $\mathbf{f}: \mathrm{X} \to \mathrm{Y}$ una funzione. Se **f** è iniettiva, allora **f** ha una inversa sinistra.

Dimostrazione — Sia $x_0 \in \mathrm{X}$, e per ogni $y \in \mathrm{Y}$ poniamo

$$\mathbf{s}(y) := \begin{cases} \text{l'unico } x \in \mathrm{X} \text{ tale che } \mathbf{f}(x) = y & \text{se } y \in \mathbf{f}(\mathrm{X}); \\ x_0 & \text{se } y \notin \mathbf{f}(\mathrm{X}). \end{cases}$$

È immediato verificare che **s** è un'inversa sinistra per **f**.

Osservazione 3.8.1

Siano X, Y insiemi e $\mathbf{f}: \mathrm{X} \to \mathrm{Y}$ una funzione. Se **f** ha una inversa destra, **f** è suriettiva.

Dimostrazione — Sia **d** una inversa destra per **f**. Per ogni $y \in \mathrm{Y}$, è

$$y = \mathbf{f}(\mathbf{d}(y)) \quad \text{con} \quad \mathbf{d}(y) \in \mathrm{X}$$

dunque **f** è suriettiva.

Teorema 3.8.2

Siano X, Y insiemi e $\mathbf{f}: X \to Y$ una funzione. Se **f** è suriettiva, allora **f** ha una inversa destra.

Dimostrazione – Per l'assioma di separazione, per ogni $y \in Y$ esiste l'insieme

$$X_y := \{x \in X \,/\, \mathbf{f}(x) = y\}$$

ed esiste

$$\overline{X} := \{Z \in \wp(X) \,/\, Z = X_y \text{ per qualche } y \in Y\}.$$

$\overline{X}$ è una famiglia di sottoinsiemi di X indiciata da Y. Poiché **f** è suriettiva, nessun elemento di $\overline{X}$ è vuoto.

Per l'assioma della scelta ($\mathcal{A}_c$ – enunciato (3)) esiste una funzione $\mathbf{d}: Y \to X$ tale che $\mathbf{d}(y) \in X_y$ per ogni $y \in Y$, e tale **d** è una inversa destra per **f**.

Teorema 3.8.3 (L'esistenza dell'inversa destra equivale all'assioma della scelta)

Supponiamo che, comunque presi gli insiemi X, Y e una funzione $\mathbf{f}: X \to Y$ suriettiva, tale funzione abbia una inversa destra.

Allora, per ogni insieme A i cui elementi sono a due a due disgiunti, esiste un insieme B tale che ogni elemento di B appartiene a un elemento di A, e in ogni elemento non vuoto di A c'è uno e un solo elemento che appartiene a B (cioè vale l'enunciato ($\mathcal{A}_c$) dell'assioma della scelta).

Dimostrazione – Posto $X := \bigcup A$ e $Y := A\backslash\{\emptyset\}$, sia $\mathbf{f}: X \to Y$ la funzione che ad ogni x associa l'unico elemento di A a cui x appartiene (ricordiamo che per ipotesi gli elementi di A sono a due a due disgiunti). Se **d** è un'inversa destra per **f**, possiamo porre

$$B := \mathbf{d}(A\backslash\{\emptyset\}).$$

Poiché **d** è un'inversa destra per **f**, ogni elemento b di B è della forma $\mathbf{d}(W)$ con $W \in A$, e $\mathbf{f}(\mathbf{d}(W)) = W \in A$, cioè b appartiene a un elemento di A; e per ogni $H \in A\backslash\{\emptyset\}$

– $\mathbf{d}(H) \in H$ (ricordando la definizione di **f**) perché $\mathbf{f}(\mathbf{d}(H)) = H$;

– $\mathbf{d}(H)$ è infine l'unico elemento di B che appartiene a H. Infatti se $\mathbf{d}(K) \in H$ con $\mathbf{d}(K) \in B$ (cioè $K \in A\backslash\{\emptyset\}$) deve essere $K = \mathbf{f}(\mathbf{d}(K))$ cioè (ricordando la definizione di **f**) K è l'unico elemento di A a cui appartiene $\mathbf{d}(K)$, e siccome $\mathbf{d}(K) \in H$ con $H \in A$ deve essere $K = H$ e quindi $\mathbf{d}(K) = \mathbf{d}(K)$.

3.9 - L'assioma della scelta e la misura in $\mathbb{R}$ secondo Lebesgue.

Concludiamo questo capitolo con un'altra applicazione di $\boldsymbol{\mathcal{A}_c}$: la dimostrazione dell'esistenza di un sottoinsieme di $\mathbb{R}$ non misurabile secondo Lebesgue.

Non ci servirà la definizione di "misura secondo Lebesgue" dei sottoinsiemi di $\mathbb{R}$, ma soltanto il fatto che tale misura è una funzione $\mu_{\mathcal{L}}$ da un sottoinsieme non vuoto $\mathcal{L}$ di $\wp(\mathbb{R})$ in $\mathbb{R}$ che verifica le seguenti quattro proprietà:

(i) $\mathcal{L}$ è un $\sigma-$*anello*, cioè: se $\mathrm{A},\mathrm{B}\in\mathcal{L}$, è anche $\mathrm{A}\backslash\mathrm{B}\in\mathcal{L}$; se $\mathcal{F}=\{\mathrm{A}_i\}_{i\in\mathbb{N}}$ è una famiglia (indiciata da $\mathbb{N}$)([10]) di insiemi che appartengono a $\mathcal{L}$, anche $\cup\mathcal{F}\in\mathcal{L}$.

(ii) $\mu_{\mathcal{L}}$ è *non negativa*, ossia: $\mu_{\mathcal{L}}(\mathrm{A})\geq 0$ per ogni $\mathrm{A}\in\mathcal{L}$.

(iii) $\mu_{\mathcal{L}}$ è $\sigma-$*additiva*, cioè: se $\mathcal{F}=\{\mathrm{A}_i\}_{i\in\mathbb{N}}$ è una famiglia (indiciata da $\mathbb{N}$) di insiemi a due a due disgiunti che appartengono a $\mathcal{L}$, $\mu_{\mathcal{L}}(\cup\mathcal{F})=\sum_{i=1}^{\infty}\mu_{\mathcal{L}}(\mathrm{A}_i)$.

(iv) $\mu_{\mathcal{L}}$ è *invariante rispetto alle isometrie*, cioè: se $\mathrm{A}\in\mathcal{L}$ e τ è un'isometria di $\mathbb{R}$, $\tau(\mathrm{A})\in\mathcal{L}$ e $\mu_{\mathcal{L}}(\tau(\mathrm{A}))=\mu_{\mathcal{L}}(\mathrm{A})$.

In effetti, poiché la funzione che ad ogni sottoinsieme di $\mathbb{R}$ associa il numero reale 0 verifica le quattro proprietà sopra riportate con $\mathcal{L}:=\mathbb{R}$, ci servirà anche il fatto che la misura secondo Lebesgue *non è banale*, ossia a qualche sottoinsieme di $\mathbb{R}$ associa un numero strettamente maggiore di zero. Inoltre, per semplificarci la vita, daremo come acquisito il fatto che ogni intervallo della forma $(x_0,x_0+1]$ oppure $[x_0,x_0+1)$ (con $x_0\in\mathbb{R}$) appartiene a $\mathcal{L}$ e ha misura secondo Lebesgue uguale a 1.

Notiamo anche che dalla (i) segue subito che: se $\mathrm{A},\mathrm{B}\in\mathcal{L}$, è anche $\mathrm{A}\cap\mathrm{B}\in\mathcal{L}$; infatti $\mathrm{A}\cap\mathrm{B}=\mathrm{A}\backslash(\mathrm{A}\backslash\mathrm{B})$.

Per costruire un sottoinsieme di $\mathbb{R}$ non misurabile secondo Lebesgue (cioè non appartenente a $\mathcal{L}$), definiamo nell'intervallo $(0,1]$ (aperto su 0 e chiuso su 1) la seguente relazione $\sim$:

$$x\sim y \quad \text{se e soltanto se} \quad x-y\in\mathbb{Q}\,.$$

È immediato verificare che $\sim$ è una relazione di equivalenza in $(0,1]$. L'assioma della scelta (nella prima formulazione) garantisce l'esistenza di un insieme A al quale appartiene esattamente un elemento per ogni classe di equivalenza rispetto a $\sim$. Dimostreremo adesso che A non può appartenere a $\mathcal{L}$.

Per ogni $q\in\mathbb{Q}\cap[0,1)$, poniamo:

$\mathrm{A}^{q,-}:=\{a\in\mathrm{A}\,/\,a+q\geq 1\}=\mathrm{A}\cap[1-q,2-q)$;

$\mathrm{A}^{q,+}:=\{a\in\mathrm{A}\,/\,a+q<1\}=\mathrm{A}\cap[-q,1-q)$;

$\mathrm{A}_q:=\{x\in(0,1]\,/\,x=a+q \text{ con } a\in\mathrm{A}^{q,+} \text{ oppure } x=a+q-1 \text{ con } a\in\mathrm{A}^{q,-}\}$.

---

[10] con la terminologia che introdurremo nella sez. 4.2 si dice che $\mathcal{F}$ è una famiglia *numerabile* di insiemi.

Osserviamo adesso che, per ogni $q \in \mathbb{Q} \cap [0,1)$,

$$\text{se } \mathrm{A} \in \mathcal{L}, \text{ allora } \mathrm{A}_q \in \mathcal{L} \text{ e si ha } \mu_{\mathcal{L}}(\mathrm{A}_q) = \mu_{\mathcal{L}}(\mathrm{A})\,.$$

Infatti, gli insiemi $\mathrm{A}^{q,-}$ e $\mathrm{A}^{q,+}$ appartengono a $\mathcal{L}$ perché intersezione di elementi di $\mathcal{L}$; quindi $\mathrm{A}_q \in \mathcal{L}$, perché A_q è unione disgiunta dell'immagine di $\mathrm{A}^{q,-}$ mediante una traslazione verso sinistra di ampiezza $1-q$ e dell'immagine di $\mathrm{A}^{q,+}$ mediante una traslazione verso destra di ampiezza q. Inoltre, $\mathrm{A} = \mathrm{A}^{q,-} \cup \mathrm{A}^{q,+}$ con $\mathrm{A}^{q,-} \cap \mathrm{A}^{q,+} = \emptyset$ e quindi (ricordando la (iv))

$$\mu_{\mathcal{L}}(\mathrm{A}) = \mu_{\mathcal{L}}(\mathrm{A}^{q,-} \cup \mathrm{A}^{q,+}) = \mu_{\mathcal{L}}(\mathrm{A}^{q,-}) + \mu_{\mathcal{L}}(\mathrm{A}^{q,+}) = \mu_{\mathcal{L}}(\mathrm{A}_q)\,.$$

Se mostriamo che gli insiemi A_q al variare di q in $\mathbb{Q} \cap [0,1)$ costituiscono una partizione dell'intervallo $(0,1]$, abbiamo raggiunto un assurdo: infatti per la (iii) dovrebbe essere

$$1 = \mu_{\mathcal{L}}((0,1]) = \sum_q \mu_{\mathcal{L}}(\mathrm{A}_q) = \sum_q \mu_{\mathcal{L}}(\mathrm{A})$$

e questo non è compatibile con nessun possibile valore di $\mu_{\mathcal{L}}(\mathrm{A})$: dunque A non è misurabile secondo Lebesgue.

Proviamo dunque che gli insiemi A_q al variare di q in $\mathbb{Q} \cap [0,1)$ costituiscono una partizione dell'intervallo $(0,1]$.

Intanto, osserviamo che se $\mathrm{A}_q \cap \mathrm{A}_s \neq \emptyset$ deve essere $q = s$. Sia $x \in \mathrm{A}_q \cap \mathrm{A}_s$. Sarà $x = a + q$ con $a \in \mathrm{A}^{q,+}$ oppure $x = a + q - 1$ con $a \in \mathrm{A}^{q,-}$ ed anche $x = \overline{a} + s$ con $\overline{a} \in \mathrm{A}^{s,+}$ oppure $x = \overline{a} + s - 1$ con $a \in \mathrm{A}^{s,-}$; in ogni caso, $a - \overline{a} \in \mathbb{Q}$ ossia $a \sim \overline{a}$ e dunque $a = \overline{a}$ per definizione di A.

Ma allora deve essere

$$a + q = x = \overline{a} + s = a + s, \quad \text{da cui} \quad q = s\,;$$

oppure

$$a + q - 1 = x = \overline{a} + s - 1 = a + s - 1, \quad \text{da cui ancora} \quad q = s\,;$$

mentre non può essere

$$a + q = x = \overline{a} + s - 1 = a + s - 1, \quad \text{perché ne seguirebbe } s = q + 1\,;$$

né può essere

$$a + q - 1 = x = \overline{a} + s = a + s, \quad \text{perché ne seguirebbe } s = q + 1\,:$$

ricordiamo infatti che per ipotesi $q, s \in [0,1)$.

Infine, sia $\alpha \in [0,1)$ e proviamo che esiste $q \in \mathbb{Q} \cap [0,1)$ tale che $\alpha \in \mathrm{A}_q$. Sia $[\alpha]$ la classe di equivalenza (rispetto a $\sim$) individuata da α, e sia x_0 l'unico elemento di $[\alpha]$ che appartiene ad A: se $x_0 \leq \alpha$, poniamo $q := \alpha - x_0$; se $x_0 > \alpha$, poniamo $q := \alpha - x_0 + 1$. Poiché $\alpha \sim x_0$, $q \in \mathbb{Q}$ in entrambi i casi. Nel primo caso, $x_0 \in \mathrm{A}^{q,+}$ e quindi $\alpha = x_0 + q \in \mathrm{A}_q$; nel secondo caso, $x_0 \in \mathrm{A}^{q,-}$ e quindi $\alpha = x_0 + q - 1 \in \mathrm{A}_q$: in ogni caso, $\alpha \in \mathrm{A}_q$ e l'asserto è completamente provato.

4.- CARDINALITÀ

4.1 - Equipotenza.

Siano A, B insiemi.

Si dice che A è *equipotente* a B se esiste una corrispondenza biunivoca tra A e B.

Osservazione 4.1.1

Ogni insieme è equipotente a se stesso.

Dimostrazione – Sia A un insieme: la funzione $\mathbf{id}_A$ che ad ogni elemento di A associa se stesso è una corrispondenza biunivoca tra A e A.

Osservazione 4.1.2

Siano A, B insiemi. Se A è equipotente a B, allora B è equipotente ad A.

Dimostrazione – Infatti ogni corrispondenza biunivoca $A \to B$ è invertibile e la sua inversa è una corrispondenza biunivoca $B \to A$ ..

Osservazione 4.1.3

Siano A, B, C insiemi. Se A è equipotente a B e B è equipotente a C, allora A è equipotente a C.

Dimostrazione – Infatti la composizione di corrispondenze biunivoche è una corrispondenza biunivoca.

4.2 - Cardinalità.

Per quanto osservato in 4.1.1, 4.1.2 e 4.1.3, in ogni insieme di insiemi la relazione di "equipotenza" (definita in accordo con 4.1) è una relazione di equivalenza. Questo fatto suggerisce che tutti gli insiemi tra loro equipotenti abbiano in comune una proprietà astratta, che diremo *cardinalità*. Notiamo esplicitamente che per l'osservazione 1.4.4 non è possibile dare una definizione di cardinalità mediante un procedimento di "passaggio all'insieme quoziente".

Per "misurare" la cardinalità di un insieme dovremo considerare degli insiemi – campione a due a due non equipotenti. Per cominciare, rivolgiamo la nostra attenzione ai numeri naturali e all'insieme $\mathbb{N}$ dei numeri naturali.

Teorema 4.2.1

Nessun numero naturale è equipotente a un suo sottoinsieme proprio.

Dimostrazione – Procediamo per induzione. Poiché $0 = \emptyset$, 0 non ha sottoinsiemi propri e dunque l'asserto è vero per 0.

Supponiamo di aver dimostrato che: se **f** è una funzione iniettiva $n \to n$, allora $\mathbf{f}(n) = n$; e dimostriamo che la stessa cosa accade per n^+ $(= n \cup \{n\})$.

Sia **g** una funzione iniettiva $n^+ \to n^+$ e osserviamo che deve essere $n \in \mathbf{g}(n^+)$; infatti, in caso contrario, la restrizione di **g** a n sarebbe una funzione iniettiva $n \to n$ e (per l'ipotesi di induzione) dovrebbe avere come immagine n; e $\mathbf{g}(n)$ (non potendo essere n, perché abbiamo supposto che $n \notin \mathbf{g}(n^+)$) dovrebbe anch'esso appartenere a n, contro l'ipotesi che g sia iniettiva.

Dunque esiste $x_0 \in n^+$ tale che $\mathbf{g}(x_0) = n$. Se $x_0 = n$, la restrizione di **g** a n è una funzione iniettiva $n \to n$ e quindi (per l'ipotesi di induzione) ha come immagine n; dunque $\mathbf{g}(n^+) = n^+$, come si voleva dimostrare. Se invece $x_0 \neq n$, sarà $\mathbf{g}(n) = y \neq \mathbf{g}(x_0)$ e la funzione

$$\overline{\mathbf{g}} : n \to n \qquad \text{definita ponendo} \qquad \overline{\mathbf{g}}(x) := \begin{cases} \mathbf{g}(x) & \text{se } x \neq x_0 \\ y & \text{se } x = x_0 \end{cases}$$

è una funzione iniettiva $n \to n$. Pertanto $\overline{\mathbf{g}}$ ha per immagine n e di conseguenza **g** ha per immagine n^+, come si voleva dimostrare.

Un insieme A si dice *finito* se esiste $n \in \mathbb{N}$ tale che A è equipotente a n. Un insieme si dice infinito se non è finito.

Teorema 4.2.2

Se un insieme è equipotente a un suo sottoinsieme proprio, allora è infinito.

Dimostrazione – Sia A un insieme, ed esistano $A_* \subsetneq A$ e $\mathbf{f}: A \to A_*$ biunivoca. Supponiamo per assurdo che esistano $n_0 \in \mathbb{N}$ e $\mathbf{g}: A \to n_0$ biunivoca. Sia $a_0 \in A \backslash A_*$; allora $\mathbf{g}(a_0) \notin \mathbf{g}(\mathbf{f}(A))$, altrimenti esisterebbe $\overline{a} \in A$ tale che $\mathbf{g}(\mathbf{f}(\overline{a})) = \mathbf{g}(a_0)$ e quindi (poiché **g** in particolare è iniettiva) $a_0 = \mathbf{f}(\overline{a}) \in A_*$. Dunque $\mathbf{g} \circ \mathbf{f} \circ \mathbf{g}^{-1} : n_0 \to n_0$ è una funzione iniettiva ma non suriettiva, contro il teorema 4.2.1 .

Osservazione 4.2.3

L'insieme $\mathbb{N}$ dei numeri naturali è infinito.

Dimostrazione – La funzione $\mathbb{N} \to \mathbb{N}$ che a ogni numero naturale associa il suo successivo è iniettiva ma non suriettiva (per il teorema 2.4.5), quindi è una corrispondenza biunivoca tra $\mathbb{N}$ e un suo sottoinsieme proprio. Per il teorema 4.2.2, $\mathbb{N}$ è infinito.

Teorema 4.2.4

I numeri naturali e l'insieme $\mathbb{N}$ sono a due a due non equipotenti.

