Capitolo 1

Elementi di teoria degli insiemi

1.1 Premessa, nozioni primitive, prime definizioni e proprietà

Premettiamo che quanto sarà esposto sulla teoria degli insiemi riguarda la cosiddetta teoria "ingenua" degli insiemi, dedotta dalla teoria cantoriana, che si contrappone alla teoria assiomatica, per il semplice fatto che, pur basandosi strettamente sui principi elementari della logica binaria (cioè della logica a due valori: vero o falso, sì o no), fa spesso ricorso all'intuizione.

Come in ogni teoria matematica, ovvero sistema ipotetico-deduttivo, risulta essenziale assumere come primitivi alcuni concetti, concetti, cioè, che non vengono definiti, ma che (traducendo nozioni comuni facilmente accessibili a livello intuitivo) vengono caratterizzati mediante le loro proprietà. Evidentemente, dal punto di vista di un'impostazione il più assiomatica possibile, risulta conveniente assumere il numero minimo di nozioni primitive.

Pertanto nella teoria ingenua degli insiemi assumeremo come concetti primitivi la nozione di *classe* e *la relazione di appartenenza*.

Intenderemo per classe un qualunque aggregato, collezione di enti di natura qualsiasi, che chiameremo *elementi* o *oggetti* della classe stessa. Ne segue che, assegnata una data classe, è contemporaneamente data la possibilità di decidere se un qualunque oggetto esistente o pensabile sia o meno oggetto di quella classe.

Se allora A è una qualunque classe ed a è un elemento della classe A, diremo che

$$a \textit{ appartiene} \text{ alla classe } A$$

ovvero, in simboli:

$$a \in A.$$

Resta così giustificata la seconda nozione primitiva, cioè la relazione di appartenenza.

Inoltre, per denotare il fatto che un certo oggetto b *non appartiene* ad una certa classe A, si scriverà:

$$b \notin A.$$

Per assegnare una classe, è necessario specificare gli elementi che essa contiene; ciò può essere fatto in tre modi apparentemente diversi:

1) si specificano in parole le proprietà delle quali deve godere un oggetto per appartenere alla classe in questione; ad es., dicendo che A è la classe di tutti i triangoli di un certo piano, la classe resta perfettamente individuata;

2) si elencano gli elementi della classe A; ad es., se A è la classe costituita da tutti i divisori (positivi) del numero naturale 30, si scriverà:

$$A = \{1,\, 2,\, 3,\, 5,\, 6,\, 10,\, 15,\, 30\};$$

3) si scrivono simbolicamente le proprietà delle quali devono godere gli elementi della classe; ad es., se A è la classe di tutti i numeri naturali divisibili per 5, si scriverà:

$$A = \{x \in \mathbb{N} :\ 5|x\}$$

dove con $\mathbb{N}$ indicheremo per il momento la classe di tutti i numeri naturali (cioè gli interi positivi) zero escluso (anche se spesso si include lo zero in $\mathbb{N}$; per denotare la classe dei naturali zero compreso, useremo la notazione $\mathbb{N}_0$); il simbolo ":" sta ad indicare l'espressione "tale che" (per la medesima espressione si usa anche il simbolo $|$); infine la scrittura "$5|x$" traduce simbolicamente la frase "5 divide x", ovvero "5 è un divisore di x" (il fatto che "$|$" si usa per "divide" fa preferire la scrittura ":" per "tale che").

Ora, la nozione di classe è estremamente generale; siamo interessati a classi particolari, i cosiddetti insiemi.

Precisamente, diremo che una classe A è un *insieme* se esiste una classe B della quale A è un oggetto.

Notiamo che tutte le classi dei precedenti esempi risultano, di fatto, insiemi.

Sembra allora inutile fare questa distinzione tra insieme e classe; l'inutilità è soltanto apparente, in quanto la distinzione è resa necessaria al fine di evitare alcuni paradossi, come, ad esempio, il seguente.

Consideriamo la classe Σ di tutti gli insiemi pensabili; sorge la questione di decidere se Σ è o meno un insieme. Se Σ fosse un insieme, allora esisterebbe una classe Σ' della quale Σ sarebbe un elemento, e ciò contraddirebbe la definizione di Σ; pertanto Σ è una classe (antinomia della classe totale).

La nascita della teoria degli insiemi (George Cantor, 1845-1918) ha contemporaneamente dato luogo alla scoperta di numerose "antinomie" relative alla teoria stessa, che mostravano la sua possibilità di definire in maniera rigorosa un insieme, onde la soluzione "ingenua" che è stata adottata[1]. Comunque, un esame approfondito della questione, oltre ad essere tutt'altro che semplice, esula dai limiti di questa esposizione; per l'esame, rimandiamo ai testi di logica e di critica sui fondamenti della matematica.

Osserviamo che le classi che avremo occasione di trattare saranno quasi sempre insiemi; quindi, d'ora in avanti, salvo esplicito avviso, consideriamo esclusivamente insiemi, descrivibili pertanto nei modi detti, con l'ausilio di altri simboli che saranno via via introdotti. Notiamo pure che il termine "classe" verrà anche adottato con un altro significato (come abbreviazione sia di "classe di equivalenza", che di "classe laterale"); dal contesto apparirà sempre chiaro, però, il significato del termine stesso.

1.2 Inclusione tra insiemi. Eguaglianza di sue insiemi. Insieme vuoto. Insieme universale.

Siano A e B due insiemi qualsivoglia. Se accade che ogni elemento dell'insieme B è anche elemento dell'insieme A, diremo che B *è contenuto* in A; in simboli:

$$B \subseteq A$$

La "relazione" che intercorre tra B ed A prende il nome di relazione di *inclusione* (in senso lato); se poi esiste qualche elemento di A che non è elemento di B (il che non è implicito nella definizione precedente), diremo che B *è strettamente contenuto in* A (inclusione in senso stretto) e scriveremo:

$$B \subset A$$

Introducendo alcuni simboli (dei quali faremo ampiamente uso), possiamo scrivere in maniera più contratta quanto già detto in parole; precisamente:

$$B \subseteq A \iff [\forall x \in B \Rightarrow x \in A]$$

[1] In definitiva, in molte di queste antinomie si viene a negare il principio del "terzo escluso", basilare nella logica binaria, che prevede che, se P è una qualunque affermazione, P non può essere contemporaneamente vera e falsa. Se una teoria matematica contiene una qualunque proposizione P, tale che siano vere (cioè dimostrabili) tanto P quanto la sua negativa, allora tale teoria è indecidibile, perchè contiene una contraddizione. Più in generale, si ottiene una antinomia, o paradosso, quando l'enunciato contiene una definizione impredicativa; precisamente quando un insieme M ed un oggetto m sono definiti in modo tale che m è un elemento di M, ma è definito soltanto facendo riferimento ad M, la definizione di M, o di m, si dice impredicativa.

che si legge: "B contenuto in A se, e soltanto se, quale sia x appartenente a B, risulta che x appartiene ad A".

Analogamente

$$B \subset A \iff [\forall x \in B \Rightarrow x \in A \text{ e } \exists y \in A : y \notin B]$$

cioè "B è contenuto in senso stretto in A se, e soltanto se, ogni elemento x di B è elemento di A ed esiste almeno un elemento y di A che non sia elemento di B".

Spieghiamo ora i simboli introdotti:
$\Rightarrow$ è il simbolo dell'implicazione semplice: se P e Q sono due proposizioni (affermazioni), scrivendo $P \Rightarrow Q$, intendiamo che l'affermazione Q è logica conseguenza dell'affermazione P (ma non è necessariamente vero il viceversa); ad esempio, se P è l'affermazione: "a è un parallelogramma" e Q è l'affermazione: "a è un quadrilatero", si può scrivere $P \Rightarrow Q$ ma $Q \not\Rightarrow P$ (un quadrilatero non è necessariamente un parallelogramma).
$\iff$ è il simbolo della doppia implicazione: Se P e Q sono due affermazioni, scrivendo $P \iff Q$, intendiamo dire che esse sono logicamente equivalenti (se, e soltanto se; occorre e basta; è necessario e sufficiente); ad esempio, "n è un numero pari" ed "n è divisibile per 2" (n essendo un numero naturale) sono due affermazioni equivalenti.
$\forall$ è il simbolo per indicare espressioni del tipo "per ogni", "quale che sia", ecc.; ed è uno dei cosiddetti "quantificatori", precisamente il quantificatore universale.
$\exists$ è il quantificatore esistenziale; con tale simbolo si identificano tutte le voci del verbo "esistere"; se poi si vuol precisare che un certo oggetto, oltre ad esistere, è unico, si usa la scrittura $\exists!$.

Useremo poi la congiunzione "e" per indicare che due affermazioni devono valere contemporaneamente.

Notiamo infine che si nega un simbolo, barrandolo, ad esempio:

$\nexists$	significa	"non esiste"
$\notin$	significa	"non appartiene"
$\not\Rightarrow$	significa	"non implica"

e così via.

Infine, dato che la frase "se e soltanto se" ricorre frequentemente in matematica, abbrevieremo tale espressione con "sse".

Passiamo ora a definire l' "eguaglianza" di due insiemi, tenendo presente che vogliamo "migliorare" la nozione intuitiva di eguaglianza; infatti, l'unico tipo di eguaglianza che logicamente abbia significato è la cosidetta "identità logica": due oggetti sono eguali sse sono lo stesso oggetto.

Di conseguenza, se A e B sono due insiemi, diremo che *A è eguale a B* e scriveremo:

$$A = B$$

sse ogni elemento di A è elemento di B e viceversa. Con la simbologia precedentemente introdotta, scriveremo:

$$A = B \iff [\forall x \in A \Rightarrow x \in B \text{ e } \forall y \in B \Rightarrow y \in A]$$

oppure

$$A = B \iff [x \in A \iff x \in B]$$

(le parentesi quadre vengono adottate per precisare la proposizione che viene implicata).

Ora, la seconda scrittura risulta indubbiamente più concisa della prima, ma questa, tenendo presente la definizione di inclusione, permette di scrivere:

$$A = B \iff [A \subseteq B \text{ e } B \subseteq A]$$

Quest'ultima espressione della eguaglianza di due insiemi è quella che si deve impiegare per verificare o dimostrare che due insiemi sono di fatto eguali, cioè sono lo stesso insieme.

Se non si precisa alcuna inclusione, e se non è $A = B$, si dirà che *A è diverso da B*, e si scriverà $A \neq B$.

Siano ora A e B due insiemi, e sia $A \subseteq B$; diremo che A è una parte di B, ovvero che A è un *sottoinsieme* (abbreviato in s.i.) di B. Se poi $A \subset B$, diremo che A è un s.i. *proprio* di B. Pertanto, ogni insieme si può interpretare come s.i. di sé stesso e si dirà s.i. *improprio*.

Se dati A e B, non risulta nè $A \subseteq B$ nè $B \subseteq A$, A e B si dicono anche *inconfrontabili*.

Dal punto di vista logico, ha significato considerare insiemi che non contengono alcun oggetto (ad esempio l'insieme dei triangoli con 4 vertici); un insieme di questo tipo prende il nome di *insieme vuoto* ed è convenzionalmente denotato con il simbolo $\emptyset$.
Dunque:

$$\emptyset = x : x \neq x$$

x essendo un qualunque oggetto. Poichè $x = x$, per definizione di identità logica, $x \neq x$ rappresenta una contraddizione, onde $\emptyset$ non può contenere alcun oggetto.

Notiamo che l'insieme vuoto è unico, cioè non esistono "diversi insiemi vuoti", e ciò in base alla defizione.

Assumiamo che l'insieme vuoto sia sottoinsieme di qualunque insieme; tale affermazione può però venir provata in maniera abbastanza semplice.

Talvolta si ha la necessità di considerare contemporaneamente più insiemi, e risulta conveniente poter interpretare questi come s.i. di un medesimo insieme, a tal scopo si introduce il cosidetto *insieme universale* (rispetto a un dato problema: la proprietà di essere universale è relativa al problema), che è un insieme tale da contenere come suoi sottoinsiemi (propri eøimpropri) tutti gli insiemi che interessa prendere in considerazione. Per esempio se

si considerano vari insiemi di poligoni di un piano, si può assumere come insieme universale l'insieme di tutti i poligoni del piano.

Notiamo che il simbolo "$\subseteq$" si può invertire. Precisamente, se $A \subseteq B$, cioè "A è comtenuto in B", allora è evidente che "B contiene A" e per esprimere questo fatto si scriverà

$$B \supseteq A$$

Esercizi

Esercizio 1.2.1. *Determinare alcuni dei sottoinsiemi dell'insieme A dei quadrilateri di un piano e le eventuali relazioni di inclusione tra essi.*

Sol.: Sono sottoinsiemi di A:

I = insieme dei quadrilateri inscrittibili in una circonferenza;
C = insieme dei quadrilateri circoscrittibili ad una circonferenza;
P = insieme dei parallelogrammi;
R = insieme dei rettangoli;
L = insieme dei rombi;
Q = insieme dei quadrati.

(Questi sottoinsiemi di A non esauriscono, ovviamente, la ttalità dei sottoinsiemi di A). Le relazioni di inclusione tra essi sono le seguenti, come è immediato verificare in base alle definizioni della geometria elementare:

$$Q \subseteq R \subseteq I;\ \ Q \subseteq R \subseteq P;\ \ Q \subseteq L \subseteq P;\ \ Q \subseteq L \subseteq C$$

Esercizio 1.2.2. *Determinare i sottoinsiemi propri $\neq \emptyset$ dei tre seguenti insiemi:*

$$S_1 = \{a\};\ \ S_2 = \{a, b\},\ (a \neq b);\ \ S_3 = \{a, b, c\},\ (a \neq b,\ a \neq c,\ b \neq c)$$

Sol.: I sottoinsiemi di S_1 sono $\emptyset$ ed S_1, onde S_1 non possiede sottoinsiemi propri, distinti da $\emptyset$.
I sottoinsiemi propri $\neq \emptyset$ di S_2 sono: $\{a\}$, $\{b\}$.
Infine, i sottoinsiemi propri di S_3 sono: $\{a\}$, $\{b\}$, $\{c\}$, $\{a, b\}$, $\{a, c\}$, $\{b, c\}$.

Esercizio 1.2.3. *Dimostrare che, se A è un sottoinsieme dell'insieme vuoto, allora $A = \emptyset$.*

Dim.: Osserviamo innanzitutto che, per provare che due insiemi X e Y coincidono, bisogna mostrare che valgono entrambe le relazioni di innclusione: $X \subseteq Y$ ed $Y \subseteq X$. Ora, per ipotesi, $A \subseteq \emptyset$; d'altra parte l'insieme vuoto è sottoinsieme di ogni insieme, cioè $\emptyset \subseteq A$. Ne segue $A = \emptyset$.

Esercizio 1.2.4. *Tenendo presente la seguente definizione di insieme contenente un solo elemento:*
Def.: Un insieme S è costituito esattamente da un elemento se:

1) $S \neq \emptyset$

2) l'unico s.i. proprio di S è $\emptyset$,

si definisca in maniera analoga un insieme costituito esattamente da due elementi.

Sol.: La seguente definizione traduce in maniera rigorosa la nozione intuitiva di insieme costituito da due elementi:
Def.: Diremo che l'insieme S è costituito esattamente da due elementi se:

1) S ha un s.i. proprio distinto da $\emptyset$;

2) ogni s.i. proprio di S distinto da $\emptyset$, è necessariamente costituito da un solo elemento.

Si noti che è immediato estendere la precedente definzione, ottenendo quella di insieme contenente esattamente n elementi.

1.3 Intersezione ed unione di insiemi e loro proprietà.

Assegnati due o più insiemi, è possibile costruire, a partire da questi, dei nuovi insiemi, e ciò in più modi (ottenendo - evidentemente - insiemi differenti).

Dati due insiemi A e B, i più semplici insiemi che, mediante essi, si possono costruire sono l'insieme intersezione di A e B e l'insieme unione di A e B, che ora passiamo a definire.

Precisamente, dati A e B, definiamo *insieme intersezione*, o semplicemente intersezione, di A e B, e lo denotiamo con il simbolo:

$$A \cap B$$

(da leggersi "A intersezione B"), l'insieme descritto da:

$$A \cap B = \{x : x \in A \text{ e } x \in B\};$$

$A \cap B$ è quindi l'insieme di tutti gli elementi che appartengono contemporaneamente all'insieme A ed all'insieme B (si noti la congiunzione "e" nella definizione).

Ad esempio, se A è l'insieme dei divisori di 30 e B è l'insieme dei divisori di 20, allora

$$A \cap B = \{1, 2, 5, 10\}$$

Evidentemente, è possibile che non esista alcun elemento che appartenga contemporaneamente ad A e B; in tal caso, risulta:

$$A \cap B = \emptyset$$

ed A e B si dicono *disgiunti*. Ad esempio, se A è l'insieme dei triangoli di un piano e B l'insieme dei quadrati di un piano, risulta $A \cup B = \emptyset$.

Dalla definizione di insieme intersezione segue subito che:

$$A \cap B = B \cap A$$

e ciò esprime la proprietà *commutativa* dell'intersezione.

Ancora dalla definizione segue che:

$$\begin{aligned} \forall x \in A \cap B &\Rightarrow x \in A \\ \forall x \in A \cap B &\Rightarrow x \in B \end{aligned}$$

Pertanto $A \cap B$ è un sottoinsieme sia di A che di B.

Supponiamo ora che sia $B \subseteq A$; risulta allora $A \cap B = B$. In particolare, se $A = B$, essendo $A \subseteq A$ si avrà:

$$A \cap A = A$$

che esprime *l'idempotenza* dell'intersezione.

È possibile definire anche l'intersezione di più di due insiemi. A tale scopo considereremo innanzitutto tre insiemi A, B, C ed i due insiemi $(A \cap B) \cap C$ e $A \cap (B \cap C)$.
Proviamo che

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

cioè che l'intersezione gode della proprietà *associativa*.

Per semplicità, poniamo $D = A \cap B$ ed $E = B \cap C$. Allora

$$\begin{aligned} D &= \{x : x \in A \text{ e } x \in B\} \\ E &= \{x : x \in B \text{ e } x \in C\} \end{aligned}$$

Quindi:

$$\begin{aligned} (A \cap B) \cap C = D \cap C &= \{x : x \in D \text{ e } x \in C\} \\ &= \{x : x \in A \text{ e } x \in B \text{ e } x \in C\} \end{aligned}$$

$$\begin{aligned} A \cap (B \cap C) = A \cap E &= \{x : x \in A \text{ e } x \in E\} \\ &= \{x : x \in A \text{ e } x \in B \text{ e } x \in C\} \end{aligned}$$

onde l'eguaglianza.

Dalla validità della proprietà associativa segue che possiamo omettere le parentesi (oppure associare in un modo qualsiasi gli insiemi) e scrivere:

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

Pertanto, è possibile definire l'intersezione di un numero qualsivoglia di insiemi, procedendo per gradi: si intersecano due insiemi qualsiasi, l'insieme così ottenuto si interseca con un altro insieme e si procede sino ad ottenere due insiemi soltanto, che vengono intersecati tra di loro.

Se sono assegnati n insiemi A_1, A_2, $\ldots$, A_n, si scriverà anche

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$$

dove il secondo membro rappresenta una scrittura più compatta del primo membro.

Inoltre, l'idempotenza precedentemente provata, permettedi affermare che

$$\forall n \in N,\ \underbrace{A \cap A \cap \cdots \cap A}_{n \text{ volte}} = A$$

Infine, dati A_1, A_2, $\ldots$, A_n, si ha che

$$\forall i \in \{1, 2, \ldots, n\},\ \bigcap_{i=1}^{n} A_i \subseteq A_i$$

Passiamo ora a definire l'unione di due o più insiemi.

Siano A e B due insiemi; definiamo *insieme unione*, o semplicemente unione, di A e B, e lo denotiamo con

$$A \cup B$$

l'insieme descritto da

$$A \cup B = \{x : x \in A \text{ o } x \in B\}$$

$A \cup B$ contiene quindi tutti gli elementi di A e tutti gli elementi di B; allora contiene anche $A \cap B$.

Notiamo che l' "o" della definizione di $A \cup B$ è il cosidetto 'o disgiuntivo', ovvero 'o inclusivo', che non esclude la congiunzione (cioè il fatto che $x \in A$ non esclude il fatto che $x \in B$).

Ad esempio, se $A = \{a, b, c, d\}$ e $B = \{a, b, x, y, z\}$, si avrà:

$$A \cup B = \{a, b, c, d, x, y, z\}$$

(gli elementi di $A \cap B$ si scrivono una sola volta in $A \cup B$).

Dalla definizione di unione segue subito che

$$A \cup B = B \cup A$$

cioè l'unione gode della proprietà *commutativa*.

Ancora dalla definizione segue che:

$$\begin{array}{llll} \forall x \in A, & \forall B & \Rightarrow & [x \in A \Rightarrow x \in A \cup B] \\ \forall A, & \forall x \in B & \Rightarrow & [x \in B \Rightarrow x \in A \cup B] \end{array}$$

e ciò traduce il fatto che

$$\begin{array}{ll} A \subseteq A \cup B & \forall \text{ insieme } B \\ B \subseteq A \cup B & \forall \text{ insieme } A \end{array}$$

Se ora si tengono presenti le inclusioni stabilite per l'intersezione, si ha immediatamente che:

$$A \cap B \subseteq A \subseteq A \cup B$$

$$A \cap B \subseteq B \subseteq A \cup B.$$

In particolare, se $A = B$, avremo

$$A \cup A = A;$$

infatti,

$$A \cup A = \{x : x \in A \text{ o } x \in A\} = \{x : x \in A\} = A.$$

Quindi l'unione è *idempotente*.

Si noti che $A \cup B$ si può anche definire come l'intersezione di tutti gli insiemi che contengono sia A che B.

Come nel caso dell'intersezione, prima di estendere l'unione di due insiemi ad un numero qualsivoglia di insiemi, proviamo che l'unione gode della proprietà *associativa*, cioè che - dati comunque tre insiemi A, B, C - risulta:

$$A \cup (B \cup C) = (A \cup B) \cup C.$$

Per provare questa eguaglianza occorre e basta provare che ogni elemento del primo membro è anche elemento del secondo membro e viceversa. Ora

$$\begin{array}{rcl} x \in A \cup (B \cup C) & \Rightarrow & x \in A \text{ o } x \in B \cup C \quad \Rightarrow \quad x \in A \text{ o } x \in B \text{ o } x \in C \quad \Rightarrow \\ & \Rightarrow & x \in A \cup B \text{ o } x \in C \quad \Rightarrow \quad x \in (A \cup B) \cup C. \end{array}$$

Analogamente (invertendo il verso delle implicazioni) si prova che

$$x \in (A \cup B) \cup C \Rightarrow x \in A \cup (B \cup C).$$

È pertanto lecito sopprimere le parentesi e resta definita l'unione di tre insiemi:

$$A \cup B \cup C = A \cup (B \cup C) = (A \cup B) \cup C.$$

Quindi si può definire l'unione di un numero qualsivoglia di insiemi: si determina l'unione di due di essi, di questo insieme si individua l'unione con un altro e si procede analogamente fino ad ottenere due soli insiemi, dei quali si trova l'unione.

Qualora siano assegnati n insiemi A_1, A_2, $\ldots$, A_n, per la loro unione scriveremo:

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$$

e valgono le proprietà analoghe a quelle stabilite per l'intersezione.

Tra unione ed intersezione esiste un importante legame costituito dalle cosidette leggi *distributive*; precisamente:

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ proprietà distributiva della intersezione rispetto all'unione

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ proprietà distributiva della unione rispetto all'intersezione

Proviamo la prima delle due leggi distributive (la seconda si prova in maniera analoga). Dobbiamo allora provare che

$$x \in A \cap (B \cup C) \iff x \in (A \cap B) \cup (A \cap C)$$

Ora

$$\begin{array}{rcll} x \in A \cap (B \cup C) & \Rightarrow & x \in A \text{ e } x \in B \cup C & \Rightarrow \\ & \Rightarrow & [x \in A \text{ e } [x \in B \text{ o } x \in C]] & \Rightarrow \\ & \Rightarrow & [[x \in A \text{ e } x \in B] \text{ o } [x \in A \text{ e } x \in C]] & \Rightarrow \\ & \Rightarrow & x \in (A \cap B) \cup (A \cap C); & \end{array}$$

d'altra parte

$$\begin{array}{rcll} x \in (A \cap B) \cup (A \cap C) & \Rightarrow & [x \in A \cap B \text{ o } x \in A \cap C] & \Rightarrow \\ & \Rightarrow & [[x \in A \text{ e } x \in B] \text{ o } [x \in A \text{ e } x \in C]] & \Rightarrow \\ & \Rightarrow & [x \in A \text{ e } [x \in B \text{ o } x \in C]] & \Rightarrow \\ & \Rightarrow & [x \in A \text{ e } x \in B \cup C] & \Rightarrow \\ & \Rightarrow & x \in A \cap (B \cup C); & \end{array}$$

onde l'asserto.

Notiamo che, qualora $C = A$, le leggi distributive forniscono le cosidette leggi di *assorbimento*:

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

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

in quanto $B \cap A \subseteq A$ ed $A \subseteq B \cup A$.

L'introduzione dell'unione di più insiemi permette di dare una semplice costruzione dell'insieme universale (rispetto ad un certo problema): è sufficiente assumere come insieme universale l'unione di tutti gli insiemi che interessano.

Altre proprietà relative all'unione e all'intersezione di due insiemi saranno viste negli esercizi.

Osserviamo, infine, che alla "costruzione" degli insiemi intersezione ed unione si darà nel seguito anche un altro significato, ma per fare ciò, è necessario introdurre la nozione di "operazione" su un insieme.

Esercizi

Esercizio 1.3.1. *Si dimostri che, quali che siano gli insiemi A e B, risulta:*

$$A \cup B = A \iff B \subseteq A$$

$$A \cap B = A \iff A \subseteq B$$

Dim.: Si ha:

$$[A \cup B = A] \Rightarrow [x \in A \cup B \iff x \in A] \Rightarrow B \subseteq A.$$

Il viceversa è evidente. Similmente, si ha:

$$[A \cap B = A] \Rightarrow [x \in A \cap B \iff x \in A] \Rightarrow A \subseteq B,$$

per definizione di intersezione, e viceversa.

Esercizio 1.3.2. *Si dimostri che*

$$\emptyset \cup A = A$$

e

$$\emptyset \cap A = \emptyset$$

quale che sia l'insieme A.

Dim.: Dato che l'insieme vuoto è sottoinsieme di ogni insieme, le due affermazioni sono conseguenza delle proprietà dell'unione e dell'intersezione, illustrate a pag.11 (cioè $A \cap B \subseteq A \subseteq A \cup B$, $A \cap B \subseteq B \subseteq A \cup B$.)

Esercizio 1.3.3. *Si dimostri che*

$$A \cup B = \emptyset \Rightarrow A = \emptyset \; e \; B = \emptyset$$

Dim.: Per definizione di unione, $A \cup B$ contiene tutti gli elementi che sono o in A, o in B. Se $A \cup B = \emptyset$, allora non esiste alcun elemento che appartenga ad A, e non esiste alcun elemento che appartenga a B, onde l'asserto. Ovviamente, vale anche il viceversa della proposizione ora dimostrata.

Esercizio 1.3.4. *Si provi che, quali che siano gli insiemi A e B, risulta:*

$$A \cap B \subseteq A \cup B$$

Si precisi quando vale il segno di uguaglianza.

Sol.: In virtù delle proprietà di inclusione dell'unione e dell'intersezione (vedi pag.11), si ha $A \cap B \subseteq A \subseteq A \cup B$, onde l'asserto.
Affinché valga il segno di eguaglianza, dev'essere:

$$A \cap B = A = A \cup B,$$

da cui $B = A$, come coseguenza delle proprietà di idempotenza.

Esercizio 1.3.5. *Si dimostri le proprietà commutativa dell'unione e dell'intersezione di due insiemi.*

Dim.: Per definizione di unione, si ha:

$$x \in A \cup B \;\Rightarrow\; [x \in A \text{ oppure } x \in B] \;\Rightarrow\; [x \in B \text{ oppure } x \in A] \;\Rightarrow \\ \Rightarrow\; x \in B \cup A$$

e viceversa. Similmente si prova la commutatività dell'intersezione.

Esercizio 1.3.6. *Si provi che, quali che siano i tre insiemi A, B, C,*

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

*Dim.*Applicando la proprietà associativa e le leggi distributive, si ha:

$$\begin{aligned}(A \cup B) \cap (B \cup C) \cap (C \cup A) &= ((A \cup B) \cap (B \cup C)) \cap (C \cup A) \\ &= (B \cup (A \cap C)) \cap (C \cup A) \\ &= (B \cap (C \cup A)) \cup ((A \cap C) \cap (C \cup A)) \\ &= (B \cap C) \cup (B \cap A) \cup (A \cap C).\end{aligned}$$

Esercizio 1.3.7. *Siano A, B, C tre insiemi, si provi che*

$$A \cup B = A \cup C \not\Rightarrow B = C$$

e che

$$A \cap B = A \cap C \not\Rightarrow B = C$$

Si dica se, e quando, possono valere le implicazioni.

Sol. Se $A \cap B = \emptyset$ e $A \cap C = \emptyset$, allora $A \cup B = A \cup C \Rightarrow B = C$; negli altri casi, $A \cap B$, $A \cap C \subseteq A$ sono insiemi differenti, onde non è $B = C$.

Similmente, $A \cap B = A \cap C$ implica soltanto che B e C hanno uno stesso sottoinsieme. Nel caso particolare in cui $A \cap B = \emptyset$ e $A \cap C = \emptyset$, si constata subito che B e C possono essere insiemi qualsiasi. Se $B, C \subseteq A$, allora

$$A \cap B = A \cap C \Rightarrow B = C$$

In generale si ha poi

$$A \cup B = A \cup C \text{ e } A \cap B = A \cap C \Rightarrow B = C$$

Infatti

$$A \cup B = A \cup (B \setminus (A \cap B)) = A \cup (C \setminus (A \cap C)) \Rightarrow B \setminus (A \cap B) = C \setminus (A \cap C)$$

(dato che $(B \setminus (A \cap B)) \cap A = \emptyset$ e $(C \setminus (A \cap C)) \cap A = \emptyset$),
da cui

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

cioè $A \cap B$ ha lo stesso complementare (vedi par.1.4, per la definizione di complementare) sia in B che in C (si ricordi che $A \cap B \subseteq B$ e $A \cap C \subseteq C$). Ne segue che $B = C$.

Esercizio 1.3.8. *Sia A l'insieme dei divisori del numero naturale 54 e sia B l'insieme dei multipli del numero 9; determinare $A \cup B$ ed $A \cap B$.*

Sol.: Si ha $A = \{1, 2, 3, 6, 18, 27, 54\}$ e $B = \{9n : n \in \mathbb{N}\}$.
Quindi

$$A \cup B = \{1, 2, 3, 6, 9n \text{ con } n \in \mathbb{N}\}$$

ed

$$A \cap B = \{9, 18, 27, 54\}$$

Esercizio 1.3.9. *Sia A l'insieme dei divisori di 144 e sia B l'insieme dei divisori di 512. Determinare $A \cap B$ e verificare che tale insieme contiene il massimo comun divisore dei due numeri naturali dati.*

Sol.: Abbiamo

$$A = \{1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 36, 48, 72, 144\}$$

e

$$B = \{1, 2, 4, 8, 16, 32, 64, 128, 256, 512\};$$

quindi $A \cap B = \{1, 2, 4, 8, 16\}$. Il maggiore dei numeri che sono elementi di $A \cap B$ è il massimo comun divisore di 144 e 512

Esercizio 1.3.10. *Sia A l'insieme dei multipli positivi di 3, B l'insieme dei multipli positivi di 5 e C l'insieme dei multipli positivi di 7. Determinare $A \cup B \cup C$, $A \cap B \cap C$, $A \cup (B \cap C)$ ed $A \cap (B \cup C)$.*

Sol.: Avremo: $A = \{3n : n \in \mathbb{N}\}$, $B = \{5n : n \in \mathbb{N}\}$ e $C = \{7n : n \in \mathbb{N}\}$. Quindi $A \cup B \cup C$ è costituito dai numeri che sono divisibili per 3, oppure per 5, oppure per 7, cioè:

$$A \cup B \cup C = \{3n, 5m, 7q : n, m, q \in \mathbb{N}\}.$$

$A \cap B \cap C$ è invece l'insieme dei numeri che sono contemporaneamente divisibili per 3, 5, 7, quindi che sono divisibili per $3 \cdot 5 \cdot 7 = 105$ cioè

$$A \cap B \cap C = \{105n : n \in \mathbb{N}\}.$$

$B \cap C$ è l'insieme dei numeri divisibili per 35, quindi

$$A \cup (B \cap C) = \{3n, 35m : n, m \in \mathbb{N}\}.$$

Per determinare $D = A \cap (B \cup C)$, ricordiamo che è

$$D = (A \cap B) \cup (A \cap C);$$

pertanto

$$D = \{15n, 21m : n, m \in \mathbb{N}\}.$$

Esercizio 1.3.11. *Sia A l'insieme dei multipli (interi) positivi del numero naturale 12 e sia B l'insieme dei multipli (interi) positivi del numero naturale 18. Si determini $A \cup B$ e si verifiche che tale insieme contiene il minimo comune multiplo di 12 e 18.*

Sol.: Avremo:

$$A = \{12n : n \in \mathbb{N}\}, \quad B = \{18m : m \in \mathbb{N}\};$$

quindi, per definizione di unione di due insiemi, si ha:

$$A \cup B = \{12n, 18m : n, m \in \mathbb{N}\}.$$

Ne segue che per $n = 3$ ed $m = 2$ si ottiene il numero 36, che, di fatto, è il m.c.m. di 12 e 18.

Esercizio 1.3.12. *Siano m ed n due numeri naturali assegnati e siano A e B rispettivamente l'insieme dei divisori di m e l'insieme dei divisori di n. Si caratterizzino le coppie di naturali m ed n tali che risulti $A \cap B = \{1\}$.*

Sol.: Poiché A è l'insieme dei divisori di m, si ha:

$$A = \{x \in \mathbb{N} : x \mid m\}.$$

Similmente

$$B = \{z \in \mathbb{N} : z \mid n\}.$$

Gli elementi di $A \cap B$ sono i divisori comuni di m ed n, cioè i naturali y tali che esistano $h, k \in \mathbb{N}$, per i quali risulti: $y \cdot h = n$, $y \cdot k = m$. Pertanto, affiché sia

$$A \cap B = \{y \in \mathbb{N} : [y \mid n,\ y \mid m]\} = \{1\},$$

i due numeri assegnati devono essere primi tra loro. A questo risultato si poteva pervenire anche osservando che $A \cap B$ contiene il massimo comun divisore di m ed n (in quanto contiene tutti e soli i divisori di m ed n) e questo è uguale ad 1 se, e soltanto se, i due numeri sono primi tra loro (in particolare se sono due numeri primi).

Esercizio 1.3.13. *Dimostrare che*

$$B \subset A \Rightarrow B \cup C \subset A \cup C,$$

$$B \subset A \Rightarrow B \cap C \subset A \cap C,$$

quale che sia l'insieme C.

Dim.: Da $B \subset A$ segue che ogni elemento di B è pure elemento di A. Proviamo la prima delle due implicazioni. Se $x \in B \cup C$, allora o $x \in B$, e quindi $x \in A$, per ipotesi e pertanto $x \in A \cup C$, quale che sia C; oppure $x \in C$, ma allora $x \in A \cup C$.

Proviamo la seconda implicazione. Se $x \in B \cap C$, allora x appartiene contemporaneamente a B ed a C e, in quanto elemento di B, è anche elemento di A, in virtù dell'ipotesi; ma x appartiene pure a C: ne segue che $x \in A \cap C$.

Esercizio 1.3.14. *Dati due insiemi A e B, diremo che essi sono 'confrontabili' se $A \neq B$ e se $A \subset B$, oppure se $B \subset A$. Dimostrare che se A e B sono entrambi non vuoti e sono disgiunti, cioè è $a \cap B = \emptyset$, allora A e B non sono confrontabili.*

Dim.: Supponiamo che sia $A \subset B$: allora ogni elemento di A è anche elemento di B, e pertanto che $A \cap B = A$, contro l'ipotesi.

Esercizio 1.3.15. *Siano A e B due insiemi distinti non confrontabili; dimostrare che A e B non sono necessariamente disgiunti.*

Dim.: Se A e B non sono confrontabili, allora è $A \not\subset B$ e $B \not\subset A$; ciò comporta semplicemente:

$$A \cap B \subset A \text{ ed } A \cap B \subset B$$

(l'inclusione essendo in senso stretto) e non si può quindi affermare che $A \cap B = \emptyset$: se per esempio è $A = \{a, b, c\}$, $B = \{a, b, d\}$, allora $A \cap B = \{a, b\} \neq \emptyset$.

1.4 Insieme complementare. Differenza di due insiemi. Differenza Simmetrica.

Sia ora S un insieme qualunque e sia A un s.i. di S, cioè $A \subseteq S$. Ha allora significato considerare l'insieme di tutti gli elementi di S che non appartengono ad A. Tale insieme prende il nome di *insieme complementare*, o semplicemente complementare, di A in S e viene denotato con $\mathcal{C}_S A$. Quindi,

$$\mathcal{C}_S A = \{x \in S : x \notin A\}$$

Qualora l'insieme S sia sottinteso si scriverà anche $\mathcal{C}A$ oppure A' in luogo di $\mathcal{C}_S A$.

Evidentemente, $\mathcal{C}_S(\mathcal{C}_S A) = A$.

Questa definizione di complementare suggerisce la definizione di *differenza* di due insiemi. Infatti, $\mathcal{C}_S A$ è costituito da tutti gli elementi di S "meno" gli elementi di A, cioè

$$\mathcal{C}_S A = S \setminus A$$

(si usa scrivere $S \setminus A$ invece di $S - A$, anche se la seconda scrittura si trova egualmente nella letteratura).

Possiamo eliminare l'ipotesi restrittiva $A \subseteq S$ e definire la *differenza*, o insieme differenza, di due insiemi A e B (nell'ordine) nel modo seguente:

$$A \setminus B = \{x \in A : x \notin B\};$$

dunque:

$$A \setminus B = \mathcal{C}_A B = A \setminus (A \cap B).$$

In base alla definizione, è immediato che (in generale)

$$A \setminus B \neq B \setminus A;$$

ovvero, la differenza di due insiemi non è commutativa.

Sorge allora la questione di introdurre un insieme analogo all'insieme differenza, che però goda della proprietà commutativa. Ciò è possibile, considerando la cosidetta *differenza simmetrica* di due insiemi A e B, che denoteremo con il simbolo

$$A \triangle B$$

Per definire $A \triangle B$, supponiamo che A e B siano s.i. di un medesimo insieme S (e ciò è sempre possibile: basta assumere $S \supseteq A \cup B$) e denotiamo con A' e B' i loro complementari (in S).
Avremo allora

$$A \triangle B = (A \cup B) \setminus (A \cap B) = (A \cap B') \cup (A' \cap B)$$

(l'eguaglianza delle due espressioni di $A \triangle B$ si prova facilmente: cfr. es.1.4.28)

Data la commutatività dell'unione e dell'intersezione, è immediato che

$$A \triangle B = B \triangle A,$$

onde la differenza simmetrica gode della proprietà commutativa.

Notiamo infine che, per quanto riguarda i complementari degli insiemi unione ed intersezione, sussistono le sguenti leggi di De Morgan:

$$(A \cap B)' = A' \cup B'$$

$$(A \cup B)' = A' \cap B'$$

Proviamo, ad esempio, la prima (la seconda si dimostra in maniera analoga), cioè proviamo che

$$x \in (A \cap B)' \iff x \in A' \cup B'$$

Si ha

$$\begin{array}{rcccl} x \in (A \cap B)' & \Rightarrow & x \notin A \cap B & \Rightarrow & x \notin A \text{ e } B \quad \Rightarrow \\ & \Rightarrow & x \in A' \text{ o } x \in B' & \Rightarrow & x \in A' \cup B'; \end{array}$$

d'altra parte

$$\begin{array}{rcccl} x \in A' \cup B' & \Rightarrow & x \in A' \text{ o } x \in B' & \Rightarrow & x \notin A \text{ o } x \notin B \quad \Rightarrow \\ & \Rightarrow & x \notin A \cap B & \Rightarrow & x \in (A \cap B)' \end{array}$$

onde resta provata la prima delle due leggi di De Morgan.

Notiamo il fatto fondamentale stabilito dall'inversione dell' inclusione nel passaggio al complementare, precisamente

$$A \subseteq B \iff A' \supseteq B'.$$

Infatti:

$$\begin{array}{rcccl} A \subseteq B & \Rightarrow & [\forall x \in A \Rightarrow x \in B] & \Rightarrow & [x \notin B \Rightarrow x \notin A] \quad \Rightarrow \\ & \Rightarrow & [x \in B' \Rightarrow x \in A'] & \Rightarrow & B' \subseteq A' \end{array}$$

e viceversa (scambiando il ruolo di A e B rispettivamente con quello di B' e A').

Si osservi che la relazione precedente non è altro che un'applicazione del principio di logica (principio di contrapposizione) espresso da:

$$[\mathcal{P} \Rightarrow \mathcal{Q}] \iff [\tilde{}\mathcal{Q} \Rightarrow \tilde{}\mathcal{P}]$$

dove $\tilde{}\mathcal{Q}$ denota "non $\mathcal{Q}$", cioè la negazione della proposizione $\mathcal{Q}$ e $\tilde{}\mathcal{P}$ denota "non $\mathcal{P}$".

Tale principio è quello costantemente impiegato nella cosiddetta "dimostrazione per assurdo": per provare che dall'ipotesi $\mathcal{P}$ segue la tesi $\mathcal{Q}$, occorre e basta provare che dalla negazione della tesi, $\tilde{}\mathcal{Q}$, segue la negazione dell'ipotesi $\tilde{}\mathcal{P}$.

In questi termini, la

$$A \subseteq B \iff B' \subseteq A'$$

si traduce in

$$[x \in A \Rightarrow x \in B] \iff [x \notin B \Rightarrow x \notin A] \iff [x \in B' \Rightarrow x \in A']$$

dove $\mathcal{P}$ è $''x \in A''$, $\mathcal{Q}$ è $''x \in B''$, $\tilde{}\mathcal{Q}$ è $''x \notin B''$ (ovvero $''x \in B'''$) e $\tilde{}\,\mathcal{P}$ è $''x \notin A''$ (ovvero $''x \in A'''$).

Altre proprietà relative ai complementari, alla differenza ed alla differenza simmetrica di due insiemi saranno esaminate negli esercizi.

Esercizi

Esercizio 1.4.1. *Si provi che per ogni insieme S risulta:*

$$\mathcal{C}_S\emptyset = S,\ \mathcal{C}_S S = \emptyset.$$

Dim.: Per definizione di complementare, si ha $\mathcal{C}_S\emptyset = S \setminus \emptyset = S$, in quanto l'insieme vuoto non contiene alcun elemento. Similmente, $\mathcal{C}_S S = S \setminus S = \emptyset$, perché l'insieme $S \setminus S$ contiene tutti gli elementi di S che non appartengono ad S, cioè non contiene alcun elemento.

Esercizio 1.4.2. *Sia S un qualunque insieme e sia $A \subseteq S$; si provi che:*

$$A = \mathcal{C}_S A,\ \Longleftrightarrow\ S = \emptyset$$

Dim.: Se $S = \emptyset$, allora l'unico sottoinsieme di S è S stesso, quindi coincide con il suo complementare. Viceversa, se $A = \mathcal{C}_S A$, si ha:

$$\begin{array}{rcl} [A = \mathcal{C}_S A] & \Rightarrow & [x \in A \iff x \in \mathcal{C}_S A] \quad \Rightarrow \quad [x \in A \iff x \notin A] \Rightarrow \\ & \Rightarrow & [x \in A \iff x \in S \setminus A] \quad \Rightarrow \quad [x \in A \iff [x \in S,\ x \notin A]]; \end{array}$$

si ottiene così una contraddizione logica, perché in questo modo non si può definire alcun elemento, onde $S = \emptyset$.

Esercizio 1.4.3. *Sia S un qualunque insieme e sia $A \subseteq S$. Si provi che:*

$$\mathcal{C}_S(\mathcal{C}_S A) = A.$$

Dim.: Dalla definizione di complementare, cioè dalla

$$\mathcal{C}_S A = \{x \in S : x \notin A\},$$

segue che

$$\mathcal{C}_S(\mathcal{C}_S A) = \{x \in S : x \notin \mathcal{C}_S A\} = \{x \in S : x \notin S \setminus A\} = \{x \in S : x \in A\} = A.$$

ossia l'asserto.

Esercizio 1.4.4. *Siano A e B due insiemi qualsiasi (sottoinsiemi di un medesimo insieme S); si provi che:*

$$A \subseteq B \iff A' \supseteq B'.$$

Dim.: Supponiamo che sia $A \subseteq B$; si ha allora:

$$x \in B' \Rightarrow x \notin B \Rightarrow x \notin A \rightarrow x \in A' \Rightarrow A' \supseteq B'.$$

Viceversa, sia $B' \subseteq A'$; allora si ha:

$$x \in (A')' \Rightarrow x \notin A' \Rightarrow x \notin B' \Rightarrow x \in (B')';$$

quindi

$$x \in (A')' \Rightarrow x \in (B')';$$

ma è $(A')' = A$ e $(B')' = B$, onde $x \in A \Rightarrow x \in B$, cioè $A \subseteq B$. Ne segue l'asserto.

Esercizio 1.4.5. *Si provi che per ogni sottoinsieme A di un qualunque insieme S, risulta:*

$$A \cup A' = S,\ A \cap A' = \emptyset.$$

Dim.: In virtù delle definzioni di complementare e di unione, si ha:

$$\begin{array}{rcl} A \cup A' & = & \{x \in S : [x \in A \text{ oppure } x \in A']\} \quad = \\ & = & \{x \in S : [x \in A \text{ oppure } x \notin A]\} \quad = \quad S. \end{array}$$

Similmente, tenendo conto della definizione di intersezione, si ha:

$$\begin{array}{rcl} A \cap A' & = & \{x \in S : [x \in A \text{ ed } x \in A']\} \quad = \\ & = & \{x \in S : [x \in A \text{ ed } x \notin A]\} \quad = \quad \emptyset; \end{array}$$

infatti si ottiene una contraddizione logica nella defizione dell'insieme $A \cap A'$, onde questo non contiene alcun elemento.

Esercizio 1.4.6. *Siano A e B sottoinsiemi dell'insieme S. Si provi che:*

$$A \cap B = \emptyset \Rightarrow A \subseteq B.$$

Sol.: Tenendo conto dell'ipotesi, si ha:

$$\begin{array}{rcl} [A \cap B' = \emptyset] & \Rightarrow & [x \in A \Rightarrow x \notin B'] \quad \Rightarrow \\ & \Rightarrow & [x \in A \Rightarrow x \in B] \quad \Rightarrow \quad A \subseteq B, \end{array}$$

cioè l'asserto. Si poteva provare l'enunciato anche nel modo seguente:

$$\begin{array}{rcl} [A \cap B' = \emptyset] & \Rightarrow & [x \in B' \Rightarrow x \notin A] \quad \Rightarrow \quad [x \in B' \Rightarrow x \in A'] \quad \Rightarrow \\ & \Rightarrow & B' \subseteq A' \qquad\qquad \Rightarrow \quad A \subseteq B \end{array}$$

(cfr. esercizio1.4.4).

Esercizio 1.4.7. *Siano A e B sottoinsiemi dell'insieme S; si provi che:*

$$A \cap B' = (A' \cup B)'.$$

Sol.: Si deve provare che

$$x \in A \cap B' \iff x \in (A' \cup B)'.$$

Dimostriamo $\Rightarrow$ (cioè l'implicazione nel verso da sinistra a destra).
Si ha:

$$\begin{array}{rcl} x \in A \cap B' & \Rightarrow & x \in A \text{ e } x \in B' \quad \Rightarrow \quad x \notin A' \text{ e } x \notin B \quad \Rightarrow \\ & \Rightarrow & x \notin A' \cup B \qquad \Rightarrow \quad x \in (A' \cup B)'. \end{array}$$

Ne segue $A \cap B' \subseteq (A' \cup B)'$. Viceversa ($\Leftarrow$),

$$\begin{array}{rcl} x \in (A' \cup B)' & \Rightarrow & x \notin (A' \cup B) \qquad \Rightarrow \quad x \notin A' \text{ e } x \notin B \quad \Rightarrow \\ & \Rightarrow & x \in A \text{ e } x \in B' \quad \Rightarrow \quad x \in A \cap B'. \end{array}$$

Pertanto $(A' \cup B)' \subseteq A \cap B'$.

Dalle due inclusioni opposte segue l'asserto.

Si noti che l'eguaglianza posta è un'immediata conseguenza delle leggi di De Morgan; infatti:

$$(A' \cup B)' = (A')' \cap B' = A \cap B'$$

Esercizio 1.4.8. *Si dimostri che:*

$$A \setminus B = B \setminus A \iff A = B.$$

Dim.: Se $A = B$, allora per definzione di differenza, si ha $A \setminus A = \emptyset$, onde l'asserto. Viceversa:

$$\begin{array}{lll} [A \setminus B = B \setminus A] & \Rightarrow & [x \in A \setminus B \iff x \in B \setminus A] \qquad \Rightarrow \\ & \Rightarrow & [[x \in A,\ x \notin B] \iff [x \notin A,\ x \in B]], \end{array}$$

ma in tal modo non si definisce alcun elemento, perché si ottiene una contraddizione logica, onde $A \setminus B = B \setminus A = \emptyset$, da cui $A = B$, per defizione di differenza.

Esercizio 1.4.9. *Dato comunque un insieme A, dimostrare che, quale che sia B, si ha*

$$A = (A \cap B) \cup (A \setminus B).$$

Dim.: Dobbiamo provare che ogni elemento del primo membro è elemento del secondo, e viceversa.
Sia $x \in A$, $x \notin B$, allora $x \notin A \cap B$, ma $x \in A \setminus B$; ne segue che $x \in (A \cap B) \cup (A \setminus B)$. Sia invece $x \in A$, $x \in B$, allora $x \in A \cap B$, $x \in A \setminus B$; comunque $x \in (A \cap B) \cup (A \setminus B)$. Pertanto $A \subseteq (A \cap B) \cup (A \setminus B)$.
Sia ora x un elemento del secondo membro. Se $x \in (A \cap B) \cup (A \setminus B)$, o $x \in A \cap B$, nel qual caso $x \in A$, oppure $x \in A \setminus B$ ed allora appartiene ad A; ne segue $(A \cap B) \cup (A \setminus B) \subseteq A$, onde l'asserto.

Esercizio 1.4.10. *Dati comunque due insiemi A e B dimostrare che:*

$$B \cap (A \setminus B) = \emptyset$$

Dim.: Poiché $A \setminus B$ è il complementare di B rispetto ad A, esso non contiene alcun elemento di B, onde l'asserto.

Esercizio 1.4.11. *Dati comunque due insiemi distinti A e B dimostrare che gli insiemi $A \setminus B$, $A \cap B$, $B \setminus A$, sono a due a due disgiunti.*

Dim.: Per definizione di differenza, $A \setminus B$ non contiene alcun elemento di B, e così $B \setminus A$ non contiene alcun elemento di A; ne segue $(A \setminus B) \cap (B \setminus A) = \emptyset$.
Proviamo che è:

$$(A \setminus B) \cap (A \cap B) = \emptyset.$$

Se $x \in A \setminus B$, allora $x \in A$, $x \notin B$; mentre se $x \in A \cap B$, allora $x \in A$ ed $x \in B$, onde l'asserto.

Similmente si prova che

$$(B \setminus A) \cap (A \cap B) = \emptyset.$$

Esercizio 1.4.12. *A e B siano entrambi sottoinsiemi di un medesimo insieme S. Si provi che:*

$$A \setminus B = A \cap B'$$

Dim.: Sia $x \in A \setminus B$; ciò significa che $x \in A$, $x \notin B$; ma allora $x \in B'$, quindi $x \in A \cap B'$. Pertanto $A \setminus B \subseteq A \cap B'$.
Viceversa, sia $x \in A \cap B'$, allora $x \in A$ ed $x \in B'$, cioè $x \notin B$; ne segue $x \in A \setminus B$, onde l'asserto.

Esercizio 1.4.13. *Siano A e B entrambi sottoinsiemi di un medesimo insieme S. Dimostrare che:*

$$B \setminus A \subseteq A'$$

Dim.: Se $x \in B \setminus A$, allora $x \in B$, $x \notin A$; pertanto $x \in A'$.

Esercizio 1.4.14. *Se A e B sono sottoinsiemi di S, dimostrare che:*

$$B \setminus A' = B \cap A.$$

Dim.: Se $x \in B \setminus A'$, allora $x \in B$, $x \notin A'$, cioè $x \in A$; pertanto $x \in B \cap A$. Quindi $B \setminus A' \subseteq B \cap A$.
Viceversa, se $x \in B \cap A$, allora $x \in B$, $x \in A$, cioè $x \notin A'$; ne segue che $x \in B \setminus A'$, onde $B \cap A \subseteq B \setminus A'$.

Valendo le due inclusioni opposte, i due insiemi coincidono.

Esercizio 1.4.15. *Siano A e B sottoinsiemi dell'insieme S; dimostrare che:*

$$A \cap B = \emptyset \iff A \subseteq B'.$$

Dim.: Sappiamo (vedi esercizio1.4.14) che $B \cap A = B \setminus A'$. Allora $A \cap B = \emptyset$ comporta che $B \setminus A' = \emptyset$; ciò significa che $B \subseteq A'$, da cui passando ai complementari, $B' \supseteq (A')'$ cioè $A \subseteq B'$.
Viceversa, per definzione di inclusione,

$$A \subseteq B' \Rightarrow [x \in A \Rightarrow x \in B'] \Rightarrow [x \in A \Rightarrow x \notin B] \Rightarrow A \cap B = \emptyset$$

Esercizio 1.4.16. *Se A e B sono sottoinsiemi di S, dimostrare che:*

$$A \cap B = \emptyset \Rightarrow B \cap A' = B$$

Dim.: Per quanto visto nel corso della dimostrazione dell'esercizio1.4.15, si ha $A \cap B = \emptyset \Rightarrow B \subseteq A'$; ne segue l'asserto, per la proprietà di inclusione dell'intersezione e dell'unione.

Esercizio 1.4.17. *Siano A e B sottoinsiemi di S. Dimostrare che:*

$$A' \setminus B' = B \setminus A$$

Dim.: Se $x \in A' \setminus B'$, allora $x \in A'$, $x \notin B'$, cioè $x \notin A$ e $x \in B$, da cui $x \in B \setminus A$. Viceversa, se $x \in B \setminus A$, allora $x \in B$, $x \notin A$; pertanto $x \in A'$, $x \notin B'$, cioè $x \in A' \setminus B'$, onde l'asserto.

Esercizio 1.4.18. *Siano A e B sottoinsiemi di S. Dimostrare che:*

$$A \cap B = \emptyset \Rightarrow A \cup B' = B'$$

Dim.: In virtù dell'es.1.4.15, $A \cap B = \emptyset \Rightarrow A \subseteq B'$, onde l'asserto, per le proprietà di inclusione dell'unione e dell'intersezione.

Esercizio 1.4.19. *Siano A e B due insiemi qualsiasi. Dimostrare che:*

$$A \subset B \Rightarrow A \cup (B \setminus A) = B$$

Dim.: $A \subset B$ significa che $B \setminus A = \mathcal{C}_B A$, onde l'asserto, per definizione di insieme complementare.

Esercizio 1.4.20. *Siano A e B due sottoinsiemi dell'insieme S; si provi che:*

$$A \setminus B = A \Rightarrow A \cap B = \emptyset$$

Dim.: Si ha:

$$A \setminus B = A \Rightarrow [x \in A, x \notin B \Rightarrow x \in A] \Rightarrow A \cap B = \emptyset$$

Esercizio 1.4.21. *Siano A e B due sottoinsiemi dell'insieme S; si provi che:*

$$(A \setminus B)' = B \cup A'$$

Dim.: Poiché $A \setminus B = A \cap B'$ (cfr. es.1.4.12), applicando le leggi di de Morgan (cfr. pag. 20) e tenendo conto che $(B')' = B$, si ha $(A \setminus B)' = (A \cap B')' = A' \cup B$.

Esercizio 1.4.22. *Siano m ed n due numeri naturali e siano, rispettivamente, A e B l'insieme dei multipli di m e l'insieme dei multipli di n. Si determini $A \triangle B$.*

Sol.: Si ha:

$$A = \{x \in \mathbb{N} : x = k \cdot m,\ k \in \mathbb{N}\};$$

$$B = \{y \in \mathbb{N} : y = n \cdot n,\ h \in \mathbb{N}\}.$$

Poiché $A \cup B$ contiene tutti i multipli di m e tutti i multipli di n ed $A \cap B$ contiene i naturali che siano contemporaneamente multipli di m e di n, si ha:

$$A \triangle B = \{z \in \mathbb{N} : [[m \mid z \iff n \not| z] \text{ oppure } [n \mid z \iff m \not| z]]\},$$

cioè $A \triangle B$ è l'insieme dei multipli di m che non sono multipli di n e dei multipli di n che non sono multipli di m.

Esercizio 1.4.23. *Siano A e B due sottoinsiemi di un medesimo insieme S. Si provi che:*

$$A \triangle B = A \iff B = \emptyset$$

Sol.: Per definizione di differenza simmetrica, se $x \in A \triangle B$, allora $x \in A$, oppure $x \in B$, ma $x \notin A \cap B$; quindi se $A \triangle B = A$, allora $x \in A \triangle B \iff x \in A$; pertanto B non contiene alcun elemento, onde $B = \emptyset$. Il viceversa è evidente.

Esercizio 1.4.24. *Siano A e B due sottoinsiemi di un medesimo insieme S. Si provi che:*

$$A \triangle B = A \cup B \iff A \cap B = \emptyset$$

Sol.: Tenendo conto della defizione di differenza simmetrica, si ha:

$$\begin{array}{rcll} [A \triangle B = A \cup B] & \Rightarrow & [A \cup B = A \cup B \setminus A \cap B] & \Rightarrow \\ & \Rightarrow & [(A \cup B) \cap (A \cap B) = \emptyset] & \Rightarrow \\ & \Rightarrow & [[(A \cup B) \cap A] \cap B = \emptyset] & \Rightarrow \\ & \Rightarrow & A \cap B = \emptyset & \end{array}$$

(cfr. es.1.4.20 e le leggi di assorbimento). Il viceversa è evidente.

Esercizio 1.4.25. *Siano A e B due sottoinsiemi di un medesimo insieme S. Si provi che:*

$$(A \triangle B)' = (A' \cap B') \cup (A \cap B)$$

Sol.: Per definizione di differenza simmetrica, si ha

$$A \triangle B = A \cup B \setminus A \cap B = \{x \in S : x \in A \text{ od } x \in B \text{ ed } x \notin A \cap B\};$$

onde, per definizione di complementare si ha:

$$\begin{array}{rcll} (A \triangle B)' & = & \{x \notin A \triangle B\} & = \\ & = & \{x \in S : x \notin A \text{ ed } x \notin B \text{ od } x \in A \cap B\} & = \\ & = & \{x \in S : x \in A' \text{ ed } x \in B' \text{ oppure } x \in A \cap B\} & = \\ & = & (A' \cap B') \cup (A \cap B). & \end{array}$$

Si può dimostrare l'asserto anche tenendo conto che

$$A \cup B \setminus (A \cap B) = (A \cup B) \cap (A \cap B)'$$

(cfr. es.1.4.12) ed applicando le leggi di De Morgan.