Dimostrazione – Per l'osservazione 4.2.3, nessun numero naturale è equipotente a $\mathbb{N}$. Se $n, \overline{n}$ sono numeri naturali distinti, per il teorema 2.8.3 deve essere $n \in \overline{n}$ oppure $\overline{n} \in n$, quindi (per il teorema 2.3.3) uno dei due deve essere un sottoinsieme proprio dell'altro; il teorema 4.2.1 ci consente di concludere che n e $\overline{n}$ non sono equipotenti.

Sia A un insieme. Se A è equipotente a un certo numero naturale n, diremo che A *ha cardinalità* n e scriveremo $|A| = n$. Se A è equipotente a $\mathbb{N}$, diremo che A *ha cardinalità* $\aleph_0$ (si legge: "aleph con zero") oppure che *è numerabile* e scriveremo $|A| = \aleph_0$.

Esempio 4.2.5

Il sottoinsieme di $\mathbb{N}$ costituito dai numeri pari ha cardinalità $\aleph_0$.

Dimostrazione – La funzione che a ogni numero naturale associa il suo doppio è una corrispondenza biunivoca tra $\mathbb{N}$ e l'insieme dei numeri naturali pari.

Teorema 4.2.6

Ogni insieme infinito A ha un sottoinsieme equipotente a $\mathbb{N}$.

Dimostrazione – Sia **f** una funzione di scelta su $\wp(\mathrm{A})$. Definiamo per recursione (cfr. teorema 2.5.1) una funzione $\mathbf{g}:\mathbb{N}\to\wp(\mathrm{A})$ come segue:

$$\mathbf{g}(0)=\emptyset\,;$$

$$\mathbf{g}(n^+):=\begin{cases}\mathbf{g}(n) & \text{se } \mathbf{g}(n)=\mathrm{A}\\ \mathbf{g}(n)\cup\{\mathbf{f}(\mathrm{A}\backslash\mathbf{g}(n))\} & \text{se } \mathrm{A}\backslash\mathbf{g}(n)\neq\emptyset\end{cases}$$

Osserviamo che:

(i) $\mathbf{g}(n)$ ha cardinalità n. Questo si dimostra facilmente per induzione su n: se $n=0$, è addirittura $\mathbf{g}(0)=0$; supposto che $\mathbf{g}(n)$ abbia cardinalità n, per definizione $\mathbf{g}(n^+)$ si ottiene da $\mathbf{g}(n)$ aggiungendo un elemento che non appartiene a $\mathbf{g}(n)$, quindi $\mathbf{g}(n^+)$ ha cardinalità n^+.

(ii) $\mathbf{g}(n)\subsetneq\mathbf{g}(n^+)$ (cioè $\mathrm{A}\backslash\mathbf{g}(n)\neq\emptyset$) per ogni $n\in\mathbb{N}$. Infatti, se esistesse $n_0\in\mathbb{N}$ tale che $\mathrm{A}\backslash\mathbf{g}(n_0)=\emptyset$ sarebbe $\mathbf{g}(n_0)=\mathrm{A}$. D'altro lato, $\mathbf{g}(n)$ ha cardinalità n per ogni $n\in\mathbb{N}$ (per la (i)), dunque non può essere $\mathbf{g}(n_0)=\mathrm{A}$ perché per ipotesi A è un insieme infinito.

(iii) se $n\le m$, $\mathbf{g}(n)\subset\mathbf{g}(m)$. Poiché (cfr. teorema 2.8.10) la condizione "$n\le m$" significa che esiste $k\in\mathbb{N}$ tale che $m=n+k$, possiamo dimostrare questo fatto per induzione su k. Se $k=0$, è $n=m$ ed è ovvio che $\mathbf{g}(n)\subset\mathbf{g}(m)$. Supponiamo che l'asserto sia vero quando $m=n+k_0$, e proviamo che è vero anche se $m=n+k_0^+$.

Per l'ipotesi di induzione, $\mathbf{g}(n)\subset\mathbf{g}(n+k_0)$; per la (ii), $\mathbf{g}(n+k_0)\subsetneq\mathbf{g}((n+k_0)^+)$; e per il lemma 2.6.2 $n+k_0^+=(n+k_0)^+$. Dunque

$$\mathbf{g}(n)\subset\mathbf{g}(n+k_0)\subsetneq\mathbf{g}((n+k_0)^+)=\mathbf{g}(n+k_0^+)$$

cosicché anche la (iii) è provata.

Poniamo adesso $\mathbf{h}(n):=\mathbf{f}(\mathrm{A}\backslash\mathbf{g}(n))$. Vogliamo provare che **h** è una funzione iniettiva, cosicché $\mathbf{h}(\mathbb{N})$ è un sottoinsieme di A equipotente a $\mathbb{N}$, come si voleva.

Siano $n,\ m\in\mathbb{N}$ con $n\neq m$; per il teorema 2.8.3, sarà $n<m$ oppure $m<n$. Supponiamo, per fissare le idee, che sia $n<m$ e quindi (per il lemma 2.8.8) $n^+\le m$.

Per definizione di **h**,

$$\mathbf{h}(m)=\mathbf{f}(\mathrm{A}\backslash\mathbf{g}(m))\notin\mathbf{g}(m)\,;$$

d'altro lato, per definizione di $\mathbf{g}(n^+)$,

$$\mathbf{h}(n)=\mathbf{f}(\mathrm{A}\backslash\mathbf{g}(n))\in\mathbf{g}(n^+).$$

Ma, per la (ii), $\mathbf{g}(n^+)\subset\mathbf{g}(m)$: dunque,

$$\mathbf{h}(n)\in\mathbf{g}(m)\qquad\text{mentre}\qquad\mathbf{h}(m)\notin\mathbf{g}(m)$$

cosicché $\mathbf{h}(n)\neq\mathbf{h}(m)$, come si voleva.

Teorema 4.2.7

Ogni insieme infinito è equipotente a un suo sottoinsieme proprio.

Dimostrazione – Sia A un insieme infinito, e sia $\mathbf{f}\colon \mathbb{N} \to \mathrm{A}$ una corrispondenza biunivoca tra $\mathbb{N}$ e A (che esiste per il teorema 4.2.6). Definiamo una funzione $\mathbf{g}\colon \mathrm{A} \to \mathrm{A}$ ponendo

$$\mathbf{g}(x) := \begin{cases} \mathbf{f}(n^+) & \text{se } x \in \mathbf{f}(\mathbb{N}) \text{ e } x = \mathbf{f}(n) \\ x & \text{se } x \notin \mathbf{f}(\mathbb{N}) \end{cases}$$

È immediato verificare che **g** è una funzione iniettiva con dominio A. Ma **g** non è suriettiva perché $\mathbf{f}(0) \notin \mathbf{g}(\mathrm{A})$.

Teorema 4.2.8

Un insieme è infinito se e soltanto se è equipotente a un suo sottoinsieme proprio.

Dimostrazione – Segue immediatamente dai teoremi 4.2.2 e 4.2.7.

La caratterizzazione espressa dal teorema 4.2.8 era stata scelta da Richard Dedekind (1831 – 1916) come definizione di "insieme infinito". Se non si accetta l'assioma della scelta, possono esistere insiemi "finiti nel senso di Dedekind" che non hanno come cardinalità un numero naturale.

Esercizio 4.2.9

Si dimostri che ogni insieme infinito ammette una partizione in sottoinsiemi numerabili.

Suggerimento – Si usino il teorema 4.2.6 e il lemma di Zorn.

4.3 - Insiemi finiti e insiemi numerabili.

Teorema 4.3.1

Siano A, B insiemi. Se $|\mathrm{A}| = n \in \mathbb{N}$ e $|\mathrm{B}| = m \in \mathbb{N}$, allora $|\mathrm{A} \cap \mathrm{B}|$ è un numero naturale j e

$$|\mathrm{A} \cup \mathrm{B}| = |\mathrm{A}| + |\mathrm{B}| - |\mathrm{A} \cap \mathrm{B}| = m + n - j\,.$$

In particolare, l'unione di due insiemi finiti è un insieme finito.

Dimostrazione – Poiché $\mathrm{A} \cap \mathrm{B} \subset \mathrm{A}$, se esistesse una corrispondenza biunivoca **f** tra $\mathrm{A} \cap \mathrm{B}$ e un suo sottoinsieme proprio essa si potrebbe estendere a tutto A (ponendo $\mathbf{f}(x) \coloneqq x$ per ogni $x \in$ A\(AB)) e quindi A non sarebbe finito per il teorema 4.2.2.

La relazione fra $|\mathrm{A} \cup \mathrm{B}|$, $|\mathrm{A}|$, $|\mathrm{B}|$ e $|\mathrm{A} \cap \mathrm{B}|$ si dimostra facilmente procedendo per induzione su n: lasciamo il compito al lettore quale esercizio.

Teorema 4.3.2

L'unione di un numero finito n di insiemi finiti è un insieme finito.

Dimostrazione – È una banale applicazione del principio di induzione utilizzando il teorema 4.3.1, e la si lascia al lettore per esercizio.

Lemma 4.3.3

Se un insieme infinito A ammette una partizione in una famiglia $\{\mathrm{X}_n\}_{n\in\mathbb{N}\setminus\{0\}}$ di sottoinsiemi finiti indiciata da $\mathbb{N}\setminus\{0\}$, allora $|\mathrm{A}| = \aleph_0$.

Dimostrazione – Per ipotesi, per ciascun X_j esiste una corrispondenza biunivoca σ_j tra X_j e un numero naturale n_j ($= \{0, 1, \ldots, n_j - 1\}$).

Mostriamo adesso come si definisce una corrispondenza biunivoca **f** tra A e $\mathbb{N}$. Se $a \in$ A, per ipotesi esiste uno e un solo $j \in \mathbb{N}\setminus\{0\}$ tale che $a \in \mathrm{X}_j$; posto $n_0 \coloneqq 0$, definiamo

$$\mathbf{f}(a) \coloneqq \sum_{i:=0}^{j-1} n_i + \sigma_j(a)\,.$$

Notiamo subito che per ogni $a \in$ A

$$\text{se} \quad a \in \mathrm{X}_j \quad \text{allora} \quad \sum_{i:=0}^{j-1} n_i \leq \mathbf{f}(a) < \sum_{i:=0}^{j} n_i$$

e quindi se $\mathbf{f}(a) = \mathbf{f}(b)$ gli elementi a, b devono appartenere allo stesso X_j. È facile adesso vedere che **f** è iniettiva: se $\mathbf{f}(a) = \mathbf{f}(b)$ deve essere

$$\sum_{i:=0}^{j-1} n_i + \sigma_j(a) = \mathbf{f}(a) = \mathbf{f}(b) = \sum_{i:=0}^{j-1} n_i + \sigma_j(b) \qquad \text{e quindi} \qquad \sigma_j(a) = \sigma_j(b)$$

per lo stesso j, da cui $a = b$ per l'iniettività di σ_j.

Per dimostrare che **f** è suriettiva, per ogni $m \in \mathbb{N}$ dobbiamo trovare un $a \in$ A tale che

$$\mathbf{f}(a) = m\,.$$

A tale scopo, osserviamo che esiste j_0 tale che $m < \sum_{i:=0}^{j_0} n_i$; infatti in caso contrario la somma di tutti gli n_i sarebbe $\leq m$ e quindi A sarebbe un insieme finito, contro l'ipotesi.

Sia j_0^* il minimo intero positivo tale che $m < \sum_{i:=0}^{j_0} n_i$; allora

$$\alpha = \sum_{i:=0}^{j_0^*-1} n_i \leq m < \sum_{i:=0}^{j_0^*} n_i = \alpha + n_{j_0^*}$$

cosicché

$$0 \leq m - \alpha < n_{j_0^*}$$

e quindi esiste $a \in \mathrm{X}_{j_0^*}$ tale che $a := \sigma_{j_0^*}^{-1}(m-\alpha)$. Per tale a si ha che

$$\mathbf{f}(a) = \sum_{i:=0}^{j_0^*-1} n_i + \sigma_{j_0^*}(a) = \alpha + (m-\alpha) = m$$

come si voleva.

Esercizio 4.3.4

Si discuta se nella dimostrazione del lemma 4.3.3 si usa l'assioma della scelta, alla luce del fatto che per costruire la corrispondenza biunivoca **f** bisogna "scegliere" una corrispondenza biunivoca in ciascuno degli infiniti insiemi X_i .

Teorema 4.3.5

L'insieme $\mathbb{Z}$ dei numeri interi relativi ha cardinalità $\aleph_0$.

Dimostrazione – Per ogni $n \in \mathbb{N}\backslash\{0\}$ poniamo

$$\mathrm{X}_n := \{z \in \mathbb{Z} \,/\, |z| + 1 = n\}$$

indicando con $|z|$ il "valore assoluto" di z.

Ovviamente $\mathrm{X}_1 = \{0\}$ e per ogni fissato $n \in \mathbb{N}\backslash\{0,1\}$ l'insieme X_n ha esattamente due elementi. Dunque la famiglia degli X_n costituisce una partizione di $\mathbb{Z}$ che verifica le ipotesi del lemma 4.3.3, applicando il quale si può concludere che $|\mathbb{Z}| = \aleph_0$.

Teorema 4.3.6

L'insieme $\mathbb{Q}$ dei numeri razionali ha cardinalità $\aleph_0$.

Dimostrazione – Per ogni $\alpha \in \mathbb{Q}$, sia $\frac{m}{n}$ l'unica frazione con MCD$(m, n) = 1$ che rappresenta α: chiamiamo *altezza* di α il numero intero positivo $|m| + n$. Ovviamente non esistono numeri razionali di altezza zero; e per ogni fissato $h \in \mathbb{N}\backslash\{0\}$ esiste un numero finito di numeri razionali di altezza h . Pertanto, posto

$$\mathrm{X}_h \coloneqq \{\alpha \in \mathbb{Q} \,/\, \alpha \text{ ha altezza } h\} \quad \text{per ogni } h \in \mathbb{N}\backslash\{0\}$$

la famiglia degli X_h costituisce una partizione di $\mathbb{Q}$ che verifica le ipotesi del lemma 4.3.3, applicando il quale si può concludere che $|\mathbb{Q}| = \aleph_0$.

Teorema 4.3.7

L'insieme $\mathbb{A}$ dei numeri reali algebrici ha cardinalità $\aleph_0$.

Dimostrazione – Per ogni polinomio

$$\mathbf{p}(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$$

nell'indeterminata x di grado $n \geq 1$ a coefficienti interi, diciamo *altezza* di $\mathbf{p}(x)$ il numero intero positivo

$$n + |a_n| + |a_{n-1}| + \ldots + |a_2| + |a_1| + |a_0| \,.$$

Per ogni $\alpha \in \mathbb{A}$, diciamo *altezza* di α la minima altezza dei polinomi a coefficienti interi che hanno come radice α . Ovviamente non esistono numeri algebrici di altezza zero; e per ogni fissato $h \in \mathbb{N}\backslash\{0\}$ esiste un numero finito di numeri algebrici di altezza h . Pertanto, posto

$$\mathrm{X}_h \coloneqq \{\alpha \in \mathbb{A} \,/\, \alpha \text{ ha altezza } h\} \quad \text{per ogni } h \in \mathbb{N}$$

la famiglia degli X_h costituisce una partizione di $\mathbb{A}$ che verifica le ipotesi del lemma 4.3.3, applicando il quale si può concludere che $|\mathbb{A}| = \aleph_0$.

Teorema 4.3.8

L'insieme $\mathcal{F}$ dei sottoinsiemi finiti di $\mathbb{N}$ ha cardinalità $\aleph_0$.

Dimostrazione – Per $\mathrm{S} \in \mathcal{F}$ chiamiamo *altezza* di S il numero intero positivo

$$1 + \sum_{n \in \mathrm{S}} n \,.$$

Ovviamente non esistono in $\mathcal{F}$ elementi di altezza zero; e per ogni fissato $h \in \mathbb{N}\backslash\{0\}$ esiste un numero finito di elementi di $\mathcal{F}$ di altezza h . Pertanto, posto

$$\mathrm{X}_h \coloneqq \{\mathrm{S} \in \mathcal{F} \,/\, \mathrm{S} \text{ ha altezza } h\} \quad \text{per ogni } h \in \mathbb{N}$$

la famiglia degli X_h costituisce una partizione di $\mathcal{F}$ che verifica le ipotesi del lemma 4.3.3, applicando il quale si può concludere che $|\mathcal{F}| = \aleph_0$.

Teorema 4.3.9

Il prodotto cartesiano di due insiemi numerabili è numerabile..

Dimostrazione – Siano **A**, **B** gli insiemi dati; sia **f** una corrispondenza biunivoca tra **A** e $\mathbb{N}$, e sia **g** una corrispondenza biunivoca tra **B** e $\mathbb{N}$. Per ogni $(a,b) \in \mathbf{A} \times \mathbf{B}$ chiamiamo *altezza* di (a,b) il numero naturale $1 + \mathbf{f}(a) + \mathbf{g}(b)$. Ovviamente non esistono in $\mathbf{A} \times \mathbf{B}$ elementi di altezza zero; e per ogni fissato $h \in \mathbb{N}\backslash\{0\}$ esiste un numero finito di elementi di $\mathbf{A} \times \mathbf{B}$ di altezza h. Pertanto, posto

$$\mathrm{X}_h := \{(a,b) \in \mathbf{A} \times \mathbf{B} \,/\, \mathrm{S} \text{ ha altezza } h\} \quad \text{per ogni } h \in \mathbb{N}$$

la famiglia degli X_h costituisce una partizione di $\mathbf{A} \times \mathbf{B}$ che verifica le ipotesi del lemma 4.3.3, applicando il quale si può concludere che $|\mathbf{A} \times \mathbf{B}| = \aleph_0$.

Teorema 4.3.10

Il prodotto cartesiano di un numero finito di insiemi numerabili è un insieme numerabile.

Dimostrazione – È una banale applicazione del principio di induzione utilizzando il teorema 4.3.9, e la si lascia al lettore per esercizio.

4.4 - Confronto tra cardinalità.

Siano A, B insiemi.

Se A è equipotente a un sottoinsieme di B (cioè se esiste una funzione iniettiva $\mathrm{A} \to \mathrm{B}$), scriveremo $\mathrm{A} \preceq \mathrm{B}$ (e diremo che A *è suvvalente a* B, oppure che B *domina* A). Se $\mathrm{A} \preceq \mathrm{B}$ e A non è equipotente a B, scriveremo $\mathrm{A} \prec \mathrm{B}$ (e diremo che A *è strettamente suvvalente a* B, oppure che B *domina* A *in senso stretto*).

In ogni insieme i cui elementi siano insiemi, $\preceq$ definisce una relazione evidentemente riflessiva e transitiva. Tale relazione non può in generale essere però antisimmetrica; infatti, se A, B sono insiemi distinti equipotenti si ha $\mathrm{A} \preceq \mathrm{B}$ e $\mathrm{B} \preceq \mathrm{A}$ ma $\mathrm{A} \neq \mathrm{B}$. Vale comunque il seguente importante teorema:

Teorema 4.4.1 (Schröder-Bernstein-Cantor)

Siano A, B insiemi. Se $A \preceq B$ e $B \preceq A$, allora A e B sono equipotenti.

Dimostrazione – Per ipotesi, esistono una funzione iniettiva $\mathbf{f}: A \to B$ e una funzione iniettiva $\mathbf{g}: B \to A$.

Per ogni $a_0 \in \mathbf{g}(B)$, diremo *antenati* di a

– a_0 stesso;

– ogni $b \in B$ tale che $(\mathbf{g} \circ \mathbf{f} \circ \mathbf{g} \circ \mathbf{f} \circ \ldots \circ \mathbf{g})(b) = a_0$ per qualche sequenza finita alternata di **g** e **f** nell'espressione $\mathbf{g} \circ \mathbf{f} \circ \mathbf{g} \circ \mathbf{f} \circ \ldots \circ \mathbf{g}$;

– ogni $a \in A$ tale che $(\mathbf{g} \circ \mathbf{f} \circ \mathbf{g} \circ \mathbf{f} \circ \ldots \circ \mathbf{f})(a) = a_0$ per qualche sequenza finita alternata di **g** e **f** nell'espressione $\mathbf{g} \circ \mathbf{f} \circ \mathbf{g} \circ \mathbf{f} \circ \ldots \circ \mathbf{f}$.

Per ogni $a_0 \in A \setminus \mathbf{g}(B)$, diremo che a_0 è l'*unico antenato* di a_0.

Per ogni $b_0 \in \mathbf{f}(A)$, diremo *antenati* di b

– b_0 stesso;

– ogni $a \in A$ tale che $(\mathbf{f} \circ \mathbf{g} \circ \mathbf{f} \circ \ldots \circ \mathbf{f})(a) = b_0$ per qualche sequenza finita alternata di **g** e **f** nell'espressione $\mathbf{f} \circ \mathbf{g} \circ \mathbf{f} \circ \ldots \circ \mathbf{f}$;

– ogni $b \in B$ tale che $(\mathbf{f} \circ \mathbf{g} \circ \mathbf{f} \circ \mathbf{g} \circ \ldots \circ \mathbf{g})(a) = b_0$ per qualche sequenza finita alternata di **g** e **f** nell'espressione $\mathbf{f} \circ \mathbf{g} \circ \mathbf{f} \circ \mathbf{g} \circ \ldots \circ \mathbf{g}$.

Per ogni $b_0 \in B \setminus \mathbf{f}(A)$, diremo che b_0 è l'*unico antenato* di b_0.

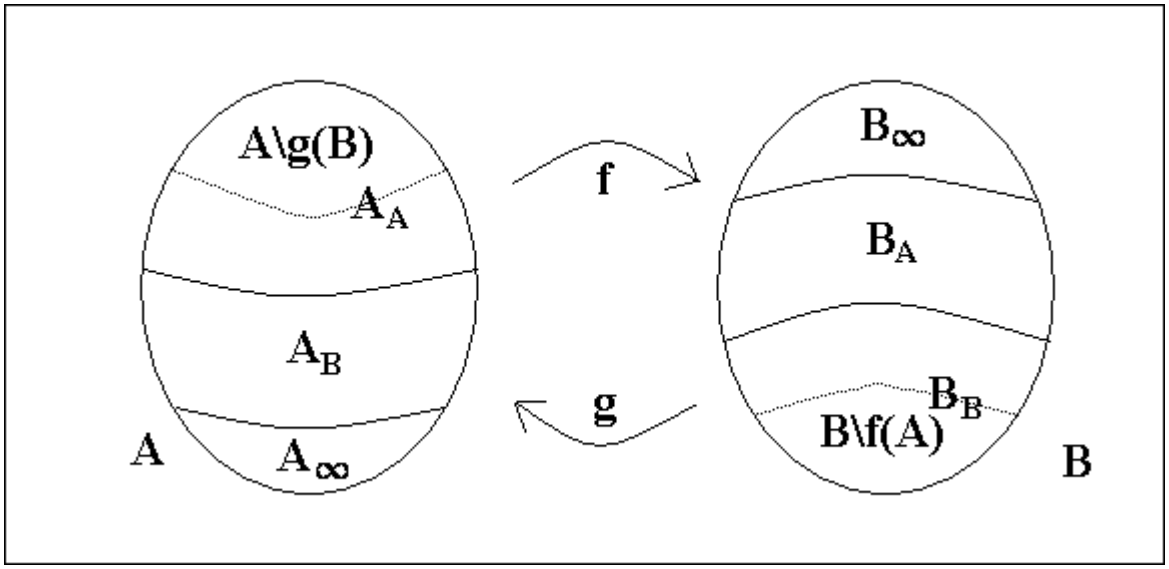
Gli elementi di A vengono così a suddividersi in tre sottoinsiemi:

A_A è l'insieme degli elementi di A che hanno un numero finito di antenati, l'ultimo dei quali appartiene ad $A \setminus \mathbf{g}(B)$;
A_B è l'insieme degli elementi di A che hanno un numero finito di antenati, l'ultimo dei quali appartiene a $B \setminus \mathbf{f}(A)$;
A_∞ è l'insieme degli elementi di A che hanno un numero infinito di antenati.

Ogni elemento di A appartiene a uno e uno solo dei tre sottoinsiemi A_A, A_B e A_∞, che quindi costituiscono una partizione di A.

Analogamente, gli elementi di B vengono a suddividersi in tre sottoinsiemi, che costituiscono una partizione di B:

B_A è l'insieme degli elementi di B che hanno un numero finito di antenati, l'ultimo dei quali appartiene ad $A \setminus \mathbf{g}(B)$;
B_B è l'insieme degli elementi di B che hanno un numero finito di antenati, l'ultimo dei quali appartiene a $B \setminus \mathbf{f}(A)$;
B_∞ è l'insieme degli elementi di A che hanno un numero infinito di antenati.



È facile verificare che $\mathbf{f}(A_A) = B_A$, $\mathbf{g}^{-1}(A_B) = B_B$, $\mathbf{f}(A_\infty) = B_\infty$.

Poiché $B = B_A \cup B_B \cup B_\infty$, la funzione $\mathbf{h}: A \to B$ così definita

$$\mathbf{h}(x) := \begin{cases} \mathbf{f}(x) & \text{se } x \in A_A \text{ oppure } x \in A_\infty \\ \mathbf{g}^{-1}(x) & \text{se } x \in A_B \end{cases}$$

è suriettiva.

Per provare l'asserto, basterà dimostrare che **h** è anche iniettiva. Siano dunque x, $y \in A$ tali che $\mathbf{h}(x) = \mathbf{h}(y)$.

Poiché $\mathbf{f}(A_A) \cap \mathbf{g}^{-1}(A_B) = B_A \cap B_B = \emptyset$, $\mathbf{f}(A_A) \cap \mathbf{f}(A_\infty) = B_A \cap B_\infty = \emptyset$ e $\mathbf{g}^{-1}(A_B) \cap \mathbf{f}(A_\infty) = B_B \cap B_\infty = \emptyset$, i due elementi x, y devono appartenere entrambi ad A_A oppure entrambi ad A_∞ oppure entrambi ad A_B; ma allora l'ipotesi $\mathbf{h}(x) = \mathbf{h}(y)$ significa $\mathbf{f}(x) = \mathbf{f}(y)$ (nei primi due casi) oppure $\mathbf{g}^{-1}(x) = \mathbf{g}^{-1}(y)$ (nel terzo caso), e si può concludere che $x = y$ perché sia **f** che $\mathbf{g}^{-1}$ sono funzioni iniettive.

Siano A, B insiemi. Se A è suvvalente a B, qualsiasi insieme equipotente ad A è suvvalente a qualsiasi insieme equipotente a B; in tal caso scriveremo dunque

$$|A| \preceq |B|$$

senza ambiguità.

Analogamente, se A è strettamente suvvalente a B scriveremo

$$|A| \prec |B| .$$

Con tale notazione, il contenuto del teorema di Schröder-Bernstein-Cantor può essere espresso come segue:

Teorema 4.4.2

Siano A, B insiemi. Si ha

$$|\mathrm{A}| = |\mathrm{B}| \quad \text{se e soltanto se} \quad |\mathrm{A}| \preceq |\mathrm{B}| \preceq |\mathrm{A}| .$$

Teorema 4.4.3 (del confronto fra cardinalità)

Siano A, B insiemi non vuoti. Esiste una funzione iniettiva $\mathrm{A} \to \mathrm{B}$ oppure esiste una funzione iniettiva $\mathrm{B} \to \mathrm{A}$, cioè $\mathrm{A} \preceq \mathrm{B}$ oppure $\mathrm{B} \preceq \mathrm{A}$.

Dimostrazione – Sia $(\mathcal{F}, \subset)$ l'insieme delle funzioni iniettive $\mathrm{A}_1 \to \mathrm{B}$ con $\mathrm{A}_1 \subset \mathrm{A}$ ordinate rispetto all'inclusione ([11]). Poiché A e B non sono vuoti, esistono $a \in \mathrm{A}$ e $b \in \mathrm{B}$, cosicché $\{(a, b)\} \in \mathcal{F}$ e dunque $\mathcal{F}$ non è vuoto.

Ogni catena di $\mathcal{F}$ è superiormente limitata: se $\mathcal{C}$ è una catena di $\mathcal{F}$, $\cup\mathcal{C}$ è una limitazione superiore per $\mathcal{C}$. Posto $\mathbf{f}_0 := \cup\mathcal{C}$, è chiaro infatti che $\mathbf{f} \subset \mathbf{f}_0$ per ogni $\mathbf{f} \in \mathcal{C}$, quindi dobbiamo soltanto verificare che $\mathbf{f}_0$ è una funzione $\overline{\mathrm{A}} \to \mathrm{B}$ per un opportuno $\overline{\mathrm{A}} \subset \mathrm{A}$, e che è iniettiva. Se $\mathbf{f}_0$ non fosse una funzione, esisterebbero $a \in \mathrm{A}$ e $b_1, b_2 \in \mathrm{B}$ tali che $(a, b_1) \in \mathbf{f}_0$ e $(a, b_2) \in \mathbf{f}_0$: per definizione di $\mathbf{f}_0$, dovrebbe essere $(a, b_1) \in \mathbf{f}_1$ e $(a, b_2) \in \mathbf{f}_2$ con $\mathbf{f}_1, \mathbf{f}_2 \in \mathcal{C}$; ma poiché $\mathcal{C}$ è una catena necessariamente $\mathbf{f}_1 \subset \mathbf{f}_2$ oppure $\mathbf{f}_2 \subset \mathbf{f}_1$ e quindi (a, b_1) e (a, b_2) apparterrebbero entrambi a $\mathbf{f}_1$ oppure apparterrebbero entrambi a $\mathbf{f}_2$, impossibile comunque perché sia $\mathbf{f}_1$ che $\mathbf{f}_2$ sono funzioni. Allo stesso modo si vede che $\mathbf{f}_0$ è iniettiva (il lettore è invitato a completare esplicitamente la verifica, quale utile esercizio).

Dunque, per il lemma di Zorn esiste in $\mathcal{F}$ almeno un elemento massimale, cioè esiste una funzione iniettiva $\varphi : \mathrm{A}_0 \to \mathrm{B}$ con $\mathrm{A}_0 \subset \mathrm{A}$ che non può essere estesa a nessuna funzione iniettiva $\mathrm{A}_* \to \mathrm{B}$ con $\mathrm{A}_0 \subsetneq \mathrm{A}_* \subset \mathrm{A}$. Ciò significa che $\mathrm{A}_0 = \mathrm{A}$ oppure che $\varphi(\mathrm{A}_0) = \mathrm{B}$: infatti se esistessero $a \in \mathrm{A} \setminus \mathrm{A}_0$ e $b \in \mathrm{B} \setminus \varphi(\mathrm{A}_0)$ si potrebbe estendere φ ad $\mathrm{A}_0 \cup \{a\}$ ponendo $\varphi(a) := b$. Nel primo caso (cioè se $\mathrm{A}_0 = \mathrm{A}$) φ è una funzione iniettiva $\mathrm{A} \to \mathrm{B}$; nel secondo caso (cioè se $\varphi(\mathrm{A}_0) = \mathrm{B}$) φ^{-1} è una funzione iniettiva $\mathrm{B} \to \mathrm{A}$.

[11] ricordiamo che ogni relazione è un insieme di coppie ordinate!

Teorema 4.4.4 (Cantor)

Per ogni insieme A,

$$|A| \prec |\wp(A)|.$$

Dimostrazione - La funzione che all'elemento x di A associa l'elemento $\{x\}$ di $\wp(A)$ è una corrispondenza biunivoca tra A e un sottoinsieme di $\wp(A)$; dunque, $A \preceq \wp(A)$. Resta da provare che A non è equipotente a $\wp(A)$.

In effetti, non può esistere alcuna funzione suriettiva da A su $\wp(A)$. Sia infatti **f** una funzione $A \to \wp(A)$. Posto

$$X := \{a \in A \,/\, a \notin \mathbf{f}(a)\}$$

non esiste alcun elemento x in A per il quale si abbia $\mathbf{f}(x) = X$. Infatti, per un tale x non potrebbe essere $x \in X$, perché ne seguirebbe $x \notin \mathbf{f}(x) = X$, né $x \notin X$, perché (essendo $X = \mathbf{f}(x)$) ne seguirebbe $x \in X$.

4.5 - Cardinalità dell'unione e del prodotto cartesiano.

Teorema 4.5.1

Se A è un insieme infinito, $|A \times \mathbb{N}| = |A|$.

Dimostrazione - Per il teorema 3.7.3, esiste un buon ordine in A tale che, detto L l'insieme degli elementi limite di A, esiste una corrispondenza biunivoca tra A e $L \times \mathbb{N}$. Dunque

$$|A \times \mathbb{N}| = |(L \times \mathbb{N}) \times \mathbb{N}| = |L \times (\mathbb{N} \times \mathbb{N})| = |L \times \mathbb{N}| = |A|$$

ricordando l'osservazione 1.12.6 e il teorema 4.3.9.

Teorema 4.5.2

Siano A, B insiemi infiniti. Se $A \preceq B$, allora

$$|A \cup B| = |B|.$$

Dimostrazione - Sia **f** una funzione iniettiva da A in B. La funzione che a ogni $x \in A \cup B$ associa la coppia ordinata $(x, 0)$ se $x \in B$ e la coppia ordinata $(\mathbf{f}(x), 1)$ se $x \in A \backslash B$ è una funzione iniettiva da $A \cup B$ in $B \times 2$ (si ricordi la notazione introdotta in 2.2.3). Dunque, ricordando il teorema 4.5.1,

$$|B| \preceq |A \cup B| \preceq |B \times 2| \preceq |B \times \mathbb{N}| = |B|$$

e quindi $|A \cup B| = |B|$ per il teorema 4.4.2.

Teorema 4.5.3

Se A è un insieme infinito, $|A \times A| = |A|$.

Dimostrazione - Per il teorema 4.2.6 esiste in A un sottoinsieme infinito B numerabile, che per il teorema 4.3.9 è equipotente a $B \times B$. Sia $\mathcal{Z}$ l'insieme delle coppie $(B, \mathbf{f})$ con $B \in \wp(A)$ tale che $|B| = |B \times B|$ e $f : B \to B \times B$ biiettiva, ordinato rispetto alla relazione

$$(B_1, \mathbf{f}_1) \leq (B_2, \mathbf{f}_2) \quad \text{sse} \quad B_1 \subset B_2 \quad \text{e} \quad \mathbf{f}_1 \text{ è la restrizione di } \mathbf{f}_2 \text{ a } B_1 .$$

Ogni catena di $\mathcal{Z}$ è maggiorata dall'unione degli insiemi che vi compaiono (con l'unione delle rispettive biiezioni). Pertanto in $\mathcal{Z}$ c'è un elemento massimale $(B_0, \mathbf{f}_0)$.

Se $|B_0| = |A|$, è chiaro che $|A| = |B_0| = |B_0 \times B_0| = |A \times A|$. In caso contrario (è il caso che vogliamo escludere!) $|B_0| \prec |A|$ (perché certamente $|B_0| \preceq |A|$ essendo $B_0 \subset A$). Posto $C := A \backslash B_0$, essendo $A = B_0 \cup C$ con $|B_0| \prec |A|$ deve essere $|C| = |A|$ per il teorema 4.5.2.

La corrispondenza biunivoca che deve esistere fra A e C porta B_0 (sottoinsieme proprio di A) in un sottoinsieme proprio C_0 di C, disgiunto da B_0 (perché $B_0 \cap C = \emptyset$). Poniamo $\overline{B} := B_0 \cup C_0$. Ogni elemento di $\overline{B} \times \overline{B}$ è della forma (x, y) con $x \in B_0 \cup C_0$ e $y \in B_0 \cup C_0$, quindi ci sono quattro possibilità: $x \in B_0$ e $y \in B_0$, $x \in B_0$ e $y \in C_0$, $x \in C_0$ e $y \in B_0$, $x \in C_0$ e $y \in C_0$. In altri termini, $\overline{B} \times \overline{B}$ è l'unione dei quattro insiemi a due a due disgiunti $B_0 \times B_0$, $B_0 \times C_0$, $C_0 \times B_0$ e $C_0 \times C_0$; poiché $B_0 \times C_0$, $C_0 \times B_0$ e $C_0 \times C_0$ sono tutti equipotenti a $B_0 \times B_0$ e dunque a B_0, anche la loro unione è equipotente a B_0 e quindi a C_0. Ciò permette di estendere la corrispondenza biunivoca $\mathbf{f}_0$ che esiste fra B_0 e $B_0 \times B_0$ a una corrispondenza biunivoca fra $\overline{B}$ e $\overline{B} \times \overline{B}$, contro la massimalità di $(B_0, \mathbf{f}_0)$.

Teorema 4.5.4

Siano A, B insiemi infiniti. Se $A \preceq B$, allora

$$|A \times B| = |B| .$$

Dimostrazione - Sia $\mathbf{f}$ una funzione iniettiva da A in B. La funzione che a ogni $(x, y) \in A \times B$ associa la coppia ordinata $(\mathbf{f}(x), y) \in B \times B$ è una funzione iniettiva da $A \times B$ in $B \times B$. Dunque, ricordando il teorema 4.5.3,

$$|B| \preceq |A \times B| \preceq |B \times B| = |B|$$

e quindi $|A \times B| = |B|$ per il teorema 4.4.2.

Teorema 4.5.5

Sia A un insieme infinito. Il prodotto cartesiano di un numero finito di copie di A è equipotente ad A.

Dimostrazione — È una banale applicazione del principio di induzione utilizzando il teorema 4.5.4, e la si lascia al lettore per esercizio.

Teorema 4.5.6

Sia A un insieme infinito. L'insieme $\bigcup_{n\in\mathbb{N}} \mathrm{A}^n$ di tutte le sequenze finite di elementi di A è equipotente ad A .

Dimostrazione – Sia $\mathbf{f}_n$ una corrispondenza biunivoca fra A^n e A (che esiste per il teorema 4.5.5). La funzione che alla sequenza finita σ di lunghezza n associa l'elemento $(\mathbf{f}_n(\sigma), n) \in \mathrm{A} \times \mathbb{N}$ è iniettiva; dunque

$$|\mathrm{A}| \preceq \left|\bigcup_{n\in\mathbb{N}} \mathrm{A}^n\right| \preceq |\mathrm{A} \times \mathbb{N}| = |\mathrm{A}|$$

ricordando il teorema 4.5.1 e il teorema 4.4.2 .

Teorema 4.5.7

Sia A un insieme infinito. L'insieme $\mathcal{F}$ di tutti i sottoinsiemi finiti di A è equipotente ad A .