Esercizio 1.4.26. *Siano A e B due sottoinsiemi di un medesimo insieme S. Si provi che:*

$$B \subset A \Rightarrow A \triangle B = A \setminus B$$

Sol.: Per le proprietà di inclusione dell'unione e dell'intersezione, si ha:

$$B \subset A \Rightarrow [A \cup B = A,\ A \cap B = B];$$

pertanto:

$$A \triangle B = (A \cup B) \setminus (A \cap B) = A \setminus B$$

Esercizio 1.4.27. *Siano A e B due sottoinsiemi di un medesimo insieme S. Si provi che:*

$$A \triangle B = \emptyset \iff A = B$$

Sol.: Se $A = B$, allora

$$A \triangle A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset,$$

per definizione di differenza. Viceversa:

$$[A \triangle B = \emptyset] \iff [(A \cup B) \setminus (A \cap B) = \emptyset] \Rightarrow (A \cup B) \subseteq (A \cap B) \Rightarrow A = B,$$

tenendo conto che risulta sempre: $(A \cap B) \subseteq (A \cup B)$.

Esercizio 1.4.28. *Si provi che quali che siano i due insiemi A e B (sottoinsiemi di un medesimo insieme S), risulta:*

$$A \triangle B = (B \cap A') \cup (A \cap B')$$

Sol.: Per defizione di differenza simmetrica, si ha:

$$\begin{array}{rcll} x \in A \triangle B & \Rightarrow & [[x \in A \text{ ed } x \notin B] \text{ oppure } [x \in B \text{ ed } x \notin A]] & \Rightarrow \\ & \Rightarrow & [[x \in A \text{ ed } x \in B'] \text{ oppure } [x \in B \text{ ed } x \in A']] & \Rightarrow \\ & \Rightarrow & [x \in A \cap B' \text{ oppure } x \in B \cap A'] & \Rightarrow \\ & \Rightarrow & x \in (A \cap B') \cup (B \cap A'); & \end{array}$$

il viceversa è evidente.

Si può provare l'asserto anche partendo dalla defizione di differenza simmetrica ed applicando il risultato stabilito nell'esercizio1.4.12 e le leggi di De Morgan.

Nella letteratura la differenza simmetrica di due insiemi A e B viene anche denotata con $A + B$. Si noti che essa traduce il cosidetto "o esclusivo", in quanto $A \triangle B = A + B$ è l'insieme di tutti gli elementi che sono o in A o in B, ma non in entrambi.

1.5 Insieme delle parti di un insieme

Consideriamo un qualunque insieme S: vogliamo mostrare che ad S resta univocamente associato un nuovo insieme, *insieme delle parti di* S, o insieme potenza di S, che denoteremo con $P(S)$.

Precisamente, $P(S)$ è l'insieme i cui elementi sono tutti e soli i s.i. di S, inclusi l'insieme vuoto e l'insieme S stesso (s.i. improprio di S).

Ad esempio, se $S = \{a, b, c\}$, allora

$$P(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{S\}\}.$$

Osserviamo che, in questo esempio, l'insieme S contiene tre elementi, e per indicare questo fatto scriveremo $|S| = 3$, mentre lo insieme $P(S)$ ha $8 = 2^3$ elementi.

In generale si può provare (vedi es. 1.5.3) che, se $|S| = n$, allora $|P(S)| = 2^n$.

Dal punto di vista della simbologia, notiamo il fatto seguente.
Se S è un qualunque insieme ed x è un suo elemento, scriviamo (come si è visto) $x \in S$. D'altra parte, se consideriamo il s.i. di S costituito dal solo elemento x, che quindi - secondo le notazioni già introdotte - indichiamo con $\{x\}$, scriveremo

$$\{x\} \subseteq S.$$

Avendo introdotto l'insieme delle parti di S, avremo anche

$$\{x\} \in P(S),$$

in quanto, essendo $\{x\}$ un s.i. di S, $\{x\}$ è un elemento di $P(S)$ (per definizione di $P(S)$).

Agli insiemi costituiti da un solo elemento si riserva un nome particolare: precisamente, è convenzione adottare per essi il nome inglese di *singleton*. Dunque $\{x\}$ è un singleton (e ciò indipendentemente da quale sia l'oggetto x, unico elemento dell'insieme).

Osserviamo infine che, nella definizione di $P(S)$, non abbiamo fatto alcuna ipotesi restrittiva sull'insieme S; pertanto, può essere anche $S = \emptyset$. In questo caso

$$P(\emptyset) = \{\emptyset\}$$

(perchè gli unici sottoinsiemi di S sono $\emptyset$ e $S = \emptyset$, quindi soltanto $\emptyset$).

Allora $\{\emptyset\}$ è un singleton ed inoltre ogni singleton si può identificare con $\{\emptyset\}$ ogniqualvolta si voglia sottolineare esclusivamente il fatto che l'insieme in questione contiene soltanto un solo elemento e non abbia interesse precisare di quale elemento si tratti.

Evidentemente, una volta determinato $P(S)$, si può considerare l'insieme delle parti di $P(S)$, che sarà $P(P(S))$, e così via.

Posto allora $P^0(S) = S$, $P^1(S) = P(S)$, $P^2(S) = P(P(S))$, avremo, in generale, la comoda notazione

$$P^m(S) = P(P(\dots P(S)\dots)).$$

Vedremo nel seguito l'importanza di iterare il procedimento di costruzione dell'insieme delle parti di un insieme, quando introdurremo la nozione di cardinalità di un insieme. Osserviamo sin d'ora che - in base a quanto detto - nel caso particolare in cui $|S| = n$, essendo $|P(S)| = 2^n$, tale procedimento fornisce un metodo per costruire insieme che abbiano un numero via via crescente di elementi.

Esercizi

Esercizio 1.5.1. *Determinare l'insieme $P(S)$ nei tre casi:*

$$S = \{a\};$$
$$S = \{a, b\}, (a \neq b);$$
$$S = \{a, b, c\}, (a \neq b, a \neq c, b \neq c).$$

Sol. Se $S = \{a\}$, $P(S)$ consta di due oggetti: $\emptyset$ ed S.
Se $S = \{a, b\}$, gli elementi di $P(S)$ sono: $\emptyset$, S, $\{a\}$, $\{b\}$.
Se $S = \{a, b, c\}$, $P(S)$ è costituito dagli otto elementi seguenti: $\emptyset$, S, $\{a\}$, $\{b\}$, $\{c\}$, $\{a, b\}$, $\{a, c\}$, $\{b, c\}$.

Esercizio 1.5.2. *Sia S un insieme contenente n elementi. Utilizzando la nozione di complementare di un insieme, si provi che $P(S)$ contiene un numero pari di elementi.*

Sol. Poichè ogni sottoinsieme A di S ammette un complementare $\mathcal{C}_S(A)$ (e questo è unico), si possono associare, a due a due, i sottoinsiemi di S; ciascuna di tali coppie è costituita da un sottoinsieme di S e dal suo complementare (in S). In tal modo si esauriscono tutti i sottoinsiemi, propri ed impropri, di S, onde questi sono in numero pari.

Esercizio 1.5.3. *Dimostrare che se l'insieme S consta di n elementi distinti, $P(S)$ consta di 2^n elementi distinti.*

Dim. Ciascun sottoinsieme di S è costituito da h elementi di S, con $0 \leq h \leq n$. Fissato h, soddisfacente alla limitazione detta, abbiamo tanti sottoinsiemi di S, aventi h elementi, quante sono le combinazioni di n oggetti ad h ad h; il numero di queste è dato dal coefficiente binomiale $\binom{n}{h}$. Pertanto, il numero N di elementi di $P(S)$ sarà $N = \sum_{h=0}^{n} \binom{n}{h}$. Applicando la formula del binomio di Newton:

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

con $a = b = 1$, si ha: $N = 2^n$.

Esercizio 1.5.4. *Dimostrare che se S è un insieme contenente $n > 0$ elementi distinti, i sottoinsiemi propri non vuoti di S sono in numero di $2^n - 2$.*

Dim. Tutti i sottoinsiemi di S sono in numero di 2^n (cfr. es. 1.5.3). Escludendo $\emptyset$ ed S, restano $2^n - 2$ insiemi.

Esercizio 1.5.5. *Siano A e B due insiemi. Si provi che*

$$A \subset B \Rightarrow P(A) \subset P(B).$$

Sol. Per definizione di inclusione si ha

$$A \subset B \Rightarrow [\forall x \in A \Rightarrow x \in B] \Rightarrow [\forall C \subset A \Rightarrow C \subset B] \Rightarrow$$
$$\Rightarrow [\forall C \in P(A) \Rightarrow C \in P(B)] \Rightarrow P(A) \subset P(B).$$

Esercizio 1.5.6. *Siano A e B due insiemi, $P(A)$ e $P(B)$ i loro insiemi delle parti. Si provi che*

$$P(A) \cap P(B) = P(A \cap B)$$
$$P(A) \cup P(B) \subset P(A \cup B).$$

Dim. Sia $X \in P(A) \cap P(B)$; allora $X \in P(A)$ e $X \in P(B) \Rightarrow X \subseteq A$ e $X \subseteq B \Rightarrow X \subseteq A \cap B \Rightarrow X \in P(A \cap B)$. Viceversa, se $Y \in P(A \cap B)$, allora $Y \subseteq A \cap B \Rightarrow Y \subseteq A$ e $Y \subseteq B \Rightarrow Y \in P(A)$ e $Y \in P(B) \Rightarrow Y \in P(A) \cap P(B)$.
Proviamo ora la seconda affermazione. Si ha:

$$X \in P(A) \cup P(B) \Rightarrow X \in P(A) \text{ o } X \in P(B) \Rightarrow$$
$$\Rightarrow X \subseteq A \text{ o } X \subseteq B \Rightarrow X \subseteq A \cup B \Rightarrow X \in P(A \cup B).$$

Proviamo ora che non è vera l'inclusione opposta. Consideriamo $a \in A \backslash B$ e $b \in B \backslash A$, allora $\{a, b\} \subseteq A \cup B \Rightarrow \{a, b\} \in P(A \cup B)$; ma $\{a, b\} \not\subseteq A$ e $\{a, b\} \not\subseteq B \Rightarrow \{a, b\} \notin P(A)$ e $\{a, b\} \notin P(B) \Rightarrow \{a, b\} \notin P(A) \cup P(B)$.

Si noti che le due affermazioni ora provate si generalizzano ad una famiglia di insiemi:

$$\cap (P(A_i) : i \in I) = P((\cap A_i : i \in I))$$
$$\cup (P(A_i) : i \in I) \subset P((\cup A_i : i \in I))$$

ove le scritture a primo membro di entrambe le affermazioni, e le analoghe scritture argomento degli insiemi "P" a secondo membro sono la generalizzazione degli insiemi unione ed intersezione al caso delle famiglie di insiemi (si veda il paragrafo **??** di questo capitolo).

1.6 Prodotto cartesiano di due o più insiemi

A partire da due o più insiemi abbiamo visto che è possibile costruire nuovi insiemi: unione, intersezione, differenza. Questi non sono però i soli insiemi costruibili.

Infatti, introdurremo ora il *prodotto cartesiano* di due o più insiemi, che gode della proprietà di dare luogo ad un insieme diverso anche se i due (o più) insiemi di partenza sono eguali (mentre, per gli insiemi costruiti sinora, risulta, $\forall A$, $A \cup A = A$, $A \cap A = A$, $A \backslash A = \emptyset$).

Siano pertanto,A e B due insiemi qualsiasi, che - per il momento - supponiamo diversi dall'insieme vuoto.

Definiamo *prodotto cartesiano* di A e B (nell'ordine), e lo denotiamo con $A \times B$, l'insieme delle coppie ordinate (a, b) nelle quali $a \in A$ e $b \in B$, cioè

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

Dalla definizione segue immediatamente che, se $A \neq B$, risulta

$$A \times B \neq B \times A,$$

cioè il prodotto cartesiano non è commutativo.

Inoltre, se $A = B$, allora $A \times A$ è un insieme distinto da A (è l'insieme delle coppie ordinate di elementi di A). Denoteremo spesso $A \times A$ con A^2.

Possiamo ora togliere la limitazione $A, B \neq \emptyset$. Infatti, se $A = \emptyset$, risulta

$$\emptyset \times B = \emptyset, \text{ quale che sia } B$$

(dato che $\emptyset$ non contiene alcun elemento, non esistono coppie il primo elemento delle quali appartenga a $\emptyset$ ed il secondo a B). Analogamente

$$\forall A, \quad A \times \emptyset = \emptyset.$$

Di conseguenza

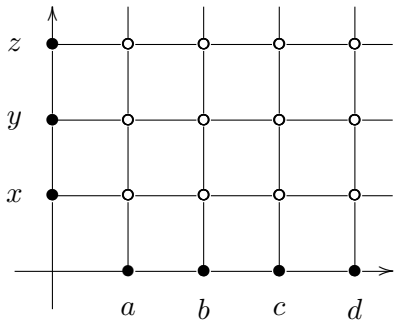
$$A \times B = B \times A \Rightarrow A = B \text{ oppure } A, \text{ o } B, \text{ o entrambi sono } \emptyset.$$

Giustifichiamo ora il nome di prodotto cartesiano dato all'insieme $A \times B$. Se consideriamo un sistema di riferimento cartesiano Oxy (per comodità ortogonale) e rappresentiamo con punti dell'asse x gli elementi di A e con punti dell'asse y gli elementi di B, allora gli elementi di $A \times B$ sono i punti del piano la cui ascissa è un punto di A e la cui ordinata è un punto di B.

Tale rappresentazione grafica risulta particolarmente conveniente qualora A e B siano insiemi contenenti rispettivamente n ed m elementi (e può anche essere $n = m$). Ad esempio, se $A = \{a, b, c, d\}$, $B = \{x, y, z\}$, allora $A \times B$ è rappresentato nella figura seguente:

$$A \times B = \{(a, x), (a, y), (a, z), (b, x), (b, y), (b, z), (c, x), (c, y), (c, z)\}$$

Figura 1.1: *Prodotto cartesiano di due insiemi distinti*



È immediato che

$$|A| = n, \quad |B| = m \Rightarrow |A \times B| = n \cdot m = |B \times A|.$$

Il piano numerico affine reale, non è altro che il prodotto cartesiano dell'insieme $\mathbb{R}$ dei numeri reali per sè stesso, cioè $\mathbb{R} \times \mathbb{R}$; questa è un'altra giustificazione del nome di prodotto cartesiano dato all'insieme $A \times B$.

Consideriamo ora il caso particolare del prodotto cartesiano $A \times A$ (con $A \neq \emptyset$, per evitare casi banali). Questo prodotto non differisce dal caso generale; però il fatto che i due insiemi siano eguali conduce a fissare l'attenzione su un particolare s.i. di $A \times A$, la cosiddetta *diagonale* del prodotto cartesiano di A per se stesso, che denoteremo con Δ_A e che è definito da

$$\Delta_A = \{(a, a) : a \in A\}.$$

Il nome di diagonale dato a questo s.i. è pienamente giustificato dalla rappresentazione grafica del prodotto cartesiano. Ad esempio, se $A = \{a, b, c, d\}$, si ha $\Delta_A = \{(a, a), (b, b), (c, c), (d, d)\}$ (vedi fig. 1.6, in cui gli elementi di Δ_A sono denotati con $\oplus$); nel caso particolare di $\mathbb{R} \times \mathbb{R}$, $\Delta_{\mathbb{R}}$ è costituito dai punti della retta $x = y$.

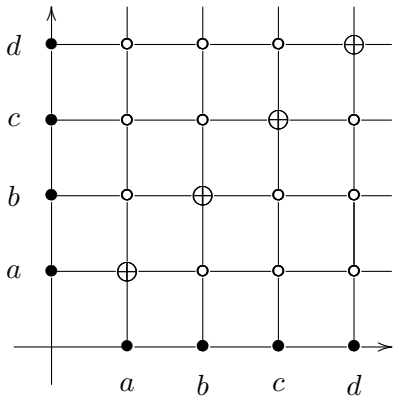
Tenendo presente la definizione di prodotto cartesiano di due insiemi, è immediato definire il prodotto cartesiano di tre insiemi A, B, C - da denotare con $A \times B \times C$ - costituito dall'insieme delle terne ordinate di elementi dei tre insiemi:

$$A \times B \times C = \{(a, b, c) : a \in A, b \in B, c \in C\}.$$

Analogamente,si definisce il prodotto cartesiano di n (intero positivo > 1) insiemi $A_1, A_2, \ldots, A_n$, come l'insieme delle n-ple ordinate di elementi degli n insiemi assegnati:

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i, i = 1, 2, \ldots, n\}$$

Figura 1.2: *Diagonale del prodotto cartesiano di A per sè stesso*



(per il prodotto cartesiano degli n insiemi $A_1, A_2, \ldots, A_n$ si usano anche le scritture $\times_{i=1}^{n} A_i$, $\prod_{i=1}^{n} A_i$).

Nel caso particolare in cui gli n insiemi A_i siano tutti eguali al medesimo insieme A, il loro prodotto cartesiano sarà l'insieme delle n-ple ordinate di elementi di A:

$$\underbrace{A \times A \times \cdots \times A}_{n \text{ volte}} = A^n = \{(a_1, a_2, \ldots, a_n) : a_i \in A, i = 1, 2, \ldots, n\}.$$

Analogamente a quanto visto nel caso di $A^2 = A \times A$ (cioè di $n = 2$), si definisce la *diagonale di* A^n, e la si denota con $\Delta_A^{(n)}$, il s.i. di A^n definito da

$$\Delta_A^{(n)} = \{(\underbrace{a, a, \ldots, a}_{n \text{ volte}}) : a \in A\}.$$

Introdotta questa notazione, sarà $\Delta_A = \Delta_A^{(2)}$.

Finora, nel prodotto cartesiano A^n, abbiamo escluso il caso $n = 1$; porremo allora

$$A^1 = A.$$

Sorge allora la questione di vedere se è possibile dare una definizione di A^0. Per giungere ad una definizione ben posta nel modo più semplice possibile, ricordiamo che abbiamo osservato che

$$|A| = m, \quad |B| = m' \Rightarrow |A \times B| = m \cdot m'.$$

Ne segue che

$$|A| = m \Rightarrow |A \times A| = m \cdot m = m^2.$$

Pertanto, è immediato che

$$|A| = m \Rightarrow |A^n| = \underbrace{m \cdot m \cdot \ldots \cdot m}_{n \text{ volte}} = m^n;$$

inoltre $|A^1| = m^1 = m$, dato che $A^1 = A$.

Quindi è lecito porre

$$|A^0| = m^0 = 1.$$

Ciò significa che A^0 è un insieme costituito da un solo elemento; di conseguenza, esso è identificabile con l'insieme $\{\emptyset\}$.
Porremo dunque

$$A^0 = \{\emptyset\}.$$

Osserviamo che - come meglio sarà visto nel seguito - non si lede la generalità pervenendo al risultato precedente con l'ipotesi che A contenga m elementi.

Estensioni del prodotto cartesiano saranno viste successivamente; ulteriori proprietà di esso sono riportate negli esercizi.

Esercizi

Esercizio 1.6.1. *Si provi che*

$$[A \subseteq B, C \subseteq C] \Rightarrow A \times C \subseteq B \times D.$$

Dim. Si ha $a \in A \Rightarrow a \in C$ e $c \in C \Rightarrow c \in D$, quindi $(a, c) \in A \times C \Rightarrow (a, c) \in B \times D$.

Esercizio 1.6.2. *Si provi che $A \times B = A \times C \Rightarrow B = C$, quale che sia l'insieme A.*

Dim. Segue immediatamente dalla definizione di prodotto cartesiano, tendendo conto che due coppie ordinate sono eguali sse sono eguali i primi elementi ed i secondi elementi.

Esercizio 1.6.3. *Se A, B, C sono tre insiemi qualsiasi, si provi che*

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

(proprietà distributiva del prodotto cartesiano rispetto all'unione).

Sol. Al solito, proviamo che ogni elemento del primo insieme appartiene al secondo, e viceversa. Si ha

$$\begin{aligned}
&[(a, b) \in A \times (B \cup C)] \Rightarrow [a \in A, b \in B \cup C] \Rightarrow \\
\Rightarrow &[a \in A, b \in B \text{ o } a \in A, b \in C] \Rightarrow \\
\Rightarrow &[(a, b) \in A \times B \text{ o } (a, b) \in A \times C] \Rightarrow \\
\Rightarrow &[(a, b) \in (A \times B) \cup (A \times C)].
\end{aligned}$$

Viceversa,

$$\begin{aligned}
&[(a, b) \in (A \times B) \cup (A \times C)] \Rightarrow [(a, b) \in A \times B \text{ o } (a, b) \in A \times C] \Rightarrow \\
\Rightarrow &[a \in A, b \in B \text{ o } a \in A, b \in C] \Rightarrow [a \in A, b \in B \text{ o } C] \Rightarrow \\
\Rightarrow &[a \in A, b \in B \cup C] \Rightarrow [(a, b) \in A \times (B \cup C)].
\end{aligned}$$

Esercizio 1.6.4. *Siano A, B, C tre insiemi qualsiasi. Si provi che:*

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

(proprietà distributiva del prodotto cartesiano rispetto all'intersezione).

Sol. Si ha:

$$\begin{aligned}
&[(a, b) \in A \times (B \cap C)] \Rightarrow [a \in A, b \in B \cap C] \Rightarrow [a \in A, b \in B \text{ e } C] \Rightarrow \\
\Rightarrow &[(a, b) \in A \times B, (a, b) \in A \times C] \Rightarrow [(a, b) \in (A \times B) \cap (A \times C)].
\end{aligned}$$

Viceversa:

$$\begin{aligned}
&[(a, b) \in (A \times B) \cap (A \times C)] \Rightarrow [(a, b) \in A \times B \text{ e } (a, b) \in A \times C] \Rightarrow \\
\Rightarrow &[a \in A, b \in B \text{ e } a \in A, b \in C] \Rightarrow [a \in A, b \in B \cap C] \Rightarrow \\
\Rightarrow &[(a, b) \in A \times (B \cap C)].
\end{aligned}$$

Esercizio 1.6.5. *Sia S un insieme qualsiasi e siano $A, B \subseteq S$; si provi che*

$$A' \times B' \neq (A \times B)'.$$

Sol. Basta provare che esiste almeno un elemento che appartiene ad uno dei due insiemi ma non all'altro.

Sia $a \in A, b' \in B'$. Allora

$$[(a, b') \notin A \times B] \Rightarrow [(a, b') \in (A \times B)'];$$

però

$$[a \in A] \Rightarrow [(a, b') \in A \times B'],$$

onde l'asserto.

Esercizio 1.6.6. *Siano $A, B \subseteq S$. Si provi che in $S \times S$ risulta*

$$(A \times B)' = (A' \times B') \cup (A \times B') \cup (A' \times B).$$

Sol. Sia $(a, b) \in (A \times B)'$; allora $(a, b) \notin A \times B$, quindi o $a \notin A$ e $b \notin B$, oppure $a \in A$, $b \notin B$, oppure $a \notin A, b \in B$: onde (a, b) appartiene al secondo membro.

Viceversa, se (a, b) appartiene al secondo membro, si ha:

$$[(a, b) \in A' \times B'] \Rightarrow [a \notin A, b \notin B] \Rightarrow [(a, b) \notin A \times B] \Rightarrow [(a, b) \in (A \times B)']$$

oppure

$$[(a, b) \in (A \times B')] \Rightarrow [a \in A, b \notin B] \Rightarrow [(a, b) \notin A \times B] \Rightarrow [(a, b) \in (A \times B)']$$

oppure

$$[(a, b) \in (A' \times B)] \Rightarrow [a \notin A, b \in B] \Rightarrow [(a, b) \notin A \times B] \Rightarrow [(a, b) \in (A \times B)'].$$

L'affermazione resta così provata.

Esercizio 1.6.7. *Siano A e B due insiemi tali che $A \times B \neq \emptyset$. Si provi che*

$$A \times B \subseteq X \times Y \Rightarrow A \subseteq X, B \subseteq Y$$

e si dica perchè la condizione $A \times B \neq \emptyset$ è necessaria.

Dim. Supponiamo vera l'implicazione. Se fosse $A \times B = \emptyset$, allora $\emptyset \subseteq X \times Y$ anche se $A \not\subseteq X$ e $B \not\subseteq Y$.

Proviamo ora l'affermazione. Per definizione di inclusione, si ha:

$$\begin{aligned} A \times B \subseteq X \times Y \Rightarrow [\forall (a, b) \in A \times B \Rightarrow (a, b) \in X \times Y] \Rightarrow \\ \Rightarrow a \in X \text{ e } b \in Y \Rightarrow A \subseteq X \text{ e } B \subseteq Y \end{aligned}$$

onde l'asserto.

1.7 Relazioni su un insieme

Sia $A \neq \emptyset$ un insieme qualsiasi (non consideriamo $A = \emptyset$ per evitare casi banali). Definiamo *relazione* (*binaria*) su A ogni s.i. del prodotto cartesiano $A \times A$. Quindi, se R è una relazione su A, cioè $R \subseteq A \times A$, allora R è un insieme di coppie ordinate (a, b), tali che $a, b \in A$.

Se $(a, b) \in R$, con $R \subseteq A \times A$, diremo anche che "a è in relazione R con b" e scriveremo allora

$$aRb.$$

Similmente, se $(x, y) \in A \times A$, ma $(x, y) \notin R$, diremo che x non è in relazione R con y" e scriveremo

$$x \not R y.$$

Ad esempio, se $A = \{a, b, c, d\}$, una relazione su A è definita da

$$R = \{(a, a), (c, a), (b, c), (c, d)\}.$$

Evidentemente, le relazioni su A, essendo tutti e soli i sottoinsiemi di $A \times A$, sono tutti e soli gli elementi di $P(A \times A)$.

Poichè R è un qualsivoglia s.i. di $A \times A$, può anche essere $R = \emptyset$: in questo caso la relazione prende il nome di *relazione vuota*.

Se poi $R = A \times A$, R prende il nome di *relazione totale*.

(Se $A \neq \emptyset$, la relazione vuota e la relazione totale sono distinte).

Un'altra relazione particolare, che si può definire su di un insieme, è la cosiddetta *relazione diagonale* o *relazione identica*, definita da $R = \Delta_A$. Il primo nome dato a questa relazione è giustificato dalla sua definizione, il secondo ne è conseguenza; infatti

$$R = \Delta_A \Rightarrow [[aRb \Leftrightarrow a = b] \text{ e } \forall a \in A, aRa].$$

Poichè le relazioni su un insieme A sono s.i. di $A \times A$, si può parlare di inclusione tra di esse; precisamente, se R ed R_1 sono relazioni su A, avremo

$$R \subseteq R_1 \Leftrightarrow [aRb \Rightarrow aR_1b].$$

Ancora dalla definizione di relazione segue che, assegnata $R \subseteq A \times A$, resta univocamente definita la *relazione complementare* R' di R (R' essendo il complementare di R in $A \times A$) ed avremo

$$aR'b \Leftrightarrow a \not R b.$$

Inoltre, se R ed R_1 sono due relazioni su A, si possono definire la relazione unione, $R \cup R_1$ e la relazione intersezione, $R \cap R_1$:

$$\begin{aligned} R \cup R_1 =& \{(a, b) \in A \times A : (a, b) \in R \text{ o } (a, b) \in R_1\} = \\ =& \{(a, b) \in A \times A : aRb \text{ o } aR_1b\}. \\ R \cap R_1 =& \{(a, b) \in A \times A : (a, b) \in R \text{ e } (a, b) \in R_1\} = \\ =& \{(a, b) \in A \times A : aRb \text{ e } aR_1b\}. \end{aligned}$$

L'unione e l'intersezione non sono però i soli modi di comporre due relazioni; l'altra composizione che vogliamo ora definire è il *prodotto* di due relazioni.

Siano, pertanto, R ed R_1 due relazioni su A; definiamo *prodotto di R per R_1* (nell'ordine) e lo denotiamo con $R_1 \circ R$ (scriviamo prima la seconda relazione e poi la prima: tale convenzione non è la sola possibile, ma risulterà utile nel seguito) la relazione

$$R_1 \circ R = \{(a,d) \in A \times A : (a,b) \in R, (c,d) \in R_1, b = c\}.$$

Dalla definizione segue subito che (in generale)

$$R_1 \circ R = R \circ R_1$$

(ovviamente, se $R = R_1$, allora $R_1 \circ R = R \circ R_1$, ma questo non è il solo caso: due relazioni R ed R_1 su A per le quali risulti $R_1 \circ R = R \circ R_1$ si dicono *permutabili*).

Per mostrare la non commutatività del prodotto di due relazioni e per meglio illustrare il prodotto stesso, consideriamo il seguente esempio.

Sia $A = \{a, b, c, d\}$ e siano rispettivamente

$$R = \{(a,a), (a,b), (b,c), (d,c)\}$$
$$R_1 = \{(b,c), (a,d), (d,d)\}.$$

Avremo allora

$$R_1 \circ R = \{(a,d), (a,c)\}$$
$$R \circ R_1 = \{(a,c), (d,c)\}.$$

Consideriamo ora una qualsiasi relazione $R \subseteq A \times A$ ed i due prodotti $\Delta_A \circ R$ e $R \circ \Delta_A$. Risulta allora

$$\Delta_A \circ R = R \circ \Delta_A = R;$$

in altri termini, la relazione diagonale si comporta come identità (elemento neutro) rispetto al prodotto di relazioni (cioè si comporta come l' "1" nel prodotto dei numeri naturali). Infatti i primi ed i secondi elementi delle coppie che costituiscono Δ_A sono tutti e soli gli elementi di A, quindi - quale che sia R - ciascuna di queste copie è "componibile" con una coppia di Δ_A e resta invariata per effetto di questa composizione.

Evidentemente, ha significato considerare il prodotto di una relazione per se stessa, per il quale adotteremo la scrittura

$$R \circ R = R^2$$

(che non crea confusione con l'analoga scrittura adottata per il prodotto cartesiano, perchè il significato dell' "esponente" appare sempre dal contesto).

Il prodotto di relazioni si può estendere a più fattori ed è immediato verificare che vale la proprietà associativa:

$$R_3 \circ (R_2 \circ R_1) = (R_3 \circ R_2) \circ R_1$$

il che autorizza ad omettere le parentesi.

Nel caso particolare in cui si consideri il prodotto della relazione R per se stessa, n volte, si scriverà

$$\underbrace{R \circ R \circ \ldots \circ R}_{n \text{ volte}} = R^n.$$

Introduciamo ora la nozione di relazione inversa di una data relazione.

Sia $R \subseteq A \times A$ una relazione su A; definiamo *relazione inversa* di R, e la denotiamo con R^{-1} la relazione seguente:

$$R^{-1} = \{(b, a) \in A \times A : (a, b) \in R\}.$$

Ad esempio se

$$A = \{a, b, c, d\} \quad \text{ed}$$
$$R = \{(a, b), (b, b), (c, d), (d, a), (d, b)\},$$

avremo

$$R^{-1} = \{(b, a), (b, b), (d, c), (a, d), (b, d)\}.$$

Dalla definizione di relazione inversa segue subito che

$$(R^{-1})^{-1} = R.$$

Siano ora R ed R_1 due relazioni su A; si prova facilmente che

$$(R_1 \circ R)^{-1} = R^{-1} \circ R_1^{-1}.$$

Verifichiamo la precedente affermazione sul seguente esempio.
Sia $A = \{a, b, c, d\}$ e siano

$$R = \{(a, b), (b, c), (c, c), (c, a), (d, b)\}$$
$$R_1 = \{(a, d), (b, b), (b, d), (c, d)\}.$$

Avremo allora

$$R_1 \circ R = \{(a, b), (a, d), (b, d), (c, d), (d, b), (d, d)\}$$

quindi

$$(R_1 \circ R)^{-1} = \{(b, a), (d, a), (d, b), (d, c), (b, d), (d, d)\}.$$

D'altra parte

$$R^{-1} = \{(b, a), (c, b), (c, c), (a, c), (b, d)\}$$
$$R_1^{-1} = \{(d, a), (b, b), (d, b), (d, c)\}.$$

onde

$$R^{-1} \circ R_1^{-1} = \{(d, c), (b, a), (b, d), (d, a), (d, d), (d, b))\};$$

ne segue l'asserto.

Esercizi

Esercizio 1.7.1. *Sia A un insieme contenente n elementi. Si dica quante relazioni si possono definire su A.*

Sol. Poichè $R \subseteq A \times A$, il numero delle relazioni definibili su A è dato dal numero degli elementi di $P(A \times A)$. Poichè

$$|A| = n \Rightarrow |A \times A| = n^2,$$

si avrà $|P(A \times A)| = 2^{n^2}$.

Esercizio 1.7.2. *Dato l'insieme $A = \{a, b, c, d\}$, siano*

$$R = \{(a, a), (a, c), (b, d)\}$$

ed

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

due relazioni su A. Si determino $R \cup S$, $R \cap S$, $R \circ S$ ed $S \circ R$.

Sol. Avremo

$$\begin{aligned} &R \cup S = \{(a, a), (a, c), (b, d), (b, a), (d, b), (b, b)\}; \\ &R \cap S = \emptyset \text{ (relazione vuota)}; \\ &R \circ S = \{(b, a), (b, c), (d, d), (b, d)\}; \\ &S \circ R = \{(b, b)\}. \end{aligned}$$

Esercizio 1.7.3. *Sia $A \neq \emptyset$ un insieme qualsiasi. Si dica quali condizioni deve soddisfare A affinchè Δ_A sia la relazione totale.*

Sol. Se R è la relazione totale, $R = A \times A$; affinchè risulti $A \times A = \Delta_A$, l'insieme A deve contenere un solo elemento.

Il viceversa è ovvio.

Esercizio 1.7.4. *Siano $R_1, \ldots, R_n$, $S_1, \ldots, S_m$ relazioni su A ($\neq \emptyset$); si provi che*

$$\begin{aligned} &(R_1 \cup R_2 \cup \ldots \cup R_n) \circ (S_1 \cup S_2 \cup \ldots \cup S_m) = \\ &= \bigcup_{i=1}^{n} \bigcup_{j=1}^{m} (R_i \circ S_j) \end{aligned}$$

(proprietà distributiva del prodotto rispetto all'unione).

Dim. Cominciamo a provare l'affermazione per $n = 2$, $m = 1$, cioè proviamo che

$$(R_1 \cup R_2) \circ S_1 = (R_1 \circ S_1) \cup (R_2 \circ S_1).$$

Posto

$$R = (R_1 \cup R_2) \circ S_1,$$
$$S = (R_1 \circ S_1) \cup (R_2 \circ S_1),$$

proviamo che $(a,b) \in R \Leftrightarrow (a,b) \in S$.

Se $(a,b) \in R$, allora $\exists x \in A$ tale che $(a,x) \in S_1$ e $(x,b) \in R_1 \cup R_2$; cioè $(x,b) \in R_1$ o $(x,b) \in R_2$. Nel primo caso $(a,b) \in R_1 \circ S_1$ e quindi $(a,b) \in S$; nel secondo caso $(a,b) \in R_2 \circ S_1$, onde $(a,b) \in S$.

Viceversa, sia $(a,b) \in S$: allora $(a,b) \in R_1 \circ S_1$ oppure $(a,b) \in R_2 \circ S_1$. Nel primo caso $\exists x \in A$ tale che $(a,x) \in S_1$ e $(x,b) \in R_1$ onde $(a,b) \in R$; similmente nel secondo.

In maniera analoga si prova che

$$(R_1 \cup R_2) \circ (S_1 \cup S_2) = (R_1 \circ S_1) \cup (R_1 \circ S_2) \cup (R_2 \circ S_1) \cup (R_2 \circ S_2)$$

e così via. (Questa proprietà distributiva continua a valere per la unione di un famiglia di insiemi, che definiremo nel seguito).

Esercizio 1.7.5. *Sia* $A = \{0,1,2,3,4,5\}$ *e siano*

$$\begin{aligned} R = \{&(0,0),(0,3),(3,0),(3,3),(1,1),(1,4),(4,1),(4,4),\\ &(2,2),(2,5),(5,2),(5,5)\}\\ S = \{&(0,0),(0,2),(2,0),(0,4),(4,0),(2,2),(4,4),(2,4),\\ &(4,2),(1,1),(1,3),(3,1),(3,3),(1,5),(5,1),(5,5),\\ &(3,5),(5,3)\} \end{aligned}$$

due relazioni su A. Si verifichi che R ed S sono permutabili (cioè $S \circ R = R \circ S$*).*

Sol. Osserviamo innanzitutto che si può scrivere:

$$\begin{aligned} R &= \Delta_A \cup \{(0,3),(3,0),(1,4),(4,1),(2,5),(5,2)\} = \Delta_A \cup \bar{R}\\ S &= \Delta_A \cup \{(0,2),(2,0),(0,4),(4,0),(2,4),(4,2),(1,3),(3,1),\\ &\qquad (1,5),(5,1),(3,5),(5,3)\} = \Delta_A \cup \bar{S}. \end{aligned}$$

Tenendo presente l'esercizio 1.7.4, avremo allora

$$\begin{aligned} S \circ R &= (\Delta_A \cup \bar{S}) \circ (\Delta_A \cup \bar{R}) =\\ &= (\Delta_A \circ \Delta_A) \cup (\Delta_A \circ \bar{R}) \cup (\bar{S} \circ \Delta_A) \cup (\bar{S} \circ \bar{R}) =\\ &= \Delta_A \cup \bar{R} \cup \bar{S} \cup (\bar{S} \circ \bar{R})\\ R \circ S &= (\Delta_A \cup \bar{R}) \circ (\Delta_A \cup \bar{S}) =\\ &= (\Delta_A \circ \Delta_A) \cup (\Delta_A \circ \bar{S}) \cup (\bar{R} \circ \Delta_A) \cup (\bar{R} \circ \bar{S}) =\\ &= \Delta_A \cup \bar{S} \cup \bar{R} \cup (\bar{R} \circ \bar{S}). \end{aligned}$$

Sarà allora sufficiente verificare che $\bar{S} \circ \bar{R} = \bar{R} \circ \bar{S}$. Risulta:

$$\begin{aligned}\bar{S} \circ \bar{R} = \{&(0,1),(0,5),(3,2),(3,4),(1,0),(1,2),(4,3),(4,5),\\ &(2,1),(2,3),(5,0),(5,4)\}\\ \bar{R} \circ \bar{S} = \{&(0,5),(2,3),(0,1),(4,3),(2,1),(4,5),(1,0),(3,4),\\ &(1,2),(5,4),(3,2),(5,0)\},\end{aligned}$$

onde l'asserto.

Esercizio 1.7.6. *Siano $R_1, \ldots, R_n, S$ relazioni su A ($\neq \emptyset$). Si provi che*

$$S \circ (R_1 \cap R_2 \cap \ldots \cap R_n) \neq (S \circ R_1) \cap (S \circ R_2) \circ \ldots \cap (S \circ R_n)$$

ed analogamente invertendo l'ordine del prodotto.

Dim. Proviamo l'affermazione per $n = 2$, cioè proviamo che, in generale

$$S \circ (R_1 \cap R_2) \neq (S_\circ R_1) \cap (S \circ R_2).$$

Sia $(a,b) \in S \circ (R_1 \cap R_2)$; allora $\exists x \in A$ tale che $(a,x) \in R_1 \cap R_2$ e $(x,b) \in S$. D'altra parte, se $(a,b) \in (S \circ R_1) \cap (S \circ R_2)$, allora $(a,b) \in (S \circ R_1)$ e $(a,b) \in (S \circ R_2)$; ciò implica che

$$\exists x \in A : (a,x) \in R_1, (x,b) \in S$$

ed

$$\exists y \in A : (a,y) \in R_2, (y,b) \in S$$

e non è necessariamente $x = y$. Ne segue l'asserto. Quindi non vale la proprietà distributiva del prodotto rispetto all'intersezione.

Esercizio 1.7.7. *Siano $R_1, \ldots, R_n$ relazioni su A ($\neq \emptyset$). Si provi che*

$$(R_1 \cup \ldots \cup R_n)^{-1} = R_1^{-1} \cup \ldots \cup R_n^{-1}$$

(proprietà distributiva dell'inversione rispetto all'unione).

Dim. Sia $(a,b) \in (R_1 \cup \ldots \cup R_n)^{-1}$; allora, per definizione di relazione inversa,$(b,a) \in R_1 \cup \ldots \cup R_n$, quindi $\exists i \in \{1,2,\ldots,n\}$ tale che $(b,a) \in R_i$; ne segue che $(a,b) \in R_i^{-1}$, dunque $(a,b) \in R_1^{-1} \cup \ldots \cup R_n^{-1}$. Viceversa, se $(a,b) \in R_1^{-1} \cup \ldots \cup R_n^{-1}$, allora $\exists j \in \{1,2,\ldots,n\}$ tale che $(a,b) \in R_j^{-1}$; ne segue che $(b,a) \in R_j$, dunque $(b,a) \in R_1 \cup \ldots \cup R_n$ e quindi $(a,b) \in (R_1 \cup \ldots \cup R_n)^{-1}$.

Tale proprietà distributiva si estende all'unione di una qualsiasi famiglia di insiemi, come vedremo.

Esercizio 1.7.8. *Siano $R_1, \ldots, R_n$ relazioni su A ($\neq \emptyset$). Si provi che*

$$(R_1 \cap \ldots \cap R_n)^{-1} = R_1^{-1} \cap \ldots \cap R_n^{-1}$$

(proprietà distributiva dell'inversione rispetto all'intersezione).

Dim. Proviamo che ogni elemento del primo membro è anche membro del secondo e viceversa. Si ha

$$\begin{aligned}&(a,b) \in (R_1 \cap \ldots \cap R_n)^{-1} \Rightarrow (b,a) \in R_1 \cap \ldots \cap R_n \Rightarrow \\ \Rightarrow &\forall i \in \{1,2,\ldots,n\}, (b,a) \in R_i \Rightarrow \\ \Rightarrow &\forall i \in \{1,2,\ldots,n\}, (a,b) \in R_i^{-1} \Rightarrow \\ \Rightarrow &(a,b) \in R_1^{-1} \cap \ldots \cap R_n^{-1}.\end{aligned}$$

Invertendo il verso delle implicazioni, si trova l'inversione opposta, onde l'asserto.

Questa proprietà distributiva si estende ad una qualunque famiglia di insiemi, come vedremo.

Esercizio 1.7.9. *Siano R, S due relazioni su A ($\neq \emptyset$) e sia $R \subseteq S$. Si provi che*

$$R \subseteq S \Rightarrow R^{-1} \subseteq S^{-1}$$

(isotonia dell'inversione rispetto all'inclusione).

Dim. Per definizione di inclusione tra relazioni si ha:

$$R \subseteq S \Leftrightarrow [(a,b) \in R \Rightarrow (a,b) \in S].$$

D'altra parte

$$(a,b) \in R \Rightarrow (b,a) \in R^{-1}, (a,b) \in S \Rightarrow (b,a) \in S^{-1},$$

onde l'asserto.

Esercizio 1.7.10. *Siano R, S due relazioni su A e sia T una fissata relazione su A. Si provi che*

$$\begin{aligned}R \subseteq S &\Rightarrow T \circ R \subseteq T \circ S \\ R \subseteq S &\Rightarrow R \circ T \subseteq S \circ T\end{aligned}$$

(isotonia del prodotto per una fissata relazione rispetto all'inclusione).

Dim. Proviamo la prima implicazione (la seconda si prova in modo analogo). Si ha

$$R \subseteq S \Rightarrow [(a,b) \in R \Rightarrow (a,b) \in S].$$

Ora, se $\exists x \in A$ tale che $(a,x) \in R$, $(x,b) \in T$, allora $(a,b) \in T \circ R$.
Ma $(a,x) \in R \Rightarrow (a,x) \in S$, onde $(a,b) \in T \circ S$.
Pertanto $T \circ R \subseteq T \circ S$.

1.8 Proprietà di una relazione. Restrizione di una relazione.

Esaminiamo ora le proprietà di cui può godere o meno una relazione.

Sia R una relazione sull'insieme A ($\neq \emptyset$). La relazione R si dice *riflessiva* sse $\Delta_A \subseteq R$; in altri termini, sse

$$\forall a \in A, (a,a) \in R.$$

La relazione R si dirà *simmetrica* sse $R = R^{-1}$; tenendo presente che - per definizione di inversa - $(a,b) \in R \Rightarrow (b,a) \in R^{-1}$, la condizione $R = R^{-1}$ si può anche esprimere nel modo seguente

$$R = R^{-1} \Leftrightarrow [(a,b) \in R \Rightarrow (b,a) \in R].$$

Invece R si dirà *antisimmetrica* sse $R \cap R^{-1} \subseteq \Delta_A$; ciò equivale a dire che

$$(a,b), (b,a) \in R \Rightarrow a = b.$$

Diremo poi che R è *transitiva* sse $R \circ R \subseteq R$; ricordando la definizione di prodotto di relazioni, tale condizione si può anche esprimere dicendo che

$$(a,b), (b,c) \in R \Rightarrow (a,c) \in R.$$

Osserviamo che la transitività comporta $R^n \subseteq R$; infatti

$$R \circ R \subseteq R \Rightarrow R \circ R \circ R = R^3 \subseteq R \circ R \subseteq R \Rightarrow R^3 \subseteq R,$$

e così via.

Infine, la relazione R si dirà *connessa* sse $R \cup R^{-1} = A^2 (= A \times A)$; ciò significa che

$$\forall (a,b) \in A^2, (a,b) \in R \text{ oppure } (a,b) \in R^{-1}.$$

Data una qualunque relazione su A, non è detto che essa goda di una o più proprietà elencate. Sorge allora la questione, data una relazione R, di costruire - se è possibile - la "più piccola" relazione $\bar{R}$ che contenga R e che goda della proprietà P che interessa.
Una relazione siffatta prende il nome di *chiusura rispetto a P* di R.
La locuzione "la più piccola" si interpreta nel modo seguente. Se R_1 è una qualunque relazione che goda della proprietà P e che contenga R, allora $R_1 \supseteq \bar{R}$, essendo $\bar{R}$ la chiusura rispetto a P di R.

Ovviamente, se R gde della proprietà P, la chiusura rispetto a P di R coincide con R. Inoltre il problema ammette sempre soluzione perchè la relazione totale gode di ogni proprietà P.

Cominciamo allora a determinare la *chiusura riflessiva* $\bar{R}$ di R.
Per definizione dovrà essere $\bar{R} \supseteq R$, $\bar{R}$ riflessiva e tale che $\forall R_1 \supseteq R$, R_1 riflessiva, sia $R_1 \supseteq \bar{R}$. Se $\bar{R}$ deve essere riflessiva, $\Delta_A \subseteq \bar{R}$; allora

$$\bar{R} = \Delta_A \cup R$$

come è immediato verificare.

Determiniamo ora la *chiusura simmetrica* S di R, cioè la relazione $S \supseteq R$ tale che $S = S^{-1}$ e che, se $\exists S_1 \supseteq R$, S_1 simmetrica, allora $S_1 \supseteq S$. La soluzione è fornita dalla relazione

$$S = R \cup R^{-1}.$$

Infatti $S \supseteq R$, per definizione di unione; S è simmetrica perchè $S^{-1} = (R \cup R^{-1})^{-1} = R^{-1} \cup R = S$; inoltre, se $S_1 \supseteq R$, S_1 simmetrica, allora $S_1 \supseteq S$ in quanto l'unione di due insiemi è il più piccolo insieme che li contenga entrambi.

Definiamo infine la *chiusura transitiva* T di R, che è la più importante tra quelle ora considerate.

Diciamo che

$$T = \bigcup_{n=1}^{\infty} R^n = R \cup (R \circ R) \cup (R \circ R \circ R) \cup \ldots$$
$$\ldots \cup (\underbrace{R \circ R \circ \ldots \circ R}_{n \text{ volte}}) \cup \ldots$$

Osserviamo innanzitutto che in tale espressione compare l'unione di un numero infinito di insiemi; tale unione si definisce nello stesso modo in cui è stata definita l'unione di un numero qualsivoglia (finito) di insiemi (si veda il par. **??**). D'altra parte, molto spesso si ottiene la chiusura transitiva con un numero finito di passi, e ciò avviene certamente in ogni caso se A è un insieme che contiene un numero finito di elementi.

Negli esercizi sarà dimostrato che T rappresenta di fatto la chiusura transitiva di R. Comunque vogliamo ora, a titolo di esempio, determinare la chiusura transitiva di una relazione R su un particolare insieme A, sottolinenado che la precedente espressione di T traduce il procedimento operativo sperimentale che consiste nell' "aggiungere ad R gli elementi (coppie di elementi di A) che mancano", onde ottenere una relazione transitiva.

Sia $A = \{a, b, c, d\}$ e sia $R = \{(a, b), (b, c), (c, c), (a, d), (d, a)\}$.

Determiniamo la chiusura transitiva T di R, quindi determiniamo R^2, R^3, ecc. Avremo

$$R^2 = R \circ R = \{(a, c), (b, c), (c, c), (a, a), (d, b), (d, d)\}$$
$$R^3 = R \circ R \circ R = \{(a, c), (b, c), (c, c), (a, b), (a, d), (d, c), (d, a)\}$$
$$R^4 = R \circ R \circ R \circ R = \{(a, c), (b, c), (c, c), (a, a), (d, c), (d, b), (d, d)\} \subseteq$$
$$\subseteq R^2 \cup R^3.$$

Quindi

$$T = R \cup R^2 \cup R^3 = \{(a,b),(b,c),(c,c),(a,d),(d,a),(a,c),(a,a),\\ (d,b),(d,d),(d,c)\}$$

Verifichiamo che T è transitiva, cioè che $T^2 \subseteq T$. Si ha

$$T^2 = T \circ T = \{(a,c),(b,c),(c,c),(a,b),(a,d),(d,b),(d,d),\\ (d,c),(d,a)\}$$

onde l'asserto.

Altri esempi saranno forniti negli esercizi.

Vogliamo ora introdurre la nozione di restrizione di una relazione.

Sia R una qualunque relazione su un insieme A ($\neq \emptyset$) e sia B un s.i. di A. Poichè R è definita su A ($R \subseteq A \times A$) e $B \subseteq A$,ha senso considerare le coppie $(a,b) \in R$ tali che $(a,b) \in B \times B$.

Resta così definita una relazione su B, che prende il nome di *restrizione* a $B \subseteq A$ di R e verrà denotata con $R|_B$, o semplicemente R_B. Pertanto

$$R|_B = \{(a,b) \in R : (a,b) \in B \times B\}$$

che equivale a dire

$$R|_B = R \cap (B \times B).$$

Ovviamente, può essere $R_B = \emptyset$ anche se $R, B \neq \emptyset$ (occorre e basta che $B \times B$ non contenga alcun elemento di R).

La considerazione della restrizione di una relazione risulta utile quando la relazione R non gode di alcuna proprietà particolare ed interessa considerare qualche s.i. di A tale che la restrizione ad esso di R sia una particolare relazione.

Di conseguenza, esistono due modi oer far sì che una relazione goda di proprietà ulteriori, rispetto a quelle deducibili dalla sua definizione; precisamente, la determinazione della chiusura della relazione rispetto a quella proprietà (con il che si amplia la relazione) e la restrizione della relazione a un s.i. (con il che si "rimpicciolisce" l'insieme in questione). È da notare che, mentre il primo metodo ammette sempre una soluzione (infatti esiste la relazione totale), il secondo non ammette necessariamnte soluzione.

Esercizi

Esercizio 1.8.1. *Siano R ed S due relazioni su A; si provi che $R \cap S$ è riflessiva sse sia R che S sono riflessive.*

Sol. Se R ed S sono riflessive, $\Delta_A \subseteq R$, $\Delta_A \subseteq S \Rightarrow \Delta_A \subseteq R \cap S$, cioè $R \cap S$ è riflessiva. Viceversa, $\Delta_A \subseteq R \cap S \Rightarrow \Delta_A \subseteq R, \Delta_A \subseteq S$, onde R ed S sono riflessive.

Esercizio 1.8.2. *Dimostrare che se $A = \emptyset$, oppure $|A| = 1$, ogni relazione su A è simmetrica.*

Dim. Se $A = \emptyset$, l'unica relazione definibile su A è la relazione vuota, che è simmetrica. Se A contiene un solo elemento, $A = \{x\}$, allora le sole relazioni su A sono la relazione vuota e la relazione totale, entrambe simmetriche.

Esercizio 1.8.3. *Sia $\mathbb{Z}$ l'insieme dei numeri interi (relativi). Si consideri la relazione R su $\mathbb{Z}$ definita da*

$$(x, y) \in R \Leftrightarrow ax + by = c,\ a, b, c \in \mathbb{Z} \text{ fissati}.$$

Si dica quali condizioni devono soddisfare a, b, c affinchè una tale relazione sia simmetrica.

Sol. Affinchè R sia simmetrica deve essere $R = R^{-1}$, onde

$$ax + by = c \Rightarrow ay + bx = c.$$

Ne segue

$$ax + by = ay + bx \Rightarrow (a - b)x = (a - b)y\ \forall x, y \in \mathbb{Z} \Rightarrow a = b.$$

Esercizio 1.8.4. *Si provi che la relazione totale non è antisimmetrica se A contiene più di un elemento.*

Sol. Poichè la relazione totale è simmetrica, affinchè sia anche antisimmetrica deve essere contenuta in Δ_A e ciò accade soltanto se $A = \emptyset$, oppure se $A = \{a\}$.

Esercizio 1.8.5. *Sia $A \neq \emptyset$ un insieme qualsiasi. Si caratterizzino le relazioni su A che sono contemporaneamente simmetriche e antisimmetriche.*

Sol. Se $R \subseteq A \times A$ è simmetrica, allora $R = R^{-1}$; se R è antisimmetrica, allora $R \cap R^{-1} \subseteq \Delta_A$. Se le due proprietà valgono contemporaneamente, segue che $R \cap R^{-1} = R \cap R = R \subseteq \Delta_A$. Il viceversa è ovvio. Quindi, tutte e solo le relazioni contenute nella relazione diagonale sono contemporaneamente simmetriche e antisimmetriche.

Esercizio 1.8.6. *Si provi che una relazione simmetrica su $A \neq \emptyset$ non può essere connessa, a meno che non sia la relazione totale.*

Dim. Sia $R \subseteq A \times A$ e sia R simmetrica, cioè $R = R^{-1}$. Affinchè R sia connessa, deve essere $R \cup R^{-1} = A^2$. Ora

$$R = R^{-1} \Rightarrow R \cup R^{-1} = R \cup R = R,$$

onde deve essere $R = A^2$.

Esercizio 1.8.7. *Sull'insieme $\mathbb{N}$ dei naturali sia definita la relazione R nel modo seguente:*

$$(a, b) \in R \Leftrightarrow a + b = 10.$$

Si dica di quali proprietà gode questa relazione.

Sol. La relazione R non è riflessiva, perchè $a + a = 10 \Rightarrow a = 5$, non valida per ogni $a \in \mathbb{N}$.

Inoltre, esistono degli elementi $a \in \mathbb{N}$, tali che $\nexists b \in \mathbb{N}$ per cui $(a, b) \in R$.

La relazione R è simmetrica; infatti $a+b = 10 \Rightarrow b+a = 10 \Rightarrow (b, a) \in R$ (essendo commutativa la somma in $\mathbb{N}$); quindi, non essendo $R \subseteq \Delta_A$, R non può essere antisimmetrica.

Infine R non è transitiva, dato che

$$(a, b) \in R, (b, c) \in R \Rightarrow a + b = 10,\ b + c = 10 \not\Rightarrow a + c = 10.$$

Esercizio 1.8.8. *Sull'insieme $A = \{a, b, c, d\}$, siano date le relazioni*

$$R = \{(a, a), (a, c), (b, d)\} \text{ ed } S = \{(b, a), (d, b), (b, b)\}$$

e le relazioni $R \cup S$, $R \cap S$, $R \circ S$, $S \circ R$ (ricavate nell'esercizio 1.7.2); si dica di quali proprietà godono queste relazioni.

Sol. Osserviamo innanzitutto che nessuna delle relazioni indicate è riflessiva.

$S \circ R$ è simmetrica ed antisimmetrica, poichè $S \circ R \subseteq \Delta_A$.

Inoltre $R \circ S$ ed $S \circ R$ sono relazioni transitive; infatti

$$(R \circ S) \circ (R \circ S) = \{(b, d)\} \subseteq R \circ S$$
$$(S \circ R) \circ (S \circ R) = \{(b, b)\} \subseteq S \circ R.$$

Esercizio 1.8.9. *Sia R una relazione simmetrica e transitiva su A tale che*

$$\forall a \in A \Rightarrow \exists b \in A : (a, b) \in R.$$

Si provi che allora R è anche riflessiva.

Dim. Infatti, dall'ipotesi, per la simmetria e la transitività di R, si ha

$$[\forall a \in A \Rightarrow \exists b \in A : (a,b) \in R] \Rightarrow$$
$$\Rightarrow (b,a) \in R \Rightarrow (a,a) \in R \Rightarrow \Delta_A \subseteq R.$$

Esercizio 1.8.10. *Sull'insieme $A = \{a,b,c,d,e\}$ sia definita la relazione $R = \{(a,b),(b,a),(a,c),(d,e)\}$. Si verifichi che R non è simmetrica e si costruisca una relazione S su A tale che $R \cup S$ sia simmetrica.*

Sol. Ricordiamo che R è simmetrica sse $R = R^{-1}$. Attualmente si ha $R^{-1} = \{(b,a),(a,b),(c,a),(e,d)\}$, dunque $R \neq R^{-1}$.

Consideriamo la relazione $S = \{(c,a),(e,d)\}$; allora $R \cup S$ è simmetrica.

Si noti che $R \cup S = R \cup R^{-1}$ ed (ed $R \cup R^{-1}$ è la chiusura simmetrica di R); d'altra parte, la relazione S considerata è la più piccola relazione su A tale che $R \cup S$ sia simmetrica; infatti, per ogni relazione R_1 tale che $R \cup R_1$ sia simmetrica, risulta $S \subseteq R_1$.

Esercizio 1.8.11. *Sia R una relazione su A ($\neq \emptyset$). Si provi che la chiusura transitiva di R è data da*

$$T = \bigcup_{n=1}^{\infty} R^n.$$

Dim. Per definizione di unione, $R = R^1 \subseteq T$. Dobbiamo provare che T è transitiva, cioè che $T \circ T \subseteq T$. Si ha

$$T \circ T = (\bigcup_{n=1}^{\infty} R^n) \circ (\bigcup_{h=1}^{\infty} R^h) = \bigcup_{n=1}^{\infty} \bigcup_{h=1}^{\infty} (R^n \circ R^h) =$$
$$= \bigcup_{n=1}^{\infty} \bigcup_{h=1}^{\infty} R^{n+h} \subseteq T$$

(si tenga presente l'esercizio 1.7.4).

Se ora T_1 è una relazione transitiva contenente R si ha

$$R^n \subseteq T_1^n \subseteq T_1 \Rightarrow T \subseteq T_1$$

(cfr. esercizio 1.7.10), onde l'asserto.

Esercizio 1.8.12. *Sia $R \subseteq A \times A$ una relazione su A ($\neq \emptyset$). Si dica quando è possibile determinare $B \subseteq A$ tale che la restrizione $R|_B$ di R a B sia riflessiva, e si costruisca un B siffatto.*

Sol. Se R è riflessiva, $R|_B$ è riflessiva per ogni $B \subseteq A$, $B \neq \emptyset$. Supponiamo, pertanto, che R non sia riflessiva. Affinchè $R|_B = R \cap (B \times B)$ sia riflessiva, dev'essere $\Delta_B \subseteq R|_B = R \cap (B \times B)$; pertanto, l'insieme $B \subseteq A$ tale che $\Delta_B = R \cap \Delta_A$ gode della proprietà che $R|_B$ sia riflessiva, e per ogni $B' \subseteq B$ vale la medesima condizione.