Dimostrazione – Scelto un buon ordine in A, ogni sottoinsieme finito di A individua la sequenza finita dei propri elementi disposti secondo tale ordine, e sottoinsiemi distinti individuano sequenze distinte. Dunque

$$|\mathrm{A}| \preceq |\mathcal{F}| \preceq \left|\bigcup_{n\in\mathbb{N}} \mathrm{A}^n\right| = |\mathrm{A}|$$

ricordando il teorema 4.5.6 e il teorema 4.4.2 .

Il prossimo teorema, che utilizzeremo nella dimostrazione del teorema 4.5.10, si può considerare una generalizzazione del lemma 4.3.3 .

Teorema 4.5.8

Siano A, B insiemi infiniti. Se

(i) $|\mathrm{A}| \preceq |\mathrm{B}|$

(ii) gli elementi di A sono a due a due disgiunti

e

(iii) $|x| \preceq |\mathrm{B}|$ per ogni $x \in \mathrm{A}$

allora $|\cup \mathrm{A}| \preceq |\mathrm{B}|$.

Dimostrazione - Sia **f** una funzione iniettiva da A in B e per ogni $x \in \mathrm{A}$ sia $\mathbf{g}_x$ una funzione iniettiva da x in B. Allora la funzione $\mathbf{h} : \cup \mathrm{A} \to \mathrm{B} \times \mathrm{B}$ definita per ogni $x \in \mathrm{A}$ e per ogni $y \in x$ da

$$\mathbf{h}(y) := (\mathbf{f}(x), \mathbf{g}_x(y))$$

è iniettiva; poiché il teorema 4.5.3 ci garantisce l'esistenza di una corrispondenza biunivoca **k** tra B × B e B, la composizione $\mathbf{k} \circ \mathbf{h}$ è una funzione iniettiva da $\cup$ A in B che prova l'asserto.

Esercizio 4.5.9

Si provi che l'ipotesi (ii) nell'enunciato del teorema 4.5.8 è superflua, mostrando che per ogni insieme A esiste un insieme A^* tale che

(a) gli elementi di A^* sono a due a due disgiunti;
(b) esiste una corrispondenza biunivoca σ tra A e A^*;
(c) per ogni $x \in A$ esiste una corrispondenza biunivoca δ_x tra x e $\sigma(x)$.

Teorema 4.5.10

Sia $\mathcal{V}$ uno spazio vettoriale. Tutte le basi di $\mathcal{V}$ hanno la stessa cardinalità.

Dimostrazione – Se $\mathcal{V}$ è finitamente generabile, il risultato è ben noto, quindi ci limitiamo al caso in cui $\mathcal{V}$ non è finitamente generabile. Siano B_1 e B_2 basi di $\mathcal{V}$.

Sia **f** la funzione che a ogni elemento di B_1 associa l'insieme (finito, per definizione di base) degli elementi di B_2 di cui è combinazione lineare. Poiché **f**(B_1) è un insieme di sottoinsiemi finiti di B_2, per il teorema 4.5.7

$$|\mathbf{f}(B_1)| \preceq |B_2| .$$

La relazione $\sim$ in B_1 definita da

$$x_1 \sim x_2 \text{ se e soltanto se } \mathbf{f}(x_1) = \mathbf{f}(x_2)$$

è una relazione di equivalenza (la verifica è immediata) e l'insieme quoziente A è equipotente a **f**(B_1). Ogni classe di equivalenza è un sottoinsieme di B_1 della forma $\mathbf{f}^{-1}(y)$ con $y \in \mathbf{f}(B_1)$.

Per ogni $y \in \mathbf{f}(B_1)$, $\mathbf{f}^{-1}(y)$ è un insieme di elementi di B_1 (quindi un insieme libero di vettori) che sono tutti combinazione lineare dell'insieme finito y di vettori, quindi $\mathbf{f}^{-1}(y)$ è un insieme finito (il numero dei suoi elementi è, al massimo, la dimensione dello spazio vettoriale generato da y).

Poiché $B_1 = \cup A$, $|A| = |\mathbf{f}(B_1)| \preceq |B_2|$ e ogni elemento di A è finito (quindi è certamente suvvalente a B_2) possiamo applicare il teorema 4.5.8 per concludere che

$$|B_1| \preceq |B_2| .$$

Ma questo ragionamento si può ripetere scambiando il ruolo di B_1 con quello di B_2 per concludere che è anche $|B_2| \preceq |B_1|$ e infine $|B_1| = |B_2|$ per il teorema 4.4.2.

4.6 - Ancora sulle cardinalità di $\mathbb{N}$ e $\mathbb{R}$.

Teorema 4.6.1

$\mathbb{N}$ non è equipotente all'intervallo aperto $(0,1)$ di $\mathbb{R}$.

Dimostrazione – Dimostriamo che qualsiasi funzione $\mathbf{f}:\mathbb{N}\to(0,1)$ non può essere suriettiva.

È noto che ogni numero reale nell'intervallo $(0,1)$ ha una rappresentazione (detta "decimale") data dalla cifra "0" seguita da una virgola e da una successione (c_n) di cifre nell'insieme $\{0,1,2,3,4,5,6,7,8,9\}$ (la cifra c_i si dice "$i-$sima cifra decimale" del numero); tale rappresentazione è unica se escludiamo che possa esistere $n_0\in\mathbb{N}$ tale che $c_n=0$ per $n>n_0$.

Sia α il numero reale dell'intervallo $(0,1)$ la cui $n-$sima cifra decimale è:

4, se l'n-sima cifra decimale di $\mathbf{f}(n)$ è 7; 7, nel caso contrario.

Poiché α differisce da $\mathbf{f}(n)$ (nella n-sima cifra decimale) per ogni $n\in\mathbb{N}$, $\alpha\notin\mathbf{f}(\mathbb{N})$ e si è così dimostrato che **f** non è suriettiva, come si voleva.

Teorema 4.6.2

$\mathbb{N}\prec\mathbb{R}$.

Dimostrazione - Poiché, come è ben noto, $\mathbb{N}\preceq\mathbb{R}$, per il teorema 4.4.1 basterà provare che $\mathbb{R}\not\preceq\mathbb{N}$.

Supponiamo, per assurdo, che sia $\mathbb{R}\preceq\mathbb{N}$. La funzione che a ogni numero naturale maggiore di 0 associa il suo reciproco (e allo zero associa $\frac{2}{3}$) è una funzione iniettiva da $\mathbb{N}$ nell'intervallo $(0,1)\subset\mathbb{R}$: dunque $\mathbb{N}\preceq(0,1)$. Ovviamente, l'immersione dell'intervallo $(0,1)$ in $\mathbb{R}$ è una funzione iniettiva dalla quale segue che $(0,1)\preceq\mathbb{R}$; allora si avrebbe che

$$\mathbb{N}\preceq(0,1)\preceq\mathbb{R}\preceq\mathbb{N}\qquad\text{da cui}\qquad|\mathbb{N}|=|(0,1)|$$

contro il teorema 4.6.1.

Osservazione 4.6.3

Non è difficile osservare che l'intervallo $(0,1)$ è equipotente a $\mathbb{R}$. Ad esempio, si può notare che la funzione

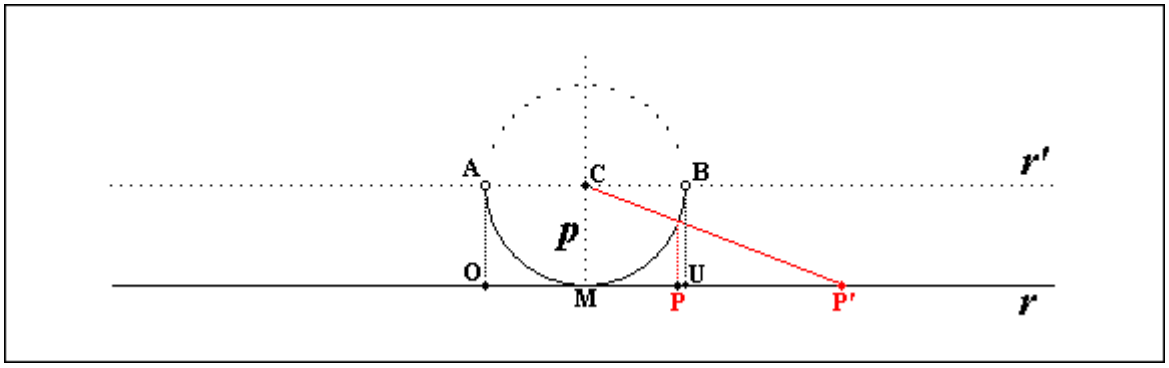
$$\mathbf{f}(x)=\pi x-\tfrac{\pi}{2}$$

è una corrispondenza biunivoca tra $(0,1)$ e $(-\frac{\pi}{2},\frac{\pi}{2})$; d'altro lato, è noto dallo studio della trigonometria che la restrizione a $(-\frac{\pi}{2},\frac{\pi}{2})$ della funzione $\mathbf{tg}(x)$ ("tangente trigonometrica") è una funzione crescente (quindi iniettiva) che ha per immagine $\mathbb{R}$. Dunque la composizione di queste due funzioni (cioè $\mathbf{tg}(\pi x-\frac{\pi}{2})$ è una corrispondenza biunivoca tra $(0,1)$ e $\mathbb{R}$.

Si può anche dare una suggestiva dimostrazione "geometrica" di questo fatto, che però dipende da un famoso risultato che lega la struttura geometrica della retta euclidea alla struttura algebrica di $\mathbb{R}$:

> Esiste una corrispondenza biunivoca φ tra l'insieme $\mathcal{R}$ dei punti di una retta r e l'insieme $\mathbb{R}$ dei numeri reali. Fissati in $\mathcal{R}$ due punti **O** (*origine*) e **U** (*punto unità*), φ resta univocamente determinata dalle condizioni
>
> (i) $\varphi(\mathbf{O}) = 0$;
>
> (ii) $\varphi(\mathbf{U}) = 1$;
>
> (iii) comunque presi $\mathbf{P_1}$, $\mathbf{P_2} \in \mathcal{R}$, il segmento $\overline{\mathbf{P_1P_2}}$ ha misura $|\varphi(\mathbf{P_1}) - \varphi(\mathbf{P_2})|$ rispetto all'unità di misura $\overline{\mathbf{OU}}$.
>
> Una corrispondenza biunivoca fra $\mathcal{R}$ e $\mathbb{R}$ che verifichi queste condizioni (i), (ii) e (iii) si dice un *sistema di riferimento cartesiano* su $\mathcal{R}$, e resta completamente individuata dalla scelta dei punti **O** e **U**.

Siano allora r una retta assegnata, **O** un punto origine e **U** un punto unità fissati su r; sia **M** il punto medio del segmento $\overline{\mathbf{OU}}$, sia p la retta perpendicolare a r passante per **M**, sia **C** un punto di p avente distanza 1 da **M**, sia r' la retta per **C** parallela a r, sia $\mathcal{C}$ la circonferenza di centro **C** e raggio 1 e siano **A**, **B** le intersezioni di $\mathcal{C}$ con r'. Sia $\mathcal{C}_1$ la semicirconferenza di estremi A, B passante per M.



Sia π_0 la proiezione ortogonale di $\mathcal{C}_1$ su r, e sia $\pi_{\mathbf{C}}$ la proiezione di $\mathcal{C}_1$ su r dal punto **C**. La composizione $\pi_{\mathbf{C}} \circ \pi_0^{-1}$ è una corrispondenza biunivoca tra il segmento $\overline{\mathbf{OU}}$ (estremi esclusi) e r; la $\varphi \circ \pi_{\mathbf{C}} \circ \pi_0^{-1} \circ \varphi^{-1}$ è dunque una corrispondenza biunivoca tra l'intervallo aperto (0, 1) e $\mathbb{R}$.

Sia A un insieme. Se A è equipotente a $\mathbb{R}$, diremo che A *ha la cardinalità del continuo* ([12]) e scriveremo $|A| = c$.

[12] o anche, in omaggio alla tradizione, *la potenza del continuo*.

Il contenuto del teorema 4.6.2 suggerisce la seguente domanda: esiste un insieme A tale che $\mathbb{N} \prec \mathrm{A} \prec \mathbb{R}$? L'ipotesi che un tale insieme non esista è nota come *ipotesi del continuo*. Nel 1940 Kurt Gödel (1906-1978) dimostrò che l'ipotesi del continuo è compatibile con il sistema di assiomi di Zermelo e Fränkel, anche comprendendo in esso l'assioma della scelta. Nel 1963 Paul Cohen (1934-2007) dimostrò che anche l'esistenza di un insieme A tale che $\mathbb{N} \prec \mathrm{A} \prec \mathbb{R}$ è compatibile con il sistema di assiomi di Zermelo e Fränkel allargato all'assioma della scelta.

Teorema 4.6.4

L'insieme $\mathcal{I}$ dei sottoinsiemi infiniti propri di $\mathbb{N}$ ha la cardinalità del continuo.

Dimostrazione – Per l'osservazione 4.6.3, basterà dimostrare che $\mathcal{I}$ è equipotente all'intervallo $(0, 1)$.

Si è già osservato nella dimostrazione del teorema 4.6.1 che ogni numero reale nell'intervallo $(0, 1)$ ha una rappresentazione (detta "decimale") data dalla cifra "0" seguita da una virgola e da una successione (c_n) di cifre nell'insieme $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ (la cifra c_i si dice "$i-$sima cifra decimale" del numero); tale rappresentazione è unica se escludiamo che possa esistere $n_0 \in \mathbb{N}$ tale che $c_n = 0$ per $n > n_0$. Di fatto, la scelta delle cifre nell'insieme dei numeri naturali da 1 a 9 è dovuta soltanto a motivi storici (legati alle nostre abitudini di calcolo); le cifre possono essere scelte in qualsiasi insieme $\{0, \ldots, s\}$ con $s \geq 2$.

In particolare, si può scegliere $s = 2$; si parla in tal caso di "rappresentazione binaria" del numero. Per ottenere l'unicità della rappresentazione, si deve anche in questo caso escludere che possa esistere $n_0 \in \mathbb{N}$ tale che $c_n = 0$ per $n > n_0$.

Sia dunque I un sottoinsieme infinito di $\mathbb{N}$; associamo a I quel numero reale nell'intervallo $(0, 1)$ la cui $(i + 1) -$ sima cifra nella rappresentazione binaria 1 se e solo se $i \in$ I. Si costruisce così, come si voleva, una corrispondenza biunivoca tra $\mathcal{I}$ e il sottoinsieme $(0, 1)$ di $\mathbb{R}$.

Teorema 4.6.5

$|\wp(\mathbb{N})| = c$.

Dimostrazione - Sia $\mathcal{F}(\mathbb{N})$ l'insieme dei sottoinsiemi finiti di $\mathbb{N}$, e sia $\mathcal{I}(\mathbb{N})$ l'insieme dei sottoinsiemi propri infiniti di $\mathbb{N}$. Si ha

$$\wp(\mathbb{N}) = \mathcal{F}(\mathbb{N}) \cup \mathcal{I}(\mathbb{N}) \cup \{\mathbb{N}\}.$$

Per il teorema 4.5.2, è sufficiente [13] osservare che $|\mathcal{F}(\mathbb{N})| = \aleph_0$ (per il teorema 4.3.8) e $|\mathcal{I}(\mathbb{N})| = c$ (per il teorema 4.6.4).

[13] Infatti, se $\mathcal{F}(\mathbb{N})$ è equipotente a $\mathbb{N}$ che è incluso in $\mathbb{R}$ che è equipotente a $\mathcal{I}(\mathbb{N})$, è chiaro che $\mathcal{I}(\mathbb{N})$ domina $\mathcal{F}(\mathbb{N})$.

Per il teorema 4.6.5, l'ipotesi del continuo si può esprimere dicendo che: non esiste alcun insieme A tale che $\mathbb{N} \prec A \prec \wp(\mathbb{N})$.

L'*ipotesi generalizzata del continuo* afferma che: per nessun insieme infinito X esiste un insieme A tale che $X \prec A \prec \wp(X)$ (si veda anche il teorema 4.4.4).

Teorema 4.6.6

L'insieme $\mathbb{C}$ dei numeri complessi ha la cardinalità del continuo.
In particolare, $|\mathbb{C}| = c$ (infatti la funzione che al numero complesso $a + b\boldsymbol{i}$ associa la coppia ordinata (a, b) è una corrispondenza biunivoca tra $\mathbb{C}$ e $\mathbb{R} \times \mathbb{R}$).

Dimostrazione - La funzione che al numero complesso $a + b\boldsymbol{i}$ associa la coppia ordinata (a, b) è una corrispondenza biunivoca tra $\mathbb{C}$ e $\mathbb{R} \times \mathbb{R}$. L'asserto segua dunque immediatamente dal teorema 4.5.4.

5.- EQUISEZIONABILITÀ NEL PIANO

5.1 - Definizione.

Sia $\mathcal{P}$ l'insieme dei punti del piano euclideo, e siano A, B $\subset \mathcal{P}$. Si dice che A è *equisezionabile con* B *in* n *parti* (oppure che A e B sono *equisezionabili in* n *parti*) se esistono n poligoni $A_1, A_2, \ldots, A_n$ contenuti in A, n poligoni $B_1, B_2, \ldots, B_n$ contenuti in B e n isometrie del piano $\sigma_1, \sigma_2, \ldots, \sigma_n$ tali che

(i) $\quad A = \bigcup_{i=1}^{n} A_i$, $\qquad A_i \cap A_j$ è un segmento per ogni i e j con $1 \leq i, j \leq n$;

(i) $\quad B = \bigcup_{i=1}^{n} B_i$, $\qquad B_i \cap B_j$ è un segmento per ogni i e j con $1 \leq i, j \leq n$;

(iii) $\quad \sigma_i(A_i) = B_i$ per $i := 1, 2, \ldots, n$.

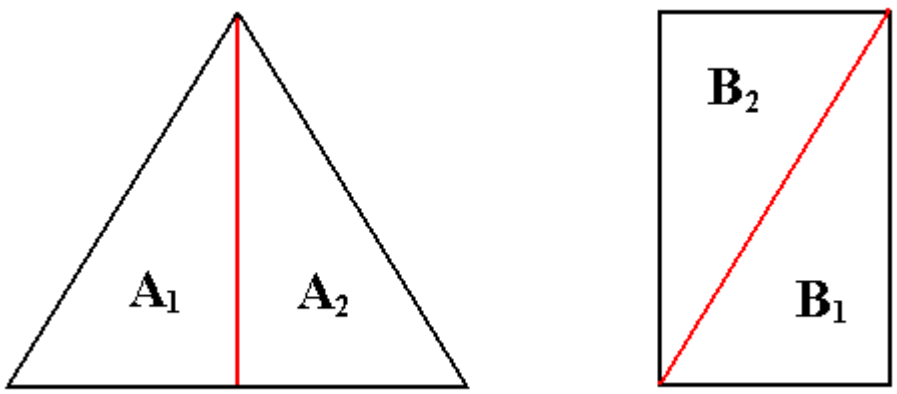
Siano A, B insiemi di punti del piano euclideo. Si dice che A *è equisezionabile con* B (oppure che A, B *sono equisezionabili*) se esiste $n \in \mathbb{N}$ tale che A e B sono equisezionabili in n parti. È facile (davvero… !) verificare che la relazione ϱ definita in $\wp(\mathcal{P})$ ponendo

$$A \varrho B \quad \text{se e soltanto se} \quad A \text{ è equisezionabile con } B$$

è una relazione di equivalenza in $\wp(\mathcal{P})$.