1.9 Relazioni d'ordine su un insieme

Sia P un insieme qualunque ($\neq \emptyset$) e sia R una relazione su P.
Diremo che R è una *relazione d'ordine* (parziale) su P se:

1) R è riflessiva (cioè $\Delta_P \subseteq R$)

2) R è antisimmetrica (cioè $R \cap R^{-1} \subseteq \Delta_P$)

3) R è transitiva (cioè $R \circ R \subseteq R$).

In tal caso la coppia $\langle P; R\rangle$ prende il nome di *insieme parzialmente ordinato* (o *poset*, dall'inglese *p*artially *o*rdered *set*).

Se poi R è anche connessa (cioè $R \cup R^{-1} = P^2$), R si dirà *relazione d'ordine totale* (o *lineare*) su P e $\langle P; R\rangle$ prenderà il nome di *insieme totalmente (linearmente) ordinato* o *catena*.

Generalmente, per relazione d'ordine (o anche ordinamento) si intende una relazione d'ordine parziale.

Se R è una relazione d'ordine su P, è convenzione denotare R con il simbolo $\leq$.

Tale consuetudine deriva dal fatto che $\langle \mathbb{N}; \leq\rangle$ è effettivamente un insieme parzialmente ordinato.

D'altra parte, se R è una relazione d'ordine, si verifica subito (cfr. esercizio **??**) che anche la sua inversa R^{-1} è una relazione d'ordine.

Se denotiamo R con $\leq$, denoteremo R^{-1} con $\geq$. Pertanto, la definizione di relazione inversa

$$(a, b) \in R \Leftrightarrow (b, a) \in R^{-1},$$

ovvero

$$aRb \Leftrightarrow bR^{-1}a,$$

comporta, nel caso di una relazione d'ordine, che

$$a \leq b \Leftrightarrow b \geq a.$$

Da ciò discende il

Principio di dualità negli insiemi parzialmente ordinati:

Se $\langle P; \leq\rangle$ è un insieme parzialmente ordinato, anche $\langle P; \geq\rangle$ è un insieme parzialmente ordinato.

Osserviamo che il principio di dualità, pur essendo banale, semplifica notevolmente molte dimostrazioni e verrà applicato non tanto ora, quanto in seguito, negli elementi di teoria dei reticoli.

Diamo ora un esempio di insieme parzialmente ordinato. Sia $P = \mathbb{N}$ e la relazione su P sia la divisibilità, $R\ (=\leq) = |$, cioè

$$\forall a, b \in \mathbb{N},\ a|b \Leftrightarrow \exists x \in \mathbb{N} \text{ tale che } ax = b$$

($a|b$ si legge "a divide b").

Proviamo che $\langle \mathbb{N}; | \rangle$ è un insieme parzialmente ordinato. Dobbiamo provare che | è riflessiva, antisimmetrica e transitiva.

La relazione | è riflessiva; infatti

$$\forall a \in \mathbb{N},\ a|a.$$

La relazione | è antisimmetrica; infatti

$$a|b,\ b|a \Rightarrow \exists x \in \mathbb{N} : ax = b,\ \exists y \in \mathbb{N} : by = a \Rightarrow axy = a \Rightarrow$$
$$\Rightarrow xy = 1 \Rightarrow x = y = 1 \Rightarrow a = b$$

(si ricordi che x ed y devono essere numeri naturali).

La relazione | è transitiva; infatti

$$a|b,\ b|a \Rightarrow \exists x \in \mathbb{N} : ax = b,\ \exists y \in \mathbb{N} : by = c \Rightarrow axy = c,\ xy \in \mathbb{N} \Rightarrow$$
$$\Rightarrow a|c.$$

Abbiamo considerato due insiemi parzialmente ordinati sul medesimo sostegno $\mathbb{N}$, precisamente $\langle \mathbb{N}; \leq \rangle$ ($\leq$ essendo la consueta relazione di $\leq$ nei naturali) ed $\langle \mathbb{N}; | \rangle$. Tra questi due insiemi parzialmente ordinati esiste una differenza fondamentale. Rispetto alla relazione $\leq$, $\mathbb{N}$ è totalmente ordinato; infatti $\forall a, b \in \mathbb{N}$ o è $a \leq B$, oppure è $b \leq a$, dunque o $(a, b) \in \leq$ oppure $(b, a) \in \leq \Rightarrow (a, b) \in \leq^{-1}$, cioè $\leq$ è anche connessa.

Invece, rispetto alla relazione |, $\mathbb{N}$ è parzialmente ordinato; infatti esistono coppie a, b doi naturali tali che $a \not| b$ e $b \not| a$ (ad esempio $a = 3$ e $b = 7$). Due elementi siffatti si dicono *inconfrontabili*.

Se $\langle P; \leq \rangle$ è un insieme parzialmente ordinato ed a, b sono inconfrontabili (cioè $a \not\leq b$ e $b \not\leq a$), si scriverà $a||b$.

Sia ora $\langle P; \leq \rangle$ un insieme parzialmente ordinato. Vogliamo mostrare che la relazione $\leq$ definisce una nuova relazione, detta *relazione di copertura*.

Precisamente, se $a, b \in P$, diremo che "b copre a", in simboli $b \succ\!\!-\!\!- a$ (ovvero che "a è coperto da b", $a -\!\!-\!\!\prec b$), se $a \leq b$ e non esiste alcun $x \in P$ tale che $a \leq x \leq b$; in altri termini

$$b \succ\!\!-\!\!- a \Leftrightarrow [a \leq b \quad \text{e} \quad a \leq x \leq b \Rightarrow x = a \quad \text{o} \quad x = b].$$

La relazione di copertura risulta particolarmente utile per tracciare i diagrammi (diagrammi di Hasse) degli insiemi parzialmente ordinati tali che P contenga n elementi.

Per tracciare un tale diagramma si rappresentano sul foglio gli elementi di P mediante circoletti con le convenzioni seguenti:

1) se $a > b$ il circoletto rappresentativo di a viene disegnato più alto di quello di b;

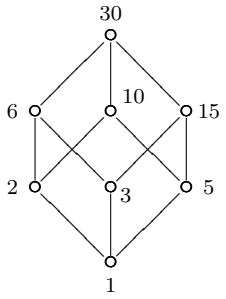
2) se $a \succ\!\!— b$ si congiunge a con b mediante una linea (segmento od arco di curva) mai orizzontale;

3) due circoletti rappresentativi di elementi di P possono appartenere ad una medesima orizzontale (da non disegnare) soltanto se sono inconfrontaili.

Illustriamo questo procedimento su un esempio. Sia P l'insieme dei divisori di 30, cioè $P = \{1, 2, 3, 5, 6, 10, 15, 30\}$ e la relazione d'ordine sia la divisibiltà.
Per tracciare più rapidamente il diagramma, scriviamo le relazioni di copertura

$$\begin{aligned}
&1 —\!\prec 2 —\!\prec 6 —\!\prec 30\\
&1 —\!\prec 2 —\!\prec 10 —\!\prec 30\\
&1 —\!\prec 3 —\!\prec 6 —\!\prec 30\\
&1 —\!\prec 3 —\!\prec 15 —\!\prec 30\\
&1 —\!\prec 5 —\!\prec 10 —\!\prec 30\\
&1 —\!\prec 5 —\!\prec 15 —\!\prec 30\ .
\end{aligned}$$

Osserviamo che ciascuno di questi sottoinsiemi di P costituisce, rispetto alla relazione definita su P, una catena.



Tale risultato vale in generale: mediante la relazione di copertuta si possono individuare le catene contenute nell'insieme parzialmente ordinato.

Notiamo inoltre che un diagramma del tipo precedente si dice *planare* se due linee qualsiasi si intersecano al più nei punti che rappresentano gli elementi; si dice *ottimale* se il numero di intersezioni "al di fuori" degli elementi di P è minimo. La proprietà, del diagramma di un insieme parzialmente ordinato, di essere planare è intrinseca, cioè se il diagramma di $\langle P; \leq \rangle$ è planare, è sempre possibile disegnarlo in modo che ciò appaia (basta "spostare" gli elementi, ferme restando le relazioni di copertura).

Altre proprietà degli insiemi parzialmente ordinati saranno viste come introduzione agli elementi di teoria dei reticoli ed altri esempi saranno riportati negli esercizi.

Osserviamo infine che un insieme parzialmente ordinato $\langle P; \rangle$ costituisce un esempio di quella che si chiama *struttura relazionale*.
Innanzitutto, definiamo relazione n-aria su A ogni s.i. di A^n.

Diremo allora *struttura relazionale*, $\mathcal{U} = \langle A, \mathcal{R} \rangle$, una coppia costituita da un insieme $\mathcal{R}$ di relazioni su A, le quali potranno essere binarie, ternarie, ...n-arie ed in numero qualsivoglia.

Nel caso di $\langle P; \leq \rangle$, $\mathcal{R}$ contiene una sola relazione binaria.

Esercizi

Esercizio 1.9.1. *Sia $P \neq \emptyset$ un insieme qualunque, ed R una relazione d'ordine su P. Dimostrare che R^{-1} è anch'essa una relazione d'ordine.*

Dim.: R è una relazione d'ordine su P se è riflessiva, antisimmetrica e transitiva. Dobbiamo dimostrare che R^{-1} gode delle stesse proprietà. R^{-1} è banalmente riflessiva: infatti se $(a, a) \in R$, allora $(a, a) \in R^{-1}$, per definizione di relazione inversa. Inoltre, se (a, b), $(b, a) \in R \Rightarrow a = b$, allora (b, a), $(a, b) \in R^{-1} \Rightarrow b = a$, quindi R^{-1} è anch'essa antisimmetrica. Infine, R^{-1} è transitiva, in quanto $(R \circ R) \subseteq R \Rightarrow (R \circ R)^{-1} \subseteq R^{-1}$ (cfr. esercizio 7.9).

Esercizio 1.9.2. *Dato l'insieme $M = \{2, 3, 4, \dots\}$, s.i. di $\mathbb{N}$, si introducano in M due relazioni d'ordine, quella di divisibilità e quella di diseguaglianza ($\leq$), definite come in $\mathbb{N}$ (la prima, $|$, è relazione d'ordine parziale, la seconda, $\leq$, totale). Si consideri il prodotto cartesiano $M \times M$ e si verifichi che la relazione $\leq$, introdotta in esso alla maniera seguente:*

$$(a, b) \leq (c, d) \Leftrightarrow a|c \quad e \quad b \leq d$$

è una relazione d'ordine

Sol. La proprietà riflessiva è evidente, in quanto $a|a$ e $b = b$. Proprietà antisimmetrica: $(a, b) \leq (c, d)$, $(c, d) \leq (a, b) \Rightarrow (a, b) = (c, d)$. Il primo membro significa: $a|c$, $b \leq d$; $c|a$, $d \leq b$, ed è vero sse $a = c$ e $b = d$, cioè $(a, b) = (c, d)$. Proprietà transitiva: $(a, b) \leq (c, d)$, $(c, d) \leq (ef) \Rightarrow (a, b) \leq (e, f)$. Il primo membro fornisce: $a|c$, $b \leq d$; $c|e$, $d \leq f$. Dalla transitività della relazione di divisibilità e della relazione $\leq$ segue allora $a|e$, $b \leq f$, quindi $(a, b) \leq (e, f)$.

Dunque, la relazione introdotta in $M \times M$ è una relazione d'ordine; si noti che si tratta di relazione d'ordine parziale, in quanto tale è la relazione di divisibilità in M e quindi esistono coppie (a, b) e (c, d) non confrontabili, non essendo confrontabili i loro primi elementi.

Esercizio 1.9.3. *Si consideri l'insieme parzialmente ordinato $\langle \mathbb{N}; \leq \rangle$, ove $\leq$ è la disuguaglianza consueta nei naturali. Si verifichi che $\langle \mathbb{N} \times \mathbb{N}; \leq \rangle$, dove, $\forall (a, b)$, $(c, d) \in \mathbb{N} \times \mathbb{N}$,*

$$(a, b) \leq (c, d) \Leftrightarrow a \leq c \quad e \quad b \leq d \quad in \quad \mathbb{N}$$

è un insieme parzialmente ordinato.

Sol.: Osserviamo innanzitutto che, se A è un insieme qualsiasi ed (x, y), $(z, t) \in A^2$ si ha $(x, y) = (z, t)$ sse $x = z$ e $y = t$. Proviamo ora che $\langle \mathbb{N} \times \mathbb{N}; \leq \rangle$ è un insieme parzialmente ordinato, cioè che $\leq$ è una relazione d'ordine. Dalla definizione segue

$$(a, b) \leq (a, b) \Leftrightarrow a \leq a \quad \text{e} \quad b \leq b,$$

onde la riflessività ($\leq$ è relazione d'ordine su $\mathbb{N}$);

$$(a,b) \leq (c,d) \quad \text{e} \quad (c,d) \leq (a,b) \Leftrightarrow a \leq c,\, b \leq d \quad \text{e} \quad c \leq a\,, d \leq b \Rightarrow$$
$$\Rightarrow a = c \quad \text{e} \quad b = d \Rightarrow (a,b) = (c,d),$$

cioè l'antisimmetria. Infine

$$(a,b) \leq (c,d) \quad \text{e} \quad (c,d) \leq (e,f) \Leftrightarrow a \leq c,\, b \leq d \quad \text{e} \quad c \leq e\,, d \leq f \Rightarrow$$
$$\Rightarrow a \leq e\,, b \leq f \Rightarrow (a,b) \leq (e,f),$$

cioè la transitività.

Si noti che $\leq$ non è una relazione d'ordine totale , anche se in $\mathbb{N}$ due elementi qualsiasi sono confrontabili. Infatti può essere $a \leq c$ e $b \geq d$, il che non permette di affermare che $(a,b) \leq (c,d)$, secondo la definizione data.

Esercizio 1.9.4. *Si consideri l'insieme totalmente ordinato $\langle \mathbb{N}; \leq \rangle$, ove $\leq$ è l'ordinamento naturale defiito in $\mathbb{N}$. Si verifichi che la relazione $\leq$ su $\mathbb{N} \times \mathbb{N}$ definita da*

$$(a,b) \leq (c,d) \Leftrightarrow \begin{cases} a < c \\ \textit{oppure} \\ a = c \quad e \quad b \leq d \end{cases}$$

è una relazione d'ordine (totale) su $\mathbb{N} \times \mathbb{N}$. tale relazione prende il nome di "ordinamento lessicografico" (infatti, sostituendo gli elementi di $\mathbb{N}$ con le lettere dell'alfabeto e considerando l'"ordine alfabetico" si ottiene l'ordinamento delle parole di un dizionario).

Sol.: La relazione $\leq$ è riflessiva; infatti $(a,b) \leq (a,b)$, in quanto $a = a$ e $b \leq b$. La relazione è antisimmetrica; si deve provare che

$$(a,b) \leq (c,d) \quad \text{e} \quad (c,d) \leq (a,b) \Rightarrow a = c,\, b = d.$$

Se $a \leq c$ e $c \leq a$, si ha $a = c$ onde l'asserto. Se $a = c$, e $b \leq d$ e $d \leq b$, si ha $b = d$, onde l'antisimmetria. Infine , se $a \leq c$, $c = a$ e $d \leq b$ si ha $a = c$ e sicuramente $b = d$.

La relazione è transitiva, cioè

$$(a,b) \leq (c,d)\,, (c,d) \leq (e,f) \Rightarrow (a,b) \leq (e,f).$$

La validità del primo membro comporta quattro casi possibili:

1. $a < c$, $c < e \Rightarrow a < e$ e quindi $(a,b) \leq (e,f)$
2. $a < c$; $c = e$, $d \leq f \Rightarrow a < e \Rightarrow (a,b) \leq (e,f)$
3. $a = c$, $b \leq d$; $c < e \Rightarrow a < e \Rightarrow (a,b) \leq (e,f)$
4. $a = c$, $b \leq d$; $c = e$, $d \leq f \Rightarrow a = e$, $b \leq f \Rightarrow (a,b) \leq (e,f)$.

Pertanto, la relazione è una relazione d'ordine, ed è totale in quanto, per definizione, non esistono coppie inconfrontabili.

Esercizio 1.9.5. *Sia $\langle P; \leq \rangle$ un insieme parzialmente ordinato. Si definisca una relazione d'ordine su $P \times P$.*

Sol.: L'ordinamento lessicografico definito nell'esercizio 9.4 non utilizza alcuna proprietà degli elementi di $\mathbb{N}$, pertanto si può definire in $P \times P$ la seguente relazione

$$\forall (a,b),\ (c,d) \in P \times P, \quad (a,b) \leq (c,d) \Leftrightarrow \begin{cases} a < c \\ \text{oppure} \\ a = c \quad \text{e} \quad b \leq d \end{cases}$$

e $\leq$ sarà una relazione d'ordine (parziale) su $P \times P$. Inoltre, se $\leq$ è una relazione d'ordine totale su P, tale è $\leq$ su $P \times P$.

Esercizio 1.9.6. *Sia $\langle P; \leq \rangle$ un insieme parzialmente ordinato. Si definisca una relazione d'ordine su $P \times P \times P$.*

Sol.: Si può estendere l'ordinamento lessicografico definito sul prodotto cartesiano di due insiemi parzialmente ordinati (cfr. esercizio 9.5) al caso di tre o più insiemi parzialmente ordinati.

Precisamente, la relazione $\leq$ su $P \times P \times P$, definita da

$$(a,b,c) \leq (e,f,g) \Leftrightarrow \begin{cases} a < e \\ \text{oppure} \\ a = e,\ b < f \\ \text{oppure} \\ a = e,\ b = f,\ c \leq g \end{cases}$$

è una relazione d'ordine (parziale, in generale; totale, se tale è la relazione d'ordine su P), come si verifica facilmente.

Esercizio 1.9.7. *Sia $\langle P; \leq \rangle$ un insieme parzialmente ordinato e sia $\emptyset \subset H \subseteq P$; si provi che la restrizione ad H, $\leq_H$, della relazione d'ordine su P è una relazione d'ordine su H.*

Dim.: Per definizione di restrizione di una relazione, si ha

$$\forall x, y \in H,\ x \leq_H y \Leftrightarrow x \leq y \quad \text{in} \quad P,$$

onde l'asserto.

Esercizio 1.9.8. *Si provi che ogni s.i. si una catena $\mathcal{C}$ è una catena, rispetto alla relazione d'ordine definita su $\mathcal{C}$.*

Dim.: Sia $\langle \mathcal{C}; \leq \rangle$ una catena, cioè un insieme totalmente ordinato, e sia $\emptyset \subset H \subseteq \mathcal{C}$. Allora $\langle H; \leq_H \rangle$ è un insieme parzialmente ordinato (cfr. es. 9.7), ma, per definizione di restrizione, è anche totalmente ordinato; infatti

$$\begin{aligned} x, y \in H \Rightarrow x, y \in \mathcal{C} \Rightarrow x \leq y \quad \text{o} \quad y \leq x \quad \text{in} \quad \mathcal{C} \\ \Rightarrow x \leq_H y \quad \text{o} \quad y \leq_H x \quad \text{in} \quad H. \end{aligned}$$

Esercizio 1.9.9. *Sia $\langle P; \leq \rangle$ un insieme parzialmente ordinato. Si dia un procedimento di costruzione delle catene contenute in P.*

Sol.: Fissato $a \in P$, si consideri un qualunque $x \in P$ tale che $a \leq x$; si consideri poi $y \in P$ tale che $x \leq y$ e si proceda nello stesso modo (la costruzione avrà termine dopo n passi soltanto se non esiste un $t \geq w$, w essendo l'ultimo elemento trovato; in quasto caso la catena avrà *lunghezza* n e conterrà $n + 1$ elementi).

L'insieme $\{a, x, y, \dots\}$ è manifestamente una catena, stante la transitività di $\leq$. Per evitare casi banali (catene costituite da un solo elemento) si considereranno, come elementi di partenza, elementi $a \in P$ per i quali esista almeno un $x \geq a$. Si noti che, a partire da $a \in P$, si possono, in generale, costruire più catene.

Esercizio 1.9.10. *Tenendo presente l'esercizio 9.9, si costruiscano le catene di $\langle \mathbb{N}; | \rangle$, ($|$ essendo la divisibilità).*

Sol.: Le catene di $\langle \mathbb{N}; | \rangle$ sono del tipo:

$$\begin{array}{ll} \{1, 2, 4, 8, \dots\} & \\ \{1, 3, 6, 12, 24, \dots\} & \{1, 3, 9, 18, 36, \dots\} \\ \{1, 4, 8, 16, 32, \dots\} & \\ \{1, 5, 10, 20, \dots\} & \{1, 5, 15, 30, \dots\} \end{array}$$

In particolare, si possono considerare le catene del tipo

$$\{n^j \,:\, j \in \mathbb{N}_0\}$$

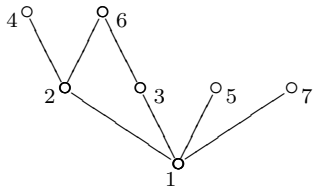
(infatti, $\forall j, k \in \mathbb{N}_0$, $n^j | n^k$ oppure $n^k | n^j$). Ogni sottocatena di quelle considerate è ancora una catena di $\langle \mathbb{N}; | \rangle$.

Esercizio 1.9.11. *Dato l'insieme $A = \{1, 2, 3, 4, 5, 6, 7\}$, $A \subset \mathbb{N}$, si consideri la relazione $R \subseteq A^2$, definita da*

$$\forall x, y \in A,\ (x, y) \in R \Leftrightarrow x | y.$$

Si verifichi che R è una relazione d'ordine e si tracci il diagramma dell'insieme parzialmente ordinato $\langle A; | \rangle$.

Sol.: Poiché R è la restrizione ad A della relazione di divisibilità su $\mathbb{N}$, che è una relazione d'ordine, $\langle A; R\rangle = \langle A; |\,\rangle$ è un insieme parzialmente ordinato. Per tracciare il diagramma, scriviamo le relazioni di copertura:



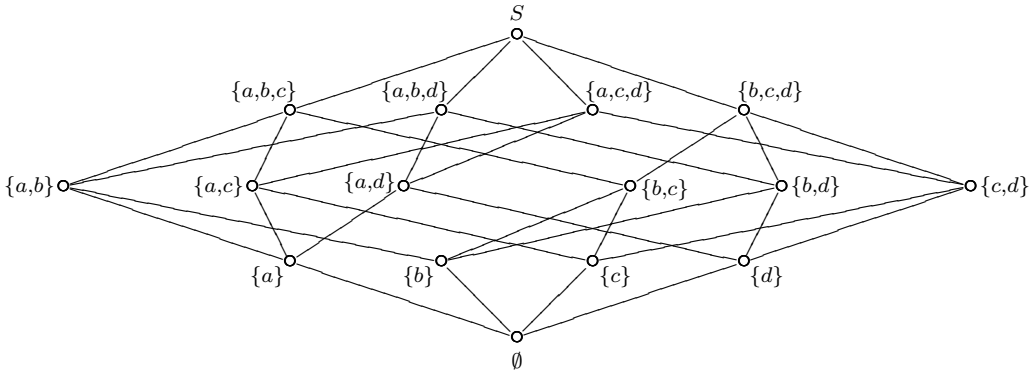
$$1 \prec\!\!\!\cdot\; 2 \prec\!\!\!\cdot\; 4$$
$$1 \prec\!\!\!\cdot\; 2 \prec\!\!\!\cdot\; 6$$
$$1 \prec\!\!\!\cdot\; 3 \prec\!\!\!\cdot\; 6$$
$$1 \prec\!\!\!\cdot\; 5$$
$$1 \prec\!\!\!\cdot\; 7.$$

Esercizio 1.9.12. *Si disegni il diagramma di $\langle P(S); \subseteq\rangle$ con $S = \{a, b, c, d\}$.*

Sol.: Per definizione di inclusione insiemistica, $\subseteq$ è una relazione d'ordine su $P(S)$ (cfr. es. 9.14). Determiniamo i s.i. di S, cioè gli elementi di $P(S)$, e scriviamo le relazioni di copertura tra di essi (in questo caso $A, B \in P(S)$, $A \succ\!\!\!\cdot\; B \;\Rightarrow B \subset A$ e $\nexists C \in P(S)$, $C \neq A, B$ tale che $B \subset C \subset A$):

$$\emptyset \prec\!\!\!\cdot\; \{a\} \prec\!\!\!\cdot\; \{a, b\} \prec\!\!\!\cdot\; \{a, b, c\} \prec\!\!\!\cdot\; S$$
$$\emptyset \prec\!\!\!\cdot\; \{a\} \prec\!\!\!\cdot\; \{a, b\} \prec\!\!\!\cdot\; \{a, b, d\} \prec\!\!\!\cdot\; S$$
$$\emptyset \prec\!\!\!\cdot\; \{a\} \prec\!\!\!\cdot\; \{a, c\} \prec\!\!\!\cdot\; \{a, b, c\} \prec\!\!\!\cdot\; S$$
$$\emptyset \prec\!\!\!\cdot\; \{a\} \prec\!\!\!\cdot\; \{a, c\} \prec\!\!\!\cdot\; \{a, c, d\} \prec\!\!\!\cdot\; S$$
$$\emptyset \prec\!\!\!\cdot\; \{a\} \prec\!\!\!\cdot\; \{a, d\} \prec\!\!\!\cdot\; \{a, b, d\} \prec\!\!\!\cdot\; S$$
$$\emptyset \prec\!\!\!\cdot\; \{a\} \prec\!\!\!\cdot\; \{a, d\} \prec\!\!\!\cdot\; \{a, c, d\} \prec\!\!\!\cdot\; S$$

Le altre $6 \cdot 3 = 18$ catene ottenute con le relazioni di copertura si determinano analogamente scambiando i nomi degli elementi di S.



Esercizio 1.9.13. *Sia $\langle P; \leq\rangle$ un insieme parzialmente ordinato. Diremo che P è "ben ordinato" se per ogni $H \subseteq P$, $H \neq \emptyset$, $\exists h \in H$ tale che $\forall x \in H \Rightarrow h \leq x$. Si provi che un insieme ben ordinato è una catena.*

Dim.: Si deve provare che, se $\langle P; \leq\rangle$ è ben ordinato, allora esso è totalmente ordinato, cioè due elementi qualsiasi di P sono confrontabili. Siano

$a, b \in P$, $a \neq b$; consideriamo $H = \{a, b\}$; per ipotesi H ammette un elemento "più piccolo", quindi o è $a \leq b$ (ed a è il più piccolo elemento di $\{a, b\}$), oppure è $b \leq a$ (e b è il più piccolo elemento di $\{a, b\}$). Ne segue l'asserto.

Esercizio 1.9.14. *Sia S un insieme qualunque; si provi che $\langle P(S); \subseteq \rangle$, dove $\subseteq$ è l'inclusione insiemistica, è un insieme parzialmente ordinato.*

Dim.: Si deve provare che la relazione di inclusione è riflessiva, antisimmetrica e transitiva. Si ha

$$\forall A \in P(S), \quad (\text{cioè } A \subseteq S) \quad \Rightarrow A \subseteq A,$$

per definizione di inclusione, onde la riflessività. Si ha poi

$$A, B \in P(S),\ A \subseteq B, B \subseteq A \Rightarrow A = B,$$

per definizione di uguaglianza tra due insiemi, onde la proprietà antisimmetrica. Infine

$$A, B, C \in P(S),\ A \subseteq B,\ B \subseteq C \Rightarrow A \subseteq C.$$

Infatti $A \subseteq B \Leftrightarrow [\forall x \in A \Rightarrow x \in B]$; $B \subseteq C \Leftrightarrow [\forall x \in B \Rightarrow x \in C]$; ne segue che $\forall x \in A \Rightarrow x \in C$, cioè $A \subseteq C$.

Esercizio 1.9.15. *Sia $A \neq \emptyset$ un insieme qualsiasi, e sia $\mathcal{R}(A)$ l'insieme delle relazioni su A. Si verifichi che $\langle \mathcal{R}(A); \subseteq \rangle$ è un insieme parzialmente ordinato.*

Sol.: Per definizione di relazione,$R \in \mathcal{R}(A) \Rightarrow R \subseteq A \times A \Rightarrow R \in P(A \times A)$. D'altra parte $\langle P(A \times A); \subseteq \rangle$ è un insieme parzialmente ordinato (cfr. es. 9.14); poiché $\mathcal{R}(A)$ è un s.i. di $P(A \times A)$ esso è parzialmente ordinato rispetto a $\subseteq$ (che è la restrizione della relazione d'ordine definita su $P(A \times A)$)>

Esercizio 1.9.16. *Sia $A \neq \emptyset$ un insieme qualunque e sia $\mathcal{E}(A)$ l'insieme delle equivalenze[2] su A. Si verifichi che $\langle \mathcal{E}(A); \subseteq \rangle$ è un insieme parzialmente ordinato.*

Sol.: Dato che $\mathcal{E}(A) \subseteq \mathcal{R}(A)$, l'asserto segue dall'esercizio 9.15. (si tenga presente la definizione di restrizione).

[2]*Nota*: per la definizione e le proprietà delle equivalenze si veda il successivo paragrafo 10.

1.10 Relazioni di equivalenza su un insieme. Insieme quoziente.

Sia $A \neq \emptyset$ e sia R una relazione su A. Diremo che R è una *relazione di equivalenza* (o equivalenza) se

1. R è riflessiva $(\Delta_A \subseteq R)$
2. R è simmetrica $(R = R^{-1})$
3. R è transitiva $(R \circ R \subseteq R)$.

Ad esempio, se A è l'insieme delle rette di un piano ed R è la relazione di parallelismo, allora R è una relazione di equivalenza; infatti

1. $\forall a \in A,\ a//a$ (riflessiva)
2. $\forall a, b \in A :\ a//b \Rightarrow B//a$ (simmetrica)
3. $\forall a, b, c \in A :\ a//b,\ b//c \Rightarrow a//c$ (transitiva).

Se A è l'insieme dei triangoli di un piano e R è la similitudine, R è un'equivalenza. Altri esempi saranno dati negli esercizi. Se R è una relazione di equivalenza su A, la denoteremo spesso con in simbolo $\mathcal{E}$ (invece che con R, e ciò per ricordare che si tratta di un'equivalenza).

Introduciamo ora la nozione di classi di equivalenza, rispetto ad un'equivalenza $\mathcal{E} \subseteq A \times A$. Sia $A \in A$ un qualunque elemento di A; diciamo *classe di equivalenza* rispetto ad $\mathcal{E}$ individuata da a il seguente s.i. di A:

$$[a]\mathcal{E} = \{x \in A :\ (a, x) \in \mathcal{E}\} = \{x \in A :\ (x, a) \in \mathcal{E}\}$$

(dato che $\mathcal{E}$ è simmetrica. Quando non vi sia possibilità di confusione scriveremo $[a]$ in luogo di $[a]\mathcal{E}$.

Dalla definizione segue che

$$\forall y \in [a],\ [y] = [a].$$

Le classi di equivalenza godono di alcune proprietà importanti.

Proposizione 1.10.1. *Se $\mathcal{E} \subset A \times A$ è un'equivalenza su A, ogni $a \in A$ appartiene ad una classe di equivalenza.*

Dim.: Poiché $\mathcal{E}$ è riflessiva, per ogni $a \in A$, $(a, a) \in \mathcal{E}$ e quindi $a \in [a]$. ne segue pure che non esistono classi di equivalenza vuote.

Proposizione 1.10.2. *Se $\mathcal{E} \subseteq A \times A$ è un'equivalenza su A, allora due classi di equivalenza qualsiasi o sono disgiunte o coincidono.*

Dim.: Basterà provare che $[a] \cap [b] \neq \emptyset \Rightarrow [a] = [b]$. Ora, $[a] \cap [b] \neq emptyset \Rightarrow \exists x \in [a] \cap [b]$. Pertanto, $x \in [a] \Rightarrow (a, x) \in \mathcal{E}$ e $x \in [b] \Rightarrow (x, b) \in \mathcal{E}$. Ma $\mathcal{E}$ è transitiva: ne segue che $(a, b) \in \mathcal{E}$, ossia $a \in [b]$ e $b \in [a]$, onde le classi coincidono.

Notiamo che, su ogni insieme A, si possono sempre definire due relazioni di equivalenza, precisamente la relazione identica $|mathcalE = \Delta_A$ e la relazione totale $\mathcal{E} = A \times A$ (e queste sono distinte se A contiene più di un elemento).

La nozione di classi di equivalenza permette di associare alla coppia $\langle A; \mathcal{E} \rangle$, $A \neq \emptyset$, $\mathcal{E} \subseteq A \times A$, $\mathcal{E}$ equivalenza su A, un nuovo insieme, *insieme quoziente* di A modulo la relazione di equivalenza $\mathcal{E}$ (o insieme quoziente di A rispetto all'equivalenza $\mathcal{E}$), che sarà denotato con $A/\mathcal{E}$. Precisamente, gli elementi di $A/\mathcal{E}$ sono tutte e sole le classi di equivalenza rispetto ad $\mathcal{E}$:

$$A/\mathcal{E} = \{[a]\mathcal{E} \,:\, a \in A\}$$

e questo è, di fatto, un nuovo insieme in base alla prop 10.2.

Nel caso particolare in cui $|mathcalE = \Delta_A$, ogni classe $[a]\Delta_A$ contiene il solo elemento a, onde $A/\Delta_A = A$; se invece $\mathcal{E} = A \times A$, tutti gli elementi di A appartengono ad una medesima classe $[a]A \times A = A$, pertanto $A/A \times A = \{A\}$, ($\{A\}$ essendo un insieme che contiene come unico elemento l'insieme A).

Nel primo esempio considerato, $A///$ è costituito da tutte le classi di rette tra loro parallele, quindi ciascuna classe si può identificare con la direzone di tutte le sue rette, onde si può dire che $A///$ è l'insieme delle direzioni del piano; nel caso della similitudine nell'insieme A dei triangoli del piano, gli elementi di $A/\mathcal{E}$ le classi contenenti tutti triangoli simili tra loro e ciascuna di esse si può identificare con la terna degli angoli di tutti i triangoli della classe.

Diamo ora un altro esempio di relazione di equivalenza e di costruzione dell'insieme quoziente. Sia $A = \{a, b, c, d\}$; la relazione $\mathcal{E} = \delta_A \cup \{(a, b), (b, a), (b, d), (d, b), (a, d), (d, a)\}$ è manifestamente un'equivalenza; infatti $\Delta_A \subseteq \mathcal{E}$, $\mathcal{E} = \mathcal{E}^{-1}$, $\mathcal{E}|circ\mathcal{E} \subseteq \mathcal{E}$ (come è immediato verificare). Costruiamo $A/\mathcal{E}$; i suoi elementi sono le classi di equivalenza, quindi

$$\begin{aligned}
[a] &= \{a, b, d\} \\
[b] &= \{b, a, d\} = [a] \\
[c] &= \{c\} \\
[d] &= \{d, a, b\} = [a].
\end{aligned}$$

Pertanto

$$A/\mathcal{E} = \{[a], [c]\}.$$

Altre proprietà delle relazioni di equivalenza saranno viste negli esercizi.

Si noti che la conoscenza dell'insieme $E(A)$ di tutte le relazioni di equivalenza su di un insieme A ($\neq \emptyset$) consente la conoscenza di tutte le relazioni di equivalenza sull'insieme $A/\mathcal{E}$, per ogni $\mathcal{E} \in E(A)$. Precisamente, le equivalenze su $A/\mathcal{E}$ sono tutte e sole le equivalenze del tipo $\mathcal{F}/\mathcal{E}$, $\mathcal{F} \in E(A)$ tale che $\mathcal{F} \supseteq \mathcal{E}$, definite da $([a]\mathcal{E}, [b]\mathcal{E}) \in \mathcal{F}/\mathcal{E} \Leftrightarrow (a, b) \in \mathcal{F}$. Nell'es. 10.8 si prova che $\mathcal{F}/\mathcal{E}$ è un'equivalenza su $A/\mathcal{E}$. Viceversa, qualunque equivalenza $\mathcal{E}^*$ su $A/\mathcal{E}$ definisce un'equivalenza $\mathcal{F}$ su A ponendo

$$(a, b) \in \mathcal{F} \Leftrightarrow ([a]\mathcal{E}, [b]\mathcal{E}) \in \mathcal{E}^*$$

(la verifica che $\mathcal{F}$ è un'equivalenza è immediata). Ne segue che $\mathcal{E}^* = \mathcal{F}/\mathcal{E}$ con $\mathcal{F} \supseteq \mathcal{E}$.

Esercizi

Esercizio 1.10.1. *Siano $\mathcal{E}_1$ ed $\mathcal{E}_2$ due relazioni di equivalenza su A; si provi che $\mathcal{E}_1 \cap \mathcal{E}_2$ è un'equivalenza su A.*

Dim.: Si deve provare che $\mathcal{E}_1 \cap \mathcal{E}_2$ è riflessiva, simmetrica e transitiva. Osserviamo che $\mathcal{E}_1 \cap \mathcal{E}_2 \neq \emptyset$: infatti

$$\Delta_A \subseteq \mathcal{E}_1, \mathcal{E}_2 \Rightarrow \Delta_A \subseteq \mathcal{E}_1 \cap \mathcal{E}_2.$$

Tenendo conto che $\mathcal{E}_1$ ed $|mathcalE_2$ sono equivalenze si ha

$$\forall a \in A,\ (a,a) \in \mathcal{E}_1 \quad \text{e} \quad (a,a) \in \mathcal{E}_2 \Rightarrow (a,) \in \mathcal{E}_1 \cap \mathcal{E}_2$$

(proprietà riflessiva);

$$\begin{aligned}(a,b) \in \mathcal{E}_1 \cap \mathcal{E}_2 \Rightarrow (a,b) \in \mathcal{E}_1 \quad \text{e} \quad (a,b) \in \mathcal{E}_2 \Rightarrow \\ \Rightarrow (b,a) \in \mathcal{E}_1 \quad \text{e} \quad (b,a) \in \mathcal{E}_2 \Rightarrow (b,a) \in \mathcal{E}_1 \cap \mathcal{E}_2\end{aligned}$$

(proprietà simmetrica);

$$\begin{aligned}(a,b,\ (b,c)) \in \mathcal{E}_1 \cap \mathcal{E}_2 \Rightarrow (a,b),\ (b,c) \in \mathcal{E}_1 \quad \text{e} \quad (a,b),\ (b,c) \in \mathcal{E}_2 \Rightarrow \\ \Rightarrow (a,c) \in \mathcal{E}_1 \quad \text{e} \quad (a,c) \in \mathcal{E}_2 \Rightarrow (a,c) \in \mathcal{E}_1 \cap \mathcal{E}_2\end{aligned}$$

(proprietà transitiva).

Esercizio 1.10.2. *Sia R una relazione riflessiva e simmetrica su A; si provi che la chiusura transitiva di R è la più piccola relazione di equivalenza su A che contiene R.*

Dim.: Sia $\mathcal{E}$ la chiusura transitiva di R. Per definizione di chiusura transitiva, $\mathcal{E}$ è la più piccola relazione transitiva contenente R; dato che R è riflessiva segue che $\Delta_A \subseteq R$, onde $\Delta_A \subseteq \mathcal{E}$ (essendo $R \subseteq \mathcal{E}$): quindi $\mathcal{E}$ è riflessiva. D'altra parte $R = R^{-1}$ ed $\mathcal{E} = \bigcup_{n=1}^{\infty} R^n$, quindi

$$\mathcal{E}^{-1} - \left(\bigcup_{n=1}^{\infty} R^n\right)^{-1} = \bigcup_{n=1}^{\infty} (R^n)^{-1} = \bigcup_{n=1}^{\infty} (R^{-1})^n = \bigcup_{n=1}^{\infty} R^n = \mathcal{E}$$

(tenendo presente gli esercizi 7.7 e 8.11), cioè $\mathcal{E}$ è simmetrica. Ne segue l'asserto.

Esercizio 1.10.3. *Siano $\mathcal{E}_1$ ed $\mathcal{E}_2$ due relazioni di equivalenza su A. Si provi che, in generale, $\mathcal{E}_1 \cup \mathcal{E}_2$ non è una relazione di equivalenza su A.*

Dim.: Proveremo che la relazione $\mathcal{E}_1 \cup \mathcal{E}_2$ è riflessiva e simmerica ma, in generale, non è transitiva. Infatti

$$\Delta_A \subseteq \mathcal{E}_1, \mathcal{E}_2 \Rightarrow \Delta_A \subseteq \mathcal{E}_1 \cup \mathcal{E}_2,$$

onde la riflessività;

$$\mathcal{E}_1 = {\mathcal{E}_1}^{-1},\ \mathcal{E}_2 = {\mathcal{E}_2}^{-1} \Rightarrow (\mathcal{E}_1 \cup \mathcal{E}_2)^{-1} = {\mathcal{E}_1}^{-1} \cup {\mathcal{E}_2}^{-1} = \mathcal{E}_1 \cup \mathcal{E}_2$$

(cfr. es. 7.7), onde la simmetria.

Siano ora (a, b), (b, c) in $\mathcal{E}_1 \cup \mathcal{E}_2$; se $(a, b).(b, c) \in \mathcal{E}_1$ (oppure $\mathcal{E}_2$), $(a, c) \in \mathcal{E}_1$ (oppure $\mathcal{E}_2$), onde $(a, c) \in \mathcal{E}_1 \cup \mathcal{E}_2$; d'altra parte, se ad esempio, $(a, b) \in \mathcal{E}_1$, $(b, c) \in \mathcal{E}_2$, non si può affermare che $(a, c) \in \mathcal{E}_1$, oppure che $(a, c) \in \mathcal{E}_2$, pertanto non vale la proprietà transitiva.

La chiusura transitiva di $\mathcal{E}_1 \cup \mathcal{E}_2$ è però un'equivalenza (si veda l'es. 10.2); definiamo pertanto *unione reticolare* di $\mathcal{E}_1$ ed $\mathcal{E}_2$, e la denotiamo con $\mathcal{E}_1 \vee \mathcal{E}_2$, la chiusura transitiva di $\mathcal{E}_1 \cup \mathcal{E}_2$

$$\mathcal{E}_1 \vee \mathcal{E}_2 = \bigcup_{n=1}^{\infty} (\mathcal{E}_1 \cup \mathcal{E}_2)^n$$

(il nome sarà giustificato nel seguito).

Esercizio 1.10.4. *Siano $\mathcal{E}_1$ ed $\mathcal{E}_2$ due equivalenze su A. Si provi che $\mathcal{E}_1 \circ \mathcal{E}_2$ è un'equivalenza su A sse $\mathcal{E}_1$ ed $\mathcal{E}_2$ sono permutabili (ovvero commutano, cioè $\mathcal{E}_1 \circ \mathcal{E}_2 = \mathcal{E}_2 \circ \mathcal{E}_1$).*

Dim.: Supponiamo che $\mathcal{E}_2 \circ \mathcal{E}_1$ sia un'equivalenza; proviamo che

$$\mathcal{E}_2 \circ \mathcal{E}_1 = \mathcal{E}_1 \circ \mathcal{E}_2$$

Dato che $\mathcal{E}_2 \circ \mathcal{E}_1$ è un'equivalenza, essa è simmetrica, cioè

$$\mathcal{E}_2 \circ \mathcal{E}_1 = (\mathcal{E}_2 \circ \mathcal{E}_1)^{-1} = {\mathcal{E}_1}^{-1} \circ {\mathcal{E}_2}^{-1} = \mathcal{E}_1 \circ \mathcal{E}_2,$$

onde $\mathcal{E}_1$ ed $\mathcal{E}_2$ sono permutabili.

Supponiamo ora che $\mathcal{E}_1 \circ \mathcal{E}_2 = \mathcal{E}_2 \circ \mathcal{E}_1$ e proviamo che $\mathcal{E}_1 \circ \mathcal{E}_2$ è un'equivalenza. $\mathcal{E}_1 \circ \mathcal{E}_2$ è riflessiva; infatti

$$\Delta_A \subseteq \mathcal{E}_1, \mathcal{E}_2 \Rightarrow \Delta_A \subseteq \mathcal{E}_1 \circ \mathcal{E}_2$$

(dato che $\Delta_A \circ \Delta_A = \Delta_A$). $\mathcal{E}_1 \circ \mathcal{E}_2$ è simmetrica; infatti

$$(\mathcal{E}_1 \circ \mathcal{E}_2)^{-1} = {\mathcal{E}_2}^{-1} \circ {\mathcal{E}_1}^{-1} = \mathcal{E}_2 \circ \mathcal{E}_1 = \mathcal{E}_1 \circ \mathcal{E}_2.$$

Proviamo ora la transitività: si ha, tenendo conto della proprietà associativa e della permutabilità,

$$\begin{aligned}(\mathcal{E}_1 \circ \mathcal{E}_2) \circ (\mathcal{E}_1 \circ \mathcal{E}_2) &= \mathcal{E}_1 \circ (\mathcal{E}_2 \circ \mathcal{E}_1) \circ \mathcal{E}_2 = \mathcal{E}_1 \circ (\mathcal{E}_1 \circ \mathcal{E}_2) \circ \mathcal{E}_2 = \\ &= (\mathcal{E}_1 \circ \mathcal{E}_1) \circ (\mathcal{E}_2 \circ \mathcal{E}_2) \subseteq \mathcal{E}_1 \circ (\mathcal{E}_2 \circ \mathcal{E}_2) \subseteq \mathcal{E}_1 \circ \mathcal{E}_2 :\end{aligned}$$

negli ultimi due passaggi si è tenuto conto dell'isotonia del prodotto per una fissata relazione rispetto all'inclusione (vedi es 7.10).

Esercizio 1.10.5. *Si costruisca un esempio per verificare che l'unione di due equivalenze su A non è un'equivalenza.*

Sol.: Consideriamo $A = \{a, b, c, d\}$; le due relazioni

$$\mathcal{E}_1 = \Delta_A \cup \{(a, b), (ba)\} \quad \text{ed} \quad \mathcal{E}_2 = \Delta_A \cup \{(b, c), (c, b)\}$$

sono manifestamente due equivalenze su A (la proprietà riflessiva e simmetrica sono ovvie, ed inoltre $\mathcal{E}_1 \circ \mathcal{E}_1 = \Delta_A \subseteq \mathcal{E}_1$, $\mathcal{E}_2 \circ \mathcal{E}_2 = \Delta_A \subseteq \mathcal{E}_2$, onde $\mathcal{E}_1$ ed $\mathcal{E}_2$ sono transitive). Si ha:

$$\mathcal{E}_1 \cup \mathcal{E}_2 = \Delta_A \cup \{(a, b), (b, a), (b, c), (c, b)\}$$

e questa relazione non è transitiva perché, in particolare, dovrebbe contenere la coppia (a, c), mentre ciò non accade.

Esercizio 1.10.6. *Si provi che la relazione vuota su $A \neq \emptyset$ non è una relazione di equivalenza.*

Dim.: Poiché $\Delta_A \not\subseteq \emptyset$, $\emptyset$ non è riflessiva, onde non può essere un'equivalenza.

Esercizio 1.10.7. *Sia $\mathbb{N}$ l'insieme dei numeri naturali. Si provi che la relazione R definita su $|mathbbN$ da*

$$(a, b) \in R \Rightarrow \textit{m.c.d.}(a, b) = 1$$

non è una relazione di equivalenza.

Sol.: Basta provare che R non gode di una delle tre proprietà: riflessiva, simmetrica, transitiva. Poiché m.c.d.$(a, a) = a$, per $a \neq 1$, m.c.d.$(a, a) \neq 1$ onde R non è riflessiva. Si noti che R è simmetrica.

Esercizio 1.10.8. *Siano $\mathcal{E}, \mathcal{F}$ due equivalenze su A e sia $\mathcal{E} \subseteq \mathcal{F}$. Si definisca su $A/\mathcal{E}$ la relazione $\mathcal{F}/\mathcal{E}$ nel modo seguente*

$$([a]\mathcal{E}, [b]\mathcal{E}) \in \mathcal{F}/\mathcal{E} \Leftrightarrow (a, b) \in \mathcal{F}.$$

Si provi che $\mathcal{F}/\mathcal{E}$ è un'equivalenza su $A/\mathcal{E}$.

Dim.: Proviamo innanzi tutto che $\mathcal{F}/\mathcal{E}$ è ben definita, cioè che non dipende dal rappresentante delle classi; in altri termini, proviamo che

$$a' \in [a]\mathcal{E},\ b' \in [b]\mathcal{E},\ ([a]\mathcal{E}, [b]\mathcal{E}) \in \mathcal{F}/\mathcal{E} \Rightarrow (a', b') \in \mathcal{F}.$$

Ora $a' \in [a]\mathcal{E}$, $b' \in [b]\mathcal{E} \Rightarrow (a, a') \in \mathcal{E}$, $(b, b') \in \mathcal{E}$, ma $\mathcal{E} \subseteq \mathcal{F}$, quindi $(a, a') \in \mathcal{F}$, $(b, b') \in \mathcal{F}$; pertanto

$$[a']\mathcal{E} = [a]\mathcal{E} \subseteq [a]\mathcal{F}, \qquad [b']\mathcal{E} = [b]\mathcal{E} \subseteq [b]\mathcal{F};$$

ne segue che

$$(a', b') \in \mathcal{F} \Leftrightarrow (a, b) \in \mathcal{F}.$$

Proviamo ora che $\mathcal{F}/\mathcal{E}$ è un'equivalenza; tenendo presente che $\mathcal{F}$ è un'equivalenza, si ha:

$$\forall a \in A,\ (a, a) \in \mathcal{F} \Rightarrow ([a]\mathcal{E}, [a]\mathcal{E}) \in \mathcal{F}/\mathcal{E},$$

onde la riflessività;

$$\begin{aligned}[(a, b) \in \mathcal{F} \Rightarrow (b, a) \in \mathcal{F}] \Rightarrow \\ \Rightarrow [([a]\mathcal{E}, [b]\mathcal{E} \in \mathcal{F}/\mathcal{E} \Rightarrow ([b]\mathcal{E}, [a]\mathcal{E}) \in \mathcal{F}/\mathcal{E}]\,,\end{aligned}$$

cioè la simmetria. Infine, per la transitività di $\mathcal{F}$, si ha:

$$(a, b),\ (b, c) \in \mathcal{F} \Rightarrow (a, c) \in \mathcal{F},$$

da cui

$$([a]\mathcal{E}, [b]\mathcal{E}),\ ([b]\mathcal{E}, [c]\mathcal{E}) \in \mathcal{F}/\mathcal{E} \Rightarrow ([a]\mathcal{E}, [c]\mathcal{E}) \in \mathcal{F}/\mathcal{E},$$

onde l'asserto.

Esercizio 1.10.9. *Si verifichi che la relazione $R \subseteq \mathbb{Z} \times \mathbb{Z}$ definita da*

$$\forall a, b, \in \mathbb{Z},\ (a, b) \in R \Rightarrow a - b = 2x,\ x \in \mathbb{Z}$$

è una relazione di equivalenza e si definisca $\mathbb{Z}/R$.

Sol.: R è riflessiva: $a - a = 2 \cdot 0$, $0 \in \mathbb{Z}$. R è simmetrica: $a - b = 2x$, $x \in \mathbb{Z} \Rightarrow b - a = -2x = 2(-x)$, $-x \in \mathbb{Z}$. Infine, R è transitiva: $a - b = 2x$, $b - c = 2y$, $x, y \in \mathbb{Z} \Rightarrow (a-b)+(b-c) = 2x+2y \Rightarrow a-c = 2(x+y)$, $x+y \in \mathbb{Z}$. Quindi R è una relazione di equivalenza. $\mathbb{Z}/R$ è costituito rispettivamente dalla classe dei numeri pari e da quella dei numeri dispari. Infatti, se $a \in \mathbb{Z}$ è pari, $a = 2m$, allora

$$[a] = [2m] = \{b \in \mathbb{Z} : 2m - b = 2x\} \Rightarrow b = 2m - 2x \Rightarrow b \quad \text{pari.}$$

Se invece $a \in \mathbb{Z}$ è dispari, $a = 2m + 1$, allora

$$[a] = [2m+1] = \{b \in \mathbb{Z} : 2m+1-b = 2x\} \Rightarrow b = 2(m-x)+1 \Rightarrow b \quad \text{è dispari.}$$

Si possono scegliere come rappresentanti di queste due classi, rispettivamente 0 ed 1, onde gli elementi di $\mathbb{Z}/R$ sono $[0]$ ed $[1]$.

Esercizio 1.10.10. *Sia $\mathcal{E}$ una relazione su $\mathbb{N} \times \mathbb{N}$ ($\mathbb{N}$ essendo l'insieme dei numeri naturali), definita da*

$$(a, b)\mathcal{E}(c, d) \Leftrightarrow a + d = b + c$$

Si verifichi che $\mathcal{E}$ è un'equivalenza e si determini $|mathbbN \times \mathbb{N}/\mathcal{E}$.

Sol.: La relazione $\mathcal{E}$ è manifestamente riflessiva e simmetrica (perché la somma è commutativa). Proviamo che è transitiva, cioè che

$$(a,b)\mathcal{E}(c,d),\ (c,d)\mathcal{E}(e,f) \Rightarrow (a,b)\mathcal{E}(e,f).$$

Si ha

$$(a,b)\mathcal{E}(c,d),\ (c,d)\mathcal{E}(e,f) \Rightarrow a+d=b+c,\ c+f=e+d \Rightarrow$$
$$\Rightarrow a+d+c+f=b+c+e+d \Rightarrow a+f=b+e$$

(perché in $\mathbb{N}$ vale la legge di cancellazione $x+z=y+z \Rightarrow x=y$, come sarà visto meglio nel seguito), onde la transitività.

Determiniamo l'insieme quoziente. Avremo

$$[(a,b)] = \{(x,y)\ :\ a+y=b+x\},$$

cioè ciascuna di queste classi rappresenta un intero relativo. pertanto $\mathbb{N} \times \mathbb{N}/\mathcal{E} = \mathbb{Z}$ ed $|mathcalE$ prende anche il nome di relazione di equidifferenza.

Esercizio 1.10.11. *Sia A l'insieme dei punti di un piano e sia $o \in A$ un punto fissato. Si verifichi che la relazione $\mathcal{E} \subseteq A \times A$ definita da*

$$\forall x,y \in A,\ (x,y) \in \mathcal{E} \Leftrightarrow d(o,x) = d(o,y)$$

($d(o,x)$ essendo la distanza di o da x) è un'equivalenza e si determini $A/\mathcal{E}$.

Sol.: $\mathcal{E}$ è manifestamente una relazione di equivalenza, dato che è definita da un'eguaglianza numerica (i numeri rappresentando le distanze). Determiniamo ora $A/\mathcal{E}$. Si ha

$$\forall x \in A,\ [x]\mathcal{E} = \{y \in A\ :\ d(o,x) = d(o,y)\}$$

quindi $[x]\mathcal{E}$ è l'insieme dei punti della circonferenza di centro o e raggio $d(o,x)$

Esercizio 1.10.12. *Sia S l'insieme dei punti di un piano π (che denoteremo con $A,B,C,\dots$). Fissato in S un fascio $\mathcal{F}$ di rette parallele (che indicheremo con $r,s,t,\dots$), sia data una relazione $\mathcal{E} \subseteq S \times S$, definita da*

$$\forall A,B \in S,\ (A,B) \in \mathcal{E} \Leftrightarrow \exists r \in \mathcal{F}\ :\ A,B \in r.$$

Si verifichi che $\mathcal{E}$ è una relazione di equivalenza e si determini $S/\mathcal{E}$.

Sol.: Poiché, per ogni punto A del piano, esiste ed è unica la retta $r \in \mathcal{F}$ che lo contiene, $\mathcal{E}$ è riflessiva. Inoltre, $A,B \in r \Rightarrow B,A \in r$, quindi $\mathcal{E}$ è simmetrica. Infine, $(A,B) \in \mathcal{E}$, $(B,C) \in \mathcal{E} \Rightarrow (A,C) \in \mathcal{E}$; infatti $A,B \in r$ comporta che r sia l'unica retta di $\mathcal{F}$ che contiene B, pertanto , $(B,C) \in \mathcal{E} \Rightarrow C \in r \Rightarrow (A,C) \in \mathcal{E}$. per determinare $S/\mathcal{E}$, consideriamone gli elementi, cioè le classi di equivalenza; si ha

$$\forall A \in S,\ [A] = \{B \in S\ :\ [\exists r \in \mathcal{F}\ :\ A,B \in r]\};$$

pertanto $[A]$ è costituita da tutti i punti della retta $r \in \mathcal{F}$ passante per A. Ne segue che $S/\mathcal{E}$ ha come elementi le rette di $\mathcal{F}$ (ciascuna pensata come totalità dei suoi punti, cioè come classe di equivalenza).

1.11 La relazione di congruenza modulo m nell'insieme dei numeri interi relativi.

Sia $\mathbb{Z}$ l'insieme degli interi (relativi); fissato $m \in \mathbb{Z}$, $m \geq 2$, definiamo una particolare relazione su $\mathbb{Z}$, *la congruenza modulo* m, nel modo seguente:

$$a \equiv b \,(\mathrm{mod}\ m) \Leftrightarrow m|(a-b)$$

(da leggersi "a congruo a b, modulo m, sse m divide la differenza $a-b$"). proviamo che

Proposizione 1.11.1. *La congruenza modulo m su $\mathbb{Z}$ ($m \in \mathbb{N}$, $m \geq 2$) è una relazione di equivalenza su $\mathbb{Z}$.*

Dim.: Occorre provare che tale relazione è riflessiva, simmetrica e transitiva. Si ha subito $a \equiv a \mod m$, in quanto $m|(a-a)$, $\forall a \in \mathbb{Z}$, onde la riflessività. Inoltre, se $a \equiv b \mod m$, allora $m|(a-b)$, cioè esiste $x \in \mathbb{Z}$ tale che $mx = a-b$; ne segue che $-mx = -(a-b) = b-a \Rightarrow m(-x) = b-a \Rightarrow m|(b-a)$, onde la simmetria. Sia ora $a \equiv b \,(\mathrm{mod}\ m)$, $b \equiv c \,(\mathrm{mod}\ m)$; proviamo che $a \equiv c \,(\mathrm{mod}\ m)$, cioè la transitività. dall'ipotesi segue che

$$m|(a-b) \Rightarrow \exists x \in \mathbb{Z} : mx = a-b$$
$$m|(b-c) \Rightarrow \exists y \in \mathbb{Z} : my = b-c.$$

Sommando membro a membro le espressioni a destra delle implicazioni si ottiene

$$mx + my = a - b + b - c \Rightarrow m(x+y) = a - c \Rightarrow m|(a-c),$$

dato che $x + y \in \mathbb{Z}$. Pertanto, la congruenza $\mod m$ è un'equivalenza su $\mathbb{Z}$.

Ricordiamo ora che nell'insieme degli interi (relativi) è definita la divisione con resto, cioè

$$\forall a, b \in \mathbb{Z},\ b \neq 0, a \geq b \Rightarrow q, r \in \mathbb{Z} : a = bq + r \quad \text{e} \quad 0 \leq r < |b|$$

dove $|b|$ è il valore assoluto di b ed il resto è sempre non negativo. Il fatto che il resto della divisione in $\mathbb{Z}$ sia non negativo si prova immediatamente. L'affermazione è banalmente vera se $b|a$ (nel qual caso $r = 0$), oppure se a e b sono entrambi positivi. Supponiamo ora che a e b siano entrambi negativi. Se $|a| > |b|$, esiste un intero positivo q tale che $|a| < |bq|$, onde $a = bq + r$, con r positivo (dato che $bq < 0$). Se $a < 0$, $b > 0$, $|a| > |b|$, allora, con q negativo, si ha $a = bq + r$ ed $r > 0$ ($|bq| > |a|$); infine, se $a > 0$, $b < o$, con $q < 0$ e $a > bq$ si ottiene $r > 0$.

Ciò premesso, proviamo che la congruenza modulo m su $\mathbb{Z}$ si può anche definire nel modo seguente:

$$a \equiv b \,(\mathrm{mod}\ m) \Leftrightarrow \quad \begin{array}{l} a \text{ e } b \text{ hanno il medesimo resto} \\ \text{quando siano divisi per } m. \end{array}$$

Proviamo l'equivalenza delle due affermazioni. Sia $a \equiv b \,(\mathrm{mod}\ m)$, cioè $m|(a-b)$; allora $\exists x \in \mathbb{Z}$, tale che $mx = a - b$. Dividendo sia a che b per m si ottiene $a = mq + r$, $b = mq' + r'$, da cui

$$a - b = mq + r - (mq' + r') = m(q - q') + r - r'.$$

Ma , per ipotesi, $a - b = mx$, onde

$$mx = m(q - q') + r - r' \Rightarrow m(x - q + q') = r - r'.$$

Ora m divide il primo membro, quindi m deve dividere il secondo, cioè $m|(r - r')$; ma r ed r' sono entrambi non nulli e strettamente minori di m , onde $|r - r'| < m$. Ne segue che

$$m|(r - r') \Rightarrow r - r' = 0 \Rightarrow r = r'.$$

Viceversa, supponiamo che a e b, divisi per m diano lo stesso resto; proviamo che $m|(a - b)$. Si ha $a = mq + r$, $b = mq' + r$; sottraenedo membro a membro, si ottiene

$$a - b = m(q - q') + r - r = m(q - q'),$$

da cui $m|(a - b)$, in quanto $q - q' \in \mathbb{Z}$.

Dato che al congruenza modulo m è un'equivalenza su $\mathbb{Z}$, determiniamo l'insieme quoziente, che denoteremo con $\mathbb{Z}_m$. Sia $a \in \mathbb{Z}$; per definizione di classe di equivalenza, $[a] \in \mathbb{Z}_m$ è definita da

$$\begin{array}{l} [a] = \{x \in \mathbb{Z} \,:\, a \equiv x \,(\mathrm{mod}\ m)\} = \{x \in \mathbb{Z} \,:\, m|(a - x)\} = \\ \quad = \{x \in \mathbb{Z} \,:\, a \quad \text{ed} \quad x \quad \text{hanno lo stesso resto se divisi per} \quad m\} \end{array}$$

Ora, i resti possibili nella divisione per m di tutti gli elementi di $\mathbb{Z}$ sono soltanto gli m interi (non negativi): $0, 1, 2, \ldots, m - 1$, in quanto il resto deve essere positivo o nullo e strettamente minore del divisore, cioè di m. Abbiamo allora:

Proposizione 1.11.2. *Tutti e soli gli elementi di $\mathbb{Z}_m$ sono le m classi* $[0], [1], \ldots, [m-1]$.

Dim.: Sia $a \in \mathbb{Z}$ e sia $a = mq + r$ con $0 \leq r < m$. proviamo che $[a] = [r]$; ciò equivale a provare che $a \equiv r \,(\mathrm{mod}\ m)$, per le proprietà delle classi di equivalenza. Avremo

$$\begin{array}{c} a = mq = r \Rightarrow a - r = mq \Rightarrow m|(a - r) \Rightarrow \\ \Rightarrow a \equiv r \,(\mathrm{mod}\ m) \Rightarrow a \in [r] \Rightarrow [a] = [r]. \end{array}$$

Ne segue l'asserto.

È allora lecito assumere come rappresentanti delle classi elementi di $\mathbb{Z}_m$ gli interi $0, 1, \ldots, m-1$. Si noti che $[0]$ contiene tutti e soli i multipli di m.

Tenendo presente che in $\mathbb{Z}$ sono definite, in base alla aritmetica elementare, due operazioni, addizione e moltiplicazione, vogliamo provare che in $\mathbb{Z}_m$ si possono definire, usando le operazioni $+$ e $\cdot$ definite in $\mathbb{Z}$, due operazioni, addizione e moltiplicazione, che godono di quasi tutte le proprietà di cui godono le stesse operazioni in $\mathbb{Z}$. Ciò non è vero in generale, ma dipende dal fatto che la relazione di equivalenza che abbiamo considerato in $\mathbb{Z}$ è una particolare relazione di equivalenza ed il nome di congruenza (modulo m) che ad essa è stato dato giustifica questa particolarità, come vedremo meglio nel seguito.

Siano dunque $[a]$,$[b] \in \mathbb{Z}_m$; definiamo la somma delle due classi nel modo seguente:

$$(+) \qquad [a] + [b] = [a + b] \qquad (\forall [a], [b] \in \mathbb{Z}_m)$$

Proviamo che la definizione è ben posta, cioè che non dipende dai rappresentanti delle classi. Ciò significa provare che

$$a' \equiv a \,(\mathrm{mod}\ m) \quad \text{e} \quad b' \equiv b \,(\mathrm{mod}\ m) \Rightarrow a' + b' \equiv a + b \,(\mathrm{mod}\ m).$$

Infatti: $a' \equiv a \,(\mathrm{mod}\ m)$ e $b' \equiv b \,(\mathrm{mod}\ m) \Rightarrow \exists x, y \in \mathbb{Z} : a' - a = mx$ e $b' - b = my \Rightarrow a' = mx + a$ e $b' = my + b \Rightarrow a' + b' = a + b + m(x + y) \Rightarrow (a' + b') - (a + b) = m(x + y) \Rightarrow (a' + b') \equiv (a + b) \,(\mathrm{mod}\ m)$, cioè l'asserto.

Ricordiamo ora che la somma negli interi gode delle seguenti proprietà:

1. $\forall a, b, c \in \mathbb{Z} \Rightarrow (a + b) + c = a + (b + c)$ (prop. associativa)
2. $\exists 0 \in \mathbb{Z} : \forall a \in \mathbb{Z},\ a + 0 = 0 + a = a$
3. $\forall a \in \mathbb{Z},\ \exists -a \in \mathbb{Z} : a + (-a) = (-a) + a = 0$
4. $\forall a, b \in \mathbb{Z} \Rightarrow a + b = b + a$ (prop. commutativa)

Proviamo che la somma definita in $\mathbb{Z}_m$ gode delle medesime proprietà. Avremo

$$\begin{aligned} &\forall [a], [b], [c] \in \mathbb{Z}_m, \\ &\quad ([a] + [b]) + [c] = [a + b] + [c] = [a + b + c] = \\ &\qquad\qquad = [a] + [b + c] = [a] + ([b] + [c]), \end{aligned}$$

onde vale la proprietà associativa. Consideriamo ora $[0] \in \mathbb{Z}_m$; si ha:

$$\forall [a] \in \mathbb{Z}_m, [a] + [0] = [a + 0] = [a] = [0 + a] = [0] + [a];$$

dunque $[0]$ è elemento neutro rispetto alla somma (cioè sommato a sinistra o a destra a qualunque elemento di $\mathbb{Z}_m$ lo riproduce). Proviamo ora che

per ogni classe, elemento di $\mathbb{Z}_m$, esiste l'opposta, che sommata ad essa da lo "zero" di $\mathbb{Z}_m$, cioè la classe $[0]$. Sia $[a] \in \mathbb{Z}_m$; possiamo sempre supporre che $a \in \{0, 1, \ldots, m-1\}$. Allora anche $m - a \in \{0, 1, \ldots, m-1\}$. Quindi

$$[a] + [m-a] = [a + m - a] = [a - a + m] = [0 + m] = [m] = [0]$$

Pertanto la classe $-[a] = [-a] = [m-a]$ è l'opposta della classe $[a]$. Infine, dato che la somma in $\mathbb{Z}$ è commutativa, si ha

$$\forall [a], [b] \in \mathbb{Z}_m,\ [a] + [b] = [a + b] = [b + a] = [b] + [a],$$

onde la somma è commutativa anche in $\mathbb{Z}_m$. Quindi si può dire, in termini non rigorosi, che la congruenza $\mod m$ su $\mathbb{Z}$ "trasferisce" l'operazione di somma definita in $\mathbb{Z}$, con le sue proprietà, all'insieme quoziente $\mathbb{Z}_m$.

Utilizzando il prodotto definito in $\mathbb{Z}$, si può, analogamente, definire un prodotto in $\mathbb{Z}_m$; però, come vedremo, non tutte le proprietà del primo si trasferiscono al secondo. Ricordiamo che il prodotto in $\mathbb{Z}$ gode delle seguenti proprietà:

1. $\forall a, b, c \in \mathbb{Z} \Rightarrow (ab)c = a(bc)$ (prop. associativa)
2. $\exists 1 \in \mathbb{Z}$, tale che $a \cdot 1 = 1 \cdot a = a$, $\forall a \in \mathbb{Z}$
3. $\forall a, b \in \mathbb{Z},\ ab = ba$ (prop. commutativa)
4. $\forall a, b \in \mathbb{Z}, ab = 0 \Rightarrow a = 0$ o $b = 0$, cioè vale la *legge di annullamento del prodotto*.

Definiamo allora un prodotto in $\mathbb{Z}_m$ nel modo seguente:

$$(\cdot) \qquad [a][b] = [ab] \qquad (\forall [a], [b] \in \mathbb{Z}_m)$$

proviamo innanzi tutto che la definizione è ben posta, cioè non dipende dai rappresentanti delle classi. Ciò significa provare che

$$a \equiv a' \,(\mathrm{mod}\ m)\,,\ b \equiv b' \,(\mathrm{mod}\ m) \Rightarrow ab \equiv a'b' \,(\mathrm{mod}\ m).$$

Si ha

$$\begin{aligned} a \equiv a' \,(\mathrm{mod}\ m)\,,\ b \equiv b' \,(\mathrm{mod}\ m) &\Rightarrow \exists x, y \in \mathbb{Z} : a' = a + mx,\ b' = b + my \Rightarrow \\ &\Rightarrow a'b' = (a + mx)(b + mx) \Rightarrow a'b' = ab + m(bx + ay + mxy) \Rightarrow \\ &\Rightarrow a'b' \equiv ab \,(\mathrm{mod}\ m), \end{aligned}$$

onde l'asserto.

Il prodotto definito in $\mathbb{Z}_m$ è associativo; infatti:

$$\begin{aligned} &\forall [a], [b], [c] \in \mathbb{Z}_m, \\ &\qquad [a]([b][c]) = [a] \cdot [bc] = [abc]; \quad ([a][b])[c] = [ab] \cdot [c] = [abc]. \end{aligned}$$

Esiste un elemento neutro rispetto al prodotto, cioè un elemento che moltiplicato a destra o a sinistra per qualunque elemento di $\mathbb{Z}_m$ riproduce quest'ultimo. Infatti, se consideriamo $[1] \in \mathbb{Z}_m$, avremo

$$\forall [a] \in \mathbb{Z}_m,\ [a] \cdot [1] = [a \cdot 1] = [a] = [1 \cdot a] = [1] \cdot [a].$$

Quindi $[1]$ è unità (elemento neutro rispetto al prodotto) di $\mathbb{Z}_m$. Però in $\mathbb{Z}_m$, in generale, non vale la legge di annullamento del prodotto; precisamente proviamo la

Proposizione 1.11.3. *Sse m è un numero primo, in $\mathbb{Z}_m$ vale la legge di annullamento del prodotto, cioè*

$$[a] \cdot [b] = [0] \Rightarrow [a] = [0] \quad \textit{oppure} \quad [b] = [0].$$

Dim.: Osserviamo innanzitutto che, per ogni $[x] \in \mathbb{Z}_m$, in base alla definizione di prodotto,

$$[0][x] = [0x] = [0],$$

cioè $[0]$ è annullatore del prodotto.

Supponiamo che m non sia un numero primo, e proviamo che allora esistono elementi non nulli di $\mathbb{Z}_m$ tali che il loro prodotto sia lo zero di $\mathbb{Z}_m$. Elementi siffatti prendono il nome di *divisori dello zero* (in $\mathbb{Z}_m$). Se m non è primo, m ammette una fattorizzazione non banale

$$m = st \quad \text{con} \quad 1 < s < m,\ 1 < t < m$$

Poiché abbiamo assunto come elementi di $\mathbb{Z}_m$ quelli rappresentati dalle classi $[0], [1], \ldots, [m-1]$, le classi $[s]$ e $[t]$ sono elementi di $\mathbb{Z}_m$ ($\neq 0$) e risulta

$$[s][t] = [m] = [0],$$

cioè esistono divisori dello zero. Inoltre tutti e soli i divisori dello zero di $|mathbbZ_m$ sono le calssi $[x]$, con $1 < x < m$ tale che $(m, x) \neq 1$ (dove (m, x) denota il massimo comun divisore di m ed x). Infatti, se $(m, x) = d \neq 1$, allora $d|x$, $d|m$, per cui

$$x = ad,\ m = bd,$$

onde esiste $[y]$ tale che $[x][y] = [0]$; basta assumere $y = b$, in quanto, allora

$$[x][y] = [ad][b] = [abd] = [a][bd] = [a][m] = [a][0] = [0].$$

Viceversa, sia $[x][y] = [0]$, $[x], [y] \neq [0]$ in $\mathbb{Z}_m$, m non primo; proviamo che $(m, x) \neq 1$ (e similmente $(m, y) \neq 1$). Si ha

$$[x][y] = [0] \Rightarrow [xy] = [m] \Rightarrow xy = km,\ k \in \mathbb{Z}.$$

Se $x|m$, l'affermazione è banalmente vera, perché $(m, x) = x$. Se $x \not| m$, sia $x = x_1 \cdot x_2 \cdots x_n$ la decomposizione in fattori primi di x; sarà

$$x_1 \cdot x_2 \cdots x_n \cdot y = mk$$

e quindi deve esistere qualche x_j che divide m (dato che x_j è primo, e dividendo il primo membro divide il secondo, e dato che non tutti gli x_j possono essere fattori di k perché ciò implicherebbe $y = mh \Rightarrow [y] = [mh] = [m] = [0]$, contro l'ipotesi).

Infine, proviamo che se m è un numero primo, che denotiamo con p, in $\mathbb{Z}_p$ non esistono divisori dello zero. Gli elementi di $\mathbb{Z}_p$ sono $[0], [1], \ldots, [p-1]$; fissati comunque $[x]$ ed $[y]$ tra di essi (e $\neq 0$), si ha

$$[x][y] = [xy] \neq [p];$$

infatti, se così non fosse, sarebbe

$$xy \equiv 0 \mod p \Rightarrow p|xy,$$

onde, essendo p primo, o $p|x$ oppure $p|y$, contro l'ipotesi $[x], [y] \neq [0]$. la proposizione è così completamente provata.

Altre considerazioni relative agli insiemi $\mathbb{Z}_m$, in particolare $\mathbb{Z}_p$, considerati assieme alle operazioni $+$ e/o $\cdot$ saranno svolte nel seguito.

Esercizi

Esercizio 1.11.1. *Si provi che la congruenza* $\mod 1$ *su* $\mathbb{Z}$ *è la relazione totale su* $\mathbb{Z}$.

Sol.: In base alla definizione di congruenza $\mod m$ su $\mathbb{Z}$,

$$a \equiv b \,(\mod m) \Leftrightarrow m|(a-b).$$

Ora $\forall z \in \mathbb{Z}$, $1|z$. Ne segue che la relazione risulta la relazione totale (quindi di equivalenza) e $\mathbb{Z}_1$ contiene un solo elemento. Ciò giustifica l'ipotesi $m \geq 2$.

1.12 Famiglie di insiemi. Unione ed intersezione di una famiglia di insiemi. Ricoprimenti e partizioni.

Introduciamo la nozione di famiglia di insiemi dipendente da un insieme di indici. Sia $\mathcal{A}$ un insieme di insiemi (cioè ogni elemento di $\mathcal{A}$ è un insieme) e sia I un insieme qualsivoglia, che chiameremo *insieme degli indici* e supporremo $\neq \emptyset$. Diremo che un sottoinsieme $\mathcal{F}$ del prodotto cartesiano $\mathcal{A} \times I$ ($\mathcal{F} \subseteq \mathcal{A} \times I$) è una *famiglia di insiemi* dipendente dall'insieme I di indici (si dice anche famiglia indiciata di insiemi), se sono soddisfatte le condizioni seguenti:

1. $\forall i \in I \Rightarrow \exists (A, i) \in \mathcal{F}$
2. $(A, i), (A, j) \in \mathcal{F} \Rightarrow i = j$
3. $(A, i), (B, i) \in \mathcal{F} \Rightarrow A = B$.

(Si noti che, generalizzando la definizione di famiglia di insiemi, spesso si sopprimono l'una o l'altra o entrambe le condizioni 2) e 3); comunque, per la nostra trattazione, preferiamo mantenere queste condizioni; inoltre non è necessario supporre $I \neq \emptyset$).

Per semplicità di scrittura, se $(A, i) \in \mathcal{F}$, scriveremo A_i in luogo di (A, i). Inoltre, denoteremo la famiglia $\mathcal{F}$ anche con

$$\mathcal{F} = (A_i \,:\, i \in I).$$

(Nella letteratura si trova spesso denotata $\mathcal{F}$ con $\{A_i\}_{i \in I}$). Diamo ora alcuni esempi di famiglie di insiemi.

1. Sia $I = \{1, 2, \ldots, 7\}$, allora $\mathcal{F} = (A_1, A_2, \ldots, A_7) = (A_i \,:\, i \in I)$ è una famiglia di insiemi.
2. Sia $\mathcal{A}$ l'insieme dei cerchi del piano; la totalità dei cerchi aventi raggio razionale costituisce una famiglia di insiemi $\mathcal{F}$, che possiamo scrivere

   $$\begin{aligned} \mathcal{F} &= (A \in \mathcal{A} \,:\, \text{raggio di } A \text{ sia razionale}) = \\ &= (A \in \mathcal{A} \,:\, \text{raggio } i \text{ di } A \text{ sia elemento di } \mathbb{Q}) = \\ &= (A_i \,:\, i \in \mathbb{Q}) = (A_i \,:\, i \in I) \end{aligned}$$

   (avendo posto $I = \mathbb{Q}$ ed avendo denotato con A il cerchio di $\mathcal{A}$ avente raggio i).
3. Si fissi un riferimento cartesiano ortogonale monometrico Oxy nel piano e si consideri l'intervallo $[0, 1]$ dell'asse reale x. Assunto $I = [0, 1]$, per ogni numero reale $i \in I$, si consideri il segmento A_i della parallela all'asse y, passante per il punto $(i, 0)$ dell'asse x, avente lunghezza $3i$. Si ottiene una famiglia $(A_i \,:\, i \in I)$ di segmenti.

Definiamo ora l'insieme unione e l'insieme intersezione degli insiemi di una famiglia.

Sia $(A_i \,:\, i \in I)$ una famiglia di insiemi; diciamo *unione della famiglia* l'insieme

$$A = \bigcup (A_i \,:\, i \in I) = \{x \,:\, [\exists i \in I \,:\, x \in A_i]\}$$

(cioè A è l'insieme di tutti gli elementi che appartengono ad almeno un insieme della famiglia). Talvolta si scrive anche

$$\bigcup (A_i \,:\, i \in I) = \bigcup_{i \in I} A_i.$$

Analogamente, data la famiglia di insiemi $(A_i \,:\, i \in I)$, definiamo *intersezione della famiglia* l'insieme

$$A = \bigcap (A_i \,:\, i \in I) = \{x \,:\, [\forall i \in I \Rightarrow x \in A_i]\};$$

quindi l'intersezione è l'insieme di tutti gli elementi che appartengono contemporaneamente a tutti gli insiemi della famiglia. Talvolta si scrive anche $\bigcap_{i \in I} A_i$ in luogo di $\bigcap (A_i \,:\, i \in I)$.

Si può provare che per l'unione e l'intersezione di una famiglia di insiemi valgono ancora le leggi associative. Si definisce poi il complementare di un insieme M, al modo solito, e valgono le leggi di De Morgan:

$$\mathcal{C}_M(\bigcup (A_i \,:\, i \in I)) = \bigcap (\mathcal{C}_M A_i \,:\, i \in I)$$

e l'analoga, ottenuta scambiando il ruolo di $\cup$ e $\cap$.

Infine, per generalizzare le leggi distributive (dell'intersezione rispetto all'unione e dell'unione rispetto all'intersezione), consideriamo due famiglie di insiemi $(A_i \,:\, i \in I)$ e $(B_j \,:\, j \in J)$; avremo

$$\left(\bigcap_{i \in I} A_i\right) \cup \left(\bigcap_{j \in J} B_j\right) = \bigcap_{(i,j) \in I \times J} (A_i \cup B_j);$$

$$\left(\bigcup_{i \in I} A_i\right) \cap \left(\bigcup_{j \in J} B_j\right) = \bigcup_{(i,j) \in I \times J} (A_i \cap B_j)$$

(avendo usato, per comodità di scrittura, l'altra notazione). Se S è un qualunque insieme, queste leggi distributive si particolarizzano in

$$S \cup \left(\bigcap_{j \in J} B_j\right) = \bigcap_{j \in J} (S \cup B_j);$$

$$S \cap \left(\bigcup_{j \in J} B_j\right) = \bigcup_{j \in J} (S \cap B_j).$$

In base alla definizione, si prova poi facilmente che , per quanto riguarda la differenza, se S è un insieme qualsiasi valgono le seguenti leggi distributive:

$$\left(\bigcup_{i\in I} A_i\right) \setminus S = \bigcup_{i\in I}(A_i \setminus S); \left(\bigcap_{i\in I} A_i\right) \setminus S \qquad = \bigcap_{i\in I}(A_i \setminus S).$$

Non definiamo qui il prodotto cartesiano di una famiglia di insiemi, in quanto, per tale definizione, è necessaria la nozione di applicazione, che daremo nel seguito; vedremo anche, in quella sede, che la definizione di famiglia di insiemi si può interpretare in altro modo.

Introduciamo ora le due nozioni di ricoprimento e partizione di un insieme. Sia A un insieme qualsivoglia, e sia $(A_i : i \in I)$ una famiglia di insiemi. Diremo che $(A_i : i \in I)$ è un *ricoprimento* di A, se

$$A \subseteq \bigcup(A_i : i \in I).$$

Ne segue, tenendo presente la definizione di unione, che

$$\forall a \in A \Rightarrow \exists i \in I : a \in A_i.$$

Evidentemente, se $A = \emptyset$, ogni famiglia di insiemi è un ricoprimento di A. Se interpretiamo $P(A)$ come famiglia di insiemi (di fatto è la famiglia di tutti e soli i sottoinsiemi di A), abbiamo un esempio di ricoprimento di A in cui, addirittura

$$A = \bigcup P(A) = \bigcup(B : B \subseteq A).$$

Qualora si particolarizzi la nozione di ricoprimento, si ottiene la nozione di partizione. Precisamente:

Una famiglia $(A_i : i \in I)$ di insiemi è una *partizione* dell'insieme A sse sono soddisfatte le due condizioni:

1. $A = \bigcup(A_i : i \in I)$;
2. $\forall i, j \in I,\ A_i \cap A_j \neq \emptyset \Rightarrow A_i = A_j$.

Osserviamo subito che, ferma restando la condizione 1), la condizione 2) è equivalente alla condizione

2'. $\forall a \in A \Rightarrow \exists!\, i \in I : a \in A_i$.

Infatti, dalla 1) segue che

$$\forall a \in A \Rightarrow \exists i \in I : a \in A_i;$$

per la 2), $a \in A_i$ e $A \in A_j \Rightarrow a \in A_i \cup A_j \Rightarrow A_i = A_j$, onde l'unicità. Viceversa, 2')⇒ 2), in quanto

$$\forall a \in A \Rightarrow \exists! i \in I : a \in A_i \Rightarrow [a \in A_i \quad \text{e} \quad a \in A_j \Rightarrow i = j \Rightarrow A_i = A_j],$$

per definizione di famiglia di insiemi.

Un esempio di partizione banale si ottiene assumendo $I = \{1\}$, $A_1 = A$. Un altro esempio di partizione di A è formato dalla famiglia di tutti i s.i. di A che contengono un solo elemento:

$$\mathcal{F} = (\{a\} \,:\, a \in A).$$

Osserviamo che una partizione di A è sempre un s.i. di $P(A)$ (si tenga presente che una partizione è una famiglia di insiemi, ed è un insieme di insiemi), mentre ciò non è necessariamente vero per il ricoprimento; inoltre, se $(A_i \,:\, i \in I)$ è una partizione di A, è sempre

$$(A_i \,:\, i \in I) \subset P(A)$$

e l'inclusione è in senso stretto.

Proviamo ora la seguente:

Proposizione 1.12.1. *Sia $A \neq \emptyset$ (per evitare casi banali) un insieme qualsiasi e sia $\mathcal{P} = (A_i \,:\, i \in I)$ una partizione di A; allora $\mathcal{P}$ definisce univocamente un'equivalenza $\mathcal{E}_\mathcal{P}$ su A quando si ponga*

$$\forall x, y \in A,\ (x, y) \in \mathcal{E}_\mathcal{P} \Leftrightarrow \exists i \in I \,:\, x, y \in A_i.$$

Viceversa, se $\mathcal{E}$ è una qualunque equivalenza su A ($\neq \emptyset$), $\mathcal{E}$ definisce univocamente una partizione $\mathcal{P}_\mathcal{E}$ di A quando si ponga

$$\mathcal{P}_\mathcal{E} = ([a]\mathcal{E} \,:\, a \in A).$$

Inoltre,

$$\mathcal{E}_{\mathcal{P}_\mathcal{E}} = \mathcal{E} \quad e \quad \mathcal{P}_{\mathcal{E}_\mathcal{P}} = \mathcal{P}.$$

Dim.: Proviamo che $\mathcal{E}_\mathcal{P}$, che è manifestamente una relazione su A, è una equivalenza. $\mathcal{E}_\mathcal{P}$ è riflessiva; infatti, tenendo presente la definizione di partizione e di $\mathcal{E}_\mathcal{P}$, si ha:

$$\forall x \in A \Rightarrow \exists i \in I \,:\, x \in A_i \Rightarrow x, x \in A_i \Rightarrow (x, x) \in \mathcal{E}_\mathcal{P}.$$

$\mathcal{E}_\mathcal{P}$ è simmetrica; infatti

$$(x, y) \in \mathcal{E}_\mathcal{P} \Rightarrow \exists i \in I \,:\, x, y \in A_i \Rightarrow \exists i \in I \,:\, y, x \in A_i \Rightarrow (y, x) \in \mathcal{E}_\mathcal{P}.$$

$\mathcal{E}_\mathcal{P}$ è transitiva; infatti

$$\begin{aligned}(x, y),\ (y, z) \in \mathcal{E}_\mathcal{P} \Rightarrow \exists i \in I \,:\, x, y \in A_i \quad \text{ed} \quad \exists j \in I \,:\, y, z \in A_j \Rightarrow \\ \Rightarrow y \in A_i \quad \text{e} \quad y \in A_j \Rightarrow y \in A_i \cap A_j \Rightarrow \\ \Rightarrow A_i = A_j \Rightarrow z \in A_i \Rightarrow x, z \in A_i \Rightarrow (x, z) \in \mathcal{E}_\mathcal{P}.\end{aligned}$$

Proviamo ora che $\mathcal{P}_\mathcal{E}$ è una partizione. Per definizione di equivalenza, ogni elemento di A è contenuto in una classe (quella da esso individuata), quindi

$$\bigcup([a]\mathcal{E} \,:\, a \in A) = A,$$

cioè è soddisfatta la prima condizione di partizione. (Si noti che in questa scrittura non si intende assumere A come insieme di indici, poiché si contraddirebbe la definizione di famiglia precedentemente data, in quanto - in generale - una classe di equivalenza non contiene un solo elemento).

D'altra parte, abbiamo provato che, per le classi di equivalenza risulta

$$[a]\mathcal{E} \cap [b]\mathcal{E} \neq \emptyset \Rightarrow [a]\mathcal{E} = [b]\mathcal{E};$$

pertanto è soddisfatta la seconda condizione e $\mathcal{P}_\mathcal{E}$ è effettivamente una partizione.

Infine, l'ultima affermazione è conseguenza di quanto dimostrato, onde l'asserto. Si può pertanto dire che le nozioni di partizione e di equivalenza "coincidono", nel senso che ciascuna determina l'altra.

Esercizi

Esercizio 1.12.1. *Sia I l'insieme dei numeri naturali primi. Si consideri la famiglia $(A_i \,:\, i \in I)$ definita da:*

$$A_i = \{x \in \mathbb{N} \,:\, x \text{ è multiplo di } i\}.$$

Si determini $\bigcup(A_i \,:\, i \in I)$.

Sol. Poiché ciascun numero naturale $\neq 1$ o è primo, oppure ammette almeno un numero primo come divisore, si ha

$$\bigcup(A_i \,:\, i \in I) = \mathbb{N} \setminus \{1\}$$

(in $\mathbb{N}$ essendo escluso lo zero).

Se poi si considera anche 1 come numero primo (in quanto ammette come divisore soltanto se stesso e l'unità), si ha

$$\bigcup(A_i \,:\, i \in I) = \mathbb{N}.$$

Esercizio 1.12.2. *Siano $(A_i \,:\, i \in I)$ e $(B_j \,:\, j \in J)$ due famiglie di insiemi ($I \times J \neq \emptyset$). Si provi che*

$$\Big(\bigcup_{i\in I} A_i\Big) \cap \Big(\bigcup_{j\in J} B_j\Big) = \bigcup_{(i,j)\in I\times J} (A_i \cap B_j),$$

$$\Big(\bigcap_{i\in I} A_i\Big) \cup \Big(\bigcap_{j\in J} B_j\Big) = \bigcap_{(i,j)\in I\times J} (A_i \cup B_j).$$

Dim. Proviamo la prima eguaglianza. Si ha

$$x \in \Big(\bigcup_{i\in I} A_i\Big) \cap \Big(\bigcup_{j\in J} B_j\Big) \Rightarrow \exists i \in I,\ \exists j \in J \,:\, x \in A_i \quad \text{e} \quad x \in B_j \Rightarrow$$

$$\Rightarrow x \in A_i \cap B_j \Rightarrow x \in \bigcup_{(i,j)\in I\times J} (A_i \cap B_j).$$

Viceversa,

$$x \in \bigcup_{(i,j)\in I\times J} (A_i \cap B_j) \Rightarrow$$

$$\Rightarrow \exists (i,j) \in I \times J \,:\, x \in A_i \cap B_j \Rightarrow x \in A_i \quad \text{e} \quad x \in B_j \Rightarrow$$

$$\Rightarrow x \in \bigcup_{i\in I} A_i \quad \text{e} \quad x \in \bigcup_{j\in J} B_j \Rightarrow x \in \Big(\bigcup_{i\in I} A_i\Big) \cap \Big(\bigcup_{j\in J} B_j\Big).$$

Proviamo ora la seconda eguaglianza:

$$x \in \Big(\bigcap_{i\in I} A_i\Big) \cup \Big(\bigcap_{j\in J} B_j\Big) \Rightarrow x \in \bigcap_{i\in I} A_i \quad \text{o} \quad x \in \bigcap_{j\in J} B_j \Rightarrow$$

$$\Rightarrow \forall i \in I, \quad x \in A_i \quad \text{o} \quad \forall j \in J, \quad x \in B_j \Rightarrow$$

$$\Rightarrow \forall i \in I, \quad x \in A_i \cup B_j \quad \text{o} \quad \forall j \in J, \quad x \in A_i \cup B_j \Rightarrow$$

$$\Rightarrow x \in \bigcap_{(i,j)\in I\times J} (A_i \cup B_j).$$

Viceversa,

$$x \in \bigcap_{(i,j)\in I\times J} (A_i \cup B_j) \Rightarrow \forall (i,j) \in I \times J, \quad x \in A_i \cup B_j \Rightarrow$$

$$\Rightarrow \forall i \in I, \quad x \in A_i \quad \text{o} \quad \forall j \in J, \quad x \in B_j \Rightarrow$$

$$\Rightarrow x \in \bigcap_{i\in I} A_i \quad \text{o} \quad x \in \bigcap_{j\in J} B_j \Rightarrow x \in \Big(\bigcap_{i\in I} A_i\Big) \cup \Big(\bigcap_{j\in J} B_j\Big).$$

Esercizio 1.12.3. *Si provi che, se* $(A_i \ : \ i \in I)$ *è una qualunque famiglia di insiemi, qualunque sia l'insieme* B*, risulta*

$$B \cap \Big(\bigcup_{i\in I} A_i\Big) = \bigcup_{i\in I} (B \cap A_i) \quad e \quad B \cup \Big(\bigcap_{i\in I} A_i\Big) = \bigcap_{i\in I} (B \cup A_i).$$

Dim. Sia $x \in B \cap \Big(\bigcup_{i\in I} A_i\Big)$; allora $x \in B$ e $x \in \bigcup_{i\in I} A_i$; pertanto, per qualche $i \in I$, $x \in A_i$ e quindi $x \in B \cap A_i$, onde $x \in \bigcup_{i\in I} (B \cap A_i)$. Viceversa, se $x \in \bigcup_{i\in I} (B \cap A_i)$, per qualche $i \in I$, $x \in B \cap A_i$, cioè $x \in B$ e $x \in A_i$, quindi $x \in B$ e $x \in \bigcup_{i\in I} A_i$, da cui $x \in B \cap \Big(\bigcup_{i\in I} A_i\Big)$.

Proviamo ora la seconda eguaglianza. Sia $x \in B \cup \Big(\bigcap_{i\in I} A_i\Big)$; allora $x \in B$ o $x \in \bigcap_{i\in I} A_i$. Se $x \in B$, sicuramente $\forall i \in I$, $x \in B \cup A_i$, onde $x \in \bigcap_{i\in I} (B \cup A_i)$; se, invece, $x \in \bigcap_{i\in I} A_i$, allora $\forall i \in I$, $x \in A_i$, quindi $\forall i \in I$, $x \in (B \cup A_i)$; ne segue che $x \in \bigcap_{i\in I} (B \cup A_i)$. Viceversa, se $x \in \bigcap_{i\in I} (B \cup A_i)$, allora $\forall i \in I$, $x \in B \cup A_i \Rightarrow x \in B$ o $x \in A_i$; nel primo caso, $x \in B \Rightarrow x \in B \cup \Big(\bigcap_{i\in I} A_i\Big)$, nel secondo $x \in A_i$, $\forall i \in I \Rightarrow x \in \bigcap_{i\in I} A_i \Rightarrow x \in B \cup \Big(\bigcap_{i\in I} A_i\Big)$.

Esercizio 1.12.4. *Sia* $\mathbb{R}$ *l'insieme dei numeri reali e sia* $\mathbb{Q}$ *l'insieme dei numeri razionali. Si consideri la famiglia di insiemi* $(A_i \ : \ i \in \mathbb{Q})$*, definita da*

$$A_i = \{x \in \mathbb{R} \ : \ x \geq i\}.$$

Si dimostri che $\bigcup_{i\in\mathbb{Q}} A_i = \mathbb{R}$ *e* $\bigcap_{i\in\mathbb{Q}} A_i = \emptyset$.

Dim. Osserviamo innanzitutto che gli A_i non sono a due a due disgiunti, ma sono tali che, se $i > j$, allora $A_i \subset A_j$ (si considera l'ordinamento naturale degli indici razionali, da $-\infty$ a $+\infty$).
Quindi, ciascuno degli A_i è contenuto nel precedente. Poiché:

$$\forall x \in \mathbb{R} \quad \Rightarrow \quad [\exists i \in \mathbb{Q} \,:\, i \leq x] \quad \Rightarrow \quad x \in A_i \,,$$

si ha che $\mathbb{R} \subseteq \bigcup_{i \in \mathbb{Q}} A_i$. Viceversa:

$$\forall x \in \bigcup_{i \in \mathbb{Q}} A_i \quad \Rightarrow \quad x \in \mathbb{R} \quad \Rightarrow \quad \bigcup_{i \in \mathbb{Q}} A_i \subseteq \mathbb{R} \,.$$

Ne segue che $\bigcup_{i \in \mathbb{Q}} A_i = \mathbb{R}$.

Dal fatto che le inclusioni tra gli insiemi della famiglia sono tutte in senso stretto, segue poi che $\bigcap_{i \in \mathbb{Q}} A_i = \emptyset$.

Si noti che la famiglia $(A_i \,:\, i \in \mathbb{Q})$ costituisce un ricoprimento (non una partizione) dell'insieme $\mathbb{R}$.

Esercizio 1.12.5. *Si consideri la semiretta reale positiva e la famiglia di intervalli aperti* $(T_n = (0, 1/n), : n \in \mathbb{N},\ n > 0)$. *Dimostrare che*

$$\forall s, t \in \mathbb{N} \quad \Rightarrow \quad T_s \cup T_t = T_m \,, \quad m = \textit{ minore tra s e t.}$$

Dimostrare, inoltre, che, comunque si fissi il s.i. $A \subseteq \mathbb{N}$, *risulta*

$$\bigcup_{i \in A} T_i = T_a \,, \quad a \quad : \quad \forall l \in A,\ a \leq l \,.$$

Provare infine che $T_s \cap T_t = T_M$ *, dove* M *è il maggiore tra* s *e* t.

Dim. Osserviamo innanzitutto che se $i > j$, allora $1/i < 1/j$ e quindi $T_i \subset T_j$. Pertanto, $T_s \cup T_t = T_m$, dove m è il minore tra s e t. Se A è un sottoinsieme di $\mathbb{N}$, esso contiene un naturale a, che è il minore di tutti quelli appartenenti ad A. La precedente relazione di inclusione comporta allora che $T_a \subset T_i$, $\forall i \in A, i > a$.
Ne segue che $\bigcup_{i \in A} T_i = T_a$.

Come conseguenza della proprietà $A \subseteq B \Rightarrow A \cup B = B$ (essendo A e B insiemi qualsiasi), e dall'osservazione precedente, avremo poi $T_s \cap T_t = T_M$, dove M è il maggiore tra s e t.

Esercizio 1.12.6. *Determinare tutte le partizioni di un insieme* S *costituito da tre elementi.*

Sol. Sia $S = \{a, b, c\}$. Si devono costruire tutte le famiglie di sottoinsiemi di S verificanti le due condizioni che definiscono una partizione.

La *partizione banale* è costituita dalla famiglia contenente, come unico insieme, S stesso.

Abbiamo poi la famiglia, contenente tre insiemi, in cui ciascun insieme contiene un solo elemento di S; infine, abbiamo le tre famiglie, ciascuna costituita da due insiemi, uno dei quali contiene due elementi di S e l'altro uno: per esempio $\{\{a\}, \{b, c\}\}$.

Si noti che, alla totalità degli insiemi di ciascuna delle cinque famiglie suddette, si può aggiungere l'insieme vuoto.

Esercizio 1.12.7. *Trovare tutte le partizioni dell'insieme* $S = \{a, b, c, d\}$.

Sol. Avremo la partizione banale, in cui l'unico insieme della famiglia si riduce ad S stesso; la partizione costituita dalla famiglia composta di quattro insiemi, ognuno dei quali contiene un solo elemento di S; tre partizioni individuate ciascuna da una famiglia contenente due insiemi, ognuno dei quali contiene due elementi di S; per esempio $\{\{a, b\},\ \{c, d\}\}$; quattro partizioni, ciascuna determinata da una famiglia composta di due insiemi, contenenti rispettivamente un elemento e tre elementi di S: per esempio $\{\{a\},\ \{b, c, d\}\}$; infine sei partizioni definite dalle sei famiglie, ciascuna composta da tre insiemi, due dei quali contengono un solo elemento di S ed il terzo ne contiene due: per esempio $\{\{a\},\ \{b\},\ \{c, d\}\}$.

Le partizioni possibili sono quindi in numero di quindici.

Esercizio 1.12.8. *Dare un esempio di partizione dell'insieme* $\mathbb{N}$ *dei numeri naturali.*

Sol. Una partizione non banale di $\mathbb{N}$ è manifestamente quella costituita dai due insiemi $\mathbb{P}$ e $\mathbb{D}$, rispettivamente dei numeri pari e dei numeri dispari, ossia:

$$\mathbb{P} = \{n \in \mathbb{N} \quad : \quad n = 2k,\ k \in \mathbb{N}\}$$

e

$$\mathbb{D} = \{n \in \mathbb{N} \quad : \quad n = 2k + 1,\ k \in \mathbb{N}\}\ .$$

Esercizio 1.12.9. *Si provi che, per ogni insieme* A*, si ha*

$$A = \bigcup (x\ : x \in P(A)\}$$

cioè $A = \bigcup P(A)$*, mentre* $A \subset P(\bigcup A)$*.*

Dim. Per definizione di $P(A)$, $x \in P(A) \Rightarrow x \subseteq A$, onde è vera la prima affermazione. La seconda affermazione segue dal fatto che

$$\bigcup A = \{a\ :\ a \in A\}$$

onde A è s.i. proprio di $P(A)$.

Esercizio 1.12.10. *Sia* $(T_i\ i \in I,\ I = \mathbb{Z})$ *la famiglia di intervalli*

$$T_i = \{x \in \mathbb{R} \ : \ i \leq x < i + 1\}$$

della retta reale S *(rappresentativa dell'insieme* $\mathbb{R}$ *dei numeri reali). Si dica se* $(T_i \ : \ i \in I)$ *costituisce una partizione* $\mathcal{P}$ *di* S *e, in caso affermativo, si determini la relazione di equivalenza ad essa associata* $(\mathcal{E}_{\mathcal{P}})$.

Sol. Evidentemente $\bigcup(T_i \ : \ i \in I) = S$; inoltre $T_i \cap T_j = \emptyset$, se $i \neq j$. Infatti, se $j = i + 1$, i due intervalli sono consecutivi, ma privi di elementi in comune; se $j \neq i$, $j \neq i + 1$, i due intervalli sono "*separati*". Quindi, $(T_i \ : \ i \in I)$ è una partizione di S.

Ne segue che i T_i costituiscono le classi di equivalenza di $\mathcal{E}_{\mathcal{P}}$ e risulta

$$\forall x, y \in \mathbb{R}, \quad (x, y) \in \mathcal{E}_{\mathcal{P}} \quad \Longleftrightarrow \quad \exists i \in I \ : \ x, y \in T_i$$

(allora, scrivendo x ed y come allineamento decimale, x ed y hanno la stessa parte intera sse $(x, y) \in \mathcal{E}_{\mathcal{P}}$).

1.13 Corrispondenze tra insiemi.

Generalizziamo ora la nozione di relazione su un insieme A.

Siano A, B due insiemi qualsiasi non vuoti. Diremo corrispondenza da A verso B, oppure tra A e B, ogni s.i. F del prodotto cartesiano $A \times B$, cioè $F \subseteq A \times B$.

Evidentemente, una corrispondenza di A verso A è una relazione su A.

Notiamo che taluni definiscono corrispondenza "tra A e B" un s.i. di $(A \times B) \cup (B \times A)$, e corrispondenza di "$A$ con B" un s.i. di $A \times B$; per tale motivo è forse preferibile la locuzione di corrispondenza di "A verso B".

Se $F \subseteq A \times B$ è una corrispondenza da A verso B, definiamo *corrispondenza inversa* di F, e la denotiamo F^{-1}, la corrispondenza da B verso A, $F^{-1} \subseteq B \times A$, data da

$$F^{-1} = \{(b, a) \ : \ (a, b) \in F\}.$$

Sia ora $F \subseteq A \times B$ una corrispondenza; definiamo *dominio di* F e lo denotiamo con $D(F)$ il seguente s.i. di A:

$$D(F) = \{a \in A \ : \ [\exists b \in B \ : \ (a, b) \in F]\}.$$

Analogamente, definiamo *immagine di* F e la denotiamo con $Im(F)$ il seguente s.i. di B:

$$Im(F) = \{b \in B \ : \ [\exists a \in A \ : \ (a, b) \in F]\}.$$

(Se F è una corrispondenza da A verso B, B prende talvolta il nome di *codominio di* F).

Passando alla corrispondenza inversa, segue immediatamente dalle definizioni di dominio e di immagine, che

$$D(F^{-1}) = Im(F); \quad Im(F^{-1}) = D(F).$$

Qualora $F = \emptyset$, la corrispondenza prende il nome di *corrispondenza vuota* e, se $F = A \times B$, la corrispondenza è la *corrispondenza totale*.

Sia ora $a \in A$; data $F \subseteq A \times B$, definiamo *immagine di* a *mediante* F, e la denotiamo con $F(a)$, il seguente s.i. di B:

$$F(a) = \{b \in B \ : \ (a, b) \in F\}.$$

Evidentemente $F(a) \subseteq Im(F)$ ed inoltre

$$F(a) = \emptyset \quad \iff \quad a \notin D(F).$$

Analogamente, se $b \in B$ ed $F \subseteq A \times B$, definiamo *controimmagine* o *immagine inversa* (si tratta infatti dell'immagine nella corrispondenza inversa) *di* b *mediante* F, e la denotiamo con $F^{-1}(b)$, il seguente s.i. di A

$$F^{-1}(b) = \{a \in A \ : \ (a, b) \in F\} = \{a \in A \ : \ (b, a) \in F^{-1}\}.$$

Ovviamente, $F^{-1}(b) \subseteq Im(F^{-1}) = D(F)$ e

$$F^{-1}(b) = \emptyset \quad \Longleftrightarrow \quad b \notin D(F^{-1}) = Im(F).$$

Analogamente a quanto è stato fatto per le relazioni, se $F, G \subseteq A \times B$, si possono definire la corrispondenza unione

$$F \cup G \subseteq A \times B, \quad F \cup G = \{(a,b) \in A \times B \ : \ (a,b) \in F \quad \text{o} \quad (a,b) \in G\}$$

e la corrispondenza intersezione

$$F \cap G \subseteq A \times B, \quad F \cap G = \{(a,b) \in A \times B \ : \ (a,b) \in F \quad \text{e} \quad (a,b) \in G\}.$$

Definiamo ora il prodotto di due corrispondenze.
Siano $F \subseteq A \times B$ e $G \subseteq C \times D$ due corrispondenze qualsivoglia. Diremo *prodotto* di F per G, nell'ordine, e lo denoteremo con $G \circ F$, la corrispondenza di A verso D, definita da:

$$G \circ F = \{(a,d) \ : \ (a,b) \in F, \ (c,d) \in G, \ b = c\}.$$

Evidentemente se $B \cap C = \emptyset$, allora $G \circ F = \emptyset$.
Si prova poi subito che

$$(G \circ F)^{-1} = F^{-1} \circ G^{-1}.$$

Dato che le relazioni su di un insieme sono corrispondenze dell'insieme con se stesso, si possono comporre relazioni con corrispondenze.

Ad esempio, se R è una relazione su A, ($R \subseteq A \times A$), F è una relazione da A verso B ($F \subseteq A \times B$) ed S è una relazione su B, ha significato la corrispondenza da A verso B data da $S \circ F \circ R$, ed è evidente come si possano generalizzare prodotti di questo tipo.

In particolare, se Δ_A è la relazione identica su A, per ogni $F \subseteq A \times B$, si ha

$$F \circ \Delta_A = F \ ;$$

similmente, se Δ_B è la relazione identica su B, per ogni $F \subseteq A \times B$, risulta

$$\Delta_B \circ F = F \ .$$

Data la definizione di prodotto di due corrispondenze, ha evidentemente significato considerare anche i prodotti

$$F^{-1} \circ F \subseteq A \times A \quad \text{ed} \quad F \circ F^{-1} \subseteq B \times B \ ,$$

che sono, rispettivamente, una relazione su A ed una relazione su B.

Mediante tali prodotti si possono caratterizzare alcune corrispondenze da A verso B. Precisamente, diremo che la corrispondenza $F \subseteq A \times B$ è *univoca a sinistra* sse $F^{-1} \circ F \subseteq \Delta_A$.

Analogamente, diremo che $F \subseteq A \times B$ è *univoca a destra* sse $F \circ F^{-1} \subseteq \Delta_B$.

(L'uso degli aggettivi sinistro e destro deriva dal fatto che l'insieme A è a sinistra del simbolo $\times$ di prodotto cartesiano, mentre B è a destra del medesimo simbolo).

Illustriamo il significato delle due definizioni ora date.

La corrispondenza $F \subseteq A \times B$ è univoca a sinistra sse

$$\forall a, a' \in A,\ \forall b \in B, \quad (a,b) \in F \text{ e } (a',b) \in F \quad \Rightarrow \quad a = a' ;$$

cioè, elementi distinti di A non possono avere la medesima immagine in B.
Proviamo che, in questa ipotesi, $F^{-1} \circ F \subseteq \Delta_A$.
Sia $(a,b) \in F$, allora $(b,a) \in F^{-1}$, per definizione di corrispondenza inversa; quindi $(a,a) \in F^{-1} \circ F$. D'altra parte, se $(a,b) \in F$ e $(b,a') \in F^{-1}$, per ipotesi $a' = a$, onde $F^{-1} \circ F \subseteq \Delta_A$.

Viceversa, se $F^{-1} \circ F \subseteq \Delta_A$, non possono esistere coppie del tipo (a,b) ed $(a',b) \in F$ con $a' \neq a$, poiché, se così fosse, al prodotto $F^{-1} \circ F$ apparterrebbero le coppie (a,a') ed (a',a) che non appartengono a Δ_A.

Analogamente, $F \subseteq A \times B$ è univoca a destra sse

$$\forall a \in A,\ \forall b, b' \in B, \quad (a,b) \in F \text{ e } (a,b') \in F \quad \Rightarrow \quad b = b' ;$$

cioè, uno stesso elemento non può avere più di un corrispondente.
ne segue che $F \circ F^{-1} \subseteq \Delta_B$, e viceversa (si dimostra come l'unicità a sinistra).

Si noti che se $F \subseteq A \times B$ è univoca a sinistra (destra), la sua inversa è univoca a destra (sinistra).

Per le corrispondenze valgono proprietà analoghe a quelle già dimostrate per le relazioni, e che si provano nello stesso modo. Pertanto, tali proprietà saranno semplicemente elencate.

Proposizione 1.13.1. *Il prodotto tra corrispondenze è associativo; cioè, se $F \subseteq A \times B$, $G \subseteq C \times D$, $H \subseteq L \times M$, allora*

$$(H \circ G) \circ F = H \circ (G \circ F) .$$

Proposizione 1.13.2. *La corrispondenza vuota è uno "zero" per il prodotto tra corrispondenze; cioè per ogni corrispondenza $F \subseteq A \times B$, risulta*

$$\emptyset \circ F = F \circ \emptyset = \emptyset$$

(e non è necessario precisare tra quali coppie di insiemi si definisce la corrispondenza, come è evidente).

Proposizione 1.13.3. *Se $F \subseteq A \times B$ è una corrispondenza qualunque, allora*

$$(F^{-1})^{-1} = F$$

(e questa proprietà prende anche il nome di identità per doppia inversione*).*

Proposizione 1.13.4. *Il prodotto tra corrispondenze è distributivo rispetto alla loro unione; cioè se* $(F_i \,:\, i \in I)$ *e* $(G_j \,:\, j \in J)$ *sono due famiglie di corrispondenze tra coppie di insiemi, si ha*

$$(\bigcup_{j\in J} G_j) \circ (\bigcup_{i\in I} F_i) = \bigcup_{i\in I}\bigcup_{j\in J} (G_j \circ F_i)$$

(cfr. es.1.7.4)

Si noti che, in generale (come per le relazioni), il prodotto di corrispondenze non è distributivo rispetto alla loro intersezione.

Proposizione 1.13.5. *Se* $(F_i \,:\, i \in I)$ *è una famiglia di corrispondenze tra coppie di insiemi si ha (cfr. es. 1.7.7 e 1.7.8):*

$$(\bigcup_{i\in I} F_i)^{-1} = \bigcup_{i\in I} F_i^{-1}\,,$$

$$(\bigcap_{i\in I} F_i)^{-1} = \bigcap_{i\in I} F_i^{-1}\,.$$

Siano A e B due insiemi fissati. Se si considera la totalità delle corrispondenze da A verso B, si può parlare di inclusione tra esse; precisamente, se $F, G \subseteq A \times B$, si ha

$$F \subseteq G \quad \Rightarrow \quad [(a,b) \in F \quad \Rightarrow \quad (a,b) \in G]\,.$$

Sussistono allora le due proposizioni seguenti:

Proposizione 1.13.6. *Se* $F, G \subseteq A \times B$ *sono due corrispondenze qualsiasi e* $H \subseteq A \times B$ *è una corrispondenza fissata, si ha*

$$F \subseteq G \quad \Rightarrow \quad F \circ H \subseteq G \circ H\,,$$

$$F \subseteq G \quad \Rightarrow \quad H \circ F \subseteq H \circ G\,,$$

(cfr. es. 1.7.10).

Diamo ora alcuni esempi di corrispondenze.

1. Sia $\mathbb{N}$ l'insieme dei numeri naturali (zero escluso) e sia $\mathbb{Q}^+$ l'insieme dei razionali positivi (zero escluso). La $F = \{(n, \frac{h}{n}) \,:\, h \in \mathbb{Q}^+\}$ è una corrispondenza da $\mathbb{N}$ verso $\mathbb{Q}^+$. Per ogni $n \in \mathbb{N}$, $F(n)$ è l'insieme di tutti i razionali (positivi) il cui denominatore è divisibile per n, quindi $D(F) = \mathbb{N}$. Viceversa, per ogni razionale $\frac{r}{t} \in \mathbb{Q}^+$ $(r, t \in \mathbb{N})$, $F^{-1}(\frac{r}{t})$ è non vuota perché è costituita da tutti i razionali che sono divisi da t (quindi contiene almeno 1 e t) . Pertanto $Im(F) = \mathbb{Q}^+$. Ne segue che la corrispondenza non è né univoca a sinistra né a destra (basta tenere presente quali siano le immagini e le controimmagini).

2. Siano $A = \{a, b, c, d\}$, $B = \{x, y, z, t, v\}$ e sia $F = \{(a, y), (b, t), (a, z)\}$. F è una corrispondenza da A verso B, in cui $D(F) = \{a, b\}$, $Im(F) = \{y, z, t\}$; inoltre, $F^{-1} = \{(y, a), (t, b), (z, a)\}$ ed

$$F^{-1} \circ F = \{(a, a), (b, b), (a, a)\} = \{(a, a), (b, b)\} \subseteq \Delta_A \ ;$$

quindi, F è univoca a sinistra. D'altra parte,

$$F \circ F^{-1} = \{(y, y), (y, z), (t, t), (z, y), (z, z))\} \nsubseteq \Delta_B \ ,$$

cioè F non è univoca a destra.

3. Sia A l'insieme dei rettangoli del piano e sia B l'insieme dei numeri razionali positivi, la $F \subseteq A \times B$ definita da

$$F = \{(a, b) \ : \ a \in A, \text{ b misura dell'area di } a, \ b \in B\}$$

è una corrispondenza. $D(F)$ è l'insieme di tutti i rettangoli pei i quali la misura dell'area è razionale. $Im(F)$ è tutto B (si può sempre considerare un rettangolo di lati b ed $1 \in \mathbb{Q}^+$). Inoltre, $\forall a \in D(F)$, $\exists! b \in B$ tale che $(a, b) \in F$; quindi

$$\forall a \in A, \ \forall b, b' \in B, \quad (a, b) \in F \text{ e } (a, b') \in F \quad \Rightarrow \quad b = b' \ ;$$

ne segue che F è univoca a destra. Però F non è univoca a sinistra (basta tener conto che $\forall b \in B$, non esiste, in generale, un solo rettangolo la cui area ha per misura b).

Altri esempi di corrispondenze saranno visti negli esercizi.

Esercizi

Esercizio 1.13.1. *Si consideri la corrispondenza*

$$F \subseteq \mathbb{Z} \times \mathbb{Z}$$

(di fatto corrispondenza) definita da

$$\forall z \in \mathbb{Z}, \quad F(z) = \{x, y \in \mathbb{Z}, \text{ tale che sia } x + y = z\} .$$

Si determini la corrispondenza inversa di F.

Sol. Osserviamo innanzitutto che, $\forall z \in \mathbb{Z}$, esistono infinite coppie $x, y \in \mathbb{Z}$, tali che risulti $x + y = z$, e queste coppie non si considerano ordinate, in quanto ciascuna di esse costituisce semplicemente un elemento di $P(\mathbb{Z})$. infatti, fissato z, per ogni intero y esiste ed è unico l'intero $x = z - y$.

Inoltre, $Im(F) = \mathbb{Z}$.

Determiniamo ora la corrispondenza inversa. Si ha $F^{-1}(x) = \mathbb{Z}, \forall x \in \mathbb{Z}$. Infatti, fissato $x \in \mathbb{Z}$, comunque si scelga $y \in \mathbb{Z}$, esiste $z \in \mathbb{Z}$, tale che risulti $x + y = z$.

Esercizio 1.13.2. *Sia S l'insieme dei numeri naturali pari (zero escluso) e sia S' l'insieme dei numeri naturali dispari. si consideri la corrispondenza $F \subseteq S \times S'$, definita da*

$$\forall x \in S, \quad F(x) = \{x' \in S' \ : \ x' < x \text{ in } \mathbb{N}\} .$$

Si determinino $Im(F)$ e la corrispondenza inversa.

Sol. Osserviamo innanzitutto che, per ogni coppia x, y di elementi di S, per i quali sia $x < y$, risulta $F(x) \subset F(y)$. Pertanto $Im(F) = S'$. Per determinare la corrispondenza inversa, teniamo conto che ogni $x' \in S'$ (cioè ogni naturale dispari) appartiene all'immagine di tutti gli $x \in S$ tali che, pensando x ed x' come elementi di $\mathbb{N}$, sia $x > x'$; quindi la controimmagine di x' è il sottoinsieme di S definito da

$$F^{-1}(x') = \{n \in \mathbb{N} \ : \ n = 2k + (x' + 1) \ , \ k \in \mathbb{N} \cup \{0\}\} .$$

onde la corrispondenza inversa associa ad ogni naturale dispari tutti i naturali pari ad esso successivi (considerando in $\mathbb{N}$ l'ordinamento naturale).

Esercizio 1.13.3. *Sia E l'insieme delle equazioni di secondo grado a coefficienti razionali, e sia $\mathbb{R}$ l'insieme dei numeri reali. Si consideri la corrispondenza $F \subseteq E \times \mathbb{R}$, definita da*

$$F = \{(a, r) \ : \ a \in E, \ r \in \mathbb{R}, \ r \text{ è radice dell'equazione } a \in E\} .$$

Si determinino $D(F)$, $Im(F)$ e F^{-1}.

Sol. In case alla definizione di F, $D(F) = \{a \in E \ : \ \Delta \geq 0\}$, ove Δ è il discriminante dell'equazione $a \in E$. Inoltre,

$$Im(F) = \mathbb{Q} \cup \{\text{irrazionali quadratici}\}$$

(dove $\mathbb{Q}$ è l'insieme dei numeri razionali, ed un irrazionale quadratico è un numero reale, non razionale, che sia radice di un'equazione algebrica di 2° grado a coefficienti razionali), onde $Im(F) \subset \mathbb{R}$.

Infine, $F^{-1} \subseteq \mathbb{R} \times E$ è definita da

$$F^{-1} = \{(r, a) \quad : \quad r \in \mathbb{R} \text{ ed r è radice di un'equazione algebrica di 2° grado } a \in E, \text{ a coefficienti razionali}\}.$$

Esercizio 1.13.4. *Sia A l'insieme dei punti di una circonferenza C fissata nel piano; sia B l'insieme dei punti di una retta r, esterna a C, fissata, e sia O un punto fissato nel piano, esterno a C e non appartenente ad r. Si consideri la corrispondenza $F \subseteq B \times A$ definita da*

$$F = \{(x, y) \quad : \quad x \in B, y \text{ è punto di intersezione di } C \text{ con la retta congiungente } x \text{ con } O\}.$$

Si determinino $D(F)$, $Im(F)$, F^{-1}.