Esempio 5.1.1

Un triangolo isoscele A e un rettangolo B equisezionabili in due parti. Si noti che i segmenti $A_1 \cap A_2$ e $B_1 \cap B_2$ non sono congruenti.



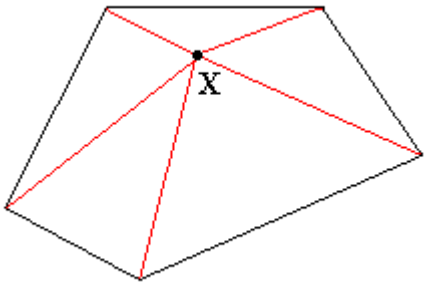
5.2 - Alcuni risultati sull'equisezionabilità.

Teorema 5.2.1

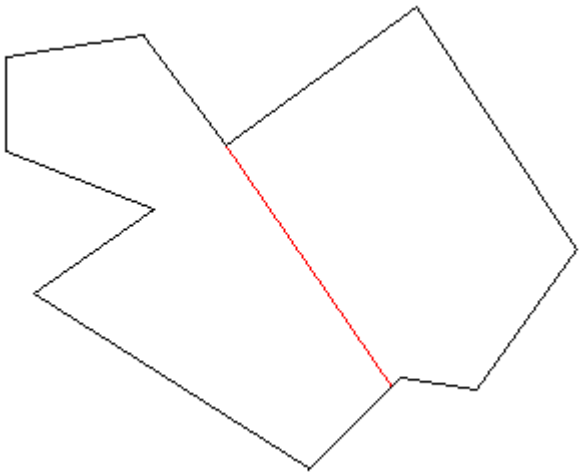
Ogni poligono è equisezionabile con l'unione di un numero finito di triangoli.

Dimostrazione - Si procede per induzione sul numero n di angoli interni concavi del poligono $\mathcal{P}$.

Se $n = 0$, il poligono $\mathcal{P}$ è convesso, quindi congiungendo un qualsiasi punto X interno a $\mathcal{P}$ con ciascun vertice di $\mathcal{P}$ si ha una equisezione di $\mathcal{P}$ con una unione di triangoli.



Supposto vero l'asserto per tutti i poligoni con meno di n angoli interni concavi, sia ora $\mathcal{P}$ un poligono che possiede n angoli interni concavi, e sia ABC uno di essi. Prolungando il lato AB fino a incontrare il bordo di $\mathcal{P}$, si ha una equisezione di $\mathcal{P}$ con l'unione di due poligoni ciascuno dei quali ha meno di n angoli interni concavi e quindi, per l'ipotesi di induzione, è equisezionabile con una unione di triangoli.

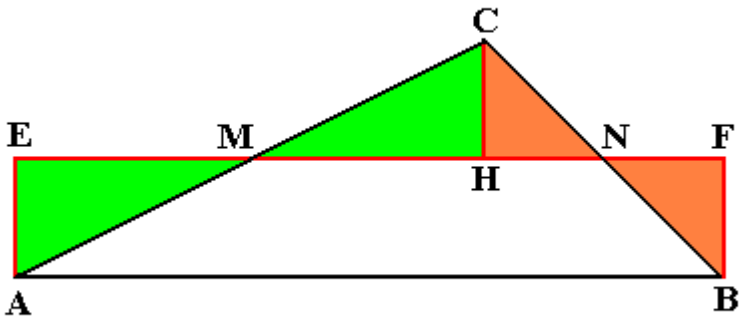


Per la transitività della relazione di equisezionabiltà, anche $\mathcal{P}$ è equisezionabile con una unione di triangoli.

Teorema 5.2.2

Ogni triangolo è equisezionabile con un rettangolo.

Dimostrazione - Sia ABC il triangolo dato, e supponiamo che AB ne sia il lato maggiore (cosicché l'eventuale angolo ottuso è quello con vertice in C). Siano M, N rispettivamente i punti medi dei lati AC e CB, cosicché la retta MN è parallela al lato AB; siano rispettivamente E, H e F le proiezioni ortogonali di A, B e C sulla retta MN.



Il quadrilatero ABFE è un rettangolo perché le rette AE e BF, essendo per costruzione ortogonali alla retta MN, sono ortogonali anche alla retta AB (perché questa, come si è osservato, è parallela alla MN). Tale rettangolo è equisezionabile con il triangolo dato perché

– il trapezio ABNM è comune al triangolo e al rettangolo;

– i triangoli AEM e MHC sono congruenti in quanto triangoli rettangoli (per costruzione) con AM = MC (per costruzione di M) e gli angoli AME e CMH congruenti perché opposti al vertice;

– i triangoli CHN e BFN sono congruenti in quanto triangoli rettangoli (per costruzione) con CN = NB (per costruzione di N) e gli angoli HNC e BNF congruenti perché opposti al vertice.

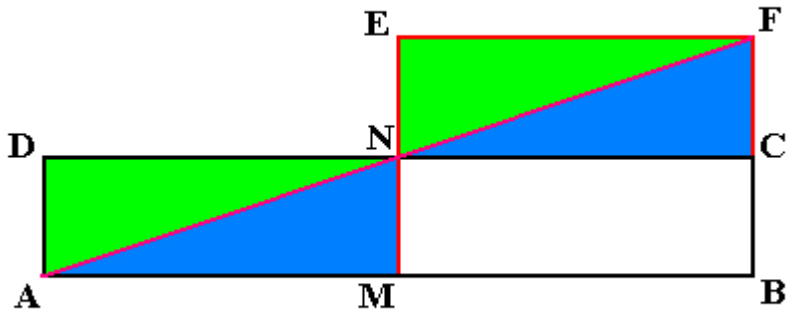
Teorema 5.2.3

Ogni rettangolo è equisezionabile con un rettangolo in cui il rapporto tra base e altezza è compreso tra 1 e 4.

Dimostrazione - Per ogni rettangolo, possiamo scegliere base e altezza in modo che il loro rapporto sia maggiore o uguale a 1; ed esiste certamente un numero naturale n tale che quel rapporto non è superiore a n. Proviamo, per induzione su n, che: se nel rettangolo ABCD il rapporto fra la base AB e l'altezza BC (è maggiore o uguale a 1 e) non supera n, allora ABCD è equisezionabile con un rettangolo in cui il rapporto fra base e altezza (è maggiore o uguale a 1 e) non è superiore a 4.

Se $n \leq 4$, l'asserto è ovvio; possiamo allora supporre che l'asserto sia vero per ogni rettangolo in cui il rapporto fra base e altezza (è maggiore o uguale a 1 e) non è superiore a $n-1$ e dimostrarlo per un rettangolo ABCD nel quale il rapporto fra base e altezza (è maggiore o uguale a 1 e) non è superiore a n (ma è superiore a 4).

Detti M il punto medio della base AB e N il punto medio del lato opposto DC, sia E $\neq$ M l'altro punto della retta MN tale che MN = NE, sia r la retta per E parallela alla retta AB e sia F il punto in cui r incontra la retta BC.



Il rettangolo ABCD è equisezionabile (in tre parti) col rettangolo MBFE: infatti i triangoli AMN e NCF sono congruenti perché (per costruzione) triangoli rettangoli coi cateti congruenti; e così sono congruenti i triangoli NDA e FEN. Nel rettangolo MBFE la base è la metà della base di ABCD, mentre l'altezza è il doppio dell'altezza di ABCD, quindi il rapporto fra base e altezza è un quarto di quello che era in ABCD; poiché in ABCD tale rapporto era superiore a 4 ma non superiore a n, in MBFE esso è superiore a 1 ma non superiore a $\frac{n}{4}$ che a sua volta è minore di $n-1$ (se fosse $\frac{n}{4} \geq n-1$ ne seguirebbe che $n \geq 4n-1$ ossia $3n \leq 1$ contro l'ipotesi che $4 < n$).

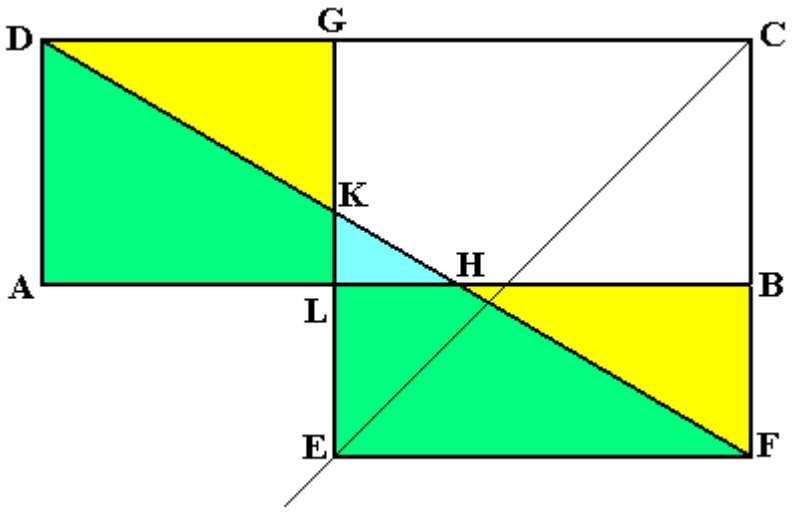
Dunque, per l'ipotesi di induzione, il rettangolo MBFE è equisezionabile con un rettangolo in cui il rapporto tra base e altezza è compreso tra 1 e 4. Per la proprietà transitiva dell'equisezionabilità, anche ABCD è equisezionabile con un rettangolo in cui il rapporto tra base e altezza è compreso tra 1 e 4. L'asserto è così completamente provato.

Teorema 5.2.4

Ogni rettangolo è equisezionabile con un quadrato.

Dimostrazione - Per il teorema 5.2.3, e per la transitività della relazione di equisezionabilità, possiamo supporre che nel rettangolo dato il rapporto tra base e altezza sia compreso tra 1 e 4.

Sia ABCD il rettangolo dato, con base AB di misura b e altezza BC di misura h. Sulla bisettrice dell'angolo retto BCD scegliamo un punto E in modo che sia $EC = \sqrt{2bh}$; dette rispettivamente F e G le proiezioni ortogonali di E sulla retta CB e sulla retta CD, vogliamo dimostrare che il rettangolo ABCD è equisezionabile col quadrato EFCG (di lato $\ell := \sqrt{bh}$).



La retta DF incontra il lato AB in un punto H; infatti essa incontra la retta AB perché D e F sono situati in semipiani opposti rispetto a tale retta, e deve incontrarla in un punto della striscia di piano individuata dalle rette AD e BC: tale striscia di piano infatti è un insieme convesso perché intersezione di due insiemi convessi (il semipiano individuato dalla retta AD contenente la retta BC e il semipiano individuato dalla retta BC contenente la retta AB).

Con ragionamento analogo si vede che la retta DF incontra il segmento EG in un punto K; infatti essa incontra la retta EG perché D e F sono situati in semipiani opposti rispetto a tale retta, e deve incontrarla in un punto della striscia di piano individuata dalle rette DC ed EF: tale striscia di piano infatti è un insieme convesso perché intersezione di due insiemi convessi (il semipiano individuato dalla retta DC contenente la retta EF e il semipiano individuato dalla retta EF contenente la retta DC). Ma noi vogliamo mostrare che il punto K appartiene al segmento GL (essendo L l'intersezione fra il lato AB del rettangolo e il lato EG del quadrato). Basta osservare che il triangolo DGK è simile al triangolo DCF: essi infatti sono triangoli rettangoli che hanno in comune l'angolo in D. Ne segue che

$$GK : GD = CF : CD$$

ossia, passando alle misure (e indicando con x la misura di GK), che

$$x : b - \ell \ = \ell : b$$

da cui

$$bx = (b - \ell)\ell = b\ell - \ell^2 = b\ell - bh$$

e quindi, dividendo per b ambo i membri

$$x = \ell - h = \sqrt{bh} \ - h \leq \sqrt{4h^2} \ - h = 2h - h = h$$

essendo per ipotesi $b \leq 4h$: ciò prova che il punto K giace all'interno del segmento GL .

I triangoli AHD e FCD sono simili, perché triangoli rettangoli con gli angoli acuti congruenti (l'angolo AHD è congruente all'angolo FDC perché alterni interni rispetto alle parallele AB e CD tagliate dalla trasversale DH; l'angolo ADH è congruente all'angolo DFC perché alterni interni rispetto alle parallele AD e FC tagliate dalla trasversale DF). In particolare i lati opposti agli angoli congruenti sono proporzionali:

$\mathrm{CF} : \mathrm{AD} = \mathrm{CD} : \mathrm{AH}$ ossia $\sqrt{bh} : h = b : \mathrm{AH}$ e quindi $\mathrm{AH} = \sqrt{bh}$.

I triangoli AHD e EFK sono allora congruenti, perché entrambi rettangoli (per costruzione) e inoltre: l'angolo ADH è congruente all'angolo EKF perché corrispondenti rispetto alle parallele AD e EG tagliate dalla trasversale DK; $\mathrm{AH} = \sqrt{bh} = \mathrm{EF}$.

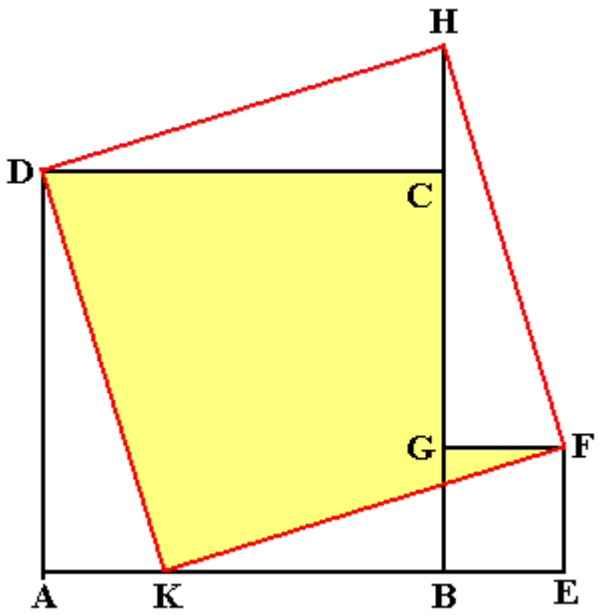
In particolare, $\mathrm{AD} = \mathrm{EK} = h$ e quindi $\mathrm{GK} = \mathrm{EG} - \mathrm{EK} = \sqrt{bh} \ - h = \mathrm{BF}$. Se ne deduce che anche i triangoli rettangoli KGD e FBH sono congruenti: infatti l'angolo GDK è congruente all'angolo BHF perché corrispondenti rispetto alle parallele AB e CD tagliate dalla trasversale DF . Si conclude che il rettangolo ABCD ($= \mathrm{DAH} \cup \mathrm{DKG} \cup \mathrm{GKHBC}$) è equisezionabile col quadrato EFCG ($= \mathrm{KEF} \cup \mathrm{HFB} \cup \mathrm{GKHBC}$) .

Teorema 5.2.5

Sia n un numero intero positivo. L'unione di n quadrati è equisezionabile con un quadrato.

Dimostrazione - Basta provare l'asserto per $n := 2$ e poi procedere per induzione su n utilizzando la proprietà transitiva della relazione di equisezionabilità.

Siano allora ABCD e BEFG due quadrati: senza perdere in generalità, possiamo supporre che il lato AB del primo quadrato sia maggiore o uguale al lato BE del secondo quadrato, che i lati AB e BE siano consecutivi sulla stessa retta e che il vertice G del secondo quadrato apparenga al lato BC del primo quadrato (eventualmente $\mathrm{G} = \mathrm{C}$). Scegliamo un punto K sul lato AB in modo che AK sia congruente a BE (eventualmente $\mathrm{K} = \mathrm{B}$), e un punto H sul prolungamento del lato BC in modo che CH sia congruente a BE: i quattro triangoli rettangoli DAK, KEF, FGH e DCH sono tutti congruenti fra loro perché hanno i cateti, per costruzione, congruenti ai lati AB e BE dei due quadrati ABCD e BEFG. Dunque l'unione dei due quadrati ABCD e BEFG ($= \mathrm{DAK} \cup \mathrm{KEF} \cup \mathrm{DKFGC}$) è equisezionabile col quadrato KFHD ($= \mathrm{HGF} \cup \mathrm{DCH} \cup \mathrm{DKFGC}$).



Teorema 5.2.6

Ogni poligono è equisezionabile con un quadrato.

Dimostrazione - Sia $\mathcal{P}$ un poligono. Per il teorema 5.2.1, $\mathcal{P}$ è equisezionabile con l'unione di un numero finito di triangoli, ciascuno dei quali (per il teorema 5.2.2) è equisezionabile con un rettangolo e dunque (per il teorema (5.2.4) con un quadrato.

Pertanto $\mathcal{P}$ è equisezionabile con l'unione di un numero finito di quadrati e quindi (per il teorema 5.2.5) con un quadrato.

5.3 - Equisezionabilità e superficie.

L'idea intuitiva che sta alla base della definizione di equisezionabilità è che figure equisezionabili abbiano la stessa superficie. Ammettendo questa idea, possiamo però affermare che vale il viceversa, almeno per i poligoni? Cioè: poligoni che hanno la stessa superficie sono necessariamente equisezionabili?

Se accettiamo anche il fatto (ragionevole) che quadrati con la stessa superficie devono essere congruenti, la risposta è affermativa. Infatti nella sezione precedente abbiamo visto che ogni poligono è equisezionabile con un quadrato: dunque, poligoni con la stessa superficie devono essere equisezionabili con quadrati congruenti e quindi equisezionabili fra loro.

In altre parole: se la *superficie* di un poligono è una proprietà tale che

(i) poligoni equisezionabili hanno la stessa superficie

(ii) due quadrati con la stessa superficie sono congruenti

allora i teoremi della sez. 5.2 provano che due poligoni hanno la stessa superficie se e solo se sono equisezionabili.

6.- EQUISCOMPONIBILITÀ NELLO SPAZIO: IL TEOREMA DI BANACH-TARSKI

Both Banach and Tarski were Poles
with anti-euclidean goals.
They proved, so I hear,
the parts of a sphere
to equal a couple of wholes.

Craig Smoryński

6.1 - Richiami sulle azioni di un gruppo.

Siano G un gruppo e Ω un insieme. Si dice *azione di* G *su* Ω un omomorfismo di G nel gruppo Sym(Ω) di tutte le permutazioni su Ω. Se è data un'azione di G su Ω, si dice anche che G *opera su* Ω (mediante la data azione).

Nel seguito adotteremo sistematicamente la "notazione esponenziale": se è data un'azione del gruppo G sull'insieme Ω, scriveremo sempre ω^g per indicare l'immagine di ω mediante la permutazione associata a $g \in \mathrm{G}$.

Siano G un gruppo e Ω un insieme, e sia data un'azione di G su Ω. Un elemento ω di Ω si dice un *punto fisso* per la data azione di G su Ω se $\omega^g = \omega$ per ogni $g \in \mathbf{G}$.

Teorema 6.1.1

Siano G un gruppo e Ω un insieme, e sia data un'azione di G su Ω. La relazione $\sim$ in Ω definita da

$$\omega_1 \sim \omega_2 \quad \Leftrightarrow \quad \text{esiste } g \in \mathrm{G} \text{ tale che } \omega_1^g = \omega_2$$

è una relazione di equivalenza in Ω.

Dimostrazione – La $\sim$ è riflessiva perché $\omega^{1_\mathrm{G}} = \omega$ per ogni $\omega \in \Omega$; è simmetrica perché se $\omega_1 \sim \omega_2$ esiste $g \in \mathrm{G}$ tale che $\omega_1^g = \omega_2$ e quindi $\omega_1 = (\omega_1^g)^{g^{-1}} = \omega_2^{g^{-1}}$ ossia $\omega_2 \sim \omega_1$; ed è transitiva perché se $\omega_1 \sim \omega_2$ e $\omega_2 \sim \omega_3$ esistono $g, h \in \mathrm{G}$ tali che $\omega_1^g = \omega_2$ e $\omega_2^h = \omega_3$ cosicché $\omega_1^{gh} = (\omega_1^g)^h = \omega_2^h = \omega_3$ ossia $\omega_1 \sim \omega_3$.

Siano G un gruppo e Ω un insieme, e sia data un'azione di G su Ω. Le classi di equivalenza individuate in Ω dalla relazione di equivalenza $\sim$ considerata nel teorema 6.1.1 si dicono le *orbite* dell'azione di G su Ω. Se $\omega \in \Omega$, l'orbita dell'azione di G su Ω a cui appartiene ω si indica con $O_G(\omega)$.

Osservazione 6.1.2

Siano G un gruppo e Ω un insieme, e sia data un'azione di G su Ω. Le orbite dell'azione di G su Ω sono una partizione di Ω.

Siano G un gruppo e Ω un insieme, e sia data un'azione di G su Ω. Se $\omega \in \Omega$, si dice *stabilizzatore di* ω *in* G (rispetto alla data azione di G su Ω) l'insieme

$$G_\omega := \{g \in G / \omega^g = \omega\}.$$

Teorema 6.1.3

Siano G un gruppo e Ω un insieme, e sia data un'azione di G su Ω. Per ogni $\omega \in \Omega$, lo stabilizzatore in G di ω è un sottogruppo di G.

Dimostrazione – Sia $\omega \in \Omega$; Poiché certamente $1_G \in G_\omega$, e quindi G_ω non è vuoto, possiamo dimostrare che G_ω è un sottogruppo di G verificando che è chiuso rispetto al prodotto e all'inverso. Siano $g_1, g_2 \in G_\omega$ (cosicché $\omega^{g_1} = \omega^{g_2} = \omega$); allora $\omega^{g_1 g_2} = (\omega^{g_1})^{g_2} = \omega^{g_2} = \omega$, ossia $g_1 g_2 \in G_\omega$. Infine, se $g \in G_\omega$ (cosicché $\omega^g = \omega$) si ha $\omega = \omega^{1_G} = \omega^{g g^{-1}} = (\omega^g)^{g^{-1}} = \omega^{g^{-1}}$ cioè $g^{-1} \in G_\omega$ come si voleva.

Teorema 6.1.4

Siano G un gruppo e Ω un insieme, e sia data un'azione di G su Ω. Per ogni $\omega \in \Omega$, la cardinalità dell'orbita a cui appartiene ω è uguale all'indice in G dello stabilizzatore in G di ω.

Dimostrazione – Si tratta di dimostrare che c'è una corrispondenza biunivoca fra l'insieme delle classi laterali destre di G_ω in G e l'orbita a cui appartiene ω.

Se $g \in G$, poniamo

$$\varphi(G_\omega g) := \omega^g$$

e dimostriamo che φ è ben definita, è iniettiva ed è suriettiva.

Per dimostrare che φ è ben definita, supponiamo che sia $G_\omega x = G_\omega y$ con $x, y \in G$ e proviamo che $\omega^x = \omega^y$. In effetti, poiché $G_\omega x = G_\omega y$ si ha $xy^{-1} \in G_\omega$ ossia $\omega^{xy^{-1}} = \omega$ da cui $\omega^x = \omega^{(xy^{-1}y)} = \left(\omega^{xy^{-1}}\right)^y = \omega^y$ come si voleva.
Per dimostrare che φ è iniettiva, supponiamo che sia $\varphi(G_\omega x) = \varphi(G_\omega y)$ con $x, y \in G$ e proviamo che $G_\omega x = G_\omega y$. Per definizione di φ, se $\varphi(G_\omega x) = \varphi(G_\omega y)$ si ha $\omega^x = \omega^y$ e dunque

$$\omega^{(xy^{-1})} = \left(\omega^x\right)^{y^{-1}} = \left(\omega^y\right)^{y^{-1}} = \omega^{(yy^{-1})} = \omega^{1_G} = \omega$$

ossia $xy^{-1} \in G_\omega$; ciò prova, come si voleva, che $G_\omega x = G_\omega y$.
È infine immediato che φ è suriettiva: ogni elemento dell'orbita di ω è infatti della forma ω^g per un opportuno $g \in G$, e quindi proviene mediante φ da $G_\omega g$.

6.2 - Alcune possibili azioni di un gruppo su se stesso.

Ci sono alcuni modi standard per fare operare un gruppo su se stesso. Vale la pena di ricordare i più famosi, soprattutto perché uno di essi ci servirà in seguito.

Sia G un gruppo.

Si dice che G opera su se stesso *mediante traslazione* se per ogni $g \in G$ la permutazione associata a g è quella che porta l'elemento x di G nell'elemento xg, cioè se (nella notazione esponenziale che abbiamo dichiarato di adottare) per ogni $g \in G$

$$x^g := xg \quad \text{per ogni } x \in G.$$

Si dice che G opera su se stesso *mediante traslazione inversa* se per ogni $g \in G$ la permutazione associata a g è quella che porta l'elemento x di G nell'elemento $g^{-1}x$, cioè se (nella notazione esponenziale che abbiamo dichiarato di adottare) per ogni $g \in G$

$$x^g := g^{-1}x \quad \text{per ogni } x \in G.$$

Si dice che G opera su se stesso *mediante il coniugio* se per ogni $g \in G$ la permutazione associata a g è quella che porta l'elemento x di G nell'elemento $g^{-1}xg$, cioè se (nella notazione esponenziale che abbiamo dichiarato di adottare) per ogni $g \in G$

$$x^g := g^{-1}xg \quad \text{per ogni } x \in G.$$

Si lascia al lettore l'utile (e facile) esercizio di verificare che quelle sopra descritte sono effettivamente tre azioni di G su se stesso.

6.3 - Equiscomponibilità.

Siano $\mathbf{\Omega}$ un insieme, A, B $\subset \mathbf{\Omega}$, G un gruppo che opera su $\mathbf{\Omega}$ e $n \in \mathbb{N}$. Si dice che A è G – *equiscomponibile con* B *in* n *parti* (oppure che A e B sono G – *equiscomponibili in* n *parti*) se esistono n sottoinsiemi $A_1, A_2, \ldots, A_n$ di A, n sottoinsiemi $B_1, B_2, \ldots, B_n$ di B e n elementi $g_1, g_2, \ldots, g_n$ di G tali che

(i) $\{A_1, A_2, \ldots, A_n\}$ è una partizione di A;

(ii) $\{B_1, B_2, \ldots, B_n\}$ è una partizione di B;

(iii) $A_i^{g_i} = B_i$ per $i := 1, 2, \ldots, n$.

Siano $\mathbf{\Omega}$ un insieme, A, B $\subset \mathbf{\Omega}$ e G un gruppo che opera su $\mathbf{\Omega}$. Si dice che A e B sono G – *equiscomponibili* se esiste $n \in \mathbb{N}$ tale che A e B sono G – equiscomponibili in n parti. Si verifica senza particolari difficoltà che la relazione ϱ definita in $\wp(\mathbf{\Omega})$ ponendo

$$A \varrho B \quad \text{se e soltanto se} \quad A \text{ è G} - \text{equiscomponibile con B}$$

è una relazione di equivalenza in $\wp(\mathbf{\Omega})$.

Se $\mathbf{\Omega}$ è l'insieme dei punti dello spazio euclideo e Σ è l'insieme delle isometrie dello spazio euclideo, due sottoinsiemi di $\mathbf{\Omega}$ che siano Σ – equiscomponibili si dicono semplicemente *equiscomponibili*.

Osservazione 6.3.1

Siano $\mathbf{\Omega}$ un insieme, G un gruppo che opera su $\mathbf{\Omega}$ e A, B sottoinsiemi di $\mathbf{\Omega}$.

Se A e B sono G – equiscomponibili, per definizione esistono $n \in \mathbb{N}$, $A_1, \ldots, A_n$ sottoinsiemi di A, $B_1, \ldots, B_n$ sottoinsiemi di B e $g_1, \ldots, g_n \in$ G tali che $\{A_1, A_2, \ldots, A_n\}$ è una partizione di A, $\{B_1, B_2, \ldots, B_n\}$ è una partizione di B e $A_i^{g_i} = B_i$ per $i := 1, 2, \ldots, n$.

La funzione $\alpha : A \to B$ definita da

$$\alpha(a) := a^{g_i} \quad \text{se } a \in A_i$$

è ben definita (perché $\{A_1, A_2, \ldots, A_n\}$ è una partizione di A) ed è una corrispondenza biunivoca tra A e B (perché $\{B_1, B_2, \ldots, B_n\}$ è una partizione di B, e ogni g_i induce una corrispondenza biunivoca tra A_i e B_i): diremo che α *implementa* la G – equiscomponibilità tra A e B.

Viceversa, supponiamo che esistano una corrispondenza biunivoca α tra A e B e una partizione $\{A_1, A_2, \ldots, A_n\}$ di A tali che la restrizione di α a ciascun A_i coincide con un opportuno $g_i \in$ G: allora $\{A_1^{g_1}, A_2^{g_2}, \ldots, A_n^{g_n}\}$ è una partizione di B, A e B sono G – equiscomponibili, e la loro G – equiscomponibilità è implementata da α.

Esempio 6.3.2

Siano $\mathbf{\Omega} := \mathbb{Z}$, $A := \mathbb{Z}^+ \cup \{0\}$, $B := \mathbb{Z}$ e $G := \mathrm{Sym}(\mathbb{Z})$. Allora A e B sono $G-$ equiscomponibili, ponendo

$A_1 := \mathbb{P}$ (il sottoinsieme di A formato dai numeri pari) , $A_2 := \mathbb{D}$ (il sottoinsieme di A formato dai numeri dispari);

$B_1 := \mathbb{Z}^+ \cup \{0\}$, $B_2 := \mathbb{Z}^-$;

$$x^{g_1} := \begin{cases} \frac{x}{2} & \text{se } x \text{ è pari e non negativo} \\ -x & \text{se } x \text{ è dispari e positivo} \\ 2x & \text{se } x \text{ è negativo} \end{cases}$$

$$x^{g_2} := \begin{cases} -\frac{x+1}{2} & \text{se } x \text{ è dispari e positivo} \\ x & \text{se } x \text{ è pari e non negativo} \\ -2x-1 & \text{se } x \text{ è negativo} \end{cases}$$

Questo esempio è banale, e non ci dice molto più del fatto, già ben noto, che i numeri interi sono "tanti quanti" i numeri naturali.

6.4 - Un criterio di G-equiscomponibilità: il teorema di Banach-Schröder-Bernstein.

Teorema 6.4.1 (Banach – Schröder – Bernstein)

Siano $\mathbf{\Omega}$ un insieme, $A, B \subset \mathbf{\Omega}$, G un gruppo che opera su $\mathbf{\Omega}$ e n, m numeri interi positivi.

Se A è $G-$ equiscomponibile in n parti con un sottoinsieme di B e B è $G-$ equiscomponibile in m parti con un sottoinsieme di A, allora A e B sono $G-$ equiscomponibili in $n+m$ parti.

Dimostrazione – Per ipotesi, esistono una corrispondenza biunivoca α tra A e un sottoinsieme di B che ne implementa la $G-$equiscomponibilità e una corrispondenza biunivoca β tra B e un sottoinsieme di A che ne implementa la $G-$equiscomponibilità.

La situazione è dunque analoga a quella del teorema 4.4.1, e ancora una volta per gli elementi di A e di B possiamo definire gli *antenati*:

per ogni $a \in \beta(B)$, diremo antenati di a sia a stesso che tutti gli antenati di $\beta^{-1}(a)$ (per la definizione dei quali, si veda sotto);

per ogni $a \in A \backslash \beta(B)$, diremo che a è l'unico antenato di a ;

per ogni $b \in \alpha(A)$, diremo antenati di b sia b stesso che tutti gli antenati di $\alpha^{-1}(b)$ (per la definizione dei quali, si veda sopra);

per ogni $b \in B \backslash \alpha(A)$, diremo che b è l'unico antenato di b .

Possiamo anche qui individuare una partizione di A in tre sottoinsiemi A_A, A_B e A_∞ e una partizione di B in tre sottoinsiemi B_A, B_B e B_∞ definiti come segue:

A_A è l'insieme degli elementi di A che hanno un numero finito di antenati, l'ultimo dei quali appartiene ad $A\backslash\beta(B)$;
A_B è l'insieme degli elementi di A che hanno un numero finito di antenati, l'ultimo dei quali appartiene a $B\backslash\alpha(A)$;
A_∞ è l'insieme degli elementi di A che hanno un numero infinito di antenati;

B_A è l'insieme degli elementi di B che hanno un numero finito di antenati, l'ultimo dei quali appartiene ad $A\backslash\beta(B)$;
B_B è l'insieme degli elementi di B che hanno un numero finito di antenati, l'ultimo dei quali appartiene a $B\backslash\alpha(A)$;
B_∞ è l'insieme degli elementi di B che hanno un numero infinito di antenati.

Infine, possiamo concludere come nella dimostrazione del teorema 4.4.1 che la funzione $\gamma : A \to B$ così definita

$$\gamma(x) := \begin{cases} \alpha(x) & \text{se } x \in A_A \text{ oppure } x \in A_\infty \\ \\ \beta^{-1}(x) & \text{se } x \in A_B \end{cases}$$

è una corrispondenza biunivoca tra A e B. Resta da mostrare che essa implementa una $G-$equiscomponibilità fra A e B (in $m+n$ parti).

Per ipotesi, esiste una partizione $\{A_1, A_2, \ldots, A_n\}$ di A tale che la restrizione di α a ciascun A_i coincide con un opportuno $x_i \in G$, ed esiste una partizione $\{B_1, B_2, \ldots, B_m\}$ di B tale che la restrizione di β a ciascun B_j coincide con un opportuno $y_j \in G$ (e quindi la restrizione di β^{-1} a ciascun $\beta(B_j)$ coincide con $y_j^{-1} \in G$). Allora

$$A_1 \cap (A_A \cup A_\infty), \quad A_2 \cap (A_A \cup A_\infty), \quad A_3 \cap (A_A \cup A_\infty), \quad \ldots, \quad A_n \cap (A_A \cup A_\infty),$$
$$\beta(B_1) \cap A_B, \quad \beta(B_2) \cap A_B, \quad \beta(B_3) \cap A_B, \quad \ldots, \quad \beta(B_m) \cap A_B$$

è una partizione di A su ogni elemento della quale la restrizione di γ (cioè, a seconda dei casi, di α o di β^{-1}) coincide con un elemento di G, e le immagini costituiscono una partizione di B: ciò completa la dimostrazione del teorema.

6.5 - Richiami sui gruppi liberi.

Sia I un insieme, e siano $x_1, x_2, \ldots, x_n \in I$. Consideriamo altrettanti elementi che indicheremo con $x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}$ [14].

Si dice *parola* di lunghezza k su $x_1, x_2, \ldots, x_n, x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}$ una $k-$pla ordinata di elementi di $\{x_1, x_2, \ldots, x_n, x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}\}$ con $k \in \mathbb{N}$ (se $k = 0$ non ha ovviamente senso parlare di $0-$ple ordinate, però si accetta l'esistenza di un'unica parola di lunghezza 0, detta "parola vuota", nella quale non compare nessuno degli elementi $x_1, x_2, \ldots, x_n, x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}$).

[14] Potrebbero essere, ad esempio, gli elementi del prodotto cartesiano $\{x_1, x_2, \ldots, x_n\} \times \{1\}$.

Se $w_1 \coloneqq (a_1, a_2, \ldots, a_h)$ e $w_2 \coloneqq (b_1, b_2, \ldots, b_k)$ sono due parole su $x_1, x_2, \ldots, x_n, x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}$ di lunghezza rispettivamente h e k, si dice *concatenazione* di w_1 e w_2 e si indica con $w_1 \diamond w_2$ la parola di lunghezza $h + k$

$$w_1 \diamond w_2 \coloneqq (a_1, a_2, \ldots, a_h, b_1, b_2, \ldots, b_k).$$

Una parola $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ su $x_1, x_2, \ldots, x_n, x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}$ si dice *riducibile* se esistonoi $i \in \{1, 2, \ldots, k-1\}$ e $j \in \{1, 2, \ldots, n\}$ tali che $(\alpha_i = x_j$ e $\alpha_{i+1} = x_j^{-1})$ oppure $(\alpha_i = x_j^{-1}$ e $\alpha_{i+1} = x_j)$; *ridotta* se non è riducibile. Si dice *riduzione* di una parola su $x_1, x_2, \ldots, x_n, x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}$ la soppressione di coppie (x_i, x_i^{-1}) oppure (x_i^{-1}, x_i) di elementi contigui della forma: si vede senza particolari difficoltà che se una parola è riducibile e si opera su di essa mediante successive riduzioni fino ad ottenere una parola ridotta, quest'ultima non dipende dall'ordine in cui si procede nelle successive riduzioni.

La concatenazione di due parole ridotte non è in generale ridotta (perché l'ultimo elemento della prima parola potrebbe essere x_i e il primo elemento della seconda x_i^{-1}, o viceversa); diremo *concatenazione forte* ([15]) di due parole ridotte w_1 e w_2, e indicheremo con $w_1 * w_2$, la parola ridotta ottenuta mediante successive riduzioni su $w_1 \diamond w_2$.

Teorema 6.5.1

Sia I un insieme, e siano $x_1, x_2, \ldots, x_n \in \mathrm{I}$. Consideriamo altrettanti elementi che indicheremo con $x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}$. L'insieme delle parole ridotte su $x_1, x_2, \ldots, x_n, x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}$ è un gruppo rispetto all'operazione di concatenazione forte, detto *gruppo libero* su $x_1, x_2, \ldots, x_n$.

Dimostrazione — La parola vuota è elemento neutro per la concatenazione (e quindi anche per la concatenazione forte). Ogni parola ridotta w ha un'inversa, ottenuta prendendo in ordine inverso gli elementi che compongono w e sostituendo ogni x_i con x_i^{-1} e ogni x_i^{-1} con x_i. Si verifica infine senza particolari difficoltà che la concatenazione forte è associativa.

Teorema 6.5.2

Sia G un gruppo, e sia $\{g_1, g_2, \ldots, g_n\}$ un insieme di generatori di G. Se per ogni parola ridotta non vuota $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ su $g_1, g_2, \ldots, g_n, g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}$ si ha $\alpha_1 \alpha_2 \ldots \alpha_k \neq 1_{\mathbf{G}}$, allora G è isomorfo al gruppo libero su $x_1, x_2, \ldots, x_n$.

Dimostrazione — La funzione $g_i \to x_i$ (per $i \coloneqq 1, 2, \ldots, n$) induce l'isomorfismo desiderato.