Sol. Siano t e t' i punti di r intersezione con r delle tangenti condotte per O a C. Evidentemente

$$D(F) = \{x \in r \quad : \quad x \text{ appartiene al segmento di estremi } t \text{ e } t'\};$$

inoltre $Im(F)$ è tutto A (cioè la circonferenza C). Dalla definizione di F, segue poi che F è univoca a sinistra (elementi distinti di B non possono avere la medesima immagine in A). Di conseguenza, F^{-1} è univoca a destra; $F^{-1} \subseteq A \times B$ è definita da

$$F^{-1} = \{(y, x) \quad : \quad y \text{ è un punto della circonferenza } C \text{ ed } x \text{ è la sua proiezione da } O \text{ su } r\}.$$

(Di fatto F^{-1} è un'applicazione di A in B; cfr. n. 1.14).

Esercizio 1.13.5. *Siano C e C' due circonferenze di un piano π, considerate come insiemi dei loro punti, fra di loro esterne, e sia O un punto di π, appartenente alla congiungente i centri di C e C' ed esterno ad entrambe. Si consideri la corrispondenza $F \subseteq C \times C'$ che, ad ogni punto P di C, associa il sottoinsieme $\{P', P''\}$ di C' costituito dai due punti di intersezione di C' con la retta OP. Si determini la corrispondenza F^{-1}, inversa della corrispondenza F.*

Sol. Osserviamo innanzitutto che $F(P) = \emptyset$ se la retta OP è esterna a C'; $F(P)$ contiene un solo punto di C' se la retta OP è tangente a C'; negli altri casi, $F(P) = \{P', P''\}$. Per determinare la corrispondenza inversa, consideriamo il generico punto P' di C'; la retta OP' interseca la circonferenza C in due punti P e $\bar{P}$, oppure in un punto (se è tangente), o infine in nessun punto, onde la controimmagine di P' è, rispettivamente, $\{P, \bar{P}\}$, l'insieme $\{T\}$ (essendo T il punto di tangenza di OP' con C), oppure $\emptyset$.

Si noti che, stante la definizione della corrispondenza F, F^{-1} si ottiene immediatamente scambiando il ruolo di C con quello di C'.

Esercizio 1.13.6. *Sia S l'insieme dei punti di un piano euclideo π; fissato in π un riferimento cartesiano ortogonale monometrico, sia S' l'insieme dei quadrati di π, aventi lato di lunghezza fissata h e lati paralleli agli assi coordianti. Si consideri la corrispondenza $F \subseteq S \times S'$ che, ad ogni punto $P \in S$, associa i quadrati di S' aventi un vertice in P. Si determinino $F(P)$, $Im(F)$ e la corrispondenza inversa di F.*

Sol. Dalla definizione della corrispondenza assegnata, segue immediatamente che $F(P)$ è costituito dai quattro quadrati di S' che hanno il vertice comune nel punto P. Abbiamo poi $Im(F) = S'$, in quanto ogni quadrato di S' ha quattro vertici che sono punti di S, e, pertanto, appartiene all'immagine di tali punti.

Detto q il generico quadrato di S', ne segue che $F^{-1}(q)$ è l'insieme dei quattro vertici di q (che sono elementi di S), onde $F^{-1} \subseteq S \times S'$, associa ad ogni quadrato di S' l'insieme dei suoi vertici.

Esercizio 1.13.7. *Sia $F \subseteq \mathbb{Q}^+ \times \mathbb{Q}^+$ la corrispondenza che, ad ogni razionale $x = m/n \in \mathbb{Q}^+$, con m ed n primi tra loro ed m non negativo, associa tutti i razionali non negativi $x' = a/n$, con $a \in \mathbb{Z}^+$, primo con n. Si determinino $F(x)$, $Im(F)$ e la corrispondenza inversa della corrispondenza F.*

Sol. In base alla definizione della corrispondenza F, si ha

$$F(\frac{m}{n}) = \{a/n \ : \ [a, n \in \mathbb{Z}^+, \text{m.c.d.}(a, n) = 1]\}.$$

Ne segue che $Im(F) = \mathbb{Q}^+$. La corrispondenza inversa coincide con F, in quanto ogni $a/n \in \mathbb{Q}^+$ appartiene all'immagine di ciascun $m/n \in \mathbb{Q}^+$, con m.c.d.$(a, n) = 1$, quindi l'insieme di tali elementi di $\mathbb{Q}^+$ costituisce la controimmagine di a/n.

1.14 Applicazioni tra insiemi. Prodotto cartesiano di una famiglia di insiemi.

Consideriamo ora un particolare tipo di corrispondenze tra due insiemi, le cosiddette applicazioni.

Siano S ed S' due insiemi qualsiasi; una corrispondenza da S verso S' si dice *applicazione di S in S'*, se sono soddisfatte le due condizioni seguenti:

1. il dominio della corrispondenza è tutto S;
2. l'immagine di ogni elemento di S è costituita da un solo elemento di S'.

È consuetudine denotare le applicazioni con lettere minuscole latine o greche, ed inoltre, se f è un'applicazione di S in S', si scrive:

$$f \ : \ S \to S' \ .$$

Per ogni $x \in S$, denoteremo con $f(x) = x' \in S'$ l'immagine di x mediante f. Come per le corrispondenze, chiameremo immagine di f, $Im(f)$, il s.i. di S' definito da:

$$Im(f) = \{x' \in S' \ : \ [\exists x \in S \ : \ x' = f(x)]\}.$$

Si noti che, stante la definizione di applicazione, ogni elemento di S ha l'immagine costituita da un solo elemento (cioè la corrispondenza è univoca a destra); ma ciò non esclude che più elementi di S possano avere la medesima immagine in S'.

Sia $f : S \to S'$ un'applicazione; poiché f è una corrispondenza, ha significato considerare la corrispondenza inversa $f^{-1} \subseteq S \times S'$. In base all'osservazione precedente, in generale, l'inversa di una applicazione non è una applicazione, in quanto non sono necessariamente soddisfatte le due condizioni affinché una corrispondenza sia un'applicazione (e non è neppure sufficiente che ne sia soddisfatta una sola).

Come per le corrispondenze, $\forall x' \in S'$, definiremo controimmagine di x' nella corrispondenza inversa f^{-1}, cioè

$$f^{-1}(x') = \{x \in S \ : \ x' = f(x)\}.$$

Evidentemente,

$$f^{-1}(x') \neq \emptyset \quad \iff x' \in Im(f).$$

La considerazione della corrispondenza inversa di una applicazione permette una classificazione delle applicazioni.

Precisamente, sia $f : S \to S'$ un'applicazione di S in S'; diremo che f è *un'applicazione suriettiva* od una *suriezione* sse

$$Im(f) = S'$$

(in questo caso, per la corrispondenza inversa f^{-1} è soddisfatta la condizione 1 delle applicazioni: $D(f^{-1}) = S'$).

diremo poi che l'applicazione $f : S \to S'$ è iniettiva, se la controimmagine di ogni elemento è costituita da un solo elemento, cioè:

$$\forall x' \in Im(f) \quad \Rightarrow \quad \exists! \, x \in S \, : \, x' = f(x)$$

(ovvero

$$\forall x' \in Im(f) \quad \Rightarrow \quad \exists! \, x \in S \, : \, x = f^{-1}(x') \, ,$$

ovvero

$$\forall x' \in D(f^{-1}) \quad \Rightarrow \quad \exists! \, x \in S \, : \, x = f^{-1}(x') \,).$$

Quindi, se f è iniettiva, è soddisfatta la condizione 2 per la corrispondenza f^{-1}, cioè questa è univoca a destra, onde f è univoca a sinistra.

Si può provare (cfr es. 1.14.7) che $f : S \to S'$ è iniettiva sse

$$\forall f(x), f(y) \in Im(f), \quad f(x) = f(y) \quad \to \quad x = y \, .$$

Un'applicazione può essere contemporaneamente iniettiva e suriettiva: in tal caso essa si dice *biiettiva*, ovvero una *biiezione* ovvero *corrispondenza biunivoca*.

Quindi, se $f : S \to S'$ è una biiezione, allora $Im(f) = S'$, cioè $D(f^{-1}) = S'$ e

$$\forall x' \in S' \quad \exists! \, x \in S \, : \, x' = f(x)$$

$$(\text{ovvero } \forall x' \in S' \quad \exists! \, x \in S \, : \, x = f^{-1}(x')).$$

Pertanto, la f^{-1} soddisfa le condizioni 1 e 2 delle applicazioni, cioè è anch'essa una applicazione; d'altra parte, $(f^{-1})^{-1} = f$, onde resta provata la

Proposizione 1.14.1. *Sia $f : S \to S'$ un'applicazione di S in S'; sse f è una biiezione di S su S', la corrispondenza inversa è una applicazione e precisamente una biiezione di S' su S,*

Sia ora $f : S \to S'$ un'applicazione iniettiva di S in S' ($Im(f) \subseteq S'$), allora f prende anche il nome di *immersione* di S in S'.

Diamo ora alcuni esempi di applicazioni.

1. Siano $S = \{a, b, c, d\}$, $S' = \{x, y, z, t, u\}$; definiamo $f : S \to S'$, mediante

   $$f(a) = f(b) = y. \quad f(c) = t, \quad f(d) = z;$$

   allora f è un'applicazione di S in S', in quanto $Im(f) = \{y, z, t\} \subset S'$; inoltre f non è iniettiva, dato che $f^{-1}(y) = \{a, b\}$.

2. Sia $\mathbb{N}$ l'insieme dei numeri naturali e sia $\mathbb{P}$ l'insieme dei numeri pari. La corrispondenza che, ad ogni $n \in \mathbb{N}$ associa $2n \in \mathbb{P}$ è un'applicazione; precisamente è una biiezione, in quanto

$$\forall m \in \mathbb{P} \quad \Rightarrow \quad \exists!\, n = \frac{m}{2} \in \mathbb{N}\,,$$

onde la $f : \mathbb{N} \to \mathbb{P}$ suddefinita è suriettiva ed iniettiva.

3. Sia $\mathbb{Z}$ l'insieme dei numeri interi relativi e sia $\mathbb{N}$ l'insieme dei naturali (zero incluso). La corrispondenza che ad ogni $x \in \mathbb{Z}$ associa il suo valore assoluto è manifestamente una applicazione $f : \mathbb{Z} \to \mathbb{N}$ (in quanto sono soddisfatte le due condizioni). Ora, f è suriettiva, dato che $\forall n \in \mathbb{N}$, $f^{-1}(n) \neq$; precisamente, $f^{-1}(n) = \{n, -n\}$, $f^{-1}(0) = \{0\}$.

   Ma f non è iniettiva, in quanto la controimmagine di ogni elemento dell'immagine (tranne 0) non contiene un solo elemento.

4. Sia $\mathbb{N}$ l'insieme dei naturali e $\mathbb{Z}$ l'insieme dei numeri interi. Definiamo l'applicazione $f : \mathbb{N} \to \mathbb{Z}$ mediante

$$\forall n \in \mathbb{N}, \quad f(n) = 3n \in \mathbb{Z}$$

   (è immediato verificare che f è di fatto un'applicazione).

   tale f non è su; infatti, $Im(f)$ è costituita dagli interi positivi divisibili per 3 e quindi è un s.i. proprio di $\mathbb{Z}$.

   Però f è iniettiva dato che

$$f(n) = f(m) \quad \Rightarrow \quad 3n = 3m \quad \Rightarrow \quad n = m\,.$$

Altri esempi, nonché altre semplici proprietà delle applicazioni saranno viste negli esercizi.

Definiamo l'uguaglianza di due applicazioni. Siano $f : S \to S'$ e $g : S \to S'$ due applicazioni di S in S'. Diremo che f e g sono $eguali$ e scriveremo $f = g$ sse

$$\forall x \in S \quad \Rightarrow \quad f(x) = g(x)\,.$$

In termini non molto rigorosi, si può dire che due applicazioni sono eguali se operano nello stesso modo tra gli stessi insiemi.

Osserviamo ora che, quando si definisce una applicazione $f : S \to S'$, non si esclude il caso in cui $S = S'$.
Si parlerà allora di applicazione f di S in se stesso, oppure su se stesso. Qualora $f : S \to S$ è una biiezione, f prende anche il nome di *trasformazione di S*.

Un caso particolare di applicazione di S su S è costituita dalla *applicazione identica* $e_S : S \to S$, definita da $e_S(x) = x$, $\forall x \in S$. L'identità e_S (altri simboli consueti sono i_S, I, u_S) è manifestamente una biiezione.

Inoltre, se $f : S \to S$ è una biiezione, allora f^{-1} è una biiezione ed $f^{-1} \circ f = f \circ f^{-1} = e_S$, il prodotto essendo definito tenendo presente che le applicazioni sono corrispondenze.

Siano ora $f : S \to S'$, $g : S' \to S''$ due applicazioni; resta allora definita l'*applicazione prodotto* $g \circ f : S \to S''$ e scriveremo

$$\forall x \in S, \quad g \circ f(x) = g(f(x)) = g(x') = x'' \ ,$$

essendo $x' = f(x)$.

Tenendo presente quanto già provato per le corrispondenze (ed il fatto che $e_S = \Delta_S$), sussistono i seguenti risultati:

Proposizione 1.14.2. *Sia $f : S \to S'$ un'applicazione, e_S, $e_{S'}$, sono rispettivamente l'identità su S e l'identità su S', si ha*

$$f \circ e_S = f, \quad e_{S'} \circ f = f, \quad e_{S'} \circ f \circ e_S = f \ .$$

Proposizione 1.14.3. *Sia $f : S \to S'$, $g : S' \to S''$, $h : S'' \to S'''$ sono applicazioni, allora sono definiti i prodotti $g \circ f$ e $h \circ g$, e vale la proprietà associativa*

$$(h \circ g) \circ f = h \circ (g \circ f) \ .$$

Si noti che non è definito, in generale, il prodotto $h \circ f$, perché questo non è sempre un'applicazione ($Im(f) \subseteq S'$ ed $h : S'' \to S'''$); se $S' = S''$, allora ha senso l'applicazione $h \circ f$.

Proposizione 1.14.4. *Sia $f : S \to S'$ e $g : S' \to S''$ sono biiezioni, anche $g \circ f$ è una biiezione e risulta*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1} \ .$$

Osserviamo che si può sempre definire $(g \circ f)^{-1}$, ma questa è una corrispondenza e vale l'eguaglianza precedente.

Altre proprietà delle applicazioni saranno viste negli esercizi.

In analogia a quanto fatto per le relazioni su un insieme, definiamo ora la restrizione (sul dominio) di una applicazione $f : S \to S'$.

Sia $A \subseteq S$, diciamo *restrizione* ad A dell'applicazione $f : S \to S'$ e la denotiamo con $f|_A$ (talvolta semplicemente con f_A), l'applicazione

$$f|_A \quad : \quad A \to S' \ ,$$

definita da:

$$\forall x \in A \quad \Rightarrow \quad f|_A(x) = f(x) \in S' \ .$$

Si noti che $Im(f|_A) \subseteq Im(f)$, ma può valere il segno di eguaglianza.

Ad esempio, se $f : S \to S'$ non è iniettiva si può scegliere $A \subseteq S$ in modo tale che $f|_A$ sia iniettiva.

Basta procedere nel modo seguente: per ogni $x' \in Im(f)$, si considera la controimmagine $f^{-1}(x')$ e si fissa $\bar{x} \in f^{-1}(x')$, in modo arbitrario. Assunto

$$A = \{\bar{x} \in S \ : \ \bar{x} \in f^{-1}(x'),\ x' \in Im(f),\ \bar{x} \text{ fissato}\};$$

$f|_A : A \to S'$ è manifestamente iniettiva.

Osserviamo che la suddetta costruzione è lecita sse si ammette il *postulato di Zermelo* delle infinite scelte libere (o *assioma di scelta*), che possiamo enunciare nella forma originaria (pur esistendo moltissime formulazioni equivalenti):

"Per ogni insieme M, i cui elementi siano insiemi P disgiunti e non vuoti, esiste almeno un insieme N che contiene precisamente un elementi di ciascuno degli insiemi P".

Si può "invertire" il procedimento di restrizione (sul dominio) di una applicazione $f : S \to S'$ definendo l'estensione sul dominio. Precisamente se $B \supseteq S$ e $g : B \to S'$ è un'applicazione, diremo che g è una *estensione* di f se $g|_S = f$.

In maniera analoga si può definire la restrizione sul codominio di $f : S \to S'$ (il codominio di f essendo S').
Si consideri $A' \subseteq S'$ tale che $A' \supseteq Im(f)$. Diciamo *restrizione sul codominio* di f ad A' l'applicazione $f|^{A'} : S \to S'$ tale che

$$\forall x \in S \quad \Rightarrow \quad f|^{A'}(x) = f(x)\ .$$

La restrizione sul codominio risulta molto utile quando una applicazione $f : S \to S'$ non è su e la si vuole sostituire, senza alterarla, con un'applicazione su.

Tenendo presente la definizione di suriezione, è evidente che

$$f|^{Im(f)} : S \to Im(f)$$

è un'applicazione su.

In particolare, se $f : S \to S'$ è un'applicazione iniettiva, la restrizione sul codominio ad $Im(f)$ è una biiezione (perché è anche su), cioè

$$f : S \to S' \text{ iniettiva} \quad \Rightarrow \quad f|^{Im(f)} : S \to Im(f) \text{ biiettiva}\ .$$

Si definisce anche l'estensione sul codominio.
Precisamente, sia $f : S \to S'$ un'applicazione e sia $B' \supseteq S'$. Una applicazione $g : S \to B'$, tale che $g|^{S'} = f$ è un'*estensione sul codominio* di f a B'.

Vogliamo ora fare alcune osservazioni sul simbolismo. Se $f : S \to S'$ è un'applicazione, abbiamo denotato con $f(x)$ l'immagine di $x \in S$ mediante f. tale scrittura prende il nome di scrittura funzionale; di conseguenza, se $g \circ f : S \to S''$ è un'applicazione prodotto abbiamo scritto

$$g \circ f(x) = g(f(x)).$$

Accanto a tale scrittura, è spesso usata la cosiddetta scrittura operatoria. Se $f : S \to S'$, è un'applicazione, l'immagine di $x \in S$ mediante f viene denotata con xf; in questo caso, poi, il prodotto di due applicazioni f e g (nell'ordine) si scrive fg, onde

$$(x)fg = (xf)g.$$

Una terza scrittura per denotare l'immagine di $x \in S$ nella applicazione $f : S \to S'$ è la scrittura esponenziale x^f; in tal caso, denotando con fg il prodotto di f per g (nell'ordine) si ha

$$x^{fg} = (x^f)^g.$$

La definizione data di applicazione è conseguenza delle precedenti argomentazioni svolte sulle corrispondenze; però è possibile definire le applicazioni senza far ricorso alle corrispondenze.

Precisamente, chiameremo applicazione f di S in S', dove S ed S' sono insiemi qualsivoglia, una terna $\langle S, S'; f\rangle$, dove f è una "legge" che ad ogni elemento x di S associa uno, ed uno solo, elemento $x' = f(x)$ di S', immagine di x mediante f.

Evidentemente, le due definizioni coincidono, in quanto la "legge f" individua esattamente il s.i. di $S \times S'$, costituito dalle coppie $(x, f(x))$, che rappresenta la corrispondenza f (anche se questa è particolare essendo una applicazione).

Definire un'applicazione come terna, risulta utile al fine di stabilire l'uguaglianza di due applicazioni; precisamente:

$$\langle S, S'; f\rangle = \langle A, A'; g\rangle \quad \Longleftrightarrow \quad S = A,\ S' = A',\ f = g\ .$$

Abbiamo definito le applicazioni in termini di corrispondenze; sorge allora la questione inversa, cioè quella di definire le corrispondenze in termini di applicazioni.
ciò è possibile nel modo seguente.

Sia $F \subseteq A \times B$ una corrispondenza di A verso B; allora F definisce univocamente un'applicazione $f : A \to P(B)$ nel modo seguente:

$$\forall a \in E, \quad f(a) = F(a) \in P(B)\ .$$

Evidentemente, se $a \notin D(F)$, $f(a) = \emptyset \in P(B)$, quindi $D(f) = A$.
Inoltre,

$$Im(f) = \{F(a) \in P(B)\ :\ \forall b \in F(a),\ (a, b) \in F\}$$

e

$$\bigcup Im(f) = \bigcup Im(F)$$

(gli elementi di $Im(f)$ sono s.i. di B; mentre gli elementi di $Im(F)$ sono elementi di B).

Se ora $F^{-1} \subseteq B \times A$ è l'inversa di F, questa definisce l'applicazione $f^{-1} : B \to P(A)$ in maniera analoga.

È abbastanza chiaro che trattare le corrispondenze in questo modo crea complicazioni inutili; abbiamo citato queste osservazioni soltanto per motivi di completezza.

In base alla definizione di applicazione, tenendo presente come è stata definita una famiglia di insiemi, si può constatare che tale definizione contiene la nozione di applicazione. Precisamente, una famiglia $(A_i \ : \ i \in I)$ di insiemi dipendente dall'insieme I di indici non è altro che l'immagine di un'applicazione $f : I \to \mathcal{A}$ che sia iniettiva (infatti $A_i = A_j \Rightarrow i = j$), $\mathcal{A}$ essendo un insieme di insiemi ed avendo posto $A_i = f(i)$.

Sia $(A_i \ : \ i \in I)$ una famiglia di insiemi; il *prodotto cartesiano* di tali insiemi, che si denoterà con $\prod(A_i \ : \ i \in I)$ è definito come l'insieme di tutte le applicazioni

$$f \ : \ I \quad \to \quad \bigcup(A_i \ : \ i \in I)$$

tali che $f(i) \in A_i$, per tutti gli $i \in I$.

Nel caso particolare in cui $A_i = A, \forall i \in I$, $\prod(A_i \ : \ i \in I)$ prende il nome di *potenza diretta* di A e viene denotato con A^I.

Proviamo ora che, se $I = \{1, 2, \ldots, n\}$, la definizione precedente coincide con la definizione di prodotto cartesiano $A_1 \times \cdots \times A_n$ come insieme delle n-ple $(a_1, \ldots, a_n)$, tali che $a_i \in A_i$. Basterà provare questa affermazione nel caso particolare $n = 2$.

Pertanto sia $I = \{1, 2\}$ e poniamo $A_1 = A$, $A_2 = B$, allora

$$A \times B = \{f \ : \ I \ \to \ A \cup B, \text{ tali che } f(1) \in A \text{ ed } f(2) \in B\} \ .$$

Ora, $f(1) \in A \Rightarrow f(1) = a \in A$, $f(2) \in B \Rightarrow f(2) = b \in B$, quindi ciascuna delle applicazioni che costituiscono $A \times B$ individua uno e un solo elemento di A ed uno e un solo elemento di B, cioè individua una coppia $(a, b) \in A \times B$ (secondo la definizione del n. 1.6).
D'altra parte, la definizione di f comporta che le restrizioni

$$f|_{\{1\} \subset I} \quad I \quad \to A \quad \text{ed} \quad f|_{\{2\} \subset I} \quad I \quad \to B$$

siano iniettive, e quando si considerano tutte le f siffatte, l'insieme di queste due restrizioni ha per immagine, rispettivamente, uno ed un solo elemento di di A ed uno ed un solo elemento di B. Ne segue che, considerate tutte queste applicazioni, si ottengono tutte e sole le coppie $(a, b) \in A \times B$.

Viceversa se $(a, b) \in A \times B$, costruiamo $f : I \to A \times B$ in modo tale che $f^{-1}(a) = 1 \in I$ ed $f^{-1}(b) = 2 \in I$, onde la f è univocamente determinata.

In conclusione, la definizione di prodotto cartesiano di una famiglia di insiemi contiene la consueta definizione di prodotto cartesiano di n insiemi e la generalizza.

Osserviamo infine che il prodotto cartesiano di una famiglia di insiemi si trova talvolta scritto anche come $\prod_{i \in I} A_i$, $\bigtimes_{i \in I} A_i$, oppure $\bigtimes (A_i \ : \ i \in I)$. Le notazioni che adotteremo sono quella introdotta nella definizione e la prima di queste ultime.

Esercizi

Esercizio 1.14.1. *Si provi che un'applicazione $f : A \to B$ si può caratterizzare come una corrispondenza $f \subseteq A \times B$ tale che*

$$1) \quad f^{-1} \circ f \supseteq \Delta_A \, ;$$

$$2) \quad f \circ f^{-1} \subseteq \Delta_B \, .$$

Dim. La condizione 2) significa che f è una corrispondenza univoca a destra, quindi garantisce che l'immagine di un elemento di A sia un unico elemento di B, condizione necessaria perché una corrispondenza sia un'applicazione.

La condizione 1) assicura invece che $D(f) = A$; infatti, se $D(f) = A$, $\forall a \in A \; \exists b \in B$ tale che $(a, b) \in f$ e quindi $(b, a) \in f^{-1}$, cioè $\forall a \in A$ $\exists b \in B$ tale che $(b, a) \in f^{-1}$. Pertanto, $\forall a \in A \; (a, a) \in f^{-1} \circ f$; ne segue che $\Delta_A \subseteq f^{-1} \circ f$, cioè la condizione 1).

Viceversa, se vale la 1), cioè se $\Delta_A \subseteq f^{-1} \circ f$, $\forall a \in A$, $(a, a) \in f^{-1} \circ f$, quindi esiste b tale che $(a, b) \in f$ (e pertanto $(b, a) \in f^{-1}$), cioè $D(f) = A$. Ne segue che le 1) e 2) caratterizzano le corrispondenze che sono applicazioni.

Esercizio 1.14.2. *Data l'applicazione $f : \mathbb{Z} \to \mathbb{Z}$ (ove $\mathbb{Z}$ è l'insieme degli interi relativi), definita da*

$$f(n) = n^2, \; \forall n \in \mathbb{Z} \, ,$$

si determini $Im(f)$. Si determinino inoltre le controimmagini dei seguenti s.i. di $\mathbb{Z}$: $\mathbb{Z}^+$, $\mathbb{Z}$, $\{3\}$, $\{0, 1, 2, \ldots, 9\}$.

Sol. Dalla definizione di f segue che $Im(f)$ è l'insieme dei quadrati di $\mathbb{Z}$ (cioè l'insieme di tutti gli interi che siano quadrati di interi).

Si ha poi

$$f^{-1}(\mathbb{Z}^+) = \mathbb{Z}; \quad f^{-1}(\mathbb{Z}) = \mathbb{Z} \, .$$

$$f^{-1}(\{0, 1, 2, \ldots, 9\}) = \{0, \pm 1, \pm 2, \pm 3\}; \quad f^{-1}(\{3\}) = \emptyset.$$

(Si ricordi che la controimmagine di ogni elemento non contenuto nella immagine è vuota).

Esercizio 1.14.3. *Sia $f : S \to S'$ un'applicazione e sia $A' \subset S'$. Si provi*

$$f^{-1}(\mathcal{C}_{S'} A') = \mathcal{C}_S f^{-1}(A') \, .$$

Dim. Per definizione di controimmagine, si ha $x \in f^{-1}(\mathcal{C}_{S'} A') \iff$ $\iff \quad f(x) \in \mathcal{C}_{S'} A' \iff f(x) \notin A' \iff x \notin f^{-1}(A')$. Infatti, $f(x) \in A' \iff x \in f^{-1}(A')$ e, per contrapposizione, si ha: $x \notin f^{-1}(A') \iff f(x) \notin A'$. Ma $x \notin f^{-1}(A') \iff x \in \mathcal{C}_S f^{-1}(A')$, onde l'asserto.

Esercizio 1.14.4. *Si provi che se l'applicazione $f : A \to B$ è suriettiva, allora è caratterizzata da*

$$1) \quad f^{-1} \circ f \supseteq \Delta_A \, ;$$
$$2) \quad f \circ f^{-1} = \Delta_B \, ,$$

cioè tali condizioni individuano quelle corrispondenze che sono applicazioni suriettive.

Dim. Poiché f è un'applicazione, si ha $f^{-1} \circ f \supseteq \Delta_A$, $f \circ f^{-1} = \Delta_B$ (cfr. es. 1.14.1). D'altra parte f è suriettiva, e quindi $D(f^{-1} = B)$. Ne segue (per la condizione 1) dell'es. 1.14.1) che $(f^{-1})^{-1} \circ f^{-1} = f \circ f^{-1} \supseteq \Delta_B$. Dalle due inclusioni opposte segue $f \circ f^{-1} = \Delta_B$.

Esercizio 1.14.5. *Sia $\mathbb{Z}^+$ l'insieme degli interi non negativi e sia m un intero positivo fissato. Si consideri l'applicazione $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ definita da*

$$\forall x \in \mathbb{Z}^+, \quad f(x) = x', \quad \text{con } x' \text{ resto della divisione di } x \text{ per } m.$$

si determinino $Im(f)$ ed $f^{-1}(x')$, $\forall x' \in Im(f)$

Sol. Posto $x = mq + x'$, si ha $0 \leq x' \leq m - 1$. Pertanto $Im(f) = \{0, 1, 2, \ldots, m-1\}$. Ne segue che la controimmagine di ogni $x' \in Im(f)$ è costituita da tutti gli interi positivi che, divisi per m, danno resto x'. Ovviamente f è una suriezione di $\mathbb{Z}^+$ su $Im(f)$.

Esercizio 1.14.6. *Si provi che se l'applicazione $f : A \to B$ è iniettiva, allora f è univoca a sinistra, e si ha*

$$1) \quad f^{-1} \circ f = \Delta_A \, ;$$
$$2) \quad f \circ f^{-1} \subseteq \Delta_B \, ,$$

cioè tali condizioni individuano quelle corrispondenze che sono applicazioni iniettive.

Dim. Per ipotesi $f : A \to B$ è un'applicazione iniettiva, quindi la controimmagine di ogni elemento dell'immagine contiene un solo elemento. Allora f è una corrispondenza univoca a sinistra e $f^{-1} \circ f \subseteq \Delta_A$.

D'altra parte f è un'applicazione, onde (cfr es. 1.14.1) $f^{-1} \circ f \supseteq \Delta_A$; ne segue che $f^{-1} \circ f = \Delta_A$. La condizione 2) completa la caratterizzazione di f come applicazione (cfr es. 1.14.1).

Esercizio 1.14.7. *Sia $f : S \to S'$ un'applicazione di S in S'. Si dica quali delle seguenti implicazioni sono sufficienti a garantire l'iniettività di f:*

$$1) \quad a, b \in S, \; f(a) = f(b) \implies a = b \, ;$$
$$2) \quad a, b \in S, \; a \neq b \implies f(a) \neq f(b) \, ;$$
$$3) \quad a, b \in S, \; a = b \implies f(a) = f(b) \, ;$$
$$4) \quad a, b \in S, \; f(a) \neq f(b) \implies a \neq b \, .$$

Sol. Se vale la 1), oppure la 2), la f è iniettiva; se vale la 3), oppure la 4), non è detto che la f sia iniettiva.

Infatti, la validità della 1) comporta che la controimmagine di ciascun elemento sia ridotta ad un solo elemento.

Se vale la 2), elementi distinti hanno immagini distinte, e quindi la controimmagine di ciascun elemento è ancora ridotta ad un solo elemento.

La 3) vale per qualunque applicazione f, pertanto non può caratterizzare un'applicazione iniettiva.

Similmente, la 4) afferma semplicemente che elementi distinti di S' provengono da elementi distinti di S, ma non dice nulla sulla controimmagine di un qualunque elemento di S'; ne segue che non può caratterizzare un'applicazione iniettiva.

Esercizio 1.14.8. *Sia $f : S \to S'$ un'applicazione e sia A un sottoinsieme di S. si prove che sse f è iniettiva, si ha:*

$$f(\mathcal{C}_S A) = \mathcal{C}_{Im(f)} f(A\ )$$

Dim. Supponiamo che f sia iniettiva e proviamo che

$$x' \in f(\mathcal{C}_S A) \iff x' \in \mathcal{C}_{Im(f)} f(A)\ .$$

Poiché f è iniettiva, la controimmagine di ogni elemento di $Im(f)$ è ridotta ad un solo elemento, onde si ha

$$x' \in f(\mathcal{C}_S A) \implies [\exists! x \in \mathcal{C}_S A\ :\ x' = f(x) \in Im(f)] \implies$$

$$\implies [x \notin A \implies f(x) = x' \notin f(A)] \implies x' \in \mathcal{C}_{Im(f)} f(A)\ .$$

Viceversa,

$$x' \in \mathcal{C}_{Im(f)} f(A) \implies [x' \in f(A)] \implies x = f^{-1}(x') \notin A \implies$$

$$\implies x \in \mathcal{C}_S A \implies f(x) = x' \in f(\mathcal{C}_S A)\ .$$

Supponiamo ora che sia, per ogni sottoinsieme A di S, $f(\mathcal{C}_S A) = \mathcal{C}_{Im(f)} f(A)$ e proviamo che f è iniettiva, cioè che la controimmagine di ogni elemento dell'immagine è ridotta ad un solo elemento.

Sia $x' \in Im(f)$ un elemento tale che esistono $x, y \in S$, $x \neq y$, per i quali risulti $f(x) = f(y) = x'$, e sia A un qualunque sottoinsieme di S tale che $x \in A$, $y \notin A$, cioè $y \in \mathcal{C}_S A$. Allora

$$x' = f(x) \in f(A) \implies x' = f(x) \notin \mathcal{C}_{Im(f)} f(A)\ ;$$

mentre $x' = f(y) \in f(\mathcal{C}_S A)$, contro l'ipotesi che

$$x' \in f(\mathcal{C}_S A) \iff x' \in \mathcal{C}_{Im(f)} f(A)\ ;$$

ne segue che f è iniettiva.

Esercizio 1.14.9. *Sia $f : S \to S'$ un'applicazione; si provi che $A' \subseteq S' \Rightarrow$ $\Rightarrow f(f^{-1}(A')) \subseteq A'$ e che se f è su, vale il segno di eguaglianza.*

Dim. Per definizione di controimmagine,

$$f^{-1}(A') = \{a \in S \,:\, f(a) \in A'\}\,,$$

quindi $\forall a \in f^{-1}(A') \Rightarrow f(a) \in A'$, onde l'inclusione. Se f è su, $A' \subseteq S' \Rightarrow A' \subseteq Im(f)$; pertanto, per ogni $a' \in A'$, esiste $f^{-1}(a') \neq \emptyset$ e $\forall a \in f^{-1}(A')$, $f(a) = a' \in A'$, onde vale anche l'inclusione opposta alla precedente; ne segue l'eguaglianza.

Esercizio 1.14.10. *Si provi che l'applicazione $f : S \to S'$ è suriettiva sse, per ogni s.i. $A' \subseteq S'$, risulta $f(f^{-1}(A')) = A'$.*

Dim. Se f è suriettiva, l'affermazione è vera (cfr. es 1.14.9). Viceversa, sia $f(f^{-1}(A')) = A'$; f è su, in quanto la controimmagine di ogni elemento di S' è non vuota, data l'arbitrarietà di $A' \subseteq S'$, cioè $Im(f) = S'$.

Esercizio 1.14.11. *Sia $f : S \to S'$ un'applicazione. Si provi che*

$$A \subseteq S \implies A \subseteq f^{-1}(f(A))$$

e che se f è iniettiva, $A = f^{-1}(f(A))$.

Dim. Sia $a \in A$, allora $f(a) \in f(A)$ (per definizione di $f(A)$) e quindi $a \in f^{-1}(f(A))$, per definizione di controimmagine; però non è vero, in generale, il viceversa. Infatti, se $a' \in f(A)$ è immagine anche di $x \in S \setminus A$, $f^{-1}(a')$ contiene pure x (oltre ad almeno un elemento di A, per definizione di $f(A)$), onde non vale l'inclusione opposta. Se invece f è iniettiva, $f(a) = f(b) \Rightarrow a = b$ e quindi $f(a) \in f(A) \Rightarrow a \in A$, da cui l'eguaglianza.

Esercizio 1.14.12. *Si provi che l'applicazione $f : S \to S'$ è iniettiva sse, per ogni s.i. $A \subseteq S$, risulta $f^{-1}(f(A)) = A$.*

Dim. Se f è iniettiva, la controimmagine di ogni elemento $x' \in f(A)$ è un solo $x \in A$, onde $f^{-1}(f(A)) = A$. Viceversa, sia $f^{-1}(f(A)) = A$, per ogni $A \subseteq S$; allora la controimmagine di ogni elemento di $f(A)$ appartiene ad A. D'altra parte, valendo l'ipotesi per ogni s.i. di S, fissato comunque $x \in S$, si ha $f^{-1}(f(\{x\})) = \{x\}$, onde la controimmagine di $f(x)$ è un solo elemento $x \in S$ e quindi f è iniettiva (cfr es. 1.14.11).

Esercizio 1.14.13. *Sia $f : S \to S'$ un'applicazione e siano $A', B' \subseteq S'$. Si provi che*

$$f^{-1}(A' \cup B') = f^{-1}(A') \cup f^{-1}(B')\,;$$
$$f^{-1}(A' \cap B') = f^{-1}(A') \cap f^{-1}(B')\,.$$

Dim. Sia $x \in f^{-1}(A' \cup B')$; allora $f(x) \in f(f^{-1}(A' \cup B'))$. Per l'es. 1.14.9, risulta $f(f^{-1}(A' \cup B')) \subseteq A' \cup B'$, quindi $f(x) \in A' \cup B'$, cioè $f(x) \in A'$ oppure $f(x) \in B'$, da cui $f^{-1}(f(x)) \subseteq f^{-1}(A')$, oppure $f^{-1}(f(x)) \subseteq f^{-1}(B')$, cioè $f^{-1}(f(x)) \subseteq f^{-1}(A') \cup f^{-1}(B')$.
Ma $x \in f^{-1}(f(x))$, onde $x \in f^{-1}(A') \cup f^{-1}(B')$. Viceversa, $x \in f^{-1}(A') \cup f^{-1}(B') \Rightarrow x \in f^{-1}(A')$ oppure $x \in f^{-1}(B') \Rightarrow$ $\Rightarrow f(x) \in f(f^{-1}(A'))$ oppure $f(x) \in f(f^{-1}(B'))$; ora, per l'es 1.14.9, $f(f^{-1}(A')) \subseteq A'$ ed $f(f^{-1}(B')) \subseteq B'$, quindi $f(x) \in A'$ oppure $f(x) \in B'$; pertanto, $f(x) \in A' \cup B' \Rightarrow f^{-1}(f(x)) \subseteq f^{-1}(A' \cup B')$; ma $x \in f^{-1}(f(x))$, onde $x \in f^{-1}(A' \cup B')$.

Proviamo ora la seconda affermazione. Si ha:
$x \in f^{-1}(A' \cap B') \Rightarrow f(x) \in f(f^{-1}(A' \cap B')) \subseteq A' \cap B' \Rightarrow f(x) \in A'$ e $f(x) \in B' \Rightarrow f^{-1}(f(x)) \subseteq f^{-1}(A')$ e $f^{-1}(f(x)) \subseteq f^{-1}(B') \Rightarrow$ $\Rightarrow f^{-1}(f(x)) \subseteq f^{-1}(A') \cap f^{-1}(B')$; ma $x \in f^{-1}(f(x))$, onde $x \in f^{-1}(A') \cap f^{-1}(B')$.
Viceversa:
$x \in f^{-1}(A') \cap f^{-1}(B') \Rightarrow x \in f^{-1}(A')$ e $x \in f^{-1}(B') \Rightarrow$ $\Rightarrow f(x) \in f(f^{-1}(A')) \subseteq A'$ e $f(x) \in f(f^{-1}(B')) \subseteq B' \Rightarrow f(x) \in A' \cap B' \Rightarrow$ $\Rightarrow f^{-1}(f(x)) \subseteq f^{-1}(A' \cap B')$; ma $x \in f^{-1}(f(x))$, quindi $x \in f^{-1}(A' \cap B')$.

Si noti che le due eguaglianza provate si possono generalizzare ad una famiglia di insiemi. Precisamente, se $(A'_i : i \in I)$ è una famiglia di insiemi contenuti in S' e se $f : S \to S'$ è un'applicazione, si ha

$$f^{-1}(\bigcup_{i \in I} A'_i) = \bigcup_{i \in I} f^{-1}(A'_i) \, ;$$

$$f^{-1}(\bigcap_{i \in I} A'_i) = \bigcap_{i \in I} f^{-1}(A'_i)$$

(e queste eguaglianze si dimostrano come nel caso di due insiemi).

Esercizio 1.14.14. *Sia $f : S \to S'$ un'applicazione e siano $A' \subseteq S'$. Si provi che*

$$f^{-1}(S' \setminus A') = S \setminus f^{-1}(A') \, .$$

Dim. Teniamo presente che $f(f^{-1}(A')) \subseteq A'$ (cfr. es. 1.14.9). Sia $x \in S \setminus f^{-1}(A')$, allora $f(x) \in Im(f) \subseteq S'$ (per definizione di applicazione); ma $f(x) \notin f(f^{-1}(A')) \subseteq A'$; ne segue che $f(x) \in S' \setminus A'$, onde $f^{-1}(f(x)) \subseteq f^{-1}(S' \setminus A')$; ma $x \in f^{-1}(f(x))$ e quindi $x \in f^{-1}(S' \setminus A')$. Viceversa, sia $x \in f^{-1}(S' \setminus A')$, allora $x \notin f^{-1}(A')$, ma $x \in S$, quindi $x \in S \setminus f^{-1}(A')$, cioè l'asserto.

Esercizio 1.14.15. *Si provi che se l'applicazione $f : A \to B$ è una biiezione, allora essa è caratterizzata da*

$$1) \quad f^{-1} \circ f = \Delta_A \, ;$$

$$2) \quad f \circ f^{-1} = \Delta_B \, ,$$

cioè tali condizioni individuano le corrispondenze biunivoche (biiezioni).

Dim. Se f è una biiezione, f è iniettiva e su. Se f è iniettiva, si ha $f^{-1} \circ f = \Delta_A$ (cfr. es. 1.14.6); se f è su, si ha $f \circ f^{-1} = \Delta_B$ (cfr. es. 1.14.4), onde l'asserto. Il viceversa è ovvio, se si tiene conto della dimostrazione della dimostrazione dell'es. 1.14.1.

Esercizio 1.14.16. *Sia $f : S \to S'$ un'applicazione di S in S'. Diremo che f è un'applicazione costante di S in S' sse*

$$\forall x \in S,\ f(x) = a' \in S',\ a' \text{ fissato in } S'$$

(cioè Imf contiene un solo elemento di S'). Si dica quali condizioni devono essere soddisfatte affinché un'applicazione costante $f : S \to S'$ sia una biiezione.

Sol. Se $f : S \to S'$ è costante, Imf contiene un solo elemento $a' \in S'$. Affinché f sia una biiezione, f deve essere iniettiva e su. Dire che f è suriettiva significa $Imf = S'$, quindi S' deve contenere un solo elemento. Se f è iniettiva, la controimmagine di ogni elemento di Imf deve contenere un solo elemento di S. Poiché Imf contiene un solo elemento, anche S deve contenere un solo elemento. Pertanto f è biettiva sse S ed S' contengono ciascuno un solo elemento.

Esercizio 1.14.17. *Siano A e B insiemi non vuoti. Si provi che esiste una biiezione di $A \times B$ su $B \times A$.*

Sol. Consideriamo l'applicazione $f : A \times B \to B \times A$ definita da

$$\forall (a, b) \in A \times B,\ f((a, b)) = (b, a);$$

questa è, manifestamente, la biiezione richiesta. Si noti che, fissato $b \in B$, l'applicazione $f_b : A \times B \to A$ definita da $f_b((a, b)) = a$ è una biezione di $A \times \{b\}$ su A e, quindi, $f_b^{-1} : A \to A \times \{b\}$ è ancora una biiezione.

Esercizio 1.14.18. *Determinare l'immagine dell'applicazione $f : \mathbb{Z} \to \mathbb{Q}$, tale che, $\forall x \in \mathbb{Z}$, $f(x) = x/3$, e la controimmagine di ogni elemento di $\mathbb{Q}$.*

Sol. Si ha:

$$Imf = \left\{x' \in \mathbb{Q} : \left[x \in \mathbb{Z} : x' = x/3\right]\right\}.$$

Poiché $Imf \subset \mathbb{Q}$, f non è su. Infine, per ogni $x' \in Imf$, si ha:

$$f^{-1}(x') = 3x' = x,$$

onde f non è iniettiva.

Esercizio 1.14.19. *Sia S un qualunque insieme e sia $P(S)$ l'insieme delle parti di S. Si consideri l'applicazione $f : S \to P(S)$, definita da $\forall a \in S, f(a) = \{a\}$ e si determini Imf. Si dica inoltre se f è suriettiva, ovvero iniettiva.*

Sol. Dalla definizione di f, segue che Imf è costituito da quegli elementi di $P(S)$ che sono i s.i. di S contenenti un solo elemento (di S), onde $Imf \subset P(S)$. D'altra parte, ogni elemento $\{a\}$ di Imf individua univocamente l'elemento $a \in S$; pertanto, la controimmagine di ogni elemento di Imf è ridotta ad un solo elemento. Quindi f è un'applicazione iniettiva.

Esercizio 1.14.20. *Sia S un insieme finito. Si provi che un'applicazione $f : S \to S$ è iniettiva sse è suriettiva.*

Sol. Sia f iniettiva. Allora $a \neq b$ implica $f(a) \neq f(b)$. Quindi, per la definizione di applicazione, $Imf = S$, onde f è su. Viceversa, se f è su, per ogni x, si ha che $Imf = S$, $f^{-1}(x) \neq \emptyset$ e se $f^{-1}(x)$ contenesse più di un elemento, esisterebbe qualche elemento di S con più di un'immagine, contraddizione. Si noti che l'ipotesi che S sia finito è essenziale (cfr. n. 18). Precisamente, si può assumere l'enunciato ora provato come una caratterizzazione degli insiemi finiti. Inoltre, è molto facile mostrare che essa non è vera per gli insiemi infiniti. Ad esempio, sia $S = \mathbb{N}$ e sia $f : \mathbb{N} \to \mathbb{N}$ definita da

$$\forall n \in \mathbb{N},\ f(n) = 2n.$$

f è manifestamente iniettiva, ma non è su perché Imf è l'insieme dei numeri pari, cioè un insieme propriamente contenuto in $\mathbb{N}$.

Esercizio 1.14.21. *Sia $(A_i; i \in I)$ una partizione dell'insieme S. Resta allora individuata l'applicazione $p : S \to (A_i : i \in I)$, tale che*

$$\forall x \in S, x \in A_i, p(x) = A_i.$$

Si dica se p è suriettiva, ovvero iniettiva, e si determini la controimmagine di ciascun elemento di Imp.

Sol. L'applicazione p è su, in quanto $(A_i : i \in I)$ è una partizione di S e quindi ogni elemento di S appartiene ad esattamente un insieme della famiglia, onde $p^{-1}(A_i) \neq \emptyset$ per ogni A_i della famiglia.

Se gli insiemi A_i della famiglia non sono tutti ridotti ad un solo elemento, allora p non è iniettiva, dato che la controimmagine di A_i è costituita da tutti gli $x \in S$ tali che $x \in A_i$.

Se invece ciascun A_i della famiglia contiene un solo elemento, p è iniettiva e quindi biiettiva.

Esercizio 1.14.22. *Sia C l'insieme dei cerchi di un piano aventi raggio di lunghezza razionale, $\mathbb{Q}$ l'insieme dei numeri razionali, $\mathbb{R}$ l'insieme dei numeri reali. Si consideri l'applicazione $f : C \to \mathbb{R}$ definita da*

$$\forall x \in C, f(x) = x',$$

con x' misura dell'area del cerchio x. Si provi che f non è né iniettiva né suriettiva e si mostri che Imf non contiene alcun elemento di $\mathbb{Q}$.

Sol. Cominciamo con l'osservare che, se $r \in \mathbb{Q}$ è il raggio di $x \in C$, la misura dell'area di x è $x' = \pi r^2$; ne segue che

$$Imf = \left\{ y \in \mathbb{R} : \left[\exists r \in \mathbb{Q} : y = \pi r^2 \right] \right\}.$$

L'applicazione f non è iniettiva, in quanto esistono cerchi distinti aventi la stessa misura dell'area. La f non è suriettiva, perché $Imf \subset \mathbb{R}$ (infatti, per es., $1 \notin Imf$, in quanto non può essere $\pi = 1/r^2$, con r razionale). Infine ogni elemento di Imf, contenendo π come fattore, è manifestamente non razionale.

Esercizio 1.14.23. *Sia C l'insieme dei punti di una circonferenza e d l'insieme dei punti di un suo diametro fissato. Si consideri l'applicazione $f : C \to d$, che ad ogni punto $P \in C$ associa la sua proiezione ortogonale $P' \in d$. Si determini Imf e la controimmagine di ogni $P' \in d$; se ne deduca che f è suriettiva, ma non biiettiva.*

Sol. f è un'applicazione suriettiva; infatti, Imf è costituita dall'intero diametro d. Inoltre, la controimmagine di ogni elemento $P' \in d$ è costituita dai due punti di C, estremi della corda per P' ortogonale a d.

Esercizio 1.14.24. *Si provi che l'applicazione $f : \mathbb{N} \to \mathbb{N}$ definita da*

$$f(n) = n^2, \forall\, n \in \mathbb{N}$$

è iniettiva, ma non biiettiva.

Sol. f è iniettiva in quanto

$$f(n) = f(m) \Rightarrow n^2 = m^2 \Rightarrow n = m.$$

f non è su, dato che non tutti gli elementi di $\mathbb{N}$ sono quadrati (ad es., 2 non è un quadrato in $\mathbb{N}$, onde $f^{-1}(2) = \emptyset$).

Esercizio 1.14.25. *Dati i due insiemi $S = \{a, b, c\}$ ed $S' = \mathbb{N}$, si caratterizzino le applicazioni iniettive, suriettive e biiettive di S in S'.*

Sol. Sia f la generica applicazione di S in S'. Poiché S contiene esattamente tre elementi, Imf contiene al più tre elementi. Pertanto, dato che $S'(= \mathbb{N})$ contiene più di tre elementi, non esiste alcuna biiezione di S su S'.

Se Imf contiene esattamente tre elementi distinti, la controimmagine di ciascuno di essi è costituita da un solo elemento, onde f è iniettiva e manifestamente biiettiva di S su Imf.

Se, invece, Imf contiene due, od un solo, elementi, allora f è suriettiva tra S ed Imf, ma non iniettiva tra gli stessi insiemi.

Esercizio 1.14.26. *Si consideri l'insieme $S = \{a_1, a_2, \ldots, a_n\}$ e sia f una applicazione suriettiva di S in sé. Si dimostri che f è biiettiva.*

Sol. Per ipotesi, si ha $Imf = S$. Si tratta di provare che f è iniettiva, cioè che

$$f^{-1}(a_i) = a_j,\ i, j = 1, 2, \ldots, n$$

(ossia la controimmagine di ciascun elemento è ridotta ad un solo elemento). Gli insiemi $f^{-1}(a_i), i = 1, 2, \ldots, n$, sono non vuoti (perché f è suriettiva) e privi di elementi in comune (infatti, se $f^{-1}(a_i)$ ed $f^{-1}(a_j)$, $i \neq j$, avessero in comune un elemento a_k, $k = 1, 2, \ldots, n$, si avrebbe

$$f(a_k) = a_i,\ f(a_k) = a_j,$$

con $a_i \neq a_j$, e ciò contraddice la definizione di applicazione). Poiché $f(S) = S$, ogni insieme $f^{-1}(a_i)$ consta di un solo elemento, cioè l'asserto (cfr. es. 1.14.20).

Esercizio 1.14.27. *Sia S un insieme qualsiasi e sia $S' = \{a'\}$ un insieme contenente un solo elemento. Si dica quante e quali sono le applicazioni di S in S'.*

Sol. Poiché S' contiene un solo elemento, l'unica applicazione di S in S' è l'applicazione costante f, che associa ad ogni elemento di S l'elemento a' di S'. Una tale applicazione è una suriezione se S contiene più di un elemento, una biiezione se S contiene soltanto un elemento (cfr. es. 1.14.16).

Esercizio 1.14.28. *Dati i tre insiemi $S = \mathbb{Z}$, $S' = \mathbb{N} - \{0\}$, $S'' = \{n \in S' : [\exists m \in S' : n = m^2]\}$, si considerino le due applicazioni*

$$f : x \in \mathbb{Z} \to |x| + 1 \in S' \text{ e } g : n \in S' \to n^2 \in S''.$$

Si determinino l'applicazione prodotto $g \circ f$ e la sua immagine.

Sol. Dalle definizioni di f e g, segue che

$$g \circ f(x) = g(f(x)) = g(|x| + 1) = (|x| + 1)^2 \in S''.$$

Innanzitutto, si ha $Imf = S'$, onde f è suriettiva. Ne segue, essendo Imf il dominio di g, che $Img = Im(g \circ f)$.

Se invece $S' = \mathbb{N}$, anche S'' contiene lo zero; però Img non contiene lo zero. D'altra parte, S'' è l'insieme dei quadrati degli interi; ne segue che $Img = S'' - \{0\}$, onde g è iniettiva.

Pertanto g è biiettiva tra S' ed Img e, di conseguenza, $g \circ f$ è una suriezione di S su Img.

Esercizio 1.14.29. *Dati gli insiemi $S = \{x, y\}$ ed $S' = \{a, b, c\}$, si considerino le due applicazioni*

$$f : S \to S', \text{ tale che } f(x) = c, f(y) = a$$

e

$$g : S' \to S, \text{ tale che } g(a) = y, g(b) = y, g(c) = x.$$

Si determinino $g \circ f$ e $f \circ g$.

Sol. Si ha

$$g \circ f(x) = g(f(x)) = g(c) = x = e_S(x),$$

$$g \circ f(y) = g(f(y)) = g(a) = y = e_S(y).$$

Ne segue che $g \circ f = e_S$. D'altra parte, si ha:

$$f \circ g(a) = f(g(a)) = f(y) = a = e_{S'}(a);$$

$$f \circ g(b) = f(g(b)) = f(y) = a \neq e_{S'}(b);$$

$$f \circ g(c) = f(g(c)) = f(x) = c = e_{S'}(c);$$

pertanto $f \circ g \neq e_{S'}$. Tale risultato è conseguenza del fatto che f è iniettiva, mentre g è suriettiva.

Esercizio 1.14.30. *Siano $f : S \to S'$ e $g : S' \to S''$ due applicazioni. Si provi che $Im(g \circ f) \subseteq Img$.*

Sol. Per definizione di applicazione, $Imf \subseteq S'$; quindi, se f è su, g, definita su tutto S', è definita su tutto Imf, onde $Im(g \circ f) = Img$. D'altra parte, se f è iniettiva, cioè $Imf \subset S'$, esiste $x' \in S'$ Imf e quindi $g(x') \in Img$ (per definizione di applicazione), ma non si può affermare che $g(x') \in Im(g \circ f)$.

Esercizio 1.14.31. *Siano $f : S \to S'$ e $g : S' \to S''$ due applicazioni biiettive. Si dimostri che l'applicazione prodotto $g \circ f : S \to S''$ è biiettiva.*

Sol. Si deve dimostrare che $g \circ f$ è suriettiva e iniettiva. Dire che $g \circ f$ è suriettiva significa dire che $Im(g \circ f) = S''$, ovvero che $g \circ f(S) = S''$. Per ipotesi, $f(S) = S'$ e $g(S') = S''$; quindi $g \circ f(S) = g(S') = S''$, cioè $g \circ f$ è suriettiva.

Dire che $g \circ f$ è iniettiva significa dire che la controimmagine (in S) di ogni $x'' \in S''$ è ridotta ad un solo elemento. Siano $x' = f(x)$ ed $x'' = g(x')$. Fissato comunque $x'' \in S''$, la sua controimmagine, mediante g in S' è ridotta ad un solo elemento x', in quanto g è biietttiva; quindi la controimmagine, mediante f, di $x' \in S'$ è ridotta ad un solo elemento $x \in S$. Ne segue che $g \circ f$ è biiettiva.

Esercizio 1.14.32. *Dati i tre insiemi $S = \{a, b, c\}$, $S' = \{a', b', c'\}$, $S'' = \{x, y, z\}$, si verifichi che l'applicazione $g \circ f$, prodotto di*

$$f : S \to S', \textit{ tale che } f(a) = f(c) = a', f(b) = b'$$

e

$$g : S' \to S'', \textit{ tale che } g(a') = g(b') = x,$$

è un'applicazione costante.

Sol. Si ha

$$g \circ f(a) = g(a') = x,$$

$$g \circ f(b) = g(b') = x,$$

$$g \circ f(c) = g(a') = x;$$

onde l'asserto.

Esercizio 1.14.33. *Sia $f : S \to S'$ una biiezione. Si provi che $f^{-1} \circ f = e_S$ ed $f \circ f^{-1} = e_{S'}$, dove e_S ed $e_{S'}$ sono, rispettivamente, l'identità su S e su S'.*

Sol. Poiché f è una biiezione, $Imf = S'$ e

$$\forall x' \in S' \Rightarrow \exists! \, x \in S : x = f^{-1}(x').$$

Pertanto, per ogni $x \in S$, si ha

$$f^{-1} \circ f(x) = f^{-1}(f(x) = f^{-1}(x') = x = e_S(x) \Rightarrow f^{-1} \circ f = e_S.$$

Analogamente

$$f \circ f^{-1}(x') = f(f^{-1}(x') = f(x) = x' = e_S(x') \Rightarrow f \circ f^{-1} = e_{S'}.$$

Esercizio 1.14.34. *Siano $f : S \to S'$ un'applicazione di S in S' ed e_S, $e_{S'}$, rispettivamente, le identità su S e su S'. Si provi che*

$$f \circ e_S = f,$$

$$e_{S'} \circ f = f.$$

Sol. Sia x un qualunque elemento di S e sia $x' = f(x)$. Dimostrare che $f \circ e_S = f$, significa dimostrare che $f \circ e_S(x) = f(x)$, per ogni $x \in S$. Per definizione di prodotto di applicazioni, $f \circ e_S(x) = f(e_S(x))$; ma e_S è l'identità su S, quindi $e_S(x) = x$, onde l'asserto.

Similmente,

$$e_{S'} \circ f(x) = e_{S'}(f(x)) = e_{S'}(f(x)) = e_{S'}(x') = x' = f(x),$$

cioeè $e_{S'} \circ f = f$.

Esercizio 1.14.35. *Le due applicazioni $f : S \to S'$ e $g : S' \to S''$ ammettono le applicazioni inverse $f^{-1} : S' \to S$ e $g^{-1} : S'' \to S'$. Si dimostri che l'applicazione prodotto $g \circ f : S \to S''$ ammette l'applicazione inversa*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1} : S'' \to S.$$

Sol. Osserviamo innanzitutto che le applicazioni date sono biiettive, in quanto dotate di inverse. Si deve dimostrare, in virtù dell'es. 1.14.33, che

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = e_S$$

e che

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = e_{S''}.$$

Per ogni x di S poniamo:

$$x' = f(x) \in S', x'' = g(x') = g(f(x)) \in S''.$$

Poiché sia f che g sono dotate di applicazione inversa, sarà:

$$x = f^{-1}(x'), x' = g^{-1}(x'').$$

Fissato $x \in S$, avremo:

$$((f^{-1} \circ g^{-1}) \circ (g \circ f))(x) = ((f^{-1} \circ (g^{-1} \circ g) \circ f)(x)$$

$$= ((f^{-1} \circ e_{S'}) \circ f)(x) = (f^{-1} \circ e_{S'}) = f^{-1}(x') = x = e_S(x),$$

come conseguenza dell'associatività del prodotto e degli esercizi 1.14.33 e 1.14.34. La seconda affermazione si dimostra in maniera analoga.

Esercizio 1.14.36. *Siano S ed S' due insiemi e siano $f : S \to S'$ e $g : S' \to S$ due applicazioni tali che $g \circ f = e_S$. Si dimostri allora che f è iniettiva e g è suriettiva.*

Sol. Si deve provare che $Img = S$ e che la controimmagine, mediante f, di ogni elemento di $Imf \subseteq S'$ è ridotta ad un solo elemento. Dall'ipotesi $g \circ f = e_S$, segue $Im(g \circ f) = Ime_S = S$ (in quanto e_S è l'identità su S). D'altra parte, $Imf \subseteq S' \Rightarrow g(Imf) \subseteq S$. Dato che $g \circ f$ è la restrizione di g a Imf, si ha $Im(g \circ f) \subseteq Img$, ma , per definizione di immagine di un'applicazione, $Img \subseteq S$. Quindi $S \subseteq Img \subseteq S \Rightarrow Img = S$, onde g è suriettiva.

Proviamo ora che f è iniettiva. Sia $x' \in Imf$; esiste allora almeno un $x \in S$ tale che $x' = f(x)$; proviamo che x è unico. Supponiamo che esistano $x, y \in S, x \neq y$, tali che $x' = f(x), x' = f(y)$. Poiché g è un'applicazione di S' su S, soddisfacente alla condizione $g \circ f = e_S$, si ha:

$$g(x') = g(f(x)) = g \circ f(x) = e_S(x) = x,$$

$$g(x') = g(f(y)) = g \circ f(y) = e_S(y) = y,$$

il che contraddice la definizione di applicazione. Ne segue che f è iniettiva, quindi l'asserto.

Esercizio 1.14.37. *Siano S e S' due insiemi e siano $f : S \to S'$ e $g : S' \to S$ due applicazioni tali che $f \circ g = e_{S'}$. Si dimostri che allora g è iniettiva ed f è suriettiva.*

Sol. Segue dall'es. 1.14.36 scambiando il ruolo di S con quello di S' (e quindi il ruolo di f con quello di g).

Esercizio 1.14.38. *Dati i due insiemi S ed S', siano $f : S \to S'$ e $g : S' \to S$ due applicazioni tali che $g \circ f = e_S$ e $f \circ g = e_{S'}$. Si provi che allora f e g sono applicazioni biiettive.*

Sol. In virtù di quanto dimostrato nell'es. 1.14.36, f è iniettiva e g è suriettiva; come conseguenza dell'es. 1.14.37, g è iniettiva ed f è suriettiva. Ne segue che f e g sono entrambe biiettive, dato che sono sia iniettive che suriettive.

Esercizio 1.14.39. *Dati i due insiemi S ed S', siano $f : S \to S'$ e $g : S' \to S$ due applicazioni tali che $g \circ f = e_S$ e $f \circ g = e_{S'}$. Si provi che allora le due applicazioni sono l'una l'inversa dell'altra ($g = f^{-1}$).*

Sol. Innanzitutto, f e g sono entrambe biiettive (cfr. es 1.14.38), quindi ciascuna di esse ammette l'inversa. Sia f^{-1} l'inversa di f; si ha (cfr. es. 1.14.33) $f^{-1} \circ f = e_S$ ed $f \circ f^{-1} = e_{S'}$. Ne segue che le due applicazioni $f^{-1} \circ f$ e $g \circ f$ coincidono, in quanto, per ogni $x \in S$, si ha:

$$f^{-1} \circ f(x) = f^{-1}(f(x)) = f^{-1}(x') = e_S(x) = x$$

e

$$g \circ f(x) = g(f(x)) = g(x') = e_S(x) = x.$$

Similmente, coincidono $f \circ g$ ed $f \circ f^{-1}$. Si noti che, per assicuare che g sia l'inversa di f, sono necessarie entrambe le condizioni $g \circ f = e_S$ ed $f \circ g = e_{S'}$ (cfr. es. 1.14.36 e 1.14.37).

Rileviamo infine che le proposizioni provate negli es. 1.14.38 e 1.14.39 invertono la proposizione dell'esercizio 1.14.33, di modo che si ha:

Esercizio 1.14.40. *Condizione necessaria e sufficiente affinché due applicazioni $f : S \to S'$ e $g : S' \to S$ siano biiettive e l'una inversa dell'altra è che risulti $g \circ f = e_S$ ed $f \circ g = e_{S'}$.*

Esercizio 1.14.41. *Sia S un insieme qualsiasi e sia $A \subseteq S$. Si dimostri che l'applicazione $f : P(S) \to P(S)$, tale che, per ogni $A \in P(S)$, sia $f(A) = \mathcal{C}_S A$ è una biiezione e che $f \circ f = e_{P(S)}$.*

Sol. Osserviamo innanzitutto che, essendo $\mathcal{C}_S(\mathcal{C}_S A) = A$ per ogni $A \in P(S)$ (cfr. es. 1.14.3), ogni elemento di $P(S)$ è immagine di qualche elemento di $P(S)$, onde la f è suriettiva. D'altra parte, f è iniettiva, perché la controimmagine di $\mathcal{C}_S A \in P(S)$ è ridotta al solo elemento A di

$P(S)$; ne segue che f è una biiezione. Inoltre, per ogni $A \in P(S)$, si ha $f \circ f(A) = f(f(A)) = f(\mathcal{C}_S A) = \mathcal{C}_S(\mathcal{C}_S A) = A = e_{P(S)}(A)$, onde $f \circ f = e_{P(S)}(A)$, e quindi $f = f^{-1}$; infatti per definizione di applicazione inversa, $f \circ f^{-1} = e_{P(S)} = f^{-1} \circ f$.

Esercizio 1.14.42. *Si consideri l'applicazione $f : \mathbb{Z} \to \mathbb{Z}$ definita da*

$$f(x) = x^2, \forall x \in \mathbb{Z}.$$

Se $A = \mathbb{Z}^+$, si provi che la restrizione di f_A di f ad A è tale che $Imf_A = Imf$.

Sol. Evidentemente, Imf è il sottoinsieme di $\mathbb{Z}$ costituito dagli interi positivi che siano quadrati. La controimmagine di ogni $x' \in Imf$ è costituita dai due interi $+x$ e $-x$, tali che $x^2 = x'$. Poiché A è il sottoinsieme di $\mathbb{Z}$ costituito dagli interi positivi o nulli, la restrizione di f ad A ha, manifestamente, la medesima immagine di f.

Esercizio 1.14.43. *Sia S un insieme qualunque e sia $A \subseteq S$; detta e_A la restrizione di e_S ad A (e_S è l'applicazione identica di S su se stesso), si provi che, per ogni $X \subseteq S$, $e_A^{-1}(X) = X \cap A$.*

Sol. Poiché $e_A^{-1}(X)$ è la controimmagine, mediante e_A, di $X \subseteq S$, se $X \subseteq A$, $e_A^{-1}(X) = X$; se $X \not\subseteq A$, ha significato soltanto la controimmagine, mendiante e_A, degli elementi di A che appartengono ad $Im(e_A) = A$, cioè degli elementi di $X \cap A \subseteq A$. Ne segue l'asserto, dato che $e_A(X \cap A) = X \cap A = e_A^{-1}(X \cap A)$, per definizione di applicazione identica.

Esercizio 1.14.44. *Si consideri l'applicazione $f : \mathbb{Z} \to \mathbb{Z}^+$ definita da*

$$\forall x \in \mathbb{Z}, f(x) = 3|x|.$$

Si determini un s.i. A di $\mathbb{Z}$, tale che la restrizione $f_{|A}$ di f ad A sia un'applicazione iniettiva di A in $\mathbb{Z}^+$.

Sol. Poiché Imf è costituito dai multipli (interi) non negativi del numero 3, e la controimmagine di ogni elemento di Imf è costituito da due interi tra loro opposti si può assumere come insieme A l'insieme $\mathbb{Z}^+$. Infatti, per ogni $x \in \mathbb{Z}^+$, si ha $|x| = x$ e quindi, per ogni $x' \in Imf, x = x'/3 \in A$. Si noti che ogni insieme contenuto in A gode della medesima proprietà.

Esercizio 1.14.45. *Sia $f : S \to S'$ un'applicazione iniettiva e sia $A \subseteq S$. Si dimostri che anche $f_{|A}$, restrizione di f ad A, è iniettiva.*

Sol. Per definizione di applicazione iniettiva, la controimmagine, mediante f, di ogni $x' \in Imf$ è ridotta ad un solo elemento. Dato che f coincide con $f_{|A}$, se $x \in A \subseteq S$, e dato che $Imf_A \subseteq Imf$, se $x' \in Imf_A$, la sua controimmagine, mediante $f_{|A} = f$, è ancora ridotta ad un solo elemento, onde l'asserto.

Esercizio 1.14.46. *Sia $f : S \to S'$ un'applicazione suriettiva e sia A un s.i. di S. Dimostrare , con un esempio, che $f_{|A}$, restrizione di f ad A può essere biiettiva, senza che lo sia f.*

Sol. Una costruzione di carattere generale di un s.i. del tipo richiesto si può ottenere nella maniera seguente. Sia $x' \in Imf = S'$. Consideriamo il s.i. B di S, eventualmente vuoto, costituito da tutti gli $x \in S$, tali che, posto $x' = f(x)$, la controimmagine di x' sia ridotta a un solo elemento. Assunto $A = B$, si ha, manifestamente, che $f_{|A}$ è biiettiva tra A ed $Imf_{|A}$, quale che sia f. Si noti che, se f non è suriettiva, sostituendo Imf a S', il procedimento esposto fornisce una biiezione di A su $Imf_{|A}$. Un altro procedimento per costruire A è il seguente. Per ogni $x' \in Imf = S'$ si scelga (e con ciò si ammette il postulato di Zermelo) un ben determinato $x \in f^{-1}(x')$; l'insieme A, costituito dagli elementi così fissati, soddisfa il problema.

Sia, ad es., $S = S' = \mathbb{N}$, con $\mathbb{N}$ insieme dei numeri naturali; consideriamo l'applicazione $f : \mathbb{N} \to \mathbb{N}$, definita da

$$f(x) = x, \text{ se } x \text{ è pari; } f(x) = 1, \text{ se } x \text{ è dispari.}$$

Ovviamente, f non è biiettiva, perché la controimmagine di 1 è costituita da tutti i numeri dispari; Imf è costitutita da tutti i numeri pari e dal numero 1. Assumiamo come $A \subseteq \mathbb{N}$ l'insieme dei numeri pari; la restrizione della f suddefinita ad A coincide allora con l'identità su A, onde è una biiezione di A su $Imf_{|A}$.

Esercizio 1.14.47. *Sia S l'insieme dei numeri reali, e sia $S' = \{x' \in \mathbb{R} : -1 \leq x' \leq 1\}$. Si consideri l'applicazione $f : S \to S'$, definita da*

$$f(x) = senx = x', \forall x \in S.$$

Si determinino i s.i. A di S, tali che la restrizione di f ad A, $f_{|A}$, sia una biiezione di A su S'.

Sol. Osserviamo innanzitutto che f è manifestamente una suriezione e la controimmagine di ogni $x' \in S' = Imf$ è data da

$$f^{-1}(x') = \{y \in S : y = x + 2k\pi, k \in \mathbb{Z}, senx = x'\}.$$

Pertanto, l'insieme $A = \{x \in S : -\pi/2 \leq x \leq \pi/2\}$ è uno degli insiemi per i quali $f_{|A} : A \to S'$ è una biiezione. Infatti, per ogni $x' \in S'$, esiste, ed è unico, l'elemento $x \in A$, tale che $senx = x'$. Gli altri $s.i.$ di S che godono della stessa proprietà di A sono i s.i.

$$B_h = \{x \in \mathbb{R} : h\pi/2 \leq x \leq (h+2)\pi/2, h \in \mathbb{Z}\}$$

(evidentemente $A = B_{-1}$). Si noti che ogni s.i. di B_h è tale che la restrizione di f ad esso è un'applicazione iniettiva di B_h in S'.

Esercizio 1.14.48. *Sia* $S = \{x \in \mathbb{Q} : 1 \leq x \leq 9\}$ *e sia* $S' = \{1, 1/2\}$. *Si consideri l'applicazione* $f : S \to S'$, *definita da*

$$f(x) = 1, \text{ se } x \text{ è intero}; f(x) = 1/2, \text{ se } x \text{ non è intero}.$$

Si dica se f *è iniettiva, oppure suriettiva, e si determinino i s.i.* A *di* S *tali che la restrizione di* f *ad* A *sia una biiezione.*

Sol. L'applicazione f è suriettiva, in quanto $Imf = S'$, in conseguenza della definizione di f. Inoltre, f non è iniettiva, perché la controimmagine di $1 \in S'$ è l'insieme $\{1, 2, 3, \ldots, 9\} \subset S$. I sottoinsiemi A di S, tali che $f_{|_A} : A \to S'$ sia una biiezione, sono manifestamente tutti i sottoinsiemi di S, contenenti esattamente due elementi, uno dei quali intero e l'altro razionale non intero.

Esercizio 1.14.49. *Si consideri l'applicazione* $f : \mathbb{R}^+ \to \mathbb{R}^+$ *, definita da:*

$$f(x) = \sqrt{x}, \forall x \in \mathbb{R}^+.$$

Si determini il s.i. A *di* $\mathbb{R}^+$ *tale che la restrizione* $f_{|_A}$ *ad* A *coincida con l'identità su* A.

Sol. Per definizione di restrizione di un'applicazione, $f_{|_A} = f(x), \forall x \in A$. Affinché sia $f_{|_A}(x) = e_A(x) = x$, deve essere $\sqrt{x} = x$, onde $x = 1$, oppure $x = 0$; ne segue $A = \{0, 1\}$.

Esercizio 1.14.50. *Sia* S *un insieme,* A *un s.i. di* S, e_A *la restrizione di* e_S *(identità su* S*) ad* A. *Se* $f : S \to S'$ *è un'applicazione di* S *in* S', *si dimostri che*

$$f_{|_A} = f \circ e_A.$$

Sol. Si ha $f : S \to S'$, $f_{|_A} : A \to S'$, $e_A : A \to S$, $e_S : S \to S$, $f \circ e_A : A \to S'$. Allora, per ogni $x \in A$, risulta $f_{|_A}(x) = f(x) \in S'$, $f \circ e_A(x) = f(x)$, onde l'asserto.

Esercizio 1.14.51. *Siano* $f : A \to A'$ *e* $g : B \to B'$ *due applicazioni. Si provi che allora resta univocamente definita una applicazione*

$$f \times g : A \times B \to A' \times B'$$

da dirsi applicazione prodotto cartesiano di f *per* g.

Sol. Definiamo $f \times g$ nel modo seguente:

$$\forall (a, b) \in A \times B, f \times g((a, b)) = (f(a), g(b))$$

e proviamo che $f \times g$ è di fatto un'applicazione. Poiché f, g sono applicazioni,

$$\forall a \in A, \forall b \in B \Rightarrow \exists! f(a) \in A', g(b) \in B',$$

quindi $f \times g$ è un'applicazione.

Esercizio 1.14.52. *Siano $f : A \to A'$ e $g : B \to B'$ due applicazioni; si verifichi che $Im(f \times g) = Imf \times Img$.*

Sol. Per definizione di immagine,

$$Im(f \times g) = \{(a', b') \in A' \times B' : [\exists (a, b) \in A \times B : (a', b') = (f \times g)(a, b)]\}.$$

Per definizione di $f \times g$ (cfr. es 1.14.51),

$$Im(f \times g) = \{(a', b') \in A' \times B' : [\exists (a, b) \in A \times B : (a', b') = (f(a), g(b))]\}.$$

Ne segue l'asserto.

Esercizio 1.14.53. *Siano $f : A \to A'$ e $g : B \to B'$ due applicazioni; si provi che $f \times g$ è su sse sia f che g sono suriettive.*

Sol. Siano f e g su, cioè $Imf = A'$, $Img = B'$; allora $Imf \times Img = Im(f \times g) = A' \times B'$, ossia $f \times g$ è su. Viceversa, se $Im(f \times g) = A' \times B'$, si ha $Im(f \times g) = A' \times B' = Imf \times Img \Rightarrow Imf = A', Img = B'$, cioè f e g sono su.

Esercizio 1.14.54. *Siano $f : A \to A'$ e $g : B \to B'$ due applicazioni. Si provi che $f \times g$ è iniettiva sse f e g sono entrambe iniettive.*

Sol. Se f e g sono entrambe iniettive, $\forall a' \in Imf, \exists! a \in A : a' = f(a)$, $\forall b' \in Img, \exists! b \in A : b' = f(b)$. Quindi, $\forall (a', b') \in Im(f \times g), \exists! (a, b) \in A \times B : (a', b') = (f(a), g(b))$, cioè $f \times g$ è iniettiva. Il viceversa si prova invertendo i passaggi.

Esercizio 1.14.55. *Siano $f : A \to A'$ e $g : B \to B'$ due applicazioni. Si provi che $f \times g$ è una biiezione sse f e g sono entrambe biiezioni.*

Sol. E' diretta conseguenza di quanto provato negli esercizi 1.14.53 e 1.14.54, dato che una biiezione è un'applicazione iniettiva e su.

Capitolo 2

Il teorema fondamentale delle applicazioni

Abbiamo visto quando si può definire il prodotto di due o più applicazioni ed abbiamo constatato che esso risulta ancora una applicazione; inoltre, abbiamo esaminato alcune applicazioni particolari (suriettiva, iniettiva, biiettiva). Vogliamo ora risolvere il problema inverso della composizione di più applicazioni; precisamente, provare che ogni applicazione si può decomporre nel prodotto di più applicazioni di tipo particolare. A tale scopo premettiamo alcuni risultati fondamentali.

Proposizione 2.0.5. *Sia $f : S \to S'$ un'applicazione di S in S'. Allora f definisce univocamente una relazione di equivalenza $\mathcal{E}_f$ su S qualora si ponga*

$$\forall x, y \in S,\ (x, y) \in \mathcal{E}_f \Leftrightarrow f(x) = f(y).$$

Dim. Dato che f è una applicazione, $\forall x \in S \Rightarrow \exists! f(x) \in S'$, onde $\mathcal{E}_f$ è una relazione su S. Proviamo che $\mathcal{E}_f$ è un'equivalenza. $\mathcal{E}_f$ è riflessiva; infatti: $\forall x \in S,\ f(x) = f(x) \Rightarrow (x, x) \in \mathcal{E}_f$. $\mathcal{E}_f$ è simmetrica; infatti $\forall x, y \in S, (x, y) \in \mathcal{E}_f \Rightarrow f(x) = f(y) \Rightarrow f(y) = f(x) \Rightarrow (y, x) \in \mathcal{E}_f$. Infine, $\mathcal{E}_f$ è transitiva; infatti: $(x, y), (y, z) \in \mathcal{E}_f \Rightarrow f(x) = f(y)$ e $(f(y) = f(z) \Rightarrow f(x) = f(z) \Rightarrow (x, z) \in \mathcal{E}_f$.

Ne discende immediatamente il:

Corollario 2.0.6. *Sse l'applicazione $f : S \to S'$ è iniettiva, l'equivalenza $\mathcal{E}_f$ da essa definita è la relazione identica su S.*

Dim. Supponiamo che sia iniettiva; allora $f(x) = f(y) \Rightarrow x = y$. Pertanto:

$$[\forall x, y \in S, (x, y) \in \mathcal{E}_f \Leftrightarrow f(x) = f(y)] \Rightarrow$$
$$\Rightarrow [\forall x, y \in S, (x, y) \in \mathcal{E}_f \Leftrightarrow x = y] \Rightarrow \mathcal{E}_f = \Delta_S.$$

Viceversa, se $\mathcal{E}_f = \Delta_S$, si ha

$$f(x) = f(y) \Rightarrow (x, y) \in \Delta_S \Rightarrow x = y,$$

onde f è iniettiva.

La Proposizione 2.0.5 si può - in un certo senso - invertire. Sussiste infatti la:

Proposizione 2.0.7. *Sia $\mathcal{E}$ una relazione di equivalenza sull'insieme S. Allora $\mathcal{E}$ individua univocamente una applicazione di S su $S/\mathcal{E}$, che prende il nome di applicazione naturale definita da $\mathcal{E}$ (od associata ad $\mathcal{E}$), e che viene denotata con $nat\mathcal{E}$,*

$$nat\mathcal{E} : S \to S/\mathcal{E},$$

quando si ponga

$$nat\mathcal{E}(x) = [x]\mathcal{E}.$$

Dim. Dobbiamo provare che $nat\mathcal{E}$ è un'applicazione e che è suriettiva. Poiché $\mathcal{E}$ è un'equivalenza su S, ogni $x \in S$ appartiene ad una ed una sola classe di equivalenza rispetto ad $\mathcal{E}$, $[x]\mathcal{E}$. Quindi $nat\mathcal{E}$ è una applicazione. Proviamo ora che $nat\mathcal{E}$ è su, cioè che $Im(nat\mathcal{E}) = S/\mathcal{E}$; ciò significa che esiste la controimmagine di ogni elemento di $S/\mathcal{E}$. Sia $[x] \in S/\mathcal{E}$; dato che $[x]$ contiene almeno l'elemento x, $nat\mathcal{E}^{-1}([x])$ contiene almento x, onde $nat\mathcal{E}$ è su, e l'affermazione è provata.

Al fine di pervenire al teorema fondamentale delle applicazioni, proviamo la

Proposizione 2.0.8. *L'inclusione insiemistica è un'applicazione iniettiva.*

Dim. Sia $S \subseteq S'$; allora $\Delta_S \subseteq S \times S'$, quindi Δ_S è una corrispondenza da S verso S' ed è l'identità su S. Proviamo che Δ_S è una applicazione iniettiva di S in S'. Per definizione

$$\Delta_S = \{(x, x) : x \in S\}.$$

Ne segue che $D(\Delta_S) = S$; inoltre $Im\Delta_S = S$ e

$$\forall x \in Im\Delta_S, \exists! x : (x, x) \in \Delta_S;$$

quindi Δ_S è un'applicazione ed è iniettiva. Scriveremo i_S in luogo di Δ_S ed avremo:

$$i_S : S \to S',$$

definita da

$$\forall x \in S, i_S(x) = x$$

(e ciò implica $x \in S'$, dato che $S \subseteq S'$).

Siamo ora in grado di enunciare e provare il

Teorema fondamentale delle applicazioni: sia $f : S \to S'$ una applicazione di S in S'; allora f è il prodotto, nell'ordine, di una suriezione, $nat\mathcal{E}_f : S \to S/\mathcal{E}_f$ di una biiezione $\beta : S/\mathcal{E}_f \to Imf$ e di una immersione $i : Imf \to S'$. Brevemente, ciò si riassume dicendo che è commutativo il seguente diagramma:

$$\begin{array}{ccc} S & \xrightarrow{f} & S' \\ {\scriptstyle nat\mathcal{E}_f}\downarrow & & \uparrow{\scriptstyle i} \\ S/\mathcal{E}_f & \xrightarrow{\beta} & Imf \end{array}$$

(dire che il diagramma è commutativo, significa che si può andare da S a S' seguendo l'una o l'altra delle strade indicate dalle frecce).

Dim. Dato che $\mathcal{E}_f$ è un'equivalenza (l'equivalenza su S definita da f, cfr. Prop 2.0.5), per la Prop. 2.0.7, $nat\mathcal{E}_f$ è una applicazione di S su $S/\mathcal{E}_f$. Poiché $Imf \subseteq S'$, l'inclusione insiemistica $i : Imf \to S'$ è una immersione (applicazione iniettiva, cfr. Prop. 2.0.8).

Definiamo ora

$$\beta : S/\mathcal{E}_f \to Imf,$$

nel modo seguente:

$$\forall [x]\mathcal{E}_f \in S/\mathcal{E}_f, \beta([x]\mathcal{E}_f) = f(x).$$

β è evidentemente un'applicazione. Proviamo che è iniettiva e su. Si ha:

$$f(x) = f(y) \Rightarrow (x, y) \in \mathcal{E}_f \Rightarrow y \in [x]\mathcal{E}_f, x \in [y]\mathcal{E}_f \Rightarrow [x]\mathcal{E}_f = [y]\mathcal{E}_f,$$

onde β è iniettiva. Inoltre, β è su, per definizione di Imf, cioè la controimmagine di ogni $f(x) \in Imf$ è non vuota. Quindi β è una biiezione.

Proviamo infine che

$$f = i \circ \beta \circ nat\mathcal{E}_f.$$

Per ogni $x \in S$ si ha

$$i \circ \beta \circ nat\mathcal{E}_f(x) = i \circ \beta(nat\mathcal{E}_f(x)) = i \circ \beta([x]\mathcal{E}_f) = i(\beta([x]\mathcal{E}_f)) = i(f(x)) = f(x),$$

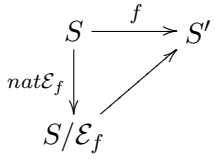
in quanto l'inclusione insiemistica i è l'identità su Imf. Il teorema è così completamente provato.

Tenendo presente il Cor. 2.0.6, se $f : S \to S'$ è iniettiva, è commutativo il diagramma:

$$\begin{array}{ccc} S & \xrightarrow{f} & S' \\ & {\scriptstyle \beta}\searrow & \uparrow{\scriptstyle i} \\ & & Imf \end{array}$$

$nat\mathcal{E}_f$ essendo, in questo caso, l'identità su S, ed $f = i \circ \beta$; inoltre $\beta = f_{|Imf}$.

Se invece $f : S \to S'$ è su, risulta commutativo il diagramma



ed $f = \beta \circ nat\mathcal{E}_f$.

Infine, se f è una biiezione, $nat\mathcal{E}_f$ è l'identità su S, i è l'identità su S' e $\beta = f$, cioè $f = e_{S'} \circ \beta \circ e_S$, ed il diagramma si siduce a

$$S \xrightarrow{f} S'.$$

Diamo ora un esempio della decomposizione fornita dal teorema fondamentale delle applicazioni. Siano

$$S = \{a, b, c, d, h, k, m, n\}, \quad S' = \{x, y, z, t, u, v, w\}$$

e l'applicazione $f : S \to S'$ sia definita da

$$f(a) = x,\ f(b) = z,\ f(c) = y,\ f(d) = z,$$

$$f(h) = x,\ f(k) = x,\ f(m) = t,\ f(n) = y.$$

Determiniamo innanzitutto $\mathcal{E}_f$, ricordando che $\mathcal{E}_f \supseteq \Delta_S$, dato che è una equivalenza. Avremo:

$$\mathcal{E}_f = \Delta_S \cup \{(a,h),(h,a),(a,k),(k,a),(h,k),(k,h),(b,d),(d,b),(c,n),(n,c)\}.$$

Quindi, gli elementi di $S/\mathcal{E}_f$, cioè le classi di equivalenza sono:

$$[a] = \{a, h, k\} = [h] = [k],$$

$$[b] = \{b, d\} = [d],$$

$$[c] = \{c, n\} = [n],$$

$$[m] = \{m\}.$$

Siamo ora in grado di costruire $\beta : S/\mathcal{E}_f \to Imf$, dato che $Imf = \{x, y, z, t\}$; precisamente

$$\beta([a]) = x,\ \beta([b]) = z, \beta([c]) = y, \beta([m]) = t.$$

Infine, $i : Imf \to S'$ è definita da

$$i(x) = x,\ i(z) = z, i(y) = y,\ i(t) = t.$$

Riassumendo, avremo per tutti gli elementi di S, i seguenti passaggi:

$$\begin{array}{ccccccc}
a & \overset{nat\mathcal{E}_f}{\longrightarrow} & [a] & \overset{\beta}{\longrightarrow} & x & \overset{i}{\longrightarrow} & x \\
b & \overset{nat\mathcal{E}_f}{\longrightarrow} & [b] & \overset{\beta}{\longrightarrow} & z & \overset{i}{\longrightarrow} & z \\
c & \overset{nat\mathcal{E}_f}{\longrightarrow} & [c] & \overset{\beta}{\longrightarrow} & y & \overset{i}{\longrightarrow} & y \\
d & \overset{nat\mathcal{E}_f}{\longrightarrow} & [b] & \overset{\beta}{\longrightarrow} & z & \overset{i}{\longrightarrow} & z \\
h & \overset{nat\mathcal{E}_f}{\longrightarrow} & [a] & \overset{\beta}{\longrightarrow} & x & \overset{i}{\longrightarrow} & x \\
k & \overset{nat\mathcal{E}_f}{\longrightarrow} & [a] & \overset{\beta}{\longrightarrow} & x & \overset{i}{\longrightarrow} & x \\
m & \overset{nat\mathcal{E}_f}{\longrightarrow} & [m] & \overset{\beta}{\longrightarrow} & t & \overset{i}{\longrightarrow} & t \\
n & \overset{nat\mathcal{E}_f}{\longrightarrow} & [c] & \overset{\beta}{\longrightarrow} & y & \overset{i}{\longrightarrow} & y
\end{array}$$

Esercizio 2.0.56. *Si consideri l'applicazione $f : S \to S'$, con $S = \mathbb{Z}_{24} = \{\overline{0}, \overline{1}, \ldots, \overline{23}\}$, $S' = \mathbb{Z}_{12} = \{\overline{0}', \ldots, \overline{11}'\}$ (dove i soprassegni, con e senza apice, denotano le classi resto rispettivamente mod 12 e mod 24, per semplicità di scrittura) definita da:*

$$\begin{array}{c}
f(\overline{0}) = f(\overline{3}) = f(\overline{6}) = f(\overline{9}) = f(\overline{12}) = \ldots = f(\overline{21}) = \overline{0}'; \\
f(\overline{1}) = f(\overline{4}) = f(\overline{7}) = f(\overline{10}) = f(\overline{13}) = \ldots = f(\overline{22}) = \overline{1}'; \\
f(\overline{2}) = f(\overline{5}) = f(\overline{8}) = f(\overline{11}) = f(\overline{14}) = \ldots = f(\overline{23}) = \overline{8}'
\end{array}$$

e si scriva per essa la decomposizione fornita dal teorema fondamentale delle applicazioni.

Sol. In base alla definizione di f, l'equivalenza da essa definita, $\mathcal{E}_f \subseteq S \times S$, individua le seguenti classi:

$$\left[\overline{0}\right] = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \ldots, \overline{21}\},$$

$$\left[\overline{1}\right] = \{\overline{1}, \overline{4}, \overline{7}, \overline{10}, \ldots, \overline{22}\},$$

$$\left[\overline{2}\right] = \{\overline{2}, \overline{5}, \overline{8}, \overline{11}, \ldots, \overline{23}\},$$

che sono gli elementi di $S/\mathcal{E}_f$. Pertanto, $nat\mathcal{E}_f : S \to S/\mathcal{E}_f$ opera nel modo seguente:

$$\begin{array}{c}
nat\mathcal{E}_f(\overline{0}) = nat\mathcal{E}_f(\overline{3}) = nat\mathcal{E}_f(\overline{6}) = \ldots = nat\mathcal{E}_f(\overline{21}) = [\overline{0}], \\
nat\mathcal{E}_f(\overline{1}) = nat\mathcal{E}_f(\overline{4}) = nat\mathcal{E}_f(\overline{7}) = \ldots = nat\mathcal{E}_f(\overline{22}) = [\overline{1}], \\
nat\mathcal{E}_f(\overline{2}) = nat\mathcal{E}_f(\overline{5}) = nat\mathcal{E}_f(\overline{8}) = \ldots = nat\mathcal{E}_f(\overline{23}) = [\overline{2}].
\end{array}$$

Quindi, la biiezione β è definita da

$$\beta([\overline{0}]) = \overline{0}',\ \beta([\overline{1}]) = \overline{4}',\ \beta([\overline{2}]) = \overline{8}',$$

essendo $\beta : S/\mathcal{E}_f \to Imf$. Infine, l'immersione $j : Imf \to S'$ è data da

$$j(\overline{0}') = \overline{0}',\ j(\overline{1}') = \overline{1}',\ j(\overline{8}') = \overline{8}',$$

cioè $j = e_{S'|Imf}$.

Esercizio 2.0.57. *Siano $S = \{a, b, c, d, g, h, k\}$ ed $S' = \{x, y, z, t\}$ due insiemi. Si costruisca un'equivalenza $\mathcal{E}$ su S in modo tale che esista una biiezione di $S/\mathcal{E}$ su S'. Si determini $nat\mathcal{E}$ e si costruisca l'applicazione $f : S \to S'$ tale che $f = \beta \circ nat\mathcal{E}$.*

Sol. Poiché l'insieme S' contiene quattro elementi, l'equivalenza $\mathcal{E} \subseteq S \times S$ deve essere tale che $S/\mathcal{E}$ contenga esattamente quattro elementi (cioè quattro classi di equivalenza). Ovviamente, una qualunque partizione di S in quattro insiemi (disgiunti!) individua un'equivalenza che soddisfa la condizione richiesta. Ad esempio, scegliamo $\mathcal{E}$ definita dalle classi

$$[a] = \{a, g\},\ [b] = \{b, c\},\ [d] = \{d, h\},\ [k] = \{k\}.$$

Allora $nat\mathcal{E} : S \to S/\mathcal{E}$ è definita da

$$nat\mathcal{E}(a) = a,\ nat\mathcal{E}(b) = b,\ nat\mathcal{E}(c) = b,\ nat\mathcal{E}(d) = d,$$
$$nat\mathcal{E}(g),\ nat\mathcal{E}(h) = d,\ nat\mathcal{E}(k) = k.$$

Si può, quindi, assumere come biiezione $\beta : S/\mathcal{E} \to S'$ la seguente:

$$\beta([a]) = x,\ \beta([b]) = y,\ \beta([d]) = z,\ \beta([k]) = t$$

(si noti che esistono $4! = 24$ biiezioni possibili). Pertanto, l'applicazione $f : S \to S'$ tale che $f = \beta \circ nat\mathcal{E}$ è definita da

$$f(a) = f(g) = x,\ f(b) = f(c) = y,\ f(d) = f(h) = z,\ f(k) = t.$$

Esercizio 2.0.58. *Si provi che, fissato $m \geq 2$, esiste un'applicazione f di $\mathbb{Z}$ su $\mathbb{Z}_m$ (insieme delle classi resto mod m).*

Sol. Per definizione, $\mathbb{Z}_m$ è l'insieme quoziente di $\mathbb{Z}$ modulo la congruenza mod m, che è un'equivalenza $\mathcal{E}$ su $\mathbb{Z}$. Pertanto $nat\mathcal{E} : \mathbb{Z} \to \mathbb{Z}_m = \mathbb{Z}/\mathcal{E}$ è la suriezione cercata.

Esercizio 2.0.59. *Si applichi il teorema fondamentale delle applicazioni ad $s : \mathbb{Z} \to \mathbb{Z}$, definita da $\forall x \in \mathbb{Z}$, $f(x) = x^2$.*

Sol. Costruiamo innanzitutto l'equivalenza $\mathcal{E}_f \subseteq \mathbb{Z} \times \mathbb{Z}$ definita da

$$\forall x, y \in \mathbb{Z},\ (x, y) \in \mathcal{E}_f \Leftrightarrow f(x) = f(y).$$

Dalla definizione di f segue che $(x, y) \in \mathcal{E}_f \Leftrightarrow y = \pm x$; quindi, ciascuna classe di equivalenza contiene un intero ed il suo opposto, $[x] = \{x, -x\}$ e $nat\mathcal{E}_f : \mathbb{Z} \to \mathbb{Z}/\mathcal{E}_f$ è definita da

$$\forall x \in \mathbb{Z},\ nat\mathcal{E}_f(x) = [x].$$

Inoltre, Imf è l'insieme dei quadrati degli interi (quindi s.i. degli interi non negativi) e $\beta : \mathbb{Z}/\mathcal{E}_f \to Imf$ è definita da $\beta([x]) = x^2$. Infine, $j : Imf \to \mathbb{Z}$ è, al solito, la restrizione sul codominio di $e_{\mathbb{Z}}$, cioè $j(x^2) = x^2$.

Esercizio 2.0.60. *Siano $S = \{a, b, c, d, h\}$ ed $S' = \{x, y, z\}$ due insiemi. Si costruisca un'applicazione $f : S \to S'$ che non sia su e si decomponga f secondo il teorema fondamentale delle applicazioni.*

Sol. Dato che f non deve essere su, Imf conterrà al più due elementi di S'. Supponiamo che sia $Imf = \{x, y\}$. Allora $\mathcal{E}_f$ deve essere tale da ripartire S in due classi di equivalenza (in quanto $S/\mathcal{E}_f$ deve contenere due elementi); scegliamo $\mathcal{E}_f$ in modo che le classi siano

$$[a] = \{a, b, h\}, \quad [c] = \{c, d\}.$$

Avremo $nat\mathcal{E}_f : S \to S/\mathcal{E}_f$ definita da

$$nat\mathcal{E}_f(a) = nat\mathcal{E}_f(b) = nat\mathcal{E}_f(h) = [a],$$

$$nat\mathcal{E}_f(c) = nat\mathcal{E}_f(d) = [c]$$

e possiamo assumere come $\beta : S/\mathcal{E}_f \to Imf$ la biiezione data da

$$\beta([a]) = x, \quad \beta([c]) = y.$$

Ne segue che $f : S \to S'$ è definita da

$$f(a) = f(b) = f(h) = x, \quad f(c) = f(d) = y,$$

(essendo $j(x) = x, j(y) = y$).

Esercizio 2.0.61. *Dato il diagramma di applicazioni della figura*
DAFARE
le due applicazioni $h : A \to C$ e $g \circ f : A \to C$ prendono il nome di cammini da A a C. Inoltre, un diagramma di applicazioni si dice commutativo se, fissati comunque due insiemi X ed Y del diagramma, due cammini qualsiasi da X a Y sono eguali. Si scrivano le condizioni che devono essere soddisfatte affinché risulti commutativo il seguente diagramma:
DAFARE

Sol. Se il diagramma è commutativo, deve risultare

$$i \circ h = f,\ g \circ i = j,\ g \circ f = j \circ h = g \circ i \circ h.$$

Esercizio 2.0.62. *Siano $f : S \to S'$ e $g : S' \to S$ due applicazioni. Si provi che esse sono l'una 'inversa dell'altra sse sono commutativi i seguenti diagrammi: DAFARE*

Sol. Se $g = f^{-1}, g \circ f = f^{-1} \circ f = e_S$ ed $f \circ g = f \circ f^{-1} = g^{-1} \circ g = e_{S'}$; onde i due diagrammi sono commutativi. Viceversa, se i due diagrammi sono commutativi, si ha $g \circ f = e_S$ ed $f \circ g = e_{S'}$, onde f e g sono l'una l'inversa dell'altra (cfr. es. 1.14.39). Si noti che se uno soltanto dei due diagrammi è commutativo, la prima applicazione è iniettiva e la seconda è su (cfr. es. 1.14.36 e 1.14.37).

Esercizio 2.0.63. *Siano $\mathcal{E}$ e $\mathcal{F}$ due relazioni di equivalenza sull'insieme S, con $\mathcal{F} \supseteq \mathcal{E}$. Si provi che esiste una biiezione di $S/\mathcal{E}/\mathcal{F}/\mathcal{E}$ su $S/\mathcal{F}$.*

Sol. Consideriamo l'applicazione $f : S/\mathcal{E} \to S/\mathcal{F}$ definita da

$$\forall [x]\mathcal{E} \in S/\mathcal{E},\ f([x]\mathcal{E}) = [x]\mathcal{F}.$$

E' immediato che f sia un'applicazione su. Quindi l'equivalenza $\mathcal{E}_f$ è definita da

$$([x]\mathcal{E}, [y]\mathcal{E}) \Leftrightarrow f([x]\mathcal{E}) = f([y]\mathcal{E}) \Leftrightarrow [x]\mathcal{F} = [y]\mathcal{F} \Leftrightarrow (x, y) \in \mathcal{F}.$$

Pertanto (cfr. es. **??**), $\mathcal{E}_f = \mathcal{F}/\mathcal{E}$ e $\beta : S/\mathcal{E}/\mathcal{E}_f = S/\mathcal{E}/\mathcal{F}/\mathcal{E} \to S/\mathcal{F}$ è la biiezione cercata.

Capitolo 3

L'insieme B^A. Funzioni caratteristiche

Siano A e B due insiemi che, per ora, supponiamo non vuoti. Ha allora significato considerare l'insieme di tutte le applicazioni $f : A \to B$; tale insieme viene, di solito, denotato con B^A. (Si noti che questa scrittura coincide con quella della potenza diretta di B con esponente A e se si interpreta A come insieme di indici, anche le due nozioni coincidono; l'unica precisazione va fatta quando A è un insieme contenente n elementi: in questo caso, in $B^n = B \times \ldots \times B$ si considerano di fatto le immagini delle applicazioni di A in B).

Se $B \neq A$, due applicazioni di B^A non si possono mai comporre per prodotto (si potrebbero comporre come corrispondenze), in quanto ciascuna di esse è applicazione di A in B. Qualora, invece, $A = B$, le applicazioni di A^A sono componibili per prodotto, cioè

$$\forall f, g \in A^A \Rightarrow g \circ f \in A^A;$$

inoltre, esiste l'applicazione identica e_A, tale che

$$\forall f \in A^A,\ e_A \circ f = f \circ e_A = f.$$

Infine, se f è una biiezione, anche $f^{-1} \in A^A$. Ovviamente, vale la proprietà associativa.

Abbiamo finora escluso il caso in cui $A, B = \emptyset$; possiamo ora eliminare questa limitazione, provando la

Proposizione 3.0.9. *Se $A \neq \emptyset$ e $B = \emptyset$, allora $\emptyset^A = \emptyset$. Se $A = \emptyset$ e $B \neq \emptyset$, allora $B^\emptyset = \{\emptyset\}$ (cioè $B^\emptyset$ contiene un solo elemento).*

Dim. Proviamo la prima affermazione. Sia $f \in \emptyset^A$, allora f è una applicazione di A nell'insieme vuoto; per definizione di applicazione, esiste Imf, che contiene almeno un elemento (ciò accade se $\mathcal{E}_f$ è la relazione totale su A); quindi non può essere $Imf \subseteq \emptyset$, ed $Imf \neq \emptyset$; ne segue l'asserto.

Proviamo ora la seconda affermazione. Sia $f \in B^{\emptyset}$, cioè $f : \emptyset \to B$ è un'applicazione dell'insieme vuoto in B; allora f è la corrispondenza vuota (ed è anche un'applicazione). D'altra parte, l'unico elemento di $B^{\emptyset}$ è l'applicazione vuota, one $B^{\emptyset} = \{\emptyset\}$ e l'affermazione è provata.

L'insieme B^A acquista significato particolare quando si scelga l'insieme B. Precisamente, vogliamo considerare il caso in cui B è un insieme contenente esattamente due elementi (cfr. es 1.2.4), che denotiamo con 0 ed 1 (si noti che, in questo caso, 0 ed 1 hanno semplicemente il significato di simboli, e, pertanto, potrebbero venir sostituiti da qualunque altra coppia di caratteri o segni), quindi

$$B = \{0, 1\}.$$

Denoteremo questo insieme anche con il simbolo $\underline{2}$, cioè

$$\underline{2} = \{0, 1\}$$

(anche $\underline{2}$ ha un significato puramente simbolico; ma vedremo nel seguito che, se $0, 1$ si intendono come i primi due numeri naturali, allora $\underline{2}$ è il successivo di 1).

Consideriamo dunque l'insieme $\underline{2}^A$, con A qualunque: $A \neq \emptyset$, dato che, altrimenti $\underline{2}^A$ contiene un solo elemento.

L'insieme $\underline{2}^A$ prende il nome di insieme delle funzioni caratteristiche di A; tale denominazione sarà completamente giustificata da quanto segue.

Sia $f \in \underline{2}^A$, allora $f : A \to \{0, 1\}$, quindi l'immagine, mediante f, di ogni $x \in A$ è 0 oppure 1.

Evidentemente esiste una applicazione di $\underline{2}^A$ la cui immagine è $\{0\}$ e ne esiste una la cui immagine è $\{1\}$. Esclusi questi due casi, ogni $f \in \underline{2}^A$ è un'applicazione su.

Fissata $f \in \underline{2}^A$, consideriamo la controimmagine di 1 mediante f; questa è il s.i. di A definito da

$$f^{-1} = \{x \in A : f(x) = 1\}$$

e per ogni altra $g \in \underline{2}^A$, $g \neq f$, risulta $f_M^{-1}(1) \neq g^{-1}(1)$. Quindi $f^{-1}(1)$ è un ben determinato s.i. di A: sia esso M, allora possiamo denotare con f_M la $f \in \underline{2}^A$ tale che $f^{-1}(1) = M \subseteq A$.

In particolare, f_A è l'applicazione di $\underline{2}^A$ tale che $f_A(1)^{-1} = A$ ed $f_{\emptyset}$ è quella per la quale $f_{\emptyset}^{-1}(1) = \emptyset$ (cioè, $Im f_{\emptyset} = \{0\} \subset \underline{2}$).

Abbiamo così provato la

Proposizione 3.0.10. *Ogni elemento $f \in \underline{2}^A$ individua uno, ed uno solo, sottoinsieme di A, $f^{-1}(1)$.*

Si noti che si poteva anche associare ad ogni $f \in \underline{2}^A$ la $f^{-1}(0) \subseteq A$ ottenendo - in tal modo - gli insiemi complementari dei precedenti.

La Prop 3.0.10 si può invertire; precisamente

Proposizione 3.0.11. *Ogni s.i. di A individua uno, ed uno solo, elemento di $\underline{2}^A$, funzione caratteristica di tale s.i..*

Dim. Sia $\emptyset \subseteq B \subseteq A$. Associamo a B l'elemento $f_B \subset \underline{2}^A$ definito nel modo seguente:

$$\forall x \in B,\ f_B(x) = 1,\ \forall x \notin B,\ f_B(x) = 0.$$

La definizione è ben posta, onde l'asserto.

Se ora ricordiamo che i s.i. di A sono esattamente gli elementi di $P(A)$, dalle due proposizioni precedenti segue immediatamente la

Proposizione 3.0.12. *Sia A un qualunque insieme; esiste una biiezione di $P(A)$ su $\underline{2}^A$.*

Dim. Per provare l'asserto, è sufficiente costruire la biiezione in questione. Poniamo

$$\phi : \underline{2}^A \to P(A),$$

tale che $\forall f \in \underline{2}^A$, $\phi(f) = B \in P(A)$ e $B = f^{-1}(1)$.

Esercizio 3.0.64. *Sia A un insieme contenente n elementi, e sia B un insieme contenente m elementi. Si provi che B^A contiene m^n elementi.*

Dim. Sia $f \in B^A$; allora f è un'applicazione di A in B e, pertanto, è individuata dalla sua immagine , $\operatorname{Im} f \subseteq B$, che contiene gli n elementi, non necessariamente distinti, di B, dati da $f(x)$, al variare di x in A. Quindi il numero di elementi di B^A coincide con il numero di disposizioni con ripetizione di m elementi (quelli di B) ad n ad n (n essendo gli elementi di A ed altrettanti le loro immagini mediante una qualunque $f \in B^A$). Tale numero è m^n, onde l'asserto.

Esercizio 3.0.65. *Dati $A = \{a, b\}$ e $B = \{x, y, z\}$, determinare gli elementi dell'insieme B^A delle applicazioni di A in B.*

Sol. Dobbiamo determinare tutte le applicazioni di A in B, che saranno in numero di $3^2 = 9$. Avremo le applicazioni costanti f_i $(i = 1, 2, 3)$, definite nella maniera seguente:

$$f_1(a) = f_1(b) = x; \quad f_2(a) = f_2(b) = y; \quad f_3(a) = f_3(b) = z.$$

Avremo poi le applicazioni iniettive g_j $(j = 1, 2, \ldots, 6)$ definite nel modo seguente:

$$\begin{array}{llll} g_1(a) = x, & g_1(b) = y; & g_2(a) = x, & g_2(b) = z; \\ g_3(a) = y, & g_3(b) = x; & g_4(a) = y, & g_4(b) = z; \\ g_5(a) = z, & g_5(b) = x; & g_6(a) = z, & g_6(b) = y. \end{array}$$

In tal modo sono esaurite le applicazioni di A in B.

Esercizio 3.0.66. *Dati $A = \{a, b, c\}$ e $B = \{x, y\}$, determinare gli elementi di B^A.*

Sol. Le applicazioni di A in B sono in numero di $2^3 = 8$ e sono precisamente le $f_1, f_2, g_1, g_2, \ldots, g_6$ definite da:

$$\begin{array}{llllll} f_1(a) = x, & f_1(b) = x, & f_1(c) = x; & f_2(a) = y, & f_2(b) = y, & f_2(c) = y; \\ g_1(a) = x, & g_1(b) = y, & g_1(c) = y; & g_2(a) = y, & g_2(b) = x, & g_2(c) = x; \\ g_3(a) = x, & g_3(b) = x, & g_3(c) = y; & g_4(a) = y, & g_4(b) = y, & g_4(c) = x; \\ g_5(a) = x, & g_5(b) = y, & g_5(c) = x; & g_6(a) = y, & g_6(b) = x, & g_6(c) = y. \end{array}$$

Esercizio 3.0.67. *Sia $S = \{a, b, c\}$. Si determini l'insieme delle funzioni caratteristiche di S e si verifichi la sua corrispondenza biunivoca con $P(S)$.*

Sol. Poiché S ha tre elementi, $P(S)$ ha $2^3 = 8$ elementi, precisamente:

$$P(S) = \{\emptyset, S, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}\}.$$

Le funzioni caratteristiche sono le seguenti:

$$\begin{array}{lll}
f_\emptyset & \text{tale che} & f_\emptyset(a) = f_\emptyset(b) = f_\emptyset(c) = 0, \\
f_S & \text{tale che} & f_S(a) = f_S(b) = f_S(c) = 1, \\
f_1 & \text{tale che} & f_1(a) = 1,\ f_1(b) = f_1(c) = 0, \\
f_2 & \text{tale che} & f_2(a) = 0,\ f_2(b) = 0,\ f_2(c) = 0, \\
f_3 & \text{tale che} & f_3(a) = f_3(b) = 0,\ f_3(c) = 1, \\
f_{12} & \text{tale che} & f_{12}(a) = f_{12}(b) = 1,\ f_{12}(c) = 0, \\
f_{13} & \text{tale che} & f_{13}(a) = 1,\ f_{13}(b) = 0,\ f_{13}(c) = 1, \\
f_{23} & \text{tale che} & f_{23}(a) = 0,\ f_{23}(b) = f_{23}(c) = 1,
\end{array}$$

ed individuano gli elementi di $P(S)$, cioé i sottoinsiemi di S, nell'ordine scritto, onde resta determinata la biiezione di 2^S su $P(S)$.

Esercizio 3.0.68. *Sia $\mathbb{D}$ l'insieme dei numeri naturali dispari (con l'ordinamento naturale $\leq$); determinare il sottoinsieme di $\mathbb{D}$, A, la cui funzione caratteristica individua la successione*

$$\{0, 1, 0, 0, 1, 1, 1, 0, 0, 0, \ldots, 0, \ldots\}.$$

Sol. Confrontando la successione data con la successione $\mathbb{D} = \{1, 3, 5, \ldots\}$, si trova $A = \{3, 9, 11, 13\}$.

Esercizio 3.0.69. *Sia A un qualunque s.i. di un insieme S e sia f_A la sua funzione caratteristica. Dimostrare che*

$$f_A = \textit{costante} \implies A = \emptyset \quad \textit{oppure} \quad A = S.$$

Dim. Poiché i valori che la funzione caratteristica di un insieme assume sono soltanto 0 ed 1 (0 quando l'elemento non appartiene all'insieme, 1 quando vi appartiene), avremo i due casi possibili:

$$f_A(x) = 0,\ \forall\, x \in S \quad \text{oppure} \quad f_A(x) = 1,\ \forall\, x \in S.$$

Nel primo caso non esiste alcun elemento $x \in S$ che sia elemento di A, cioé $A = \emptyset$; nel secondo, ogni elemento di S è anche elemento di A, e dato che $A \subseteq S$, si ha $A = S$.

Esercizio 3.0.70. *Siano A, B s.i. di un insieme S e sia f_A la funzione caratteristica di A. Dimostrare che se f_A è costante su B, allora o $B \subseteq A$, oppure $B \subseteq \mathcal{C}_A$.*

Dim. Per definizione di funzione caratteristica, $f_A(x) = 1,\ \forall\, x \in A$, $f_A(z) = 0, \forall\, z \in \mathcal{C}_A$. Se f è costante su B, sono possibili due casi:

$$f_A(y) = 1,\ \forall\, y \in B, \quad \text{oppure} \quad f_A(y) = 0,\ \forall\, y \in B.$$

Nel primo caso, $y \in B \implies y \in A$ e quindi $B \subseteq A$; nel secondo, $y \in B \implies y \in \mathcal{C}_A$ e pertanto $B \subseteq \mathcal{C}_A$.

Esercizio 3.0.71. *Siano A e B s.i. di un medesimo insieme S e siano f_A ed f_B le loro funzioni caratteristiche. Indicata con $f_{A\cap B}$ la funzione caratteristica dell'insieme $A \cap B$, si dimostri che:*

$$f_{A\cap B} = f_A \cdot f_B.$$

Dim. Sia $x \in A \cap B$, allora $x \in A$ ed $x \in B$. Pertanto, $f_{A\cap B}(x) = 1$, $f_A(x) = 1$ ed $f_B(x) = 1$, cioé:

$$f_{A\cap B}(x) = f_A(x) \cdot f_B(x) = 1 \cdot 1 = 1.$$

Sia $y \in \mathcal{C}(A \cap B)$, allora $f_{A\cap B}(y) = 0$. Ma $\mathcal{C}(A \cap B) = \mathcal{C}_A \cup \mathcal{C}_B$, da cui o $y \in \mathcal{C}_A$ e quindi $f_A(y) = 0$, oppure $y \in \mathcal{C}_B$ e pertanto $f_B(y) = 0$. Ne segue:

$$f_{A\cap B}(y) = f_A(y) \cdot f_B(y) = 0,$$

perché è nullo l'uno o l'altro dei fattori. Ne segue l'asserto.

Esercizio 3.0.72. *Siano A e B s.i. di un medesimo insieme S e siano f_A ed f_B le loro funzioni caratteristiche. Indicate con $f_{A\cup B}$ ed $f_{A\cap B}$ rispettivamente le funzioni caratteristiche di $A \cup B$ e $A \cap B$, si provi che:*

$$f_{A\cup B} = f_A + f_B - f_{A\cap B}.$$

Dim. Sia $x \in A \cup B$; allora $f_{A\cup B}(x) = 1$. D'altra parte, si ha $x \in A \cup B$ nei seguenti casi:

$$x \in A,\, x \in B; \quad x \in A,\, x \notin B; \quad x \notin A,\, x \in B,$$

nei quali abbiamo, rispettivamente:

$$\begin{array}{ll} f_A(x) + f_B(x) - f_{A\cap B}(x) & = 1 + 1 - 1 \quad = 1, \\ f_A(x) + f_B(x) - f_{A\cap B}(x) & = 1 + 0 - 0 \quad = 1, \\ f_A(x) + f_B(x) - f_{A\cap B}(x) & = 0 + 1 - 0 \quad = 1. \end{array}$$

Se ora $y \in \mathcal{C}(A \cup B)$, avremo $f_{A\cup B}(y) = 0$; d'altra parte

$$y \in \mathcal{C}(A \cup B) \Longrightarrow y \in \mathcal{C}_A \cap \mathcal{C}_B,$$

allora $f_A(y) = f_B(y) = 0$. Ne segue l'asserto.

Esercizio 3.0.73. *Sia $f : S \longrightarrow S'$ un'applicazione. Si provi che f definisca univocamente un'applicazione $f^* : 2^S \longrightarrow 2^{S'}$.*

Dim. Tenendo conto che esiste una biiezione di 2^S su $P(S)$, si può identificare 2^S con $P(S)$; pertanto, definiamo f^* nel modo seguente:

$$\forall\, A \in 2^S,\ f^*(A) = \{f(a) \,:\, a \in A\},$$

(dove con la scrittura $A \in 2^S$ indichiamo che A è individuato da una funzione caratteristica di S, cioé da un elemento di 2^S) e proviamo che f^* è un'applicazione. (Si noti che $f(A) = f^*(A)$, dove $f(A)$ è l'immagine, mediante f, di $A \subseteq S$. È stato usato un simbolo diverso per sottolineare il fatto che le due appliczioni operano tra coppie diverse di insiemi).
Dato che f è un'applicazione, $D(f) = S$. Ne segue che $D(f^*) = 2^S$. Inoltre ogni s.i. di S (cioé ogni funzione caratteristica di S) determina univocamente $A \subseteq S$ e quindi $f(A) \subseteq S'$, cioé f^* è un'applicazione.

Esercizio 3.0.74. *Sia $f : S \longrightarrow S'$ una biiezione. Si provi che $f^* : 2^S \longrightarrow 2^{S'}$ (cfr. Es. 3.0.73) è ancora una biiezione.*

Dim. Dato che f è una biiezione, $f^{-1} \circ f = e_S$ ed $f \circ f^{-1} = e_{S'}$; peranto, $\forall\, A' \in S'$ (cfr. Es. 3.0.73), $f^{*-1}(A')$ contiene un solo elemento, cioé f^* è una biiezione.
In altro modo si può provare che f^* è una biiezione, consierando $A,\ B \in 2^S$, $A \neq B$; allora esiste $x \in S$, tale che $x \in A$, $x \notin B$ (o viceversa); quindi $f(x) \in f(A)$, e dato che f è una biiezione, $f(x) \notin f(B)$ (o viceversa). Ne segue $f(A) \neq f(B)$, cioé $f^*(A) \neq f^*(B)$, quindi f^* è iniettiva. D'altra parte, essendo f su, $\forall\, x' \in S'$ esiste $f^{-1}(x')$, quindi esiste $f^{-1}(A')$ per ogni $A' \subseteq S'$, cioè f^* è su, onde l'asserto.

Esercizio 3.0.75. *Sia $f : S \longrightarrow S'$ un'applicazione suriettiva. Si provi che $f^* : 2^S \longrightarrow 2^{S'}$ (cfr. Es. 3.0.73) è suriettiva.*

Dim. Occorre provare che ogni elemento di $2^{S'}$ è immagine di almeno un elemento di 2^S. Sia $A' \in 2^{S'}$. Dato che f è su, $f^{-1}(A') = \{a \in A :\ f(a) \in A'\} \neq \emptyset$, cioé $f(f^{-1}(A)) = A'$. Ne segue che f^* è suriettiva.

Esercizio 3.0.76. *Si provi che $B^{\{a\}} = \{(a, b) :\ b \in B\}$.*

Dim. Sia $f \in B^{\{a\}}$, cioé $f : \{a\} \longrightarrow B$. Poiché $\{a\}$ contiene un solo elemento, $\operatorname{Im} f = \{b\}$, $b \in B$. Ne segue che ogni $f \in B^{\{a\}}$ indvidua una ed una sola coppia (a, b), $b \in B$. Viceversa, se $b \in B$, esiste ed è unica l'applicazione $f : \{a\} \longrightarrow B$, tale che $\operatorname{Im} f = \{b\}$. Quindi i due insiemi coincidono.

Esercizio 3.0.77. *Si provi che per qualunque insieme C, $A \subseteq B \Longrightarrow A^C \subseteq B^C$.*

Dim. Sia $f \in A^C$, cioé $f : C \longrightarrow A$; allora $\operatorname{Im} f \subseteq A \subseteq B$, onde $f \in B^C$.

3.1 Insiemi finiti ed infiniti

Finora abbiamo utilizzato in maniera intuitiva la nozione di insieme contenente n elementi, anche se (cfr. Es. 1.2.4) abbiamo definito un insieme contenente un solo elemento e mostrato come tale definizione si possa estendere ad un naturale n qualsiasi; analogamente, in maniera intuitiva, è stata accettata la nozione di insieme infinito. Vogliamo ora formalizzare queste nozioni, alla luce della teoria cantoriana degli insiemi (della quale la teoria ingenua rappresenta una "forma semplificata").
Daremo la definizione di insieme infinito di Dedekind (1888), partendo dalle osservazioni seguenti.
Consideriamo l'insieme $\mathbb{N}$ dei numeri naturali e consideriamo l'insieme A dei quadrati dei naturali (qui e nel seguito, in $\mathbb{N}$ considereremo incluso lo zero, salvo esplicito avviso contrario), l'applicazione $f : \mathbb{N} \longrightarrow A$, definita da

$$\forall\, n \in \mathbb{N}, \quad f(n) = n^2 \in A,$$

è una biiezione. Infatti, per definizione di A, ogni elemento di A è quadrato di un elemento di $\mathbb{N}$, onde f è su; inoltre

$$f(n) = f(m) \implies n^2 = m^2 \implies n = m,$$

quindi f è iniettiva. Ora A è un s.i. proprio di $\mathbb{N}$; pertanto, si ha l'apparente assurdo si un insieme ($\mathbb{N}$) che si può mettere in corrispondenza biunivoca con un suo sottoinsieme proprio (A), e ciò non è mai possibile per un insieme contenente n elementi (come è immediato verificare). Pertanto, si può dare la seguente definizione:
Un insieme S si dice *infinito* sse si può mettere in corrispondenza biunivoca con un suo sottoinsieme proprio (cioé se esistono $X \subset S$ ed $f : S \longrightarrow X$, con f biiezione).
Di conseguenza, ogni insieme non infinito sarà detto *finito*. L'esempio di $\mathbb{N}$ e dell'insieme dei quadrati degli elementi di $\mathbb{N}$ non è il solo che si possa dare (cfr. Es. 1.14.24), ma abbiamo riportato tale esempio perché ritenuto il "più antico", in quanto risale a Galileo Galilei (1638). Osserviamo sin d'ora che il primo ad usare sistematicamente la nozione di corrispondenza biunivoca tra insiemi per fondare la teoria degli insiemi, ed in particolare per gli insiemi infiniti, è stato George Cantor (1845-1918) nella sua opera "Beitraege zur Begruendung der transfiniten Menegelehre" (1895-1897).
Sia ora S un insieme finito (secondo la definizione precedente); vogliamo precisare cosa si intende con la locuzione "S ha n elementi"; intuitivamente, ciò corrisponde al fatto che "contando" gli elementi di S il procedimento ha termine, e "contiamo" esattamente n elementi. Per formalizzare questo processo intuitivo, accetiamo come noto l'insieme dei numeri naturali e consideriamo il seguente s.i. di $\mathbb{N}$:

$$\underline{n} = \{0, 1, 2, \ldots, n-1\}.$$

Diremo che tale insieme ha n elementi (se "contiamo" da 0 a $n-1$, otteniamo proprio n elementi. Come vedremo meglio nel seguito la precedente è la definizione insiemistica dei numeri naturali).
Allora, un insieme S ha n elementi sse esiste una biiezione di S su $\underline{n}$, $f : S \longrightarrow \underline{n}$, cioé se ciascun elemento di S ha come immagine mediante f uno ed uno solo dei naturali $0, 1, \ldots, n-1$ e , viceversa, ciascuno di tali naturali ha come controimmagine mediante f uno, ed uno soltanto, degli elementi di S.
Si noti che con la scrittura precedente, si ha $0 = \emptyset$, $1 = \{0\} = \{\emptyset\}$, $2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$.
Per denotare il fatto che l'insieme S contiene n elementi, scriveremo $|S| = n$. Abbiamo così stabilito quando un insieme ha n elementi, ma ciò non assicura l'esistenza di un insieme con n elementi. Proviamo dunque la

Proposizione 3.1.1. *Per ogni naturale n esiste un insieme con n elementi.*

Dimostrazione. Consideriamo $\emptyset$; per definizione, abbiamo $|\emptyset| = 0$. Ricordando la definizione di insieme delle parti di un insieme, avremo

$$|P(\emptyset)| = 1, \text{ in quanto } P(\emptyset) = \{\emptyset\}.$$

Di conseguenza

$$\begin{aligned} P(\{\emptyset\}) &= \{\emptyset, \{\emptyset\}\}, \text{ onde } |P(\{\emptyset\})| = 2; \\ P(\{\emptyset, \{\emptyset\}\}) &= \{\emptyset; \{\emptyset, \{\emptyset\}\}; \{\emptyset\}; \{\{\emptyset\}\}\}, \end{aligned}$$

da cui $|P(\{\emptyset, \{\emptyset\}\})| = 4 = 2^2$ e così via.
Notiamo che $|\{\emptyset\}| = 1$, $|\{\{\emptyset\}\}| = 1$, $|\{\ldots\{\emptyset\}\ldots\}| = 1$, come segue dalla definizione di insieme contenente un solo elemento.
Poniamo ora $P^0(\emptyset) = \emptyset$, $P^1(\emptyset) = \{\emptyset\}$,

$$\begin{aligned} P^2(\emptyset) &= P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}, \\ P^3(\emptyset) &= P(\{\emptyset, \{\emptyset\}\}) = \{\emptyset; \{\emptyset, \{\emptyset\}\}; \{\emptyset\}; \{\{\emptyset\}\}\}, \\ P^4(\emptyset) &= P(\{\emptyset, \{\emptyset, \{\emptyset\}\}, \{\emptyset\}, \{\{\emptyset\}\}\}) = \\ &= \{\emptyset; \{\emptyset, \{\emptyset, \{\emptyset\}\}, \{\emptyset\}, \{\{\emptyset\}\}\}; \{\emptyset\}; \{\{\emptyset, \{\emptyset\}\}\}; \{\{\emptyset\}\}; \{\{\{\emptyset\}\}\}; \\ &\quad \{\emptyset, \{\emptyset, \{\emptyset\}\}\}; \{\emptyset, \{\emptyset\}\}; \{\emptyset, \{\{\emptyset\}\}\}; \{\{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}\}\}; \\ &\quad \{\{\emptyset\}, \{\{\emptyset\}\}\}; \{\emptyset, \{\emptyset, \{\emptyset\}\}, \{\emptyset\}\}; \{\emptyset, \{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}\}\}; \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}; \\ &\quad \{\{\emptyset, \{\emptyset\}\}, \{\emptyset\}, \{\{\emptyset\}\}\}\}, \end{aligned}$$

ed analogamente si definisce $P^n(\emptyset)$.
Se ora consideriamo $P^n(\emptyset)$, questo contiene per costruzione, gli elementi

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

(e nell'ultimo di questi insiemi le coppie di parentesi graffe sono in numero di $n-1$); tali elementi sono manifestamente in numero di n e costituiscono un insieme di n elementi, s.i. di $P^n(\emptyset)$. Ne segue l'asserto. □

Notiamo che nella dimostrazione precedente si è fatto uso soltanto della nozione di insieme vuoto e di quella di insieme delle parti di un insieme: ciò è sempre lecito, in quanto nella teoria cantoriana degli insiemi, $\emptyset$ e $P(S)$ vengono definiti intuitivamente con procedimento genetico, mentre, nella teoria assiomatica formale degli insiemi, la loro esistenza viene postulata.

Esercizio 3.1.1. *Si provi che ogni s.i. di un insieme finito è finito.*

Dim. Sia A finito e $|A| = n$ (ricordiamo -Paragrafo **??**- che, con il simbolo $|A|$ si intende il numero di elementi contenuti nell'insieme A), e sia $B \subseteq A$. Per definizione di s.i., ogni elemento di B è elemento di A, quindi B contiene $m \leq n$ elementi, cioé B è finito.

Esercizio 3.1.2. *Si provi che, per ogni insieme finito A e per ogni insieme S, $A\backslash S$ ed $A \cap S$ sono insiemi finiti.*

Dim. Ricordando che $A\backslash S = \{a \in A : a \notin S\}$, si ha $A\backslash S \subseteq A$, onde $A\backslash S$ è finito (cfr. Es. 3.1.1). Analogamente, essendo $A \cap S \subseteq A$, $A \cap S$ è finito.

Esercizio 3.1.3. *Si provi che l'unione di m insiemi finiti è un insieme finito.*

Dim. Sia $A = A_1 \cup A_2 \cup \cdots \cup A_m$, e ciascuno degli insiemi A_i ($i = 1, 2, 3, \ldots, m$) sia finito, e contenga n_i elementi. Supponiamo che gli A_i siano a due a due disgiunti. Allora, per definizione di unione, A contiene esattamente $n_1 + n_2 + \cdots + n_m$ elementi, cioé è finito. Se gli A_i non sono a due a due disgiunti, gli eventuali elementi comuni a due o a più di essi sono considerati una sola volta, onde A è ancora finito e contiene $t < n_1 + n_2 + \cdots + n_m$ elementi; cioé l'asserto.

Esercizio 3.1.4. *Si provi che un insieme S è finito sse $P(S)$ è finito.*

Dim. Se S è finito, $|S| = n$, allora (cfr. Es. 1.5.3) $|P(S)| = 2^n$, cioé $P(S)$ è finito.
Viceversa, se $P(S)$ è finito, consideriamo il s.i. di $P(S)$ definito da $A = \{\{x\} : x \in S\}$; poiché $A \subseteq P(S)$, A è finito ed esiste una biiezione di A su S ($f(\{x\}) = x$, $\forall\, x \in S$). Pertanto S è finito.

Esercizio 3.1.5. *Si provi che un insieme contenente un s.i. infinito è esso stesso un insieme infinito.*

Dim. Sia S un insieme qualunque e sia $A \subseteq S$ un insieme infinito. Provare che $A \subseteq S$, A infinito $\Longrightarrow S$ infinito, equivale a provare che se S è finito, e $A \subseteq S \implies A$ finito.
Se S è finito, S contiene n elementi. Poiché $A \subseteq S$, A contiene $m \leq n$ elementi, cioé A è finito. Ne segue l'asserto.

Esercizio 3.1.6. *Si provi che l'unione di due insiemi qualsiasi, uno dei quali sia infinito, è un insieme infinito.*

Dim. Sia A infinito e sia B un insieme qualunque. Dato che $A \subseteq A \cup B$, quale che sia l'insieme B, la tesi segue dall'Es. 3.1.5.

3.2 Potenze di un insieme. Alcune proprietà dei numeri cardinali.

Abbiamo dato la definizione di insieme infinito e di insieme finito con n elementi (cfr. **??**); vediamo ora se, e come, si possa estendere al caso degli inisiemi infiniti la nozione di "numero" degli elementi valida per un insieme finito.
Innanzitutto osserviamo che l'unico insieme infinito che abbiamo esplicitamente considerato da questo punto di vista è stato l'insieme $\mathbb{N}$ dei numeri naturali. Introduciamo ora la seguente definizione:
Un insieme S si dice *numerabile* sse S si può mettere in corrispondenza biunivoca con $\mathbb{N}$.
Diremo anche che un insieme siffatto ha la *potenza del numerabile*.
Chiameremo poi numero *cardinale* di un insieme il "numero" dei suoi elementi, per gli insiemi infiniti nel senso che preciseremo, facendo la distinzione tra numero cardinale *finito*, e numero cardinale *transfinito* (che definiremo), se l'insieme S è infinito.
Al fine di introdurre i numeri cardinali transfiniti (e contemporaneamente "ritrovare" quelli finiti, cioè i naturali), consideriamo la classe Σ di tutti gli insiemi ed introduciamo in Σ la seguente relazione $\mathcal{E}$, che prende il nome di *equipotenza* (od equipollenza):

$$\forall\, A, B \in \Sigma,\ (A, B) \in \mathcal{E} \iff \exists f : A \longrightarrow B,\ f \text{ biiezione}.$$

Proviamo che $\mathcal{E}$ è una relazione di equivalenza.
$\mathcal{E}$ è riflessiva; infatti e_A è una biiezione, quindi $(A, A) \in \mathcal{E}, \forall\, A \in \Sigma$.
$\mathcal{E}$ è simmetrica; infatti,
$(A, B) \in \mathcal{E} \implies \exists f \in B^A$, f biiezione $\implies$ $f^{-1} \in A^B$, f^{-1} biiezione $\implies$ $(B, A) \in \mathcal{E}$.
$\mathcal{E}$ è transitiva; infatti, $(A, B), (B, C) \in \mathcal{E} \implies \exists f \in B^A, g \in C^B$, f, g biiezioni $\implies g \circ f \in C^A$, $g \circ f$ biiezione $\implies (A, C) \in \mathcal{E}$.
Consideriamo allora l'insieme quoziente $\Sigma/\mathcal{E}$; gli elementi di tale insieme, cioé le classi di equipotenza, prendono il nome di *numeri cardinali* o *potenze* degli insiemi di Σ.
(Notiamo che, nella definizione di relazione, in particolare di equivalenza, e quindi nel passaggio all'insieme quoziente, il fatto che Σ sia una classe e non un insieme non ha alcuna importanza).
Se $A \in \sigma$, denoteremo con $|A|$, invece che con $[A]$, la classe di $\Sigma/\mathcal{E}$ cui apprtiene A. Pertanto,

$$|A| = |B| \iff A \in [B],\ B \in [A] \iff \exists f : A \longrightarrow B,\ f \text{ biiezione}.$$

Se ora A è un insieme finito ed $|A| = n$ (secondo la definizione del paragrafo **??**), la classe $|A|$ contiene tutti gli insiemi con n elementi.

Abbiamo così definito il numero cardinale o potenza di un insieme e stabiito quando due numeri cardinali finiti o transfiniti sono uguali; definiamo ora la disuguaglianza tra numeri cardinali.
Siano $|A|$ e $|B|$ due cardinali, (finiti o transfiniti), diremo che

$$|A| < |B|$$

5 sse esistono $B' \subset B$ ed $f : A \longrightarrow B'$, f biiezione di A su B', ma non esiste alcun $A' \subseteq A$ tale che un'applicazione $g : B \longrightarrow A'$ sia una biiezione. (Proveremo nel seguito che tale disuguaglianza in senso stretto nell'insieme dei cardinali, se completata con l'eguaglianza, è una relazione d'ordine nell'insieme dei numeri cardinali).
In base alla disuguaglianza tra numeri cardinali ora definita ed in base alla definizione di insieme infinito si ha la seguente

Proposizione 3.2.1. *Sia A un insieme infinito qualsiasi; allora, per ogni s.i. proprio S di A, risulta $|S| < |A|$.*

Se invece A è un insieme finito, ogni s.i. proprio di A ha cardinalità strettamente minore della cardinalità di A.
Finora l'unico esempio di cardinalità transfinita che abbiamo dato è costituito da $|\mathbb{N}|$, potenza del numerabile. In effetti $\mathbb{N}$ è il "più piccolo" cardinale transfinito, nel senso che, per ogni insieme infinito A, risulta $|A| \geq |\mathbb{N}|$.
Cominciamo a stabilire il seguente risultato.

Proposizione 3.2.2. *Sia S un qualunque s.i proprio di $\mathbb{N}$, allora o S è finito, oppure $|S| = |\mathbb{N}|$.*

Dimostrazione. Supponiamo che S non sia finito; dobbiamo provare che S è numerabile, cioé che $|S| = |\mathbb{N}|$. Sia f_S la funzione caratteristica di S, elemento di $2^{\mathbb{N}}$. Considerato l'insieme $\mathbb{N}$ come successione ordinata $\{0, 1, 2, \ldots, n, \ldots\}$, f_S è individuata dai valori che assume sugli elementi di $\mathbb{N}$ nell'ordine detto, cioé da una successione arbitrara di 0 e di 1, che non è definitivamente costituita da tutti zero (cioé costituita da tutti zeri a partire da un certo punto) perché S non è finito. Associamo agli elementi di tale successione (nell'ordine detto) i naturali $0, 1, 2, \ldots, n, \ldots$; otteniamo in tal modo una corrispondenza biunivoca tra S ed $\mathbb{N}$, onde $|S| = |\mathbb{N}|$; ne segue l'asserto. □

Generalizzando, si ha il *Teorema fondamentale del numerabile*:

Proposizione 3.2.3. *Un s.i. di un insieme numerabile, o è finito o è numerabile.*

Supponiamo ora che S sia un insieme infinito e che sia $|S| < |\mathbb{N}|$. Allora S è equipotente ad un s.i. proprio di $\mathbb{N}$ e, dato che è infinito, $|S| = |\mathbb{N}|$. Pertanto

Proposizione 3.2.4. *$|\mathbb{N}|$ è il più piccolo numero cardinale transfinito.*

Osserviamo che il procedimento usato per provare l'esistenza di un insieme avente n elementi si può estendere ad un n arbitrariamente grande e quindi fornire, almeno intuitivamente, l'esistenza di un insieme numerabile. Daremo ulteriori esempi di insiemi numerabili nel successivo paragrafo **??**.
Per provare che esistono insiemi aventi potenza superiore al numerabile, cioé insiemi il cui numero cardinale sia strettamente maggiore di $|\mathbb{N}|$, cominciamo con provare la

Proposizione 3.2.5. *[Teorema di Cantor] Sia S un qualunque insieme; risulta*

$$|S| < |P(S)|.$$

Dimostrazione. Dato che $|P(S| = |2^S|$ (cfr. Prop. 3.1.1), proviamo che

$$|S| < |2^S|.$$

L'applicazione $g : S \longrightarrow 2^S$, definita da $g(a) = \{\{a\} : a \in S\}$ è manifestamente una iniezione, quindi

$$|S| \leq |2^S|.$$

Il teorema sarà provato dimostrando che $|S| \neq |2^S|$.
Supponiamo che esista una biiezione $f : S \longrightarrow 2^s$, e consideriamo l'insieme $A = \{x \in S : x \notin f(x)\}$ (tale scrittura ha senso in quanto $f(x) \in 2^S$ significa che $f(x)$ è un s.i. di S).
Dato che $A \subseteq S$, $A \in 2^S$. Quindi, poichè f è su, esiste $b \in S$ tale che $f(b) = A$. Se $b \in A$, per definizione di A, $b \notin f(b) = A$, il che è impossibile. Similmente se $b \notin A$, allora $b \in f(b) = A$, il che è impossibile.
Ne segue che l'aver supposto $|S| = |2^S|$ conduce ad una contraddizione; pertanto tale ipotesi è falsa ed il teorema è vero. □

In base al risultato di quest'ultima proposizione, definiamo *potenza del continuo* la potenza dell'insieme $P(\mathbb{N})$.
Ricordando la Prop. **??**, si ha $|P(\mathbb{N})| = |2^{\mathbb{N}}|$, quindi si può definire potenza del continuo anche il numero cardinale $|2^{\mathbb{N}}|$.
Sia ora $\mathbb{R}$ l'insieme dei numeri reali; proviamo che

Proposizione 3.2.6. *$\mathbb{R}$ ha la potenza del continuo.*

Dimostrazione. Sfruttando la proprietà transitiva dell'uguaglianza tra potenze, proviamo l'affermazione in due tempi. Precisamente, detto

$$I = \{x \in \mathbb{R} : 0 \geq x \leq 1\},$$

dimostreremo che $|I| = |2^{\mathbb{N}}|$ e poi dimostreremo che $|I| = |\mathbb{R}|$.
Utilizzando la numerazione in base 2 (cfr. Paragrafo **??**) per i numeri reali dell'intervallo I, possiamo assumere che ciascuno di essi si scriva come

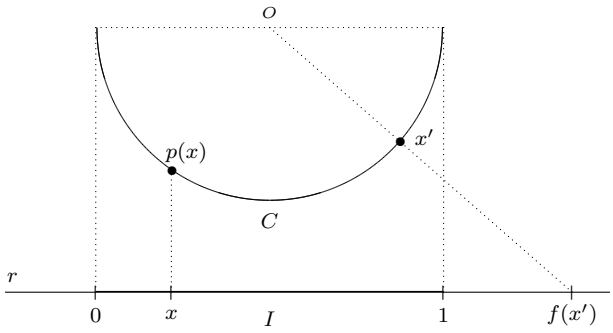
"zero virgola successione arbitraria di 0 ed 1". Pertanto, un numero $x \in I$ è individuato univocamente dalla successione arbitraria di 0 e di 1 che costituisce le cifre dopo la virgola, quando si convenga che $0,111111\ldots1\ldots$, ovvero la successione costituita da tutti "1" rappresenti $1 \in I$. Queste successioni sono esattamente di tre tipi.

1) successioni definitivamente nulle: rappresentano i numeri reali di I che, in base 10, sono del tipo $1/2^h$ ($h \geq 1$, $h \in \mathbb{N}$);

2) successioni periodiche: rappresentano i numeri razionali appartenenti ad I, che non siano del tipo precedente;

3) successioni arbitrarie né periodiche né definitivamente nulle: rappresentano gli irrazionali appartenenti all'intervallo I.

Pertanto, tenendo presente la dimostrazione della Prop. 3.2.2, ciascuna di queste successioni individua uno ed un solo elemento di $2^{\mathbb{N}}$. Viceversa, ciascun elemento di $2^{\mathbb{N}}$ individua una ed una sola successione siffatta; cioé un numero reale dell'intervallo I. Quindi, $|2^{\mathbb{N}}| = |I|$, cioé I ha la potenza del continuo.
Proviamo ora che $|I| = |\mathbb{R}|$.



Ricordando che i numeri reali si possono rappresentare mediante tutti e soli i punti di una retta r, fissiamo una retta r e su di essa l'intervallo I, e consideriamo una semicirconferenza C (come luogo dei suoi punti) tale che C sia esterna ad r, il diamtetro di C sia un segmento uguale e parallelo ad I.
Sia p la proiezione ortogonale di I su C, cioé $p : I \longrightarrow C$ è l'applicazione definita da:
$\forall\, x \in I$, $p(x) \in C$ è il punto di intersezione di C con la normale per x ad r.
p è manifestamente una biiezione. Pertanto, $C = p(I)$, onde $|C| = |I|$.
Sia ora O il centro di C e sia f la proiezione di C da 0 su r, cioé $\forall\, x' \in C$, $f(x') \in r$ è l'intersezione con r della retta Ox'. L'applicazione f è una biiezione; pertanto $|C| = |r| = |\mathbb{R}|$.
D'altra parte, il prodotto di due biiezioni è ancora una biiezione, quindi $f \circ p : I \longrightarrow \mathbb{R}$ è una biiezione. Ne segue $|I| = |\mathbb{R}|$ e, per quanto già provato, $|2^{\mathbb{N}}| = |\mathbb{R}|$, cioé l'asserto. □

Nel successivo Paragrafo **??** e negli esercizi saranno dati altri esempi di insiemi aventi la potenza del continuo.
Tenendo presente il teorema di Cantor, è immediato costruire insiemi aventi potenza superiore a quella del continuo. Infatti, se S ha la potenza del continuo, dato che $|P(S)| > |S|$, $P(S)$ ha potenza superiore alla potenza del continuo.
In base a quanto provato, il passaggio dalla potenza del numerabile alla potenza del continuo risulta alquanto spontaneo (si passa dall'insieme $\mathbb{N}$ all'insieme $P(\mathbb{N})$, ovvero all'insieme $2^{\mathbb{N}}$); sorge allora spontanea la questione dell'esistenza o meno di insiemi aventi potenza strettamente maggiore della potenza del numerabile e strettamente minore di quella del continuo. Finora non è stato possibile né provare, né negare, l'esistenza di insiemi siffatti; pertanto si accetta la seguente
Ipotesi del continuo di Cantor: Non esiste alcun insieme avente potenza maggiore di quell del numerabile e minore di quella del continuo, cioè non esiste alcun cardinale tranfinito compreso tra $|\mathbb{N}|$ e $P(\mathbb{N})$.
Osserviamo che, nella teoria assiomatica degli insiemi di Gödel-Bernays, l'ipotesi del continuo viene assunta come assioma.
È convenzione denotare la potenza del numerabile con $\aleph_0$ (aleph zero, "aleph" essendo la prima lettera dell'alfabeto ebraico) e la potenza del continuo con $\aleph_1$. Quindi, tenendo conto dell'ipotesi del continuo, $\aleph_0$ ed $\aleph_1$ sono i "primi due cardinali transfiniti"; risulta $\aleph_0 < \aleph_1$ e non esiste alcun cardinale transfinito compreso tra $\aleph_0$ e $\aleph_1$.
L'ipotesi del continuo si può generalizzare; per pervenire ad una formulazione "comoda" di tale generalizzazione, introduciamo alcune notazioni.
Poniamo

$$\begin{array}{rl} P^0(\mathbb{N}) = \mathbb{N}, & \text{onde} \quad \aleph_0 = |P^0(\mathbb{N})| = |\mathbb{N}|; \\ P^1(\mathbb{N}) = P(\mathbb{N}), & \text{onde} \quad \aleph_1 = |P(\mathbb{N})| = |\mathbb{R}|; \end{array}$$

analogamente, scriveremo:

$$\begin{array}{ccc} P^2(\mathbb{N}) = P(P(\mathbb{N})); & P^3(\mathbb{N}) = P(P(P(\mathbb{N}))); & \dots; \\ \dots; & P^t(\mathbb{N}) = P(\dots P(P(\mathbb{N}))\dots); & \dots \end{array}$$

Pertanto possiamo introdurre i seguenti cardinali transfiniti

$$\aleph_2 = |P^2(\mathbb{N})|, \quad \aleph_3 = |P^3(\mathbb{N})|, \quad \dots, \quad \aleph_t = |P^t(\mathbb{N})|.$$

Ipotesi del continuo generalizzata: Non esiste alcun cardinale transfinito compreso tra $\aleph_t$ e $\aleph_{t+1}$, quale che sia $t \in \mathbb{N}$.
Ne segue che i cardinali transfiniti ora introdotti costituiscono un insieme avente potenza del numerabile. Infatti se $A = \{\aleph_t : t \in \mathbb{N}\}$ l'applicazione

$$f : A \longrightarrow \mathbb{N},$$

definita da

$$\aleph_t \in A, \quad f(\aleph_t) = t \in \mathbb{N},$$

è manifestamente una biiezione.
Un'altra formulazione dell'ipotesi del continuo generalizzata, è la seguente:
Dato comunque un insieme infinito S, non esiste alcun insieme avente potenza strettamente maggiore di $|S|$ e strettamente minore di $|P(S)|$.

Esercizio 3.2.1. *Sia $A \neq \emptyset$ un insieme finito, $|A| = n$; si determini la cardinalità dell'insieme $T(A)$ delle trasformazioni di A su se stesso.*

Sol. Evidentemente, $T(A)$ è un s.i. di A^A e $|A^A| = n^n$. Ogni elemento di $T(A)$ è una biiezione, quindi permuta tra loro gli elementi di $T(A)$; pertanto, $|T(A)|$ sarà eguale al numero delle sostituzioni su n oggetti, cioé $n!$ (e risulta $n! < n^n$, $\forall\, n \in \mathbb{N} - \{0\}$).
Nel caso in cui $A = \emptyset$, l'unica trasformazione di A su se stesso è l'identità, onde $|T(A)| = 1$ (ed è anche $|A^A| = 1$).

Esercizio 3.2.2. *Sia S un insieme finito, $|S| = n$, e sia $E(S)$ l'insieme delle equivalenze su S. Si provi che $E(S)$ ha cardinalità*

$$p_n = \sum_{i=0}^{n-1} \binom{n-1}{i} p_i$$

e che risulta $p_0 = 1$.

Dim. Innanzitutto, se $S = \emptyset$, $|S| = 0$ e quindi l'unica relazione su S, la relazione vuota, è di equivalenza, onde $p_0 = 1$ 8per $n \geq 1$, la relazione vuota non è di equivalenza- cfr. Es. **??**.
Ricordando che ogni equivalenza definisce una partizione e viceversa, per determinare $|E(S)| = p_n$ (se $|S| = n$), basta determinare il numero di partizioni di S. Sia $a \in S$ un fissato elemento di S e sia t_i il numero delle partizioni di S per le quali a appartiene ad un insieme della partizione (classe di equivalenza) di cardinalità $n - i$ (di conseguenza $\mathcal{C}_S[a]$ ha cardinalità i). Pertanto

$$p_n = \sum_{i=0}^{n-1} t_i;$$

infatti

$$t_i = \binom{n-1}{i} p_i,$$

dato che il complementare di $[a]$ si può scegliere in $\binom{n-1}{i}$ modi diversi ($i = 0, 1, \ldots, n-1$), ed essendo tale complementare ripartibile in p_i modi diversi; quindi

$$p_n = \sum_{i=0}^{n-1} \binom{n-1}{i} p_i.$$

Esercizio 3.2.3. *Sia S un qualunque insieme. Si provi che, quale che sia a,*

$$|S| = |S^{\{a\}}|,\ |S| = |S| \times \{a\},\ |\{a\}^S| = |\{a\}|.$$

Sol. Dato che $|\{a\}| = 1$, se $f \in S^a$, $|\operatorname{Im} f| = 1$, quindi f fissa un elemento di S, ed $f, g \in S^a$ sono distinte sse $\operatorname{Im} f \neq \operatorname{Im} g$.

Ne segue che l'applicazione $\phi : S^a \longrightarrow S$, definita da $\phi(f) = \operatorname{Im} f$ è una biiezione.
Proviamo ora la seconda eguaglianza. L'applicazione

$$f : S \longrightarrow S \times \{a\},$$

definita da $\forall\, x \in S$, $f(x) = (x, a)$, è manifestamente una biiezione, onde l'asserto.
Infine, $|\{a\}| = 1$ implica che esiste una sola applicazione di S su $\{a\}$, e resta provata anche l'ultima eguaglianza.

Esercizio 3.2.4. *Si provi che, comunque si assegnino gli insiemi A, B, C, risulta*

$$|(A \times B)^C| = |A^C \times B^C|.$$

Dim. Sia $f \in (A \times B)^C$, cioé $f : C \longrightarrow A \times B$; allora, $\forall\, c \in C$, esiste $(a, b) \in A \times B$ tale che $f(c) = (a, b)$.
Consideriamo le applicazioni $g : C \longrightarrow A$ ed $h : C \longrightarrow B$ tali che $\forall\, c \in C$, $g(c) = a$ ed $h(c) = b$. Le applicazioni g ed h sono individuate univocamente da f. Viceversa, fissata comunque $(g, h) \in A^C \times B^C$, cioé $g : C \longrightarrow A$, $h : C \longrightarrow B$, consideriamo l'applicazione $f : C \longrightarrow A \times B$, tale che $\forall\, c \in C$, $f(c) = (g(c), h(c))$. L'applicazione f è univocamente definita. Pertanto esiste una biiezione di $(A \times B)^C$ su $A^C \times B^C$ e la proposizione è provata.

Esercizio 3.2.5. *Siano A, B, C tre insiemi, e sia $B \cap C = \emptyset$. Si provi che*

$$|A^{B \cup C}| = |A^B \times A^C|.$$

Dim. Proviamo che esiste una biiezione $\phi : A^{B \cup C} \longrightarrow A^B \times A^C$. Sia $f \in A^{B \cup C}$; poiché $B \cap C = \emptyset$, f individua univocamente $f|_B : B \longrightarrow A$ ed $f|_C : C \longrightarrow A$, i cui domini sono disgiunti, cioé $f|_B \in A^B$ ed $f|_C \in A^C$; quindi, ad ogni $f \in A^{B \cup C}$ resta univocamente associata la coppia $(f|_B, f|_C) \in A^B \times A^C$.
Viceversa, sia $(g, h) \in A^B \times A^C$, cioé $g : B \longrightarrow A$ ed $h : C \longrightarrow A$. Dato che $B \cap C = \emptyset$, si può costruire univocamente l'applicazione $g \cup h : B \cup C \longrightarrow A$, tale che $(g \cup h)|_B = g$ e $(g \cup h)|_C = h$. Ne segue che $\phi : A^{B \cup C} \longrightarrow A^B \times A^C$, definita da

$$\forall\, f \in A^{B \cup C}, \quad \phi(f) = (f|_B, f|_C) \in A^B \times A^C,$$

è una biiezione, onde l'asserto.

Esercizio 3.2.6. *Si provi che, quali che siano gli insiemi A, B, si ha*

$$|A \times B| = |B \times A|.$$

Dim. L'applicazione $f : A \times B \longrightarrow B \times A$, definita da

$$\forall\,(a,b) \in A \times B, \quad f((a,b)) = (b,a),$$

è manifestamente una biiezione, onde l'asserto.

Esercizio 3.2.7. *Sia S un insieme infinito qualunque. Si provi che $S \setminus \{x\}$ è un insieme infinito.*

Dim. L'affermazione è banalmente vera se $\{x\} \not\subset S$; infatti, in tal caso, $S \setminus \{x\} = S$.
Supponiamo, dunque, $\{x\} \subseteq S$. Allora $S \setminus \{x\}$ è il complementare di $\{x\}$ in S, $\mathcal{C}\{x\}$ e $\{x\} \cup \mathcal{C}\{x\} = S$. Se $\mathcal{C}\{x\}$ fosse finito, essendo $\{x\}$ finito, l'insieme $\{x\} \cup \mathcal{C}\{x\}$ sarebbe finito, contro l'ipotesi. L'assurdo prova l'asserto.

Esercizio 3.2.8. *Si provi che un insieme è infinito sse contiene un s.i. numerabile.*

Dim. Sia S un insieme e sia $A \subseteq S$ un suo s.i. numerabile, cioé sia $|A| = |\mathbb{N}|$. Dato che $\mathbb{N}$ è infinito, anche A è infinito e quindi S è infinito, poiché $|A| \leq |S|$ (cfr. Proposizione 3.2.1).
Viceversa, sia S infinito, allora $|S| \geq |\mathbb{N}|$ e, per definizione di diseguaglianza tra potenze, esiste $A \subseteq S$ tale che $|A| = |\mathbb{N}|$, onde l'asserto.

Esercizio 3.2.9. *Si provi che un insieme è infinito sse, $\forall\, x \in S$, è*

$$|S \setminus \{x\}| = |S|.$$

Dim. Se S è infinito, si ha $|S \setminus \{x\}| = |S|$, $\forall\, x \in S$ (cfr. Es. 3.2.7).
Proviamo allora il viceversa, cioé

$$|S \setminus \{x\}| = |S|,\ \forall\, x \in S \implies S \text{ infinito}.$$

basterà provare che

$$S \text{ finito} \implies |S \setminus \{x\}| \neq |S|.$$

Se S è finito, e $|S| = n$, allora

$$x \in S \implies |S \setminus \{x\}| = n - 1 \neq n,$$

onde l'asserto.
Si noti che la condizione "$\forall\, x \in S$" si può sostituire con la condizione "per qualche $x \in S$".

Esercizio 3.2.10. *Si provi che se S è un insieme infinito ed A è un insieme finito, $S \setminus A$ è un insieme infinito. Si provi inoltre che è*

$$|S \setminus A| = |S|; \quad |S \cup A| = |S|.$$

Dim. Se $S \cap A = \emptyset$, $S \setminus A = S$, quindi $S \setminus A$ è infinito ed è $|S \setminus A| = |S|$; inoltre, $S \cap A = \emptyset \implies (S \cup A) \setminus A = S$ ed essendo $A \subseteq S \cup A$, A finito, si ha, tenendo presente quanto dimostrato nell'Es. 3.2.7 (si sottrae ad $S \cup A$ l'insieme $\{x\}$, con $x \in A$, e si ripete il procedimento sull'insieme $(S \cup A) \setminus \{x\}$; tale procedimento ha termine perché A è finito, cioé contiene n elementi, per qualche $n \in \mathbb{N}$):

$$|(S \cup A) \setminus A| = |S \cup A| = |S|,$$

cioé $S \cup A$ è infinito.
Sia ora $S \cap A = \emptyset$. Poiché $S \cap A \subseteq A$, $S \cap A$ è finito; d'altra parte $S \setminus A = S \setminus (S \cap A)$; quindi, per quanto già osservato,

$$|S \setminus (S \cap A) = |S| = |S \setminus A|,$$

cioé $S \setminus A$ è infinito. Se $A \subseteq S$, è banalmente vero che $|S \cup A| = |S|$. In ogni caso,

$$S \cap A \neq \emptyset \implies S \cup A = S \cup (A \setminus (S \cap A))$$

ed $A \setminus (S \cap A)$ è finito, perché tali sono i due insiemi A ed $S \cap A$, ed è disgiunto da S. Allora, da

$$S = (S \cup (A \setminus (S \cap A))) \setminus (A \setminus (S \cap A)$$

segue

$$|S| = |S \cup (S \setminus (S \cap A))| = |S \cup A|,$$

cioé l'asserto (si tenga presente l'Es. 3.2.7).

Esercizio 3.2.11. *Si provi che un insieme S è infinito sse*

$$|S \cup \{x\}| = |S|, \text{ per qualche } x \notin S.$$

Dim. Se S è infinito ed $x \notin S$,

$$(S \cup \{x\}) \setminus \{x\} = S \implies |(S \cup \{x\}) \setminus \{x\}| = |S|,$$

ma $|(S \cup \{x\}) \setminus \{x\}| = |S \cup \{x\}|$ (cfr. Es. 3.2.10), quindi l'asserto.
Viceversa proviamo che

$$|S \cup \{x\}| = |S|, \ x \notin S \implies \text{infinito},$$

cioé che

$$S \text{ finito} \implies |S \cup \{x\}| \neq |S|, \ x \notin S.$$

Se S è finito, $|S| = n$ e $|S \cup \{x\}| = n + 1$, onde l'asserto.

Esercizio 3.2.12. *Siano A e B due insiemi qualsiasi. Si provi che*

$$|A| = |B| \implies |P(A)| = |P(B)|.$$

Dim. Se $|A| = |B|$, esiste una biiezione $f : A \longrightarrow B$; quindi, $\forall\, x \in A$, $f|_X : X \longrightarrow B$ è una biiezione di X su $f(X)$. Pertanto, $f : A \longrightarrow B$ individua una biiezione $g : P(A) \longrightarrow P(B)$, definita da

$$\forall\, X \in P(A), \quad g(X) = |_X.$$

Ne segue l'asserto.

Esercizio 3.2.13. *Siano A e B due insiemi. Si provi che $|P(A)| = |P(B)|$ non implica necessariamente $|A| = |B|$.*

Dim. Basta osservare che dall'equipotenza di due insiemi non segue quella di coppie qualsiasi di loro sottoinsiemi. Infatti A è equipotente ad un s.i. di $P(A)$, $A' = \{\{a\} : a \in A\}$ e così pure B è equipotente ad un s.i. di $P(B)$.

Esercizio 3.2.14. *Siano A e B due insiemi qualsiasi. Si provi che*

$$|A \setminus B| = |B \setminus A| \implies |A| = |B|.$$

Dim. Per definizione di differenza

$$A \setminus B = A \setminus (A \cap B),\ B \setminus A = B \setminus (A \cap B).$$

Poniamo $C = A \cap B$; allora

$$A \setminus B = A \setminus C = \mathcal{C}_A C;\ B \setminus A = B \setminus C = \mathcal{C}_B C.$$

Dall'ipotesi, segue che esiste $f : A \setminus B \longrightarrow B \setminus A$, f biiezione; cioé $f : \mathcal{C}_A C \longrightarrow \mathcal{C}_B C$. Consideriamo l'applicazione $\phi : A \longrightarrow B$ tale che $\phi|_C = e_C$, $\phi|_{\mathcal{C}_A} = f$. ϕ è una biiezione, in quanto C e $\mathcal{C}_A C$ sono disgiunti ed e_C ed f sono biiezioni. Pertanto $|A| = |B|$.

Esercizio 3.2.15. *Sia S un insieme infinito e sia $A \subseteq S$ tale che $|A| \neq |S|$. Si provi che esiste $B \subseteq S \setminus A$ tale che $|B| = |A|$.*

Dim. Dato che $A \subseteq S$ e $|A| \neq |S|$, si ha $|A| < |S|$. Ne segue che $|S \setminus A| = |S|$, quindi esiste $f : S \longrightarrow S \setminus A$, f biiezione. Pertanto, $f(A) \subseteq S \setminus A$ è equipollente ad A ($f|_A : A \longrightarrow f(A)$ è una biiezione); assunto $B = f(A)$, l'affermazione è provata.

Esercizio 3.2.16. *Siano A, B, C, tre insiemi. Si provi che*

$$B \subset A \text{ e } |B| = |B \cup C| \implies |A| = |A \cup C|.$$

Dim. Siano A, B, C infiniti; poiché $C \subseteq B \cup C$, $|C| \leq |B \cup C|$, quindi

$$|B| = |B \cup C| \implies |C| \leq |B|.$$

D'altra parte, $B \subset A \implies |B| \leq |A| \implies |C| \leq |A|$, cioé l'asserto.
Se invece gli insiemi sono finiti,

$$|B| = |B \cup C| \implies C \subseteq B \implies C \subseteq A \implies A = A \cup C \implies |A| = |A \cup C|$$

e l'affermazione è provata.

Esercizio 3.2.17. *Siano A, B, C, D quattro insiemi, tali che*

$$|A| = |C|,\ |B| = |D|,\ A \cap B = \emptyset,\ C \cap D = \emptyset.$$

Si provi che $|A \cup B| = |C \cup D|$.

Diim. Per definizione di numero cardinale,

$$|A| = |C| \implies \exists\, f \in C^A,\ f \text{ biiezione},$$

$$|B| = |D| \implies \exists\, g \in D^B,\ g \text{ biiezione}.$$

Consideriamo l'applicazione $\phi : A \cup B \longrightarrow C \cup D$ tale che $\phi|_A = f$, $\phi|_B = g$. Dato che $A \cap B = C \cap D = \emptyset$, ϕ è una biiezione. Ne segue $|A \cup B| = |C \cup D|$, cioé l'asserto.

Esercizio 3.2.18. *Siano A, B, C, D quattro insiemi tali che*

$$|A| = |C|,\ |B| = |D|.$$

Si provi che $|A \times B| = |C \times D$.

Dim. Si ha

$$|A| = |C| \implies [\exists\, f : A \longrightarrow C, f \text{ biiezione}],$$

$$|B| = |D| \implies [\exists\, g : B \longrightarrow D, g \text{ biiezione}].$$

Consideriamo l'applicazione $f \times g : A \times B \longrightarrow C \times D$, definita da

$$\forall\, (a, b) \in A \times B, \quad f \times g\,((a, b)) = (f(a), g(b)).$$

Dato che f e g sono biiezioni, anche $f \times g$ è una biiezione (cfr. Es. 1.14.55), onde l'asserto.

Esercizio 3.2.19. *Sia $f \in B^A$ un'applicazione suriettiva. Si provi che $|B| \leq |A|$.*

Dato che $\mathrm{Im}\, f = B$, non può essere $|B| > |A|$, quindi $|B| \leq |A|$.

Esercizio 3.2.20. *Siano A, B, C, D quattro insiemi soddisfacenti le seguenti condizioni:*

$$A \cap B = C \cap D = \emptyset;\ |A| = |B|;\ |C| = |D|;\ |A \cup B| = |C \cup D|.$$

Si provi che $|A| = |C|$.

Sol. Osserviamo innanzitutto che, se uno qualsiasi dei quattro inseimi è finito, sono finiti anche gli altri tre, e la proposizione si prova subito. Infatti, se A è finito, $|A| \in \mathbb{N}$, quindi $|A| = |B| \implies |B| \in \mathbb{N}$, $|A \cup B| = 2|A| \in \mathbb{N}$ (in quanto $A \cap B = \emptyset$) e $|A \cup B| = |C \cup D| \implies |C \cup D| = 2|A|$, ma $|C| = |D|$, per cui $|C \cup D| = 2|C|$ (essendo $C \cap D = \emptyset$) onde $2|C| = 2|A| \implies |A| = |C|$.

Analogamente, se $|A| \geq |\mathbb{N}|$, anche gli altri insiemi sono infiniti. In questo caso
$|A| = |B| \implies |A \cup B| = |A|$ e $|C| = |D| \implies |C \cup D| = |C|$; infatti $|A| = |B| \implies \exists f : B \longrightarrow A$, f biiezione; definiamo $\phi : A \cup B \longrightarrow A$ in modo che $\phi|_A = e_A$, $\phi|_B = f$; ϕ è una biiezione, dato che $A \cap B = \emptyset$; similmente si prova che $|C \cup D| = |C|$.
Pertanto $|A \cup B| = |C \cup D| \implies |A| = |C|$, cioé l'asserto.

Esercizio 3.2.21. *Sia A un s.i. di $\mathbb{N}$. Si provi che A è finito oppure numerabile.*

Dim. Basterà provare che ogni s.i. infinito di $\mathbb{N}$ è numerabile. Dato che $\mathbb{N}$ è un insieme ben ordinato rispetto a $\leq$, consideriamo in A l'ordinamento indotto dalla relazione $\geq$. Allora A è una successione di naturali, quindi è numerabile (ordinati gli elementi di A, si associano ad essi, nell'ordine, $0, 1, 2, \ldots$).
Si noti che questo esercizio costituisce un'altra dimostrazione della Prop. 3.2.2.

Esercizio 3.2.22. *Si provi che un insieme S ha la potenza del numerabile sse è equipotente a ciascuno dei suoi s.i. infiniti.*

Dim. Se S è numerabile, ogni suo s.i. infinito numerabile (cfr. Es.3.2.21, tenendo presente che $|S| = |\mathbb{N}| \implies \exists f : S \longrightarrow \mathbb{N}$, f biiezione).
Viceversa, supponiamo che, per ogni $A \subseteq S$, A infinito, risulti $|A| = |S|$ e proviamo che $|S| = |\mathbb{N}|$. Dato che S è infinito, S contiene un s.i. numerabile (cfr. Es. 3.2.8); sia esso B, ne segue

$$|S| = |B| \implies |S| = |\mathbb{N}|.$$

Esercizio 3.2.23. *Siano A e B due insiemi e sia $|A| = |B|$. Si provi che allora non è necessariamente vero che $|A \setminus B| = |B \setminus A|$.*

Dim. Per provare l'affermazione basta fornire un esempio in cui

$$|A| = |B| \not\implies |A \setminus B| = |B \setminus A|.$$

Sia $A = \mathbb{N}$ e sia $B = 2\mathbb{N}$ (cioé B è l'insieme dei numeri pari); allora $|A| = |B|$. D'altra parte, $A \setminus B$ è l'insieme dei numeri dispari,onde $|A \setminus B| = |\mathbb{N}|$, mentre $B \setminus A = \emptyset$, quindi $|A \setminus B| \neq |B \setminus A|$.
Esistono però casi in cui l'affermazione è vera; ad esempio, se

$$A = \{a, b, c, x, y\}, \quad B = \{a', b', c', x, y\},$$

si ha $|A| = |B|$, $A \setminus B = \{a, b, c\}$, $B \setminus A = \{a', b', c'\}$ e quindi $|A \setminus B| = |B \setminus A|$.

Esercizio 3.2.24. *Siano A, B, C, D quattro insiemi tali che $|A| = |B|, |C| = |D|$. Si provi che non è necessariamente $|A \cap B| = |C \cap D|$.*

Dim. Proveremo l'affermazione fornendo un controesempio. Sia

$$A = \mathbb{N},\ B = 3\mathbb{N},\ C = 2\mathbb{N},\ D = \{2n+1 : n \in \mathbb{N}\}.$$

Allora $|A| = |B|$ ($|3\mathbb{N}| = |\mathbb{N}|$, in quanto $f : \mathbb{N} \longrightarrow 3\mathbb{N}$, $f(n) = 3n$, $\forall\, n \in \mathbb{N}$, è una biiezione), $|C| = |D|$, ma $A \cap B = B$, onde $|A \cap B| = |\mathbb{N}|$, mentre $C \cap D = \emptyset$, quindi $|C \cap D| = 0$.

3.3 Alcuni esempi di insiemi con la potenza del numerabile e di insiemi con la potenza del continuo.

Abbiamo stabilito che l'insieme $\mathbb{N}$ dei natuali ha la potenza del numerabile (per definizione) e che l'insieme $\mathbb{R}$ dei numeri reali ha la potenza del continuo; nulla, però, è stato detto sugli insiemi $\mathbb{Z}$ (degli interi relativi), $\mathbb{Q}$ (dei razionali).
Proviamo dunque la

Proposizione 3.3.1. *L'insieme $\mathbb{Z}$ ha la potenza del numerabile.*

Dimostrazione. Tenendo presente la definizione, basterà provare che esiste una biiezione di $\mathbb{Z}$ su $\mathbb{N}$. Consideriamo l'applicazione

$$f : \mathbb{Z} \longrightarrow \mathbb{N}$$

definita da $f(0) = 0$ e $\forall\, z \in \mathbb{Z} - \{0\}$

$$\begin{array}{ll} f(z) = 2|z|, & \text{se } z < 0, \\ f(z) = 2|z| - 1, & \text{se } z > 0. \end{array}$$

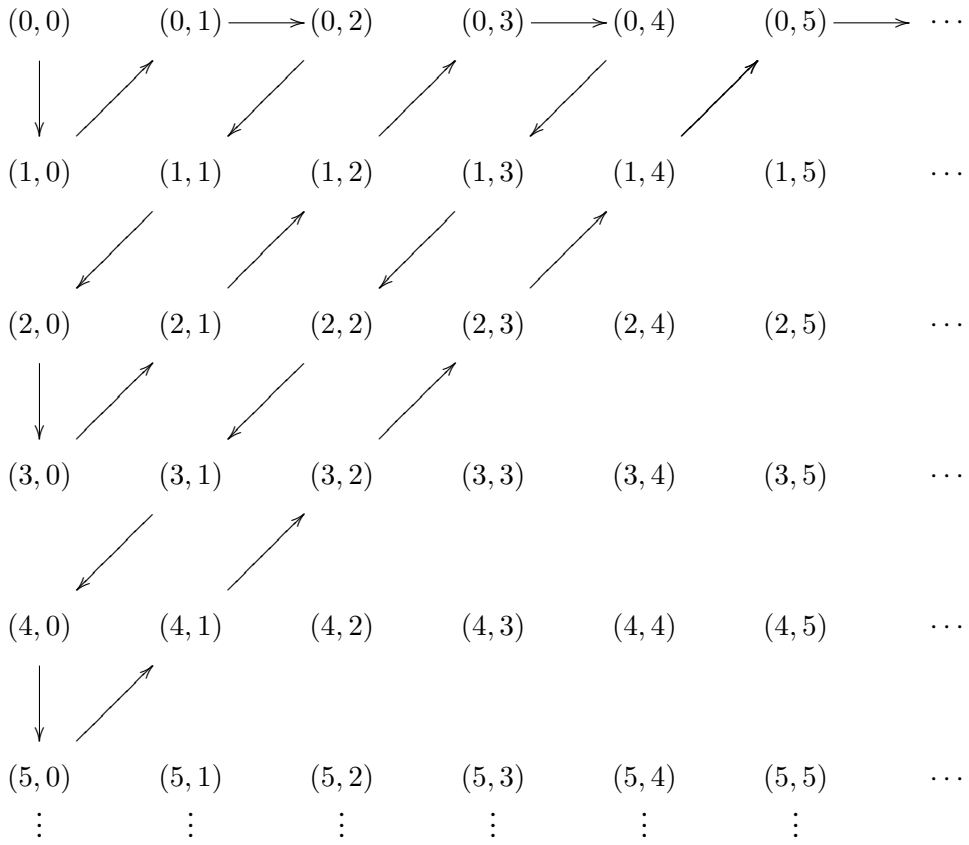
f è una biiezione; infatti f è su, dato che le immagini degli interi positivi sono i naturali dispari e quelle degli interi negativi sono i naturali pari. f è iniettiva; infatti, $\forall\, n \in \mathbb{N} - \{0\}$, se n è pari, $n = 2m$, $f^{-1}(2m) = -m \in \mathbb{Z}$; se n è dispari, $n = 2m - 1$, $f^{-1}(2m - 1) = m \in \mathbb{Z}$.
Ne segue l'asserto. □

Per stabilire la cardinalità di $\mathbb{Q}$, proviamo innanzitutto la

Proposizione 3.3.2. $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, $\mathbb{N}$ *essendo l'insieme dei numeri naturali.*

Dimostrazione. Per provare l'affermazione, useremo il *procedimento diagonale di Cantor*. Scriviamo gli elementi di $\mathbb{N} \times \mathbb{N}$ in una tabella illimitata nei due

sensi, precisamente:



Percorrendo la tabella come è indicato dalle frecce ed associando a ciascuna coppia i naturali $0, 1, 2, 3, \ldots$ (cioè $(0,0) \mapsto 0$, $(1,0) \mapsto 1$, $(0,1) \mapsto 2$, $(0,2) \mapsto 3$, $(1,1) \mapsto 4$, $(2,0) \mapsto 5$, $(3,0) \mapsto 6, \ldots$) si ottiene manifestamente una biiezione di $\mathbb{N} \times \mathbb{N}$ su $\mathbb{N}$, onde l'asserto. □

Osserviamo che questa biiezione non è unica; ad esempio si può considerare

$$(0,0) \mapsto 0,\ (0,1) \mapsto 1,\ (1,0) \mapsto 2,\ (2,0) \mapsto 3, \ldots$$

D'altra parte, si può anche provare l'affermazione verificando che l'applicazione $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, definita da

$$\forall\, (m,n) \in \mathbb{N} \times \mathbb{N}, \quad f((m,n)) = \frac{1}{2}(m+n+1)(m+n) + n,$$

è una biiezione.
Conseguenza immediata di quanto ora provato sono i seguenti

Corollario 3.3.3. *Sia S un insieme numerabile; allora $|S \times S| = |S|$.*

Dimostrazione. Basta tener presente che, se S è numerabile, esiste una biiezione di S su $\mathbb{N}$. □

Corollario 3.3.4. *Se S è un insieme numerabile ed $n \in \mathbb{N}$, si ha*

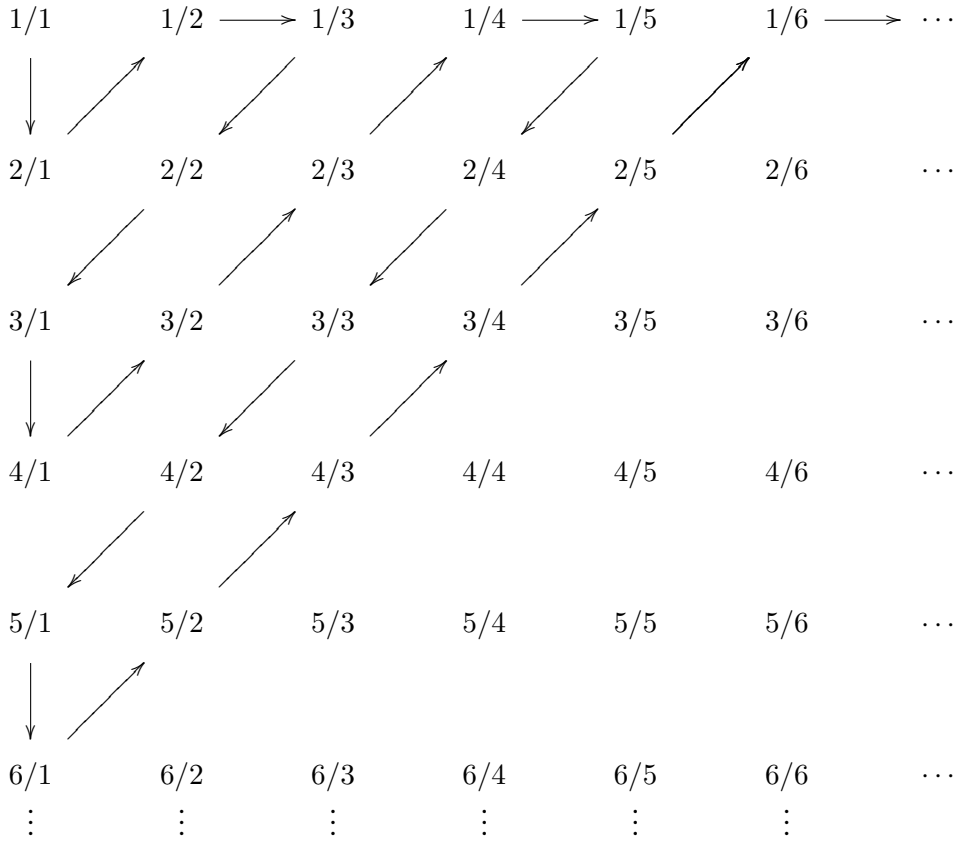
$$|S^n| = |S \times \cdots \times S| = |S|.$$

Dimostrazione. Infatti, $|S \times S| = |S| \implies |(S \times S) \times S| = |S \times S| = |S| \implies |S^3| = |S| \implies \ldots \implies |S^n| = |S|$. □

Siamo ora in grado di stabilire la

Proposizione 3.3.5. *L'insieme $\mathbb{Q}^+$ dei razionali non negativi ha la potenza del numerabile.*

Dimostrazione. Poiché ogni elemento di $\mathbb{Q}^+$ è una coppia ordinata di naturali (il secondo dei quali non nullo), il procedimento diagonale di Cantor applicato alla seguente tabella rappresentativa dei numeri razionali



fornisce la biiezione f di $\mathbb{Q}^+ - \{0\}$ su $\mathbb{N} - \{0\}$ (si pone poi $f(0) = 0$). □

Osserviamo che si ottiene una biiezione sia considerando $\mathbb{Q}^+ - \{0\}$ come $(\mathbb{N} - \{0\}) \times (\mathbb{N} - \{0\})$, sia sopprimendo nella tabella quelle frazioni che, ridotte ai minimi termini, individuano un razionale già considerato (basta cancellare la frazione e "prolungare la freccia"). Poiché tale insieme è costituito da una infinità numerabile di copie di $\mathbb{N}$ (ad esempio, tutti gli elementi della diagonale principale rappresentano il numero 1), resta stabilito che

Proposizione 3.3.6. *L'unione di un'infinità numerabile di insiemi numerabili è un insieme numerabile. In particolare, l'unione di un numero finito di insiemi numerabili ha la potenza del numerabile.*

Determiniamo infine la cardinalità di $\mathbb{Q}$.
Si ha

Proposizione 3.3.7. *L'insieme $\mathbb{Q}$ dei razionali ha la potenza del numerabile.*

Dimostrazione. Detto $\mathbb{Q}^-$ l'insieme dei razionali negativi, $\mathbb{Q} = \mathbb{Q}^- \cup \mathbb{Q}^+$; dato che $|\mathbb{Q}^-| = |\mathbb{Q}^+ - \{0\}| = |\mathbb{Q}^+| = |\mathbb{N}|$ (l'applicazione $f : \mathbb{Q}^+ - \{0\} \longrightarrow \mathbb{Q}^-$ definita da $f(\frac{m}{n}) = -\frac{m}{n}$, $m, n \in \mathbb{N}$, $n \neq 0$, è una biiezione), per la Prop. 3.3.7 si ha $|\mathbb{Q}| = |\mathbb{N}|$ (si noti che si poteva anche tener presente la Prop. 3.3.1). □

Il risultato stabilito dalla Prop. 3.3.2 non è una proprietà caratteristica degli insiemi numerabili. Infatti sussiste la

Proposizione 3.3.8. *Sia $\mathbb{R}$ l'insieme dei numeri reali. Allora*

$$|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|.$$

Dimostrazione. Proveremo l'asserto dimostrando che $|I \times I| = |I|$, dove $I = \{x \in \mathbb{R} : 0 \geq x \leq 1\}$ (cfr. Prop. 3.3.8), cioé costruendo una biiezione $f : I \times I \longrightarrow I$.
Utilizziamo ancora la numerazione in base 2 per gli elementi di I, ogni elemento di I (numero reale compreso tra 0 ed 1) si identifica con una successione arbitraria di 0 ed 1. Sia pertanto $(a_0, a_1, \dots, a_n, \dots)$, $a_j \in \{0, 1\}$, una tale successione. A tale successione si può univocamente associare la coppia di successioni

$$(a_0, a_2, a_4, \dots, a_{2t}, \dots),$$

$$(a_1, a_3, a_5, \dots, a_{2t+1}, \dots),$$

che sono ancora successioni aribtrarie di 0 ed 1.
Tale coppia di successioni è un ben determinato elemento di $I \times I$. Viceversa, fissato comunque un elemento di $I \times I$, cioé una coppia di successioni arbitrarie di 0 ed 1

$$(b_0, b_1, \dots, b_n, \dots), \quad (c_0, c_1, \dots, c_m, \dots),$$

a questa resta associata la successione

$$(b_0, c_0, b_1, c_1, b_2, c_2, \dots),$$

che è un elemento di I. Pertanto resta definita una biiezione $f : I \times I \longrightarrow I$, onde $|I \times I| = |I|$. Ma $|I| = |\mathbb{R}|$, quindi $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$, come volevasi provare. □

Ne discendono i

Corollario 3.3.9. *Se S è un qualunque insieme avente la potenza del continuo, $|S \times S| = |S|$.*

Corollario 3.3.10. *Se S ha la potenza del continuo ed $n \in \mathbb{N}$,*

$$|S^n| = |S \times \cdots \times S| = |S|.$$

Dimostrazione. Infatti $|S \times S| = |S| \implies |S \times S \times S| = |S \times S| = |S| \implies |S^3| = |S| \implies \ldots \implies |S^n| = |S|$. □

In base alla Prop. 3.3.8, possiamo anche affermare che, detto $\mathbb{C}$ l'insieme dei numeri complessi, $|\mathbb{C}| = |\mathbb{R}|$. Infatti, ogni numero complesso è una coppia ordinata di numeri reali, quindi

$$|\mathbb{C}| = |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|.$$

Osserviamo che il risultato della Prop. 3.3.6 si può invertire. Sussiste infatti la

Proposizione 3.3.11. *L'insieme $\mathbb{N}$ dei numeri naturali è unione di un'infinità numerabile (cioé l'insieme degli indici della famiglia di insiemi cui si considera l'insieme è numerabile) di insiemi numerabili, a due a due disgiunti.*

Dimostrazione. Proveremo l'asserto costruendo una famiglia $(A_i : i \in I,\ |I| = |\mathbb{N}|)$ di insiemi tali che

$$\bigcup (A_i : i \in I) = \mathbb{N},\ i \neq j \implies A_i \cap A_j = \emptyset.$$

Definiamo pertanto

$$\begin{aligned}
A_0 &= \{0, 2, 4, 6, 8, \ldots\}, (\text{ progressione aritmetica di ragione } 2)\\
A_1 &= \{1, 5, 9, 13, 17, 21, \ldots\}, (\text{ progressione aritmetica di ragione } 4)\\
A_2 &= \{3, 11, 19, 27, 35, \ldots\}, (\text{ progressione aritmetica di ragione } 8)\\
A_3 &= \{7, 23, 39, 55, 71, \ldots\}, (\text{ progressione aritmetica di ragione } 16)\\
\ldots &\quad \ldots\\
A_j &= \{n \in \mathbb{N} : [\exists\, k \in \mathbb{N} : n = 2^j(2k+1) - 1]\}, (\text{ progressione aritmetica di ragione } 2^{j+1}).
\end{aligned}$$

È evidente che $A_i \cap A_j = \emptyset$, se $i \neq j$, ed $|A_i| = |\mathbb{N}|$, $\forall\, j \in \mathbb{N}$. Inoltre, $\mathbb{N} = \bigcup (A_t : t \in \mathbb{N})$; ne segue l'asserto. □

Ne discende il

Corollario 3.3.12. *Ogni insieme numerabile è unione di un'infinità numerabile di insiemi numerabili a due a due disgiunti. In particolare, un insieme numerabile è unione di un numero finito di insiemi numerabili a due a due disgiunti.*

Un risultato analogo vale anche per insiemi aventi la potenza del continuo. Precisamente si può dimostrare la

Proposizione 3.3.13. *Siano A e B due insiemi aventi la potenza del continuo (disgiunti o no); allora $A \cup B$ ha la potenza del continuo.*
Inoltre, se $A_1, \ldots, A_n$ hanno la potenza del continuo, anche $\bigcup_{i=1}^{n} A_i$ ha la potenza del continuo. Infine, se $(A_i : i \in I)$ è una famiglia numerabile o continua (cioé $|I| = |\mathbb{N}|$, oppure $|I| = |\mathbb{R}|$) di insiemi aventi la potenza del continuo, l'insieme $\bigcup(A_i : i \in I)$ ha la potenza del continuo.