Corollario 6.5.3

Siano I, J insiemi, siano $x_1, x_2, \ldots, x_n \in \mathrm{I}$ e siano $y_1, y_2, \ldots, y_n \in \mathrm{J}$. Il gruppo libero su $x_1, x_2, \ldots, x_n$ è isomorfo al gruppo libero su $y_1, y_2, \ldots, y_n$.

[15] Questa terminologia **non** è standard!

Teorema 6.5.4

Sia I un insieme, siano $x_1, x_2, \ldots, x_n \in$ I e sia F il gruppo libero su $x_1, x_2, \ldots, x_n$.

La cardinalità di F è $\aleph_0$ (ossia, in altre parole: F è numerabile).

Dimostrazione – Se per ogni $\lambda \in \mathbb{N}$ indichiamo con X_λ l'insieme delle parole ridotte di lunghezza λ, la famiglia degli X_h costituisce una partizione di F che verifica le ipotesi del lemma 4.3.3, applicando il quale si può concludere che $|F| = \aleph_0$.

6.6 - Un significativo (e utile) esempio di G-equiscomponibilità.

Teorema 6.6.1

Sia F il gruppo libero su due elementi x e y, sia $C_2 = \{1, -1\}$ il gruppo ciclico di ordine 2 e sia $G = F \times C_2$ il prodotto diretto tra F e C_2 . Facciamo operare G su se stesso mediante traslazione.

I sottoinsiemi (di fatto, sottogruppi!) di G $F \times \{1\}$ e G sono G – equiscomponibili (in 5 parti).

Dimostrazione – Per il teorema 6.4.1, basterà mostrare che $F \times \{1\}$ è G – equiscomponibile (in 1 parte) con un sottoinsieme di G e che G è G – equiscomponibile (in 4 parti) con un sottoinsieme di $F \times \{1\}$.

Poiché $F \times \{1\}$ è un sottoinsieme di G, abbiamo subito la G – equiscomponibilità fra $F \times \{1\}$ e se stesso, in una sola parte, indotta dalla moltiplicazione per l'elemento neutro $(\emptyset, 1)$ ([16]) di G.

Viceversa, mostriamo che G è G – equiscomponibile in 4 parti con $F \times \{1\} \setminus \{(\emptyset, 1)\}$. Indichiamo con $W(x)$ l'insieme delle parole ridotte su x, y, x^{-1}, y^{-1} che terminano con x; indichiamo con $W(x^{-1})$ l'insieme di quelle che terminano con x^{-1}; indichiamo con $W(y)$ l'insieme di quelle che terminano con y; e indichiamo con $W(y^{-1})$ l'insieme di quelle che terminano con y^{-1}. È chiaro che $\{ W(x), W(x^{-1}), W(y), W(y^{-1})\}$ è una partizione di $F \setminus \{\emptyset\}$.

Indichiamo poi con $\overline{W}(x)$ l'insieme delle parole ridotte su x, y, x^{-1}, y^{-1} che **non** terminano con x, cioè poniamo $\overline{W}(x) = F \setminus W(x)$; analogamente poniamo

$$\overline{W}(x^{-1}) := F \setminus W(x^{-1}), \qquad \overline{W}(y) := F \setminus W(y), \qquad \overline{W}(y^{-1}) := F \setminus W(x^{-1}) .$$

Poniamo infine

$$G_1 := \{(w, n) \in G \,/\, w \in W(x) \text{ e } n = 1\}; \qquad G_2 := \{(w, n) \in G \,/\, w \in \overline{W}(x) \text{ e } n = 1\};$$
$$G_3 := \{(w, n) \in G \,/\, w \in W(y) \text{ e } n = -1\}; \qquad G_4 := \{(w, n) \in G \,/\, w \in \overline{W}(y) \text{ e } n = -1\}.$$

È immediato verificare che $\{G_1, G_2, G_3, G_4\}$ è una partizione di G e che

$$(\emptyset, 1)G_1 = W(x) \times 1, \qquad (x^{-1}, 1)G_2 = W(x^{-1}) \times 1,$$
$$(\emptyset, -1)G_3 = W(y) \times 1, \qquad (y^{-1}, -1)G_4 = W(y^{-1}) \times 1$$

cosicché si è provato che G è G – equiscomponibile in 4 parti con $F \times \{1\} \setminus \{(\emptyset, 1)\}$, come si voleva.

---

[16] Indichiamo con $\emptyset$ la parola vuota, cioè l'elemento neutro di F: poiché 1 è l'elemento neutro di $\{1, -1\}$, l'elemento neutro di G è appunto $(\emptyset, 1)$.

Nel seguito,* O *indicherà un punto dello spazio arbitrariamente fissato ma scelto una volta per tutte.

6.7 - Un gruppo libero generato da due rotazioni della sfera.

Riferito lo spazio a un sistema di riferimento cartesiano monometrico positivamente orientato **O*xyz*** con origine **O**, indichiamo con φ e ψ rispettivamente le rotazioni attorno all'asse delle quote e attorno all'asse delle ascisse individuate da un angolo di arccos$\frac{1}{3}$ radianti, e con φ^{-1} e ψ^{-1} le loro inverse. Dunque:

$$\varphi = \begin{pmatrix} \frac{1}{3} & \frac{-2\sqrt{2}}{3} & 0 \\ \frac{2\sqrt{2}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \varphi^{-1} = \begin{pmatrix} \frac{1}{3} & \frac{2\sqrt{2}}{3} & 0 \\ \frac{-2\sqrt{2}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\psi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & \frac{-2\sqrt{2}}{3} \\ 0 & \frac{2\sqrt{2}}{3} & \frac{1}{3} \end{pmatrix}, \qquad \psi^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & \frac{2\sqrt{2}}{3} \\ 0 & \frac{-2\sqrt{2}}{3} & \frac{1}{3} \end{pmatrix}.$$

Per dimostrare che φ e ψ generano un gruppo isomorfo al gruppo libero su x e y, in base al teorema 6.5.2 basterà mostrare che per ogni parola ridotta non vuota (α_1, α_2, …, α_k) su φ, ψ, φ^{-1}, ψ^{-1} il prodotto $\alpha_1\alpha_2\ldots\alpha_k$ è diverso dall'identità. Lo facciamo introducendo un'opportuna notazione ed alcuni teoremi dedicati allo scopo.

Per a,b,$c \in \mathbb{Z}$ e $k \in \mathbb{N}$, indichiamo con $v_k(a,b,c)$ il punto di coordinate $(\frac{a}{3^k}, \frac{b\sqrt{2}}{3^k}, \frac{c}{3^k})$ (cosicché in particolare $v_0(1,0,1) = (1,0,1)$) e per ogni isometria ϑ dello spazio indichiamo con $\vartheta(v_k(a,b,c))$ l'immagine di $v_k(a,b,c)$ per effetto di ϑ.

Lemma 6.7.1

Si ha

$\varphi(v_0(1,0,1)) = \varphi(1,0,1) = (\frac{1}{3}, \frac{2\sqrt{2}}{3}, 1) = v_1(1,2,3)$;

$\varphi^{-1}(v_0(1,0,1)) = \varphi^{-1}(1,0,1) = (\frac{1}{3}, \frac{-2\sqrt{2}}{3}, 1) = v_1(1,-2,3)$;

$\psi(v_0(1,0,1)) = \psi(1,0,1) = (1, \frac{-2\sqrt{2}}{3}, \frac{1}{3}) = v_1(3,-2,1)$;

$\psi^{-1}(v_0(1,0,1)) = \psi^{-1}(1,0,1) = (1, \frac{2\sqrt{2}}{3}, \frac{1}{3}) = v_1(3,2,1)$;

Dimostrazione – Si tratta di una immediata verifica.

Lemma 6.7.2

Sia $b \not\equiv 0$ (*mod* 3). Si ha che

(1) se non è né $a \equiv b \equiv 1$ (*mod* 3) né $a \equiv b \equiv 2$ (*mod* 3), allora

$\varphi(v_k(a,b,c)) = v_{k+1}(a',b',c')$ con $c' \equiv 0$ (*mod* 3) e inoltre

(1.1) $a' \equiv 1$ (*mod* 3) e $b' \equiv 2$ (*mod* 3)

oppure

(1.2) $a' \equiv 2$ (*mod* 3) e $b' \equiv 1$ (*mod* 3);

(2) se non è né $(a \equiv 1$ (*mod* 3) e $b \equiv 2$ (*mod* 3)$)$ né $(a \equiv 2$ (*mod* 3) e $b \equiv 1$ (*mod* 3)$)$, allora

$\varphi^{-1}(v_k(a,b,c)) = v_{k+1}(a',b',c')$ con $c' \equiv 0$ (*mod* 3) e inoltre

(2.1) $a' \equiv b' \equiv 1$ (*mod* 3)

oppure

(2.2) $a' \equiv b' \equiv 2$ (*mod* 3);

(3) se non è né $(b \equiv 1$ (*mod* 3) e $c \equiv 2$ (*mod* 3)$)$ né $(b \equiv 2$ (*mod* 3) e $c \equiv 1$ (*mod* 3)$)$, allora

$\psi(v_k(a,b,c)) = v_{k+1}(a',b',c')$ con $a' \equiv 0$ (*mod* 3) e inoltre

(3.1) $b' \equiv c' \equiv 1$ (*mod* 3)

oppure

(3.2) $b' \equiv c' \equiv 2$ (*mod* 3);

(4) se non è né $b \equiv c \equiv 1$ (*mod* 3) né $b \equiv c \equiv 1$ (*mod* 3), allora

$\psi^{-1}(v_k(a,b,c)) = v_{k+1}(a',b',c')$ con $a' \equiv 0$ (*mod* 3) e inoltre

(4.1) $b' \equiv 1$ (*mod* 3) e $c' \equiv 2$ (*mod* 3)

oppure

(4.2) $b' \equiv 2$ (*mod* 3) e $c' \equiv 1$ (*mod* 3);

Dimostrazione —

(1) Da un calcolo diretto, si ha che

$$\varphi(v_k(a,b,c)) = \begin{pmatrix} \frac{1}{3} & \frac{-2\sqrt{2}}{3} & 0 \\ \frac{2\sqrt{2}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{a}{3^k} \\ \frac{b\sqrt{2}}{3^k} \\ \frac{c}{3^k} \end{pmatrix} = \begin{pmatrix} \frac{a-4b}{3^{k+1}} \\ \frac{(2a+b)\sqrt{2}}{3^{k+1}} \\ \frac{3c}{3^{k+1}} \end{pmatrix} = \begin{pmatrix} \frac{a'}{3^k} \\ \frac{b'\sqrt{2}}{3^k} \\ \frac{c'}{3^k} \end{pmatrix}$$

con $c' \equiv 0$ (*mod* 3) e i valori di a' e b' modulo 3 come risulta (in funzione dei valori di a e b modulo 3) dalla seguente tabella:

a	b	a'	b'
0	1	2	1
1	1	0	0
2	1	1	2
0	2	1	2
1	2	2	1
2	2	0	0

Dunque

$\varphi(v_k(a,b,c)) = v_{k+1}(a',b',c')$ con a',b',c' come descritti dall'enunciato del teorema.

(2) Da un calcolo diretto, si ha che

$$\varphi^{-1}(v_k(a,b,c)) = \begin{pmatrix} \frac{1}{3} & \frac{2\sqrt{2}}{3} & 0 \\ \frac{-2\sqrt{2}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} \frac{a}{3^k} \\ \frac{b\sqrt{2}}{3^k} \\ \frac{c}{3^k} \end{pmatrix} = \begin{pmatrix} \frac{a+4b}{3^{k+1}} \\ \frac{(b-2a)\sqrt{2}}{3^{k+1}} \\ \frac{3c}{3^{k+1}} \end{pmatrix} = \begin{pmatrix} \frac{a'}{3^k} \\ \frac{b'\sqrt{2}}{3^k} \\ \frac{c'}{3^k} \end{pmatrix}$$

con $c' \equiv 0$ (*mod* 3) e i valori di a' e b' modulo 3 come risulta (in funzione dei valori di a e b modulo 3) dalla seguente tabella:

a	b	a'	b'
0	1	2	1
1	1	2	2
2	1	0	0
0	2	2	2
1	2	0	0
2	2	1	1

Dunque

$\varphi^{-1}(v_k(a,b,c)) = v_{k+1}(a',b',c')$ con a',b',c' come descritti dall'enunciato del teorema.

(3) Da un calcolo diretto, si ha che

$$\psi(v_k(a,b,c)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & \frac{-2\sqrt{2}}{3} \\ 0 & \frac{2\sqrt{2}}{3} & \frac{1}{3} \end{pmatrix} \begin{pmatrix} \frac{a}{3^k} \\ \frac{b\sqrt{2}}{3^k} \\ \frac{c}{3^k} \end{pmatrix} = \begin{pmatrix} \frac{3a}{3^{k+1}} \\ \frac{(b-2c)\sqrt{2}}{3^{k+1}} \\ \frac{4b+c}{3^{k+1}} \end{pmatrix} = \begin{pmatrix} \frac{a'}{3^k} \\ \frac{b'\sqrt{2}}{3^k} \\ \frac{c'}{3^k} \end{pmatrix}$$

con $a' \equiv 0$ (*mod* 3) e i valori di b' e c' modulo 3 come risulta (in funzione dei valori di b e c modulo 3) dalla seguente tabella:

b	c	b'	c'
1	0	1	1
1	1	2	2
1	2	0	0
2	0	2	2
2	1	0	0
2	2	1	1

Dunque

$\psi(v_k(a,b,c)) = v_{k+1}(a',b',c')$ con a', b', c' come descritti dall'enunciato del teorema.

(4) Da un calcolo diretto, si ha che

$$\psi^{-1}(v_k(a,b,c)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & \frac{2\sqrt{2}}{3} \\ 0 & \frac{-2\sqrt{2}}{3} & \frac{1}{3} \end{pmatrix}, \begin{pmatrix} \frac{a}{3^k} \\ \frac{b\sqrt{2}}{3^k} \\ \frac{c}{3^k} \end{pmatrix} = \begin{pmatrix} \frac{3a}{3^{k+1}} \\ \frac{(b+2c)\sqrt{2}}{3^{k+1}} \\ \frac{c-4b}{3^{k+1}} \end{pmatrix} = \begin{pmatrix} \frac{a'}{3^k} \\ \frac{b'\sqrt{2}}{3^k} \\ \frac{c'}{3^k} \end{pmatrix}$$

con $a' \equiv 0$ (*mod* 3) e i valori di b' e c' modulo 3 come risulta (in funzione dei valori di b e c modulo 3) dalla seguente tabella:

b	c	b'	c'
1	0	1	2
1	1	0	0
1	2	2	1
2	0	2	1
2	1	1	2
2	2	0	0

Dunque

$\psi^{-1}(v_k(a,b,c)) = v_{k+1}(a',b',c')$ con a', b', c' come descritti dall'enunciato del teorema.

Teorema 6.7.3

Per ogni parola ridotta non vuota $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ su φ, ψ, φ^{-1}, ψ^{-1} il prodotto $\alpha_1\alpha_2\ldots\alpha_k$ è diverso dall'identità.

Dimostrazione — Basterà provare che $(\alpha_1\alpha_2\ldots\alpha_k)(1,0,1) \neq (1,0,1)$. A tale scopo mostreremo (per induzione su k) che:

$(\alpha_1\alpha_2\ldots\alpha_k)(1,0,1) = v_k(a,b,c)$ con $b \not\equiv 0$ (*mod* 3) e inoltre:

se $\alpha_k = \varphi$, allora ($a \equiv 1$ (*mod* 3), $b \equiv 2$ (*mod* 3) e $c \equiv 0$ (*mod* 3))
oppure ($a \equiv 2$ (*mod* 3), $b \equiv 1$ (*mod* 3) e $c \equiv 0$ (*mod* 3)) ;

se $\alpha_k = \varphi^{-1}$, allora ($a \equiv b \equiv 1$ (*mod* 3) e $c \equiv 0$ (*mod* 3))
oppure ($a \equiv b \equiv 2$ (*mod* 3) e $c \equiv 0$ (*mod* 3)) ;

se $\alpha_k = \psi$, allora ($a \equiv 0$ (*mod* 3) e $b \equiv c \equiv 1$ (*mod* 3))
oppure ($a \equiv 0$ (*mod* 3) e $b \equiv c \equiv 2$ (*mod* 3)) ;

se $\alpha_k = \psi^{-1}$, allora ($a \equiv 0$ (*mod* 3), $b \equiv 1$ (*mod* 3) e $c \equiv 2$ (*mod* 3))
oppure ($a \equiv 0$ (*mod* 3), $b \equiv 2$ (*mod* 3) e $c \equiv 1$ (*mod* 3)) .

Per $k := 1$ l'asserto segue immediatamente dal lemma 6.7.1. Supposto vero l'asserto per k, la conclusione segue per $k+1$ dal lemma 6.7.2 ricordando che per ipotesi $(\alpha_1\alpha_2\ldots\alpha_k)$ è una parola ridotta e quindi α_{k+1} non può essere l'inversa di α_k . Il teorema è così dimostrato.

Nella prossima sezione, indicheremo con F il gruppo di isometrie generato da φ e ψ, e con G il prodotto tra F e il gruppo ciclico $\{1, -1\}$ di ordine 2. Per il teorema 6.5.1, l'applicazione che porta φ in x e ψ in y induce un isomorfismo tra F e il gruppo libero su x e y, che si estende a un isomorfismo tra G e il gruppo con lo stesso nome considerato nel teorema 6.6.1.

Indicheremo con F_0 l'insieme $F\backslash\{\boldsymbol{id}\}$ di tutti gli elementi di F diversi dall'isometria identica.

6.8 - Il teorema di Banach-Tarski.

Ci avviciniamo al risultato principale attraverso alcuni teoremi "di preparazione". Fissato un punto O nello spazio, indicheremo con $\mathcal{S}_3$ la sfera (o "palla") di centro O e raggio assegnato r, e con $\mathcal{S}_2$ la superficie sferica di centro O e raggio r.

Per quasi tutta la sezione il ruolo del raggio r sarà irrilevante, e per fissare le idee si potrebbe porre $r := 1$. Tuttavia, per dimostrare la "forma forte" del teorema di Banach Tarski (teor. 6.8.7) è necessario sapere che la "forma debole" (teor. 6.8.4) vale per ogni $r \in \mathbb{R}^+$.

Teorema 6.8.1

$\mathcal{S}_3$ è equiscomponibile ([17]) in due parti con $\mathcal{S}_3\backslash\{O\}$.

Dimostrazione – Sia $\mathcal{C}$ una circonferenza passante per O tutta contenuta in $\mathcal{S}_3$ (ad esempio, una qualsiasi circonferenza passante per O di raggio $\leq \frac{r}{4}$), e sia ρ la rotazione di un radiante attorno al centro di $\mathcal{C}$ che muta $\mathcal{C}$ in sé. Poniamo

$$A := \{P \in \mathcal{C} \,/\, P = \rho^n(O) \text{ con } n \in \mathbb{N}\backslash\{0\}\},\quad \overline{A} := A \cup \{O\},\quad B := \mathcal{S}_3\backslash\overline{A}\,.$$

Osserviamo che $\mathcal{S}_3 = B \cup \overline{A}$ e $\mathcal{S}_3\backslash\{O\} = B \cup A$, mentre $B \cap \overline{A} = B \cap A = \emptyset$.