Le Prop. 3.3.2 e 3.3.8 (ed i loro corollari) si estendono al caso di insiemi di cardinalità transfinita qualsiasi. Si può infatti provare la

Proposizione 3.3.14. *Se S è un qualunque insieme infinito $|S \times S| = |S|$.*

Proviamo ora la

Proposizione 3.3.15. *Sia S un insieme di cardinalità qualsiasi superiore al numerabile; allora S contiene un s.i. numerabile.*

Dimostrazione. L'affermazione è evidente se si considera $\mathbb{R}$ (che ha la potenza del continuo); infatti i naturali si possono considerare come un s.i. dei reali. Proviamo l'affermazione in generale. Poiché S ha cardinalità superiore al numerabile, $|S| > |\mathbb{N}|$, non esiste alcuna biiezione di S su $\mathbb{N}$. Sia $f : \mathbb{N} \longrightarrow S$ una qualunque applicazione iniettiva (certamente esistente, perchè elemento di $S^{\mathbb{N}}$). Sarà $\operatorname{Im} f \subset S$, dato che f non può essere su ($|S| > |\mathbb{N}|$), e $|\operatorname{Im} f| = |\mathbb{N}|$ in quanto $f|^{\operatorname{Im} f}$ è una biiezione (f è iniettiva). Pertanto $\operatorname{Im} f$ è il s.i. cercato di S. □

La Prop. 3.3.15 si può completare mediante la

Proposizione 3.3.16. *Sia S un insieme avente potenza superiore al numerabile e sia $A \subset S$ un insieme numerabile. Allora*

$$|S \setminus A| = |S|.$$

Dimostrazione. Proviamo l'affermazione nel caso in cui S abbia la potenza del continuo. Se $S \setminus A$ fosse numerabile, dato che A è numerabile, l'insieme $(S \setminus A) \cup A = S$ sarebbe numerabile (cfr. Prop. 3.3.6), contro l'ipotesi; pertanto $S \setminus A$ ha la potenza del continuo (in quanto $(S \setminus A) \subset S \implies |S \setminus A| \leq |S|$). L'estensione ad una cardinalità qualsiasi per S, è immediata. In particolare, l'affermazione è vera se $|A| \in \mathbb{N}$. □

Altre questioni relative ai numeri cardinali transfiniti (e finiti) saranno viste nel seguito e negli esercizi.

Esercizi

Esercizio 3.3.1. *Siano A e B due insiemi aventi la potenza del numerabile. Si provi che $A \times B$ è numerabile.*

Dim. Per definizione di potenza,

$$|A| = |\mathbb{N}| \Rightarrow \exists f : A \longrightarrow \mathbb{N}, \text{ f biiezione}$$

$$|B| = |\mathbb{N}| \Rightarrow \exists g : B \longrightarrow \mathbb{N}, \text{ g biiezione}$$

Si può allora applicare all'insieme $A \times B$ il procedimento diagonale di Cantor, onde l'asserto.

Esercizio 3.3.2. *Sia S un insieme avente potenza superiore al numerabile e sia A un insieme numerabile. Si provi che*

$$|S \cup A| = |S|$$

Dim. L'affermazione è banalmente vera se $A \subseteq S$. Supponiamo dunque $S \cap A = \emptyset$. Poichè A è un s.i. numerabile di $S \cup A$, $(S \cup A) \setminus A = S$ ha la potenza di S (per la prop. **??**).

Ovviamente, l'enunciato è vero anche se A è finito.

Esercizio 3.3.3. *Sia S un insieme infinito e sia A un insieme numerabile. Si provi che*

$$|S \cup A| = |S|$$

Dim. Se S è infinito, la sua potenza è almeno quella del numerabile. Se è superiore a quella del numerabile, l'affermazione è provata nell'es. 3.3.2.

Supponiamo allora $|S| = |\mathbb{N}|$. Se fosse $|S \cup A| > |\mathbb{N}|$, dato che A è numerabile ed $(S \cup A) \setminus A = S$, anche S avrebbe potenza superiore al numerabile. Ne segue l'asserto.

Esercizio 3.3.4. *Sia S un insieme numerabile e sia $A \neq \emptyset$ un s.i. finito di S. Si provi che gli insiemi*

$$S \cup A,\ S \setminus A,\ S \times A,\ A \times S,\ S^A$$

sono tutti numerabili

Dim. Poichè $A \subseteq S$, $S \cup A = S$ onde $|S \cup A| = |S|$.

$S \setminus A$ è il complementare di A in S; se fosse finito, $(S \setminus A) \cup A = S$ sarebbe finito, contro l'ipotesi; pertanto $S \setminus A$ è numerabile.

Per provare le altre due affermazioni, sia $A = \{a_o, \cdots, a_{n-1}\}$; allora $S \times A = (S \times \{a_0\}) \cup (S \times \{a_1\} \cup \cdots \cup (S \times \{a_{n-1}\})$. D'altra parte, per ogni $j \in \{0, 1, \ldots, n-1\}$, $|S| = |S \times \{a_j\}|$; infatti l'applicazione $f : S \longrightarrow S \times \{a_j\}$ definita da

$$f(x) = (x, a_j) \in S \times \{a_j\}, \forall x \in S,$$

è manifestamente una biiezione. L'asserto segue dal fatto che l'unione di un numero finito di insiemi numerabili è numerabile (cfr. prop. **??** e **??**).

Inoltre $|S \times A| = |A \times S|$, perchè esiste una biiezione tra i due insiemi (cfr. es. 3.2.6).

Proviamo infine che $|S^A| = |S|$. Poichè A è finito, per ogni applicazione $f : A \longrightarrow S,\ f \in S^A,\ f(A) = \mathrm{Im}f$ è un s.i. finito di S. Considerare S^A significa dunque considerare tutti i possibili s.i. finiti di S contenenti al più $|A|$ elementi. L'insieme di tali insiemi è pertanto numerabile.

Esercizio 3.3.5. *Se S è un insieme infinito ed A è un insieme numerabile, si provi che*

$$|S \times A| = |S|$$

Dim. Poichè A è numerabile, esiste $f : \mathbb{N} \longrightarrow A$, f biiezione, dunque gli elementi di A costituiscono una successione

$$< a_0, a_1, \ldots, a_n, \cdots > .$$

Pertanto

$$S \times A = \bigcup_{j \in \mathbb{N}} S \times \{a_j\}.$$

D'altra parte, $|S \times \{a_j\}| = |S|$, in quanto l'applicazione $g : S \longrightarrow S \times \{a_j\}$, definita da $f(x) = (x, a_j),\ \forall x \in S$, è manifestamente una biiezione. Ricordando che l'unione di un'infinità numerabile di insiemi aventi lo stesso cardinale transfinito (cfr. propp. **??** e **??**) ha quella cardinalità, si ha l'asserto.

Esercizio 3.3.6. *Sia S un insieme infinito, e sia $A \neq \emptyset$ un insieme tale che $|A| < |S|$. Si provi che*

$$|S \times A| = |S|$$

Dim. Se S è finito o numerabile, l'asserto è già stato provato (cfr. es. 3.3.5). Supponiamo dunque che $|A|$ sia un cardinale qualsiasi, e che $|A| \leq |S|$. Dall'ipotesi $|A| \leq |S|$ segue che esiste $B \subset S$ tale che $|A| = |B|$, onde esiste una biiezione di $S \times A$ su $S \times B$; basterà allora provare che $|S \times B| = |S|$. Ora $S \times B \subset S \times S$, e $|S \times \{b\}| = |S|$ (cfr. es. 3.2.3). Pertanto

$$|S| = |S \times \{b\}| \leq |S \times B| \leq |S \times S| = |S|,$$

onde $|S \times B| = |S|$, cioè l'asserto.

Esercizio 3.3.7. *Sia S un insieme qualsiasi. Diremo successione finita di elementi di S ogni s.i. finito di S, $A = \{a_0, a_1, \cdots, a_{n-1}\}$ che sia l'immagine di un'applicazione iniettiva f dell'insieme $\{0, 1, \ldots, n-1\}$ in S, definita da*

$$f(i) = a_i \in S,\ \forall i \in \{0, 1, \ldots, n-1\}$$

ed $\mathrm{Im}f = A = \{a_0, a_1, \cdots, a_{n-1}\}$. Si provi che l'insieme di tutte le successioni finite di un insieme numerabile è un insieme numerabile.

Dim. Se S è numerabile, $|S| = |\mathbb{N}|$ e $\forall n \in \mathbb{N},\ S^n = \mathbb{N}^n = S^{\{0,1,\ldots,n-1\}}$ è numerabile (cfr. cor. **??**); ma $S^{\{0,1,\ldots,n-1\}}$ è l'insieme di tutte le applicazioni di $\{0, 1, \ldots, n-1\}$ in S, quindi contiene come s.i. l'insieme delle applicazioni iniettive, ciascuna delle quali individua una, ed una sola, successione di S. Pertanto, l'insieme delle successioni finite di un insieme numerabile è numerabile (essendo s.i. di un insieme numerabile).

Esercizio 3.3.8. *Si consideri l'insieme $2^{\mathbb{N}}$ delle funzioni caratteristiche di $\mathbb{N}$, e, ricordando che ciascuna funzione caratteristica di $\mathbb{N}$ è una successione arbitraria di 0 ed 1 (cfr. n.* **??** *ed es. 3.0.69), sia S il s.i. di $2^{\mathbb{N}}$ contenente tutte e sole le successioni aventi un numero finito di termini eguali ad 1. Si provi che S è numerabile.*

Dim. Per ogni $n \in \mathbb{N}$, l'insieme delle applicazioni iniettive di $\{0, 1, \ldots, n-1\}$ in un insieme numerabile A è numerabile (cfr. es. 3.3.7). Poichè A è numerabile, per ciascuna delle suddette applicazioni, resta individuata una successione di 0 ed 1, funzione caratteristica dell'immagine di $\{0, 1, \ldots, n-1\}$. S risulta dunque unione di un'infinità numerabile (al variare di n in $\mathbb{N}$) di insiemi numerabili, onde è numerabile (cfr. cor. **??**).

Esercizio 3.3.9. *Si consideri l'insieme $2^{\mathbb{N}}$ ed il suo s.i. T costituito da tutte le successioni che hanno infiniti termini eguali ad 1. Si provi che $|T| = |2^{\mathbb{N}}|$ (cfr. es. 3.3.8)*

Dim. Dato che $2^{\mathbb{N}}$ ha la potenza del continuo e che T è il complementare dell'insieme S, numerabile, di tutte le successioni contenenti un numero finito di termini eguali ad 1 (cfr. es. **??**), T ha la potenza del continuo (cfr. prop. **??** ed es. 3.3.21).

Esercizio 3.3.10. *Posto $n = \{0, 1, \ldots, n-1\}$, si provi che, per ogni $n \geq 2$, l'insieme $n^{\mathbb{N}}$ ($\mathbb{N}$ essendo l'insieme dei naturali, più in generale un qualunque insieme numerabile) ha la potenza del continuo.*

Dim. Se $n = 2$ l'affermazione è vera per definizione di potenza del continuo. Supponiamo $n = 3 = \{0, 1, 2\}$. In tal caso, $3^{\mathbb{N}}$ è l'insieme di tutte le applicazioni di $\mathbb{N}$ nell'insieme $\{0, 1, 2\}$. Consideriamo l'intervallo $I = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ dell'asse reale. Usando la numerazione in base 3 per i nueri reali dell'intervallo I, ogni $x \in I$ si identifica con una successione arbitraria formata con le cifre $0, 1, 2$. Per tanto, ogni elemento f di $3^{\mathbb{N}}$ individua una tale successione (come immagine dell'applicazione f), cioè un elemento di I, e viceversa. Poichè I ha la potenza del continuo, $3^{\mathbb{N}}$ ha la potenza del continuo. L'affermazione si prova in maniera analoga per ogni naturale n.

Esercizio 3.3.11. *Sia $n = \{0, 1, \ldots, n-1\}$ un qualunque insieme finito e sia $\mathbb{R}$ l'inisieme dei numeri reali. Si provi che*

$$|\mathbb{R} \times n| = |\mathbb{R}|.$$

Dim. L'affermazione è banalmente vera se $n = 1 = \{0\}$. Infatti, l'applicazione $f : \mathbb{R} \longrightarrow \mathbb{R} \times \{0\}$, definita da $f(x) = (x, 0), \forall x \in \mathbb{R}$, è manifestamente una biiezione.

Sia ora $n = 2 = \{0, 1\}$. L'insieme $\mathbb{R} \times \{0, 1\}$ ammette la partizione nei due s.i. $A_0 = \{(x, 0) : x \in \mathbb{R}\}$ ed $A_1 = \{(x, 1) : x \in \mathbb{R}\}$, ciascuno dei quali ha la potenza di $\mathbb{R}$ (cioè quella del continuo). Pertanto $|\mathbb{R} \times \{0, 1\}| = |A_0 \cup A_1| = |\mathbb{R}|$ (cfr. prop. **??**).

Analogamente , $\mathbb{R} \times n$ ammette la partizione $(A_j : j \in \{0, 1, \ldots, n-1\})$ con $A_j = \{(x, j) : x \in \mathbb{R}\}$, quindi

$$|\mathbb{R} \times n| = \left| \bigcup_{j=0}^{n-1} A_j \right| = |\mathbb{R}|,$$

in quanto l'unione di un numero finito di insiemi aventi la potenza del continuo ha la potenza del continuo.

Esercizio 3.3.12. *Denotato con $\mathbb{Z}[x]$ l'insieme dei polinomi nella indeterminata x a coefficienti interi, si provi che $\mathbb{Z}[x]$ ha la potenza del numerabile.*

Dim. Il generico elemento di $\mathbb{Z}[x]$ è del tipo

$$p(x) = a_o + a_1 x + a_2 x^2 + \cdots + a_n x^n, a_j \in \mathbb{Z}, j \in \{0, 1, \ldots, n\}$$

e se il grado del polinomio è n, il suo coefficiente direttore a_n è non nullo. Fissato n, e detto P_n l'insieme dei polinomi di grado $\leq n$, l'applicazione

$$f : P_n \longrightarrow \mathbb{Z}^{n+1} = \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{n+1 \text{ volte}}$$

definita da

$$f(p_n(x)) = (a_0, a_1, \ldots, a_n)$$

è una biiezione. Pertanto, dato che $\mathbb{Z}^{n+1}$ ha la potenza del numerabile (cfr. cor. **??**), P_n ha la potenza del numerabile. Ora

$$\mathbb{Z}[x] = \bigcup_{n \in \mathbb{N}} P_n$$

e l'unione di una famiglia numerabile di insiemi numerabili è numerabile; ne segue l'asserto.

Esercizio 3.3.13. *Tenendo presente che si definisce numero algebrico un numero reale che sia zero di un polinomio a coefficienti razionali, si provi che l'insieme A dei numeri algebrici ha la potenza del numerabile.*

Dim. Osserviamo innazitutto che possiamo considerare i coefficienti del polinomio interi, invece che razionali. Infatti, eguagliando a zero un

polinomio a coefficienti razionali, le radici dell'equazione algebrica così ottenuta sono le radici dell'equazione algebrica a coefficienti interi ottenuta riducendo tutti i coefficienti allo stesso denominatore ed annullando il numeratore.

Dato che l'insieme dei polinomi a coefficienti interi nell'indeterminata x ha la potenza del numerabile (cfr. es. 3.3.12) e dato che ogni polinomio siffatto di grado n ha al più n zeri (reali), l'insieme A dei numeri algebrici è contenuto nell'insieme

$$\underbrace{\mathbb{Z}[x] \cup \mathbb{Z}[x] \cup \cdots \cup \mathbb{Z}[x]}_{n \text{ volte}}$$

onde è numerabile, essendo infinito.

Osserviamo che ogni numero reale non agebrico si dice trascendente, e che la partizione dei reali in numeri algebrici e numeri trascendenti è distinta dalla partizione dei reali in razionali ed irrazionali. Infatti, ad esempio $\sqrt{2}$ è un numero algebrico (zero del polinomio x^2-2), ed è irrazionale. Inoltre, tutti i numeri razionali sono algebrici (sono zeri dei polinomi di primo grado $ax + b, a, b \in \mathbb{Z}$).

Esercizio 3.3.14. *Dimostrare che l'insieme dei numeri trascendenti ha potenza superiore a quella del numerabile.*

Dim. Ricordiamo che un numero reale si dice trascendente se non è radice di alcuna equazione algebrica a coefficienti interi. L'insieme $\mathbb{R}$ dei numeri reali resta pertanto suddiviso in due insiemi disgiunti: l'insieme A dei numeri algebrici (cioè quelli che sono radici di equazioni algebriche a coefficienti interi) e l'insieme T dei numeri trascendenti. $\mathbb{R}$ ha la potenza del continuo, mentre A ha la potenza del numerabile (cfr. es. 3.3.13); ne segue che $T = \mathbb{R} \setminus A$ ha ancora la potenza del continuo (cfr. prop. **??**).

Esercizio 3.3.15. *Sia $(A_i : i \in I)$ un insieme di intervalli di $\mathbb{R}$ tali che*

$$|A_i| > 1, \ \forall i \in I, \ \textit{ed} \ A_i \cap A_j \subset A_i, A_j, \forall i, j \in I, i \neq j.$$

Si provi che I è numerabile.

Dim. Ricordiamo che un intervallo $[a, b]$ di $\mathbb{R}$ è definito da

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\};$$

inoltre, le condizioni imposte agli intervalli A_i significano che ciascun A_i contiene più di un elemento e che, a due a due, gli intervalli non si sovrappongono.

Per provare che I è numerabile, osserviamo che ciascun A_i contiene un numero razionale; infatti, se $x, y \in A_i$ sono due numeri reali non razionali (certamente esistenti per ipotesi), esiste $a \in Q$ tale che $x \leq a \leq y$ (si pensi

alla rappresentazione dei numeri reali come allineamenti decimali arbitrari). Per ciascun A_i scegliamo un razionale $a_i \in A_i$. Poichè $A_i \cap A_j \subset A_i, A_j$, si possono scegliere a_i, a_j $(a_i \in A_i, a_j \in A_j)$ in modo che sia $a_i \neq a_j$. Consideriamo l'applicazione $f : I \longrightarrow \mathbb{Q}$ definita da

$$f(i) = a_i, \forall i \in I$$

f è iniettiva per costruzione; Imf è un s.i. infinito di $\mathbb{Q}$ (perchè I è infinito per ipotesi ed f è un'immersione); ma $\mathbb{Q}$ è numerabile, ne segue che Imf è numerabile (cfr. prop. **??** o es. 3.2.21), e pertanto I è numerabile (essendo f iniettiva).

Esercizio 3.3.16. *Siano S ed S' due insiemi infiniti disgiunti equipotenti. Si provi che*

$$|S \cup S'| = |S|$$

Dim. Poichè $|S| = |S'|$, esiste $f : S' \longrightarrow S$, f biiezione ed Imf=S. Pertanto $|S \cup S'| = |S \cup \text{Im}f|$; infatti l'applicazione $g : S \cup S' \longrightarrow S \cup \text{Im}f$, definita da $g|_S = e_S,\ g|_{S'} = f$ è una biiezione, in quanto $S \cap S' = \emptyset$ ed e_S ed f sono entrambe biiezioni. D'altra parte, $S \cup \text{Im}f = S$, quindi $|S \cup \text{Im}f| = |S|$; ne segue l'asserto.

Esercizio 3.3.17. *Sia S un insieme infinito qualsiasi; si provi che per ogni insieme A risulta*

$$|A| \leq |S| \Leftrightarrow |S \cup A| = |S|$$

Dim. Proviamo l'implicazione $\Rightarrow$. Supponiamo dapprima che sia $S \cap A = \emptyset$. $|A| \leq |S|$ significa che A è equipotente ad un s.i. di un insieme S', con $|S'| = |S|$. Pertanto $S \cup A \subseteq S \cup S' \Rightarrow |S \cup A| \leq |S \cup S'| = |S|$. D'altra parte, $S \subseteq S \cup A \Rightarrow |S| \leq |S \cup A|$. Ne segue l'asserto.

Se invece, $A \cap S \neq \emptyset$, posto $A \cap S = B$, l'argomentazione precedente fornisce $|S \cup (A \setminus B)| = |S|$ e quindi l'asserto (essendo $S \cup A = S \cup (A \setminus B)$).

Viceversa, sia $|S \cup A| = |S|$. Poichè per ogni insieme S' equipotente ad S e disgiunto da S si ha $|S \cup S'| = |S|$, è sicuramente $S \cup A \subseteq S \cup S'$ e quindi $|A| \leq |S'| = |S|$, come si voleva provare.

Esercizio 3.3.18. *Siano S ed S' due insiemi disgiunti aventi la potenza del continuo. Si provi che $S \cup S'$ ha la potenza del continuo.*

Dim. L'insieme $I = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ ha la potenza del continuo (cfr. prop. **??**) ed è $|I \setminus \{1\}| = |I|$ (cfr. es. 3.2.9). Consideriamo l'intervallo $I_1 = \{x \in \mathbb{R} : 0 \leq x < \frac{1}{2}\}$; si ha $|I_1| = |I|$. Infatti, l'applicazione $f : I \longrightarrow I_1$, definita da $f(x) = \frac{x}{2}, \forall x \in I$, è manifestamente una biiezione. Consideriamo ora l'intervallo $I_2 = \{x \in \mathbb{R} : \frac{1}{2} \leq x < 1\}$; si ha $|I_2| = |I_1| = |I|$, in quanto l'applicazione $g : I_1 \longrightarrow I_2$ definita da $g(x) = x + \frac{1}{2}, \forall x \in I_1$, è manifestamente una biiezione. I_1 ed I_2 sono disgiunti, hanno entrambi la potenza del continuo ed $I_1 \cup I_2 = I$, onde $|I_1 \cup I_2| = |I| = |I_1| = |I_2| = |\mathbb{R}|$.

Se ora S ed S' hanno entrambi la potenza del continuo, esistono le biiezioni $\phi : S \longrightarrow I_1$ e $\psi : S' \longrightarrow I_2$; quindi si può definire $\theta : S \cup S' \longrightarrow I$ nel modo seguente:

$$\theta|_S = \phi, \theta|_{S'} = \psi \text{ e } \mathrm{Im}\phi \cap \mathrm{Im}\psi = \emptyset, \mathrm{Im}\phi \cup \mathrm{Im}\psi = I$$

e θ è manifestamente una biiezione. (Se si vuole esplicitamente la biiezione $\eta : S \cup S' \longrightarrow S$, la si può costruire nel modo seguente

$$S \cup S' \longrightarrow^{\theta} I \longrightarrow^{f} I \longrightarrow^{\phi^{-1}} S$$

cioè $\eta = \phi^{-1} \circ f \circ \theta$).

Esercizio 3.3.19. *Si provi che l'unione di un numero finito $n \geq 0$ di un'infinità numerabile di insiemi a due a due disgiunti, ciascuno dei quali ha la potenza del continuo, è un insieme avente la potenza del continuo.*

Dim. Nel caso $n = 2$ l'affermazione è stata provata (cfr. es. 3.3.18), ed il procidemento seguito nel corso della dimostrazione si può estendere a qualunque intero $n \geq 2$. Precisamente, siano $S_1, \ldots, S_n$ gli insiemi assegnati, ciascuno avente la potenza del continuo. Si considerino gli n intervalli

$$I_k = \left\{x \in \mathbb{R} : \frac{j-1}{n} \leq x < \frac{1}{n}\right\},\ j = 1, 2, \ldots, n,$$

questi sono a due a due disgiunti; inoltre,

$$\bigcup_{j \in \{1,2,\ldots,n\}} I_j = I = \{x \in \mathbb{R} : 0 \leq x < 1\}$$

e ciascuno di essi ha la potenza del continuo. Infatti, l'applicazione $g : I \longrightarrow I_1$ definita da $g(x) = \frac{x}{n}\ \ \forall x \in I$ è manifestamente una biiezione, e tali sono pure le applicazoni $g_h : I_1 \longrightarrow I_h,\ h = 2, 3, \ldots, n$, definite da $g_h(x) = x + \frac{h-1}{n},\ x \in I_1$. Poichè gli insiemi S_j hanno la potenza del continuo, esistono le biiezioni $f_j : S_j \longrightarrow I_j$ e si può definire l'applicazione $f : S_1 \cup \cdots \cup S_n \longrightarrow I = \bigcup I_j$ in modo che $f|_{S_j} = f_j$, per cui f è una biiezione, onde $\bigcup S_j$ ha la potenza del continuo.

Sia ora $(S_j : j \in \mathbb{N})$ una famiglia numerabile di insiemi a due a due disgiunti, ciascuno avente la potenza del continuo. Proviamo che $\bigcup_{j \in \mathbb{N}} S_j$ ha la potenza del continuo.

Consideriamo la famiglia $(I_j : j \in \mathbb{N})$ di intervalli dell'asse reale x definita da

$$I_j = \left\{x \in \mathbb{R} : \frac{1}{2^{j+1}} \leq x < \frac{1}{2^j}\right\}(j = 0, 1, 2, \ldots).$$

Questi intervalli sono a due a due disgiunti, $\bigcup_{j \in \mathbb{N}} I_j = I$ ha la potenza del continuo e ciascun intervallo ha la potenza del continuo. Infatti, $g_0 : I \longrightarrow$

I_0, definita da $g_0(x) = \frac{1}{2} + \frac{x}{2}, \forall x \in I$, è una biiezione, e analogamente sono biiezioni:

$$g_1 : I_0 \longrightarrow I_1, \text{ definita da } g_1(x) = \frac{1}{4} + \frac{x}{2}, \forall x \in I_0,$$

$$g_2 : I_1 \longrightarrow I_2, \text{ definita da } g_2(x) = \frac{1}{8} + \frac{x}{2}, \forall x \in I_1$$

$$\dots$$

$$g_j : I_{j-1} \longrightarrow I_j, \text{ definita da } g_j(x) = \frac{1}{2^{j+1}} + \frac{x}{2}, \forall x \in I_{j-1}$$

(e scritto $I = I_{-1}$ si ritrova g_0). Si può quindi definire la biiezione $f : \bigcup_{j\in\mathbb{N}} S_j \longrightarrow \bigcup_{j\in\mathbb{N}} I_j$, in modo che $f|_{S_j} = f_j, j \in \mathbb{N}$, dove $f_j : S_j \longrightarrow I_j$ è una biiezione esistente, in quanto S_j e I_j hanno entrambi la potenza del continuo. Ne segue l'asserto.

Esercizio 3.3.20. *Si provi che l'unione di due insiemi A e B, non necessariamente disgiunti, ciascuno dei quali abbia la potenza del continuo, ha la potenza del continuo.*

Dim. Se $A \cap B = \emptyset$, l'affermazione è provata nell es. 19.18. Supponiamo $A \cap B \neq \emptyset$; se $B \subseteq A$, $A \cup B = A$, onde la proposizione è vera; escluderemo pertanto questo caso. Posto $C = A \cap B$, $A \cup B = A \cup (B \setminus C)$; ora $B \setminus C$ ha al più potenza del continuo, quindi $A \cup (B \setminus C)$ ha la potenza del continuo $(A \cap (B \setminus C) = \emptyset)$, onde l'asserto.

Esercizio 3.3.21. *Sia S un insieme avente la potenza del continuo e sia $A \neq \emptyset$ un insieme finito. Si provi che $S \times A$ ha la potenza del continuo.*

Dim. L'affermazione è banalmente vera se $|A| = 1$. Infatti, posto $A = \{a\}$, l'applicazione $f : S \times \{a\} \longrightarrow S$, definita da $f((x, a)) = x$ è manifestamente una biiezione. Supponiamo pertanto $|A| \geq 2$. Se $|A| = n$, esiste una biiezione di A sull'insieme $\{0, 1, 2, \dots, n-1\}$, quindi basta provare che $|S \times \{0, 1, \dots, n-1\}| = |S|$.

Dalla definizione di prodotto cartesiano segue che

$$S \times \{0, 1, \dots, n-1\} = \bigcup_{j=0}^{n-1} S \times \{j\}$$

e gli insiemi dell'unione sono a due a due disgiunti; inoltre, ciascuno di essi ha la potenza del continuo, onde l'asserto (cfr. es. 19.19).

Esercizio 3.3.22. *Sia S un insieme avente la potenza del continuo. Si provi che $S \times \mathbb{N}$ ha la potenza del continuo.*

Dim. Estendendo l'argomentazione svolta nella dimostrazione dell'es. 3.3.21, si può scrivere:

$$S \times \mathbb{N} = \bigcup_{j \in \mathbb{N}} S \times \{j\}$$

onde $S \times \mathbb{N}$ è unione di un'infinità numerabile di insiemi a due a due disgiunti, ciascuno avente la potenza del continuo, e pertanto (cfr. es. 3.3.19) ha la potenza del continuo.

Esercizio 3.3.23. *Sia S un insieme di cardinalità superiore al numerabile e sia A un s.i. di S finito o numerabile. Si provi che*

$$|S \setminus A| = |S|$$

Dim. Supponiamo che A sia numerabile. $S \setminus A$ non può essere numerabile, perchè, se così fosse, $(S \setminus A) \cup A$ sarebbe unione di due insiemi numerabili, quindi sarebbe numerabile. Pertanto $|S \setminus A| > |A|$.

Se S ha la potenza del continuo, l'affermazione è provata, come conseguenza dell'ipotesi del continuo e del fatto che $|S \setminus A| = |S|$.

Se S ha potenza al continuo, S contiene un s.i., C, che ha potenza del continuo, e si può sempre suppore $A \subset C$ e $|C \setminus A| = |C|$. D'altra parte, $S \setminus A = (S \setminus C) \cup (C \setminus A)$; sia $f : C \setminus A \longrightarrow C$ la biiezione esistente perchè i due insiemi hanno la stessa potenza; allora $\mathrm{Im} f = C$. Considerata l'applicazione

$$g : S \longrightarrow S \text{ tale che } g|_{S \setminus C} = e_{S \setminus C}, g|_{C \setminus A} = f,$$

g è una biiezione, quindi

$$|(S \setminus C) \cup (C \setminus A)| = |(S \setminus C) \cup C| = |S|,$$

cioè l'asserto.

Ovviamente, l'affermazione è vera nel caso particolare in cui A sia finito.

Esercizio 3.3.24. *Sia S un insieme infinito ed A un insieme per il quale $|A| < |S|$. Si provi che $|S \setminus A| = |S|$.*

Dim. L'affermazione è evidente se $A \cap S = \emptyset$, perchè, in tal caso, $S \setminus A = S$. Supponiamo $A \subset S$. Dato che $S = (S \setminus A) \cup A$ e $|A| < |S|$, si ha l'asserto (cfr. es. 3.3.17).

Esercizio 3.3.25. *Sia $\mathbb{N}$ l'insieme dei numeri naturali. Si provi che*

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

Dim. Dato che $|2^{\mathbb{N}}| = |P(\mathbb{N})|$ (cfr. n. **??**), basta provare che $|\mathbb{N}^{\mathbb{N}}| = |P(\mathbb{N})|$. Per definizione , $\mathbb{N}^{\mathbb{N}}$ è l'insieme di tutte le applicazioni di $\mathbb{N}$ in sè; ciascuna di esse ha un'immagine che è un s.i. di $\mathbb{N}$, cioè elemento di $P(\mathbb{N})$.

Viceversa, fissato $A \subseteq \mathbb{N}$, non è unica, in generale, l'applicazione $f \in \mathbb{N}^{\mathbb{N}}$, tale che $\mathrm{Im}f = A$ (è unica soltante se $|A| = 1$). Se $\mathrm{Im}f$ è un insieme di cardinalità finita n, l'insieme delle applicazioni che ammettono talte immagine è numerabile (e coincide con $n^{\mathbb{N}}$); se $\mathrm{Im}f$ è numerabile (e se è infinito, non può essere che numerabile - cfr. es. 3.2.21) è unione di un numero finito o di un'infinità numerabile di insiemi finiti o numerabili, quindi l'insieme delle applicazioni che ammettono $\mathrm{Im}f$ come immagine è numerabile. Pertanto, considerando tutti gli elementi di $P(\mathbb{N})$ come $\mathrm{Im}f$, dato che $P(\mathbb{N})$ ha la potenza del continuo e per ogni $A \in P(\mathbb{N})$ esiste un'infinità numerabile di applicazioni, si ottiene come insieme delle applicazioni di $\mathbb{N}$ in $\mathbb{N}$ un insieme avente la potenza del continuo (cfr. prop. **??**).

3.4 I teoremi di Cantor-Bernstein e Schroeder-Bernstein. L'aritmetica dei cardinali

Abbiamo già definito l'eguaglianza di due numeri cardinali e la disuguaglianza in senso stretto (cfr. n. **??**); possiamo allora definire la disuguaglianza in senso lato, ponendo

$$|A| < |B| \Rightarrow |A| \leq |B| \text{ e } |A| \neq |B|.$$

In tal modo la relazione sull'insieme dei nueri cardinali (finiti e transfiniti) è una relazione riflessiva e transitiva. (Si noti che tale realzione per i cardinali finiti coincide con la consueta relazione $\leq$ su $\mathbb{N}$). La riflessività è immediata; per provare la transitività, ricordiamo che

$$|A| < |B| \text{ sse } \exists B' \subset B; |A| = |B'| \text{ ma } \nexists A' \subset A : |A'| = |B'|.$$

Ne segue

$$|A| < |B|, |B| < |C| \Rightarrow |A| < |C|;$$

infatti, se $f : A \longrightarrow B$ e $g : B \longrightarrow C$ sono rispettivamente le biiezioni di A su B' e di B su C', $g \circ f$ è una biiezione di A su un s.i. di C' e quindi di C.

La relazione $\leq$ nell'insieme dei cardinali risulta anche antisimmetrica, come è provato dal

Teorema 3.4.1 (Teorema di Schroeder-Bernstein)**.** *Per ogni coppia di numeri cardinali $|A|, |B|$, se $|A| \leq |B|$ e $|B| \leq |A|$, allora $|A| = |B|$.*

Dimostreremo in seguito tale teorema in una forma equivalente. In base a quanto detto, si può affermare che l'insieme $\mathcal{C}$ dei numeri cardinali è un insieme parzialmente ordinato. Di fatto, $\mathcal{C}$ risulta totalmente ordinato ed anche ben ordinato.

Non dimostreremo questo risultato, ma osserviamo che, dati comunque due insiemi A e B , deve essere vera almeno una delle affermazioni seguenti

1. $|A| = |B|$;
2. $|A| \neq |B|$; ma A è equipotente ad un s.i. proprio di B, cioè $|A| < |B|$ (oppure $|B| < |A|$);
3. A è equipotente ad un s.i. di B e B è equipotente ad un s.i. di A;
4. A non è equipotente ad alcun s.i. di B e B non è equipotente ad alcun s.i. di A (cioè $|A| \not< |B|, |A| \neq |B|, |B| \not< |A|$).

I casi 1. e 2. sono evidenti in base a quanto già detto; il caso 3. costituisce l'ipotesi del teorema di Cantor-Bernstein, del quale diamo soltanto l'ennunciato:

Teorema 3.4.2 (Teorema die Cantor-Bernstein)**.** *Siano A e B due insiemi qualsiasi; se A è equipotente ad un s.i. di B e B è equipotente ad un s.i di A, allora $|A| = |B|$.*

Osserviamo che di tale teorema vale anche il viceversa (si tengano presenti la prop. **??** e l'es. 3.2.21).

L'ultimo caso risulta impossibile (com'è intuitivamente evidente).

Pertanto, l'insieme dei numeri cardinali è una catena (che ammette un primo elemento $O = \{\emptyset\}$). Di consegeunza, nell'insieme dei cardinali vale la cosiddetta legge di tricotomia: Per ogni coppia di numeri cardinali $|A|$ e $|B|$, risulta $|A| < |B|$, oppure $|A| = |B|$, oppure $|B| < |A|$.

Proviamo ora il teor. di Schroeder-Bernstein, nella sua formulazione equivalente:

Teorema 3.4.3 (Teorema di Schroeder-Bernstein)**.** *Siano X, Y, X_1 tre insiemi per i quali risulta $X \supset Y \supset X_1$, $|X| = |X_1|$. Allora $|X| = |Y|$.*

Dimostrazione. Dato che $|X| = |X_1|$, esiste una biiezione $f : X \longrightarrow X_1$. Inoltre, essendo $Y \subset X$, la restrizione di f ad Y è iniettiva, quindi Y è equipotente ad un s.i. di X_1; sia esso Y_1, cioè $|Y| = |Y_1|$; ne segue

$$X \supset Y \supset X_1 \supset Y_1$$

ed $f|_Y : Y \longrightarrow Y_1$ è una biiezione. Ma $Y \subset X_1$; quindi, ripetendo il ragionamento, si determina X_2 tale che $|X_1| = |X_2|, X \supset Y \supset X_1 \supset Y_1 \supset X_2$ ed $f|_{X_1} : X_1 \longrightarrow X_2$ è una biiezione. Di conseguenza, esistono insiemi equipotenti $X, X_1, X_2, \ldots$ ed $Y, Y_1, Y_2, \ldots$ tali che

$$X \supset Y \supset X_1 \supset Y_1 \supset X_2 \supset Y_2 \supset \ldots$$

Poniamo

$$B = X \cap Y \cap X_1 \cap Y_1 \cap X_2 \cap Y_2 \cap \ldots;$$

avremo

$$X = (X \setminus Y) \cup (Y \setminus X_1) \cup (X_1 \setminus Y_1) \cup \cdots \cup B$$

$$Y = (Y \setminus X_1) \cup (X_1 \setminus Y_1) \cup (Y_1 \setminus X_2) \cup \cdots \cup B$$

Osserviamo che

$$|X \setminus Y| = |X_1 \setminus Y_1| = |X_2 \setminus Y_2| = \ldots,$$

in quanto la restrizione di $f|_{X_n \setminus Y_n} : (X_n \setminus Y_n) \longrightarrow (X_{n+1} \setminus Y_{n+1})$ è una biiezione.

Consideriamo ora l'applicazione $g : X \longrightarrow Y$, definita da

$$g(x) = \begin{cases} f(x) & \text{se } x \in X_i \setminus Y_i, \text{ oppure } x \in X \setminus Y; \\ x & \text{se } x \in Y_i \setminus X_i, \text{ oppure } x \in B\ . \end{cases}$$

E' immediato verificare che g è una biiezione. Ne segue che $|X| = |Y|$, cioè l'asserto.

□

Nel considerare i numeri cardinali, abbiamo fatto la distinzione (in alcuni casi), tra cardinali finiti (i naturali) e cardinali transfiniti; tenendo presente che nell'insieme $\mathbb{N}$ sono definite le operazioni elementari di addizione, sottrazione, moltiplicazione e elevamento a potenza, viene spontaneo cercare di introdurre operazioni analoghe per i cardinali transfiniti (che riproducano le precedenti quando i cardinali siano finiti) e cio è argomento di quanto segue.

Siano A e B due insiemi finiti disgiunti, $|A| = n, |B| = m$ in base alla definizione di unione, risulta

$$|A \cup B| = n + m = m + n = |B \cup A|;$$

quindi si può scrivere

$$|A| + |B| = |B| + |A| = m + n.$$

Pertanto, se $|A|$ e $|B|$ sono due cardinali finiti qualsiasi, la loro somma è il cardinale dell'insieme unione, $|A \cup B|$, purchè i due insiemi siano disgiunti.

Di conseguenza, quando si considerano due cardinali qualsiasi, è lecito dare la seguente definizione:

$$|A| + |B| = |A \cup B| \text{ purchè } A \cap B = \emptyset.$$

La limitazione $A \cap B = \emptyset$ si può eliminare ed è lecito eliminarla dato che A e B sono due insiemi qualsiasi, di cardinalità $|A|$ e $|B|$ rispettivamente; comunque, al fine di dare una definizione apparentemente diversa di somma di due cardinali, è necessario introdurre il prodotto di due cardinali.

Determiniamo dapprima aclune proprietà della somma dei cardinali. Denoteremo spesso i numeri cardinali, transfiniti e non, con le lettere greche minuscole (quelli finiti, saranno però spesso, indicati con $n, m, \ldots$).

Proposizione 3.4.4. *La somma di due numeri cardinali è commutativa, cioè , quali che siano i cardinali* α, β,

$$\alpha + \beta = \beta + \alpha$$

Dimostrazione. In base alla definizione,

$$\alpha = |A|, \beta = |B|, A \cap B = \emptyset \Rightarrow \alpha + \beta = |A \cup B| = |B \cup A| = \beta + \alpha$$

□

Proposizione 3.4.5. *La somma di due numeri cardinali è associativa, cio è*

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$$

Dimostrazione. Infatti, se A, B, C sono a due a due disgiunti e se $\alpha = |A|, \beta = |B|, \gamma = |C|$ si ha

$$(\alpha + \beta) + \gamma = |(A \cup B) \cup C| = |A \cup (B \cup C)| = \alpha + (\beta + \gamma).$$

□

Inoltre, si può provare che, se α e β sono due cardinali transfiniti risulta

$$\alpha + \beta = \max(\alpha, \beta),$$

(in alcuni casi l'affermazione risulta evidente, cfr. n. **??** ed esercizi).

Per definire il prodotto di due cardinali, consideriamo innanzitutto il caso di cardinali finiti. Siano A e B due insiemi qualsiasi non vuoti e sia $|A| = n, |B| = m$. Abbiamo già osservato che (cfr. es. 6) risulta

$$|A \times B| = n \cdot m.$$

E' allora lecito definire in ogni caso il prodotto di due cardinali (finiti e transfiniti) come il cardinale del prodotto cartesiano di due rappresentanti dei cardinali stessi; cioè se $|A| = \alpha$, $|B| = \beta$,

$$|A| \cdot |B| = \alpha \cdot \beta = |A \times B|.$$

Tenendo presente che $|A \times B| = |B \times A|$ (in quanto esiste una biiezione di $A \times B$ su $B \times A$, cfr. es. 18.6), si ha

Proposizione 3.4.6. *Il prodotto di due numeri cardinali è commutativo. Inoltre, essendo associativo il prodotto cartesiano, si ha*

Proposizione 3.4.7. *Il prodotto di due numeri cardinali gode della propriet à associativa, cioè*

$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

Consideriamo ora un qualunque insieme $A \neq \emptyset$ e $\emptyset$. Poichè

$$A \times \emptyset = \emptyset = \emptyset \times A$$

si ha,

Proposizione 3.4.8. *Il cardinale $O = |\emptyset|$ è anullatore del prodotto di numeri cardinali, cioè per ogni cardinale (finito o transfinito) risulta*

$$\alpha \cdot 0 = 0 \cdot \alpha = 0$$

Abbiamo provato che $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, che $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$ (cfr.n. 19); si può analogamente dimostrare che, per ogni insieme S infinito, risulta $|S \times S| = |S|$; inoltre (cfr. prop. **??** ed es. 3.4.1) $|\mathbb{N} \times \mathbb{R}| = |\mathbb{R}|$ e si può provare che se $|A| \leq |B|$, allora $|A \times B| = |B|$; quindi, se α e β sono due cardinali transfiniti qualsiasi

$$\alpha \cdot \beta = \max(\alpha, \beta).$$

Questa proprietà è analoga a quella che vale per la somma, e si può anche estendere (entro certi limiti) ad un numero maggiore di addendi, nel caso della somma, e di fattori, nel caso del prodotto.

Consideriamo ora il prodotto di un cardinale finito per un cardinale transfinito. Innanzitutto osserviamo che se $|A| = 1$, quindi $A = \emptyset$, e $|B| = \beta$ (transfinito),

$$|A \times B| = |B \times A| = |B|,$$

dato che l'applicazione $f : A \times B \longrightarrow B$, definita da

$$f((\emptyset, b)) = b \ \ \forall b \in B$$

è una biiezione.

Più in generale, se $|A| = n, A = \{0, 1, \ldots, n-1\}$, e $|B| = \beta$ (transfinito), si ha $|A \times B| = |B|$.

Infatti, se si considera l'insieme

$$M = (\{0\} \times B) \cup (\{1\} \times B) \cup \cdots \cup (\{n-1\} \times B),$$

si ha $M = A \times B$; M è unione di n insiemi disgiunti di cardinalità β quindi $|M| = \beta$ (cfr. n. **??**).

Possiamo ora eliminare la limitazione $A \cap B = \emptyset$ nella definizione di somma di potenze. Infatti, è sufficiente definire

$$|A| + |B| = |(A \times \{0\}) \cup (B \times \{1\})|,$$

in quanto

$$|(A \times \{0\})| = |A|, |B \times \{1\}| = |B|$$

ed i due prodotti cartesiani sono disgiunti.

Osserviamo che non si definisce la differenza di due cardinali transfiniti.

Infatti, mentre nel caso finito, se $|A| = n$, $|B| = m$, $m \leq n$, $B \subseteq A$, risulta

$$|A \setminus B| = n - m \text{ se } B = A, n - n = 0 \text{ cioè } A \setminus A = \emptyset,$$

per definizione di differenza di due insiemi, ciò non è vero nel caso dei cardinali transfiniti.

Ad esempio, se consideriamo $\mathbb{N}$ e $\mathbb{D}$ (insieme dei dispari) si ha

$$\mathbb{N} \setminus \mathbb{D} = \mathbb{P} \text{ (insieme dei pari)}$$

$$|\mathbb{N} \setminus \mathbb{D}| = |\mathbb{P}| = |\mathbb{N}|,$$

$$|\mathbb{N}| \setminus |\mathbb{D}| = |\mathbb{N}| \setminus |\mathbb{N}| = |\mathbb{N}|.$$

D'altra parte (cfr. es. 19.21) se $|A| < |S|$, $|S \setminus A| = |S|$.

Osserviamo che un'altra maniera per eliminare la restrizione sostituita da $A \cap B = \emptyset$, nella definizione di somma di due numeri cardinali è quella di introdurre la *somma logica* di due insiemi.

Precisamente, se A, B sono due insiemi qualsivoglia, definiamo loro *somma logica* (o unione disgiunta) l'insieme $A + B$ (od $A \dot{\cup} B$) contenente tutti gli elementi di A e tutti gli elementi di B; se un elemento appartiene sia ad A che a B viene ripetuto due volte in $A + B$, distinguendo quando è elemento di A e quando è elemento di B.

E' evidente che

$$A + B = A \cup B \Leftrightarrow A \cap B = \emptyset.$$

Pertanto, si può definire $|A| + |B| = |A + B|$.

Nell'aritmetica elementare si considera l'elevamento a potenza con esponente intero positivo o nullo; diamo ora la definizione analoga per i cardinali, cominciando con il caso dei cardinali finiti.

Siano A, $B \neq \emptyset$, $|A| = n$, $|B| = m$, due insiemi finiti qualsiasi. Consideriamo l'insieme B^A (delle applicazioni di A in B); poichè B^A contiene m^n elementi (cfr.es. 3.0.64), è lecito dare la seguente definizione

$$\left|B^A\right| = m^n = |B|^{|A|}.$$

Se ora $A = \emptyset$, $B = \emptyset$, dato che $B^\emptyset$ contiene un solo elemento (cfr. prop. **??**), si ha

$$|B^\emptyset| = m^0 = 1 = |B|^{|\emptyset|} = |B|^0$$

e si ritrova il ben noto risultato dell'aritmetica elementare.

Se invece $B = \emptyset$, $A \neq \emptyset$, $\emptyset^A = \emptyset$, e si ha

$$|\emptyset^A| = |\emptyset| = 0 = |\emptyset|^{|A|} = 0^n,$$

come è noto. Passando ai cardinali transfiniti, estendiamo la definizione precedente ponenedo, quali che siano i due insiemi A e B, con $|A| = \alpha$, $|B| = \beta$,

$$\beta^\alpha = |B^A| = |B|^|A|.$$

In questo modo viene dato un altro significato al termine potenza diretta usato per il prodotto cartesiano di una famiglia di insiemi tra loro coincidenti (cfr. n. **??**).

In particolare, se β è transfinito ed $|A|$ è finito, $|A| = n$, risulta

$$\beta^n = \beta \text{ e } \beta^0 = 1$$

(cfr. es. 3.3.20) e resta confermato il significato del prodotto cartesiano $\underbrace{A \times A \cdots \times A}_{n \text{ volte}}$.

Esercizi

Esercizio 3.4.1. *Si dimostri che il prodotto della potenza del numerabile per la potenza del continuo è eguale alla potenza del continuo.*

Dim. Consideriamo l'insieme $\mathbb{Z}$ dei numeri interi relativi e l'insieme $A = \{x \in \mathbb{R} : 0 < x \leq 1\}$. Questi due insiemi hanno, rispettivamente, la potenza del numerabile (cfr. prop. **??**) e quella del continuo (cfr. prop. **??**). Definiamo l'applicazione $f : \mathbb{Z} \times A \longrightarrow \mathbb{R}$ nel modo seguente:

$$f((i, a)) = i + a,\ i \in \mathbb{Z},\ a \in A,\ i + a \in \mathbb{R}.$$

f risulta una biiezione, in quanto, per ogni $i \in \mathbb{Z}$, i fissato, al variare di a in A, $i + a$ descrive l'insieme dei numeri reali x tali che $i < x \leq i + 1$; si ottiene così, al variare di i in $\mathbb{Z}$, una famiglia di intervalli, a due a due disgiunti, l'unione dei quali è $\mathbb{R}$. Viceversa, ogni $x \in \mathbb{R}$ si può scrivere in uno, ed in uno solo modo come somma della sua parte intera e di un numero reale compreso tra 0 ed 1 (estremi esclusi; si ricordi che $0,99999\cdots = 1$). Pertanto

$$|\mathbb{Z} \times A| = |\mathbb{R}|,$$

cioè, per definizione di prodotto di potenze,

$$|\mathbb{N}| \cdot |\mathbb{R}| = |\mathbb{R}|.$$

Esercizio 3.4.2. *Sia β un qualunque numero cardinale transfinito; si dimostri che*

$$|\mathbb{N}| + \beta = \beta.$$

Dim. Sia A un insieme infinito di potenza β e sia $B = \{b_1, b_2, \dots\}$ un insieme numerabile tale che $A \cap B = \emptyset$. La proposizione enunciata sarà vera se proviamo che $|A \cup B| = |A|$.

Dato che A è infinito, esso contiene un sottoinsieme numerabile $D = \{d_1, d_2, \dots\}$ (ed $A \setminus D$ ha la stessa potenza di A). Definiamo l'applicazione $f : A \cup B \longrightarrow A$ nel modo seguente:

$$f(x) = \begin{cases} x & \text{se } x \in A \setminus D; \\ d_{2n-1} & \text{se } x = d_n; \\ d_{2n} & \text{se } x = b_n\ . \end{cases}$$

allora f è una biiezione. Ne segue che $|A \cup B| = |A|$, onde l'asserto; per definizione di somma di potenze.

Esercizio 3.4.3. *Siano α e β due cardinali qualsiasi, uno almeno dei quali transfinito. Si provi che*

$$\alpha + \beta = \alpha\beta.$$

Dim. Se β è finito ed α transfinito, $\alpha + \beta = \alpha$, $\alpha\beta = \alpha$ per definizione; rispettivamente, di somma e prodotto di cardinali, onde l'asserto.

Se α e β sono entrambi transfiniti, l'eguaglianza segue dall'osservazione:

$$\alpha + \beta = \max(\alpha, \beta), \quad \alpha\beta = \max(\alpha, \beta).$$

Esercizio 3.4.4. *Sano A, B, C, D quattro insiemi tali che*

$$|A| = |C|, \quad |B| = |D|;$$

si provi che

$$|A^B| = |C^D|.$$

Dim. Ricordando la definizione di potenza di numeri cardinali si ha

$$|A^B| = |A|^{|B|} = |C|^{|D|} = |C^D|$$

onde l'asserto.

Esercizio 3.4.5. *Siano A, B, C tre insiemi qualsiasi, e sia $B \cap C = \emptyset$; si dimostri che*

$$|A|^{|B|} \cdot |A|^{|C|} = |A|^{|B|+|C|}.$$

Dim. Dalle definizioni di somma e di potenza di cardinali, segue:

$$|A|^{|B|} = |A^B|, |A|^{|C|} = |A^C|,\ |A|^{|B|+|C|} = |A|^{|B\cup C|} = |A^{B\cup C}|.$$

Dovremo quindi provare che $|A^B| \cdot |A^C| = |A^{B\cup C}|$, ovvero $|A^B \times A^C| = |A^{B\cup C}|$ (cfr. es. 3.2.5).

Ora, A^B è l'insieme delle applicazioni $f : B \longrightarrow A,\ A^C$ è l'insieme delle applicazioni $g : C \longrightarrow A,\ A^{B\cup C}$ è l'insieme delle applicazioni $h : B \cup C \longrightarrow A$. Dovremo quindi dimostrare che siste una biiezione di $A^B \times A^C$ su $A^{B\cup C}$, $\phi : (f, g) \longrightarrow h$. Date f e g, costruiamo h in modo tale che $h(x) = f(x)$ se $x \in B$, ed $h(x) = g(x)$ se $x \in C$. Allora, ad ogni coppia (f, g) resta associata una ed una sola h.

Viceversa, data $h : B \cup C \longrightarrow A$, poichè $B \cap C = \emptyset$, basta assumere $f = h\big|_B$ e $g = h\big|_C$. Pertanto ϕ è una biiezione, onde l'asserto.

Esercizio 3.4.6. *Siano A, B, C, tre insiemi qualsiasi; si provi che*

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

Dim. Tenuto conto delle definizioni di prodotto e di potenza di cardinali, occore provare che $|(A \times B)^C| = |A^C \times B^C|$ (cfr. es. 3.2.4), cioè che esiste una biiezione $\phi : (A \times B)^C \longrightarrow A^C \times B^C$. Un elemento di $(A \times B)^C$ è un'applicazione di C nel prodotto cartesiano $A \times B$, cioè una $f : C \longrightarrow A \times B$. Un elemento di $A^C \times B^C$ è una coppia (g, h) di applicazioni, ove $g : C \longrightarrow A$ ed $h : C \longrightarrow B$. Ora, f associa ad ogni $c \in C$ una coppia $(a, b) \in A \times B$; a partire da f, costruiamo g ed h nella maniera seguente: se $f(c) = (a, b)$, poniamo $g(c) = a$ ed $h(c) = b$. Allora, ad f resta associata una, ed una sola, coppia (g, h) (l'unicità segue dal fatto che g ed h sono costruite a partire da f facendo variare c in C).

Viceveresa, data la coppia (g, h), costruiamo f in modo che sia $f(c) = (a, b)$, quando $g(c) = a$ ed $h(c) = b$. Resta così provata l'esistenza di ϕ, onde l'asserto.

Esercizio 3.4.7. *Si provi che, per i numeri cardinali, vale la legge distributiva del prodotto rispetto alla somma.*

Dim. Si deve provare che, se α, β, γ sono cardinali qualsiasi, risulta

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

L'affermazione è ovvia se i cardinali in questione sono finiti (l'aritmetica dei cardinali finiti coincide con l'aritmetica dei naturali); in generale, in base alla definizione, occore provare che se A, B, C sono tre insiemi tali che $B \cap C = \emptyset$, e che $|A| = \alpha,\ |B| = \beta,\ |C| = \gamma$, si ha

$$|A \times (B \cup C)| = |(A \times B) \cup (A \times C)|.$$

Ciò è vero in quanto il prodotto cartesiano è distributivo rispetto all'unione (cfr. es. 1.6.3). D'altra parte, direttamente, l'applicazione $f : A \times (B \cup C) \longrightarrow (A \times B) \cup (A \times C)$, definita da $f((a, y)) = (a, y)$ è una biiezione, in quanto $B \cap C = \emptyset \Rightarrow (A \times B) \cap (A \times C) = \emptyset$, e quindi, se $y \in B,\ (a, y) \in A \times B$, se $y \in C, (a, y) \in A \times C$.

Esercizio 3.4.8. *Si dimostri che non vale la legge di cancellazione per la somma di cardinali.*

Sol. Ricordiamo inanzitutto che la legge di cancellazione per la somma (che vale in $\mathbb{N}$) è espressa da:

$$x + z = y + z \Rightarrow x = y.$$

Basterà allora dare un esempio che provi la non validità di tale legge (ciò non esclude minimamente