Poiché l'isometria ρ porta $\overline{A}$ in A e l'isometria identica muta B in sé, abbiamo provato che $\mathcal{S}_3$ è equiscomponibile con $\mathcal{S}_3\backslash\{O\}$, come si voleva.

Utilizzando la stessa idea della dimostrazione del teorema 6.8.1, ci liberiamo adesso di tutti i punti della palla che sono fissati da qualche elemento di F_0. Poiché gli elementi di F_0 sono rotazioni attorno a un asse passante per O, i punti della palla che sono fissati da qualche elemento di F_0 sono i punti di tutti gli assi degli elementi di F_0.

Teorema 6.8.2

Sia $\mathcal{D}$ l'insieme dei punti di $\mathcal{S}_3$ che sono fissati da qualche elemento di F_0. $\mathcal{S}_3\backslash\{O\}$ è equiscomponibile in due parti con $\mathcal{S}_3\backslash\mathcal{D}$.

Dimostrazione – Poiché gli elementi di F sono un'infinità numerabile (teor. 6.5.4), mentre l'insieme delle rette passanti per **O** ha la potenza del continuo, esiste certamente una retta a passante per **O** distinta da tutti gli assi delle rotazioni che costituiscono F_0; tale retta ha in comune con ciascuno di tali assi soltanto il punto **O**.

Poniamo $\mathcal{D}_0 := \mathcal{D}\backslash\{\mathbf{O}\}$ Fra tutte le rotazioni ρ di asse a, quelle per le quali $\rho^i(\mathbf{P}) = \mathbf{P}^*$ con $\mathbf{P}, \mathbf{P}^* \in \mathcal{D}_0$ sono un'infinità numerabile: infatti sono completamente determinate dalle terne $(i, \overline{\mathbf{P}}, \overline{\mathbf{P}^*})$ con $i \in \mathbb{N}$, $\overline{\mathbf{P}}, \overline{\mathbf{P}^*} \in \mathcal{D}_0 \cap \mathcal{S}_2$ dove $\overline{\mathbf{P}}$ e $\overline{\mathbf{P}^*}$ sono le intersezioni con $\mathcal{S}_2$ delle rette **OP** e **OP*** (ricordando che ognuna delle $\aleph_0$ rotazioni che formano il gruppo F ha come punti fissi soltanto i punti del suo asse).

Sia allora $\overline{\rho}$ una rotazione di asse a per la quale $\overline{\rho}^i(\mathbf{P}) \notin \mathcal{D}_0$ per ogni $i \in \mathbb{N}$ e per ogni $\mathbf{P} \in \mathcal{D}_0$. Gli insiemi $\overline{\rho}(\mathcal{D}_0)$, $\overline{\rho}^2(\mathcal{D}_0)$, $\overline{\rho}^3(\mathcal{D}_0)$, … sono tutti disgiunti con $\mathcal{D}_0$, quindi se poniamo

$$A := \bigcup_{i=1}^{\infty} \overline{\rho}^{\,i}(\mathcal{D}_0)$$

si ha che $A \cap \mathcal{D}_0 = \emptyset$. Poniamo inoltre $\overline{A} := A \cup \mathcal{D}_0$ e $B := (\mathcal{S}_3\backslash\{\mathbf{O}\})\backslash\overline{A}$, cosicché $\mathcal{S}_3\backslash\{\mathbf{O}\} = \overline{A} \cup B$ e $(\mathcal{S}_3\backslash\{\mathbf{O}\})\backslash\mathcal{D}_0 = A \cup B$, mentre $A \cap B = \overline{A} \cap B = \emptyset$.

Poiché la rotazione $\overline{\rho}$ porta $\overline{A}$ in A e l'isometria identica muta B in sé, abbiamo provato che $\mathcal{S}_3\backslash\{\mathbf{O}\}$ è equiscomponibile in due parti con $(\mathcal{S}_3\backslash\{\mathbf{O}\})\backslash\mathcal{D}_0 (= \mathcal{S}_3\backslash\mathcal{D})$, come si voleva.

[17] Ricordiamo che *equiscomponibile* significa Σ-equiscomponibile, dove Σ è il gruppo delle isometrie dello spazio (cfr. sez. 6.2).

Teorema 6.8.3

Sia $\mathcal{D}$ l'insieme dei punti di $\mathcal{S}_3$ che sono fissati da qualche elemento di F_0.

Esiste una partizione $\{\overline{\mathrm{A}}_1^*, \overline{\mathrm{A}}_2^*, \ldots, \overline{\mathrm{A}}_s^*, \overline{\mathrm{B}}_1^*, \overline{\mathrm{B}}_2^*, \ldots, \overline{\mathrm{B}}_t^*\}$ di $\mathcal{S}_3\backslash\mathcal{D}$ (con $s+t=5$) tale che $\overline{\mathrm{A}}_1^* \cup \overline{\mathrm{A}}_2^* \cup \ldots \cup \overline{\mathrm{A}}_s^*$ è equiscomponibile in s parti con $\mathcal{S}_3\backslash\mathcal{D}$ e $\overline{\mathrm{B}}_1^* \cup \overline{\mathrm{B}}_2^* \cup \ldots \cup \overline{\mathrm{B}}_t^*$ è equiscomponibile in t parti con $\mathcal{S}_3\backslash\mathcal{D}$.

Dimostrazione — Osserviamo in primo luogo che F muta $\mathcal{D}$ in sé (e quindi muta in sé anche $\mathcal{S}_3\backslash\mathcal{D}$). Infatti, se $\mathrm{P} \in \mathcal{D}$ esiste $f_0 \in \mathrm{F}_0$ tale che $f_0(\mathrm{P}) = \mathrm{P}$; allora, per ogni $f \in \mathrm{F}$ è

$$(f \circ f_0 \circ f^{-1})(f(\mathrm{P})) = (f \circ f_0)(f^{-1} \circ f)(\mathrm{P}) = (f \circ f_0)(\mathrm{P}) = f(f_0(\mathrm{P})) = f(\mathrm{P})$$

cioè $f(\mathrm{P})$ è fissato da $f \circ f_0 \circ f^{-1}$ e quindi $f(\mathrm{P}) \in \mathcal{D}$ ([18]).

Sia $\mathcal{M}$ un insieme di rappresentanti per le orbite dell'azione di F su $\mathcal{S}_3\backslash\mathcal{D}$ (tale insieme esiste per l'assioma della scelta) ([19]).

Ogni elemento di $\mathcal{S}_3\backslash\mathcal{D}$ si scrive in uno e un solo modo nella forma $f(\mathrm{M})$ con $f \in \mathrm{F}$ e $\mathrm{M} \in \mathcal{M}$. Tale forma di scrittura esiste perché ogni elemento di $\mathcal{S}_3\backslash\mathcal{D}$ appartiene ad un'orbita; ed è unica perché da $f_1(\mathrm{M}_1) = f_2(\mathrm{M}_2)$ con $f_1, f_2 \in \mathrm{F}$ e $\mathrm{M}_1, \mathrm{M}_2 \in \mathcal{M}$ segue $f_2^{-1} f_1(\mathrm{M}_1) = \mathrm{M}_2$, cosicché M_1 e M_2 appartengono alla stessa orbita, da cui $\mathrm{M}_1 = \mathrm{M}_2$: ma allora $f_2^{-1} f_1 = \boldsymbol{id}$ (perché in $\mathcal{M}$ non ci sono elementi di $\mathcal{D}$) e quindi anche $f_1 = f_2$.

Per il teorema 6.6.1, esistono una partizione $\{\mathrm{C}_1, \mathrm{C}_2, \ldots, \mathrm{C}_5\}$ di G, una partizione $\{\overline{\mathrm{C}}_1, \overline{\mathrm{C}}_2, \ldots, \overline{\mathrm{C}}_5\}$ di $\mathrm{F} \times \{1\}$ ed elementi $g_1, g_2, \ldots, g_5$ di G tali che $g_i(\mathrm{C}_i) = \overline{\mathrm{C}}_i$ per $i := 1, 2, \ldots, 5$. Poiché ogni g_i è della forma $(f_i, 1)$ oppure $(f_i, -1)$ mentre ogni elemento di $\overline{\mathrm{C}}_i$ ha la seconda componente uguale a 1, gli elementi di ciascun C_i devono avere tutti la stessa seconda componente, e precisamente: 1 se g_i è della forma $(f_i, 1)$, -1 altrimenti.

Dunque la partizione $\{\mathrm{C}_1, \mathrm{C}_2, \ldots, \mathrm{C}_5\}$ di G è di fatto l'unione di due partizioni $\{\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_s\}$ di $\mathrm{F} \times \{1\}$ e $\{\mathrm{B}_1, \mathrm{B}_2, \ldots, \mathrm{B}_t\}$ di $\mathrm{F} \times \{-1\}$ (con $s+t=5$), mentre la partizione $\{\overline{\mathrm{C}}_1, \overline{\mathrm{C}}_2, \ldots, \overline{\mathrm{C}}_5\}$ di $\mathrm{F} \times \{1\}$ si può scrivere come $\{\overline{\mathrm{A}}_1, \overline{\mathrm{A}}_2, \ldots, \overline{\mathrm{A}}_s, \overline{\mathrm{B}}_1, \overline{\mathrm{B}}_2, \ldots, \overline{\mathrm{B}}_t\}$ avendo posto $\overline{\mathrm{A}}_i := g_i(\mathrm{A}_i)$ (con g_i della forma $(f_i, 1)$ per $i := 1, \ldots, s$) e $\overline{\mathrm{B}}_j := g_{s+j}(\mathrm{B}_j)$ (con g_{s+j} della forma $(f_{s+j}, -1)$ per $j := 1, \ldots, t$).

Poniamo:

$$\overline{\mathrm{A}}_i^* := \{\mathrm{P} \in \mathcal{S}_3\backslash\mathcal{D} \,/\, \mathrm{P} = \alpha(\mathrm{M}) \text{ con } (\alpha, 1) \in \overline{\mathrm{A}}_i \text{ e } \mathrm{M} \in \mathcal{M}\}, \quad \text{per} \quad i := 1, \ldots, s;$$
$$\overline{\mathrm{B}}_i^* := \{\mathrm{P} \in \mathcal{S}_3\backslash\mathcal{D} \,/\, \mathrm{P} = \alpha(\mathrm{M}) \text{ con } (\alpha, 1) \in \overline{\mathrm{B}}_i \text{ e } \mathrm{M} \in \mathcal{M}\}, \quad \text{per} \quad i := 1, \ldots, t;$$
$$\mathrm{A}_i^* := \{\mathrm{P} \in \mathcal{S}_3\backslash\mathcal{D} \,/\, \mathrm{P} = \alpha(\mathrm{M}) \text{ con } (\alpha, 1) \in \mathrm{A}_i \text{ e } \mathrm{M} \in \mathcal{M}\}, \quad \text{per} \quad i := 1, \ldots, s;$$
$$\mathrm{B}_i^* := \{\mathrm{P} \in \mathcal{S}_3\backslash\mathcal{D} \,/\, \mathrm{P} = \alpha(\mathrm{M}) \text{ con } (\alpha, -1) \in \mathrm{B}_i \text{ e } \mathrm{M} \in \mathcal{M}\}, \quad \text{per} \quad i := 1, \ldots, t.$$

Per quanto sopra osservato, $\{\overline{\mathrm{A}}_1^*, \overline{\mathrm{A}}_2^*, \ldots, \overline{\mathrm{A}}_s^*, \overline{\mathrm{B}}_1^*, \overline{\mathrm{B}}_2^*, \ldots, \overline{\mathrm{B}}_t^*\}$, $\{\mathrm{A}_1^*, \mathrm{A}_2^*, \ldots, \mathrm{A}_s^*\}$ e $\{\mathrm{B}_1^*, \mathrm{B}_2^*, \ldots, \mathrm{B}_t^*\}$ sono tre partizioni di $\mathcal{S}_3\backslash\mathcal{D}$.

---

[18] Si osservi che $f \circ f_0 \circ f^{-1} \in \mathrm{F}_0$ perché se fosse $f \circ f_0 \circ f^{-1} = \mathbf{id}$ sarebbe anche
$$f_0 = (f^{-1} \circ f) \circ f_0 \circ (f^{-1} \circ f) = f^{-1} \circ (f \circ f_0 \circ f^{-1}) \circ f = f^{-1} \circ \mathbf{id} \circ f = \mathbf{id}$$
mentre per ipotesi $f_0 \in \mathrm{F}_0$.

[19] Ricordando il teorema 6.1.4 e il fatto che $|\mathrm{F}| = \aleph_0$ (teorema 6.4.4), si può notare che ogni orbita dell'azione di F su $\mathcal{S}_3\backslash\mathcal{D}$ è numerabile; poiché invece $\mathcal{S}_3\backslash\mathcal{D}$ ha la cardinalità del continuo, per il teorema 4.5.8 anche l'insieme delle orbite dell'azione di F su $\mathcal{S}_3\backslash\mathcal{D}$ ha la cardinalità del continuo (e lo stesso avviene dunque per $\mathcal{M}$). Che $\mathcal{M}$ abbia la cardinalità del continuo è comunque irrilevante per il prosieguo della dimostrazione.

Inoltre, poiché $g_i(A_i) = \overline{A}_i$ si ha che $f_i(A_i^*) = \overline{A}_i^*$ (se $g_i = (f_i, 1)$), e poiché $g_{s+j}(B_j) = \overline{B}_j$ si ha anche che $f_{s+j}(B_j^*) = \overline{B}_j^*$ (se $g_{s+j} = (f_{s+j}, -1)$).

Ma ciò significa appunto che

– $\overline{A}_1^* \cup \overline{A}_2^* \cup \ldots \cup \overline{A}_s^*$ è equiscomponibile con $\mathcal{S}_3\backslash\mathcal{D}$ e

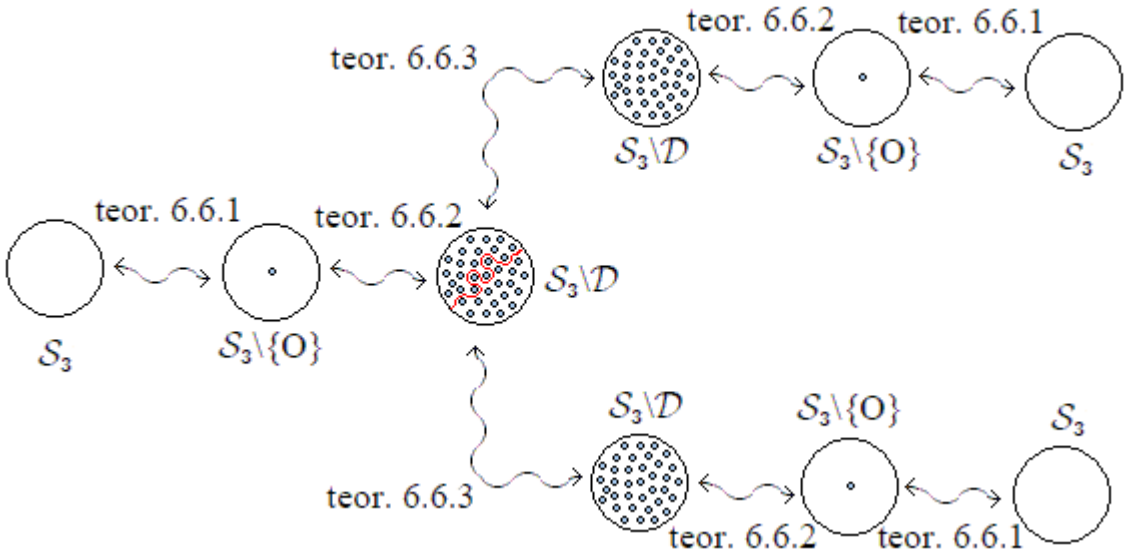
– anche $\overline{B}_1^* \cup \overline{B}_2^* \cup \ldots \cup \overline{B}_t^*$ è equiscomponibile con $\mathcal{S}_3\backslash\mathcal{D}$

con $\left(\overline{A}_1^* \cup \overline{A}_2^* \cup \ldots \cup \overline{A}_s^*\right) \cup \left(\overline{B}_1^* \cup \overline{B}_2^* \cup \ldots \cup \overline{B}_t^*\right) = \mathcal{S}_3\backslash\mathcal{D}$, come si voleva dimostrare.

Teorema 6.8.4 (Banach – Tarski, forma debole)

Ogni "palla" $\mathcal{S}_3$ (di raggio arbitrario r) è equiscomponibile (in 80 parti) con l'unione insiemistica di due copie disgiunte di se stessa.

Dimostrazione – Basta "mettere insieme" i pezzi della dimostrazione visti fin qui, come illustra questo schema:



Corollario 6.8.5

Per ogni numero intero positivo n, ogni "palla" $\mathcal{S}_3$ (di raggio arbitrario r) è equiscomponibile con l'unione insiemistica di n copie disgiunte di se stessa.

Dimostrazione – Per induzione su n: se $n = 1$ non c'è niente da dimostrare, per $n > 1$ basta usare l'ipotesi di induzione e il teorema 6.8.4 .

Corollario 6.8.6

Siano r_1, r_2 numeri reali positivi. La "palla" $\mathcal{S}_3^1$ di raggio r_1 è equiscomponibile con la "palla" $\mathcal{S}_3^2$ di raggio r_2.

Dimostrazione – Per fissare le idee, sia $r_1 \leq r_2$. Con un opportuno numero di copie della "palla" $\mathcal{S}_3^1$ di raggio r_1 (che a due a due hanno intersezione in generale non vuota) si può ricoprire la "palla" $\mathcal{S}_3^2$ di raggio r_2. Poiché, per il corollario 6.8.5, l'unione disgiunta di tali copie è equiscomponibile con la "palla" $\mathcal{S}_3^1$ di raggio r_1, la "palla" $\mathcal{S}_3^2$ di raggio r_2 risulta equiscomponibile con un sottoinsieme della "palla" $\mathcal{S}_3^1$ di raggio r_1. Viceversa, attraverso la traslazione che porta il centro di $\mathcal{S}_3^1$ nel centro di $\mathcal{S}_3^2$ si ha la equiscomposizione (in una sola parte!) di $\mathcal{S}_3^1$ con un sottoinsieme di $\mathcal{S}_3^2$. Per il teorema di Banach – Schröder – Bernstein (6.4.1), $\mathcal{S}_3^1$ è equiscomponibile con $\mathcal{S}_3^2$, come si voleva.

Teorema 6.8.7 (Banach – Tarski, forma forte)

Siano A, B due insiemi di punti dello spazio, entrambi limitati e con interno non vuoto. Allora A e B sono equiscomponibili.

Dimostrazione – Per il teorema 6.4.1 (di Banach – Schröder – Bernstein), basterà dimostrare che A è equiscomponibile con un sottoinsieme di B e che B è equiscomponibile con un sottoinsieme di A.

Per il corollario 6.8.6, una qualsiasi palla contenente A (che esiste, perché per ipotesi A è limitato) è equiscomponibile con una qualsiasi palla $\mathcal{S}_3$ contenuta in B (che esiste, perché per ipotesi B ha interno non vuoto), dunque A è equiscomponibile con un sottoinsieme di $\mathcal{S}_3$ e quindi con un sottoinsieme di B.

Invertendo il ruolo di A e B nel ragionamento del paragrafo precedente si dimostra anche che B è equiscomponibile con un sottoinsieme di A, completando così la dimostrazione del teorema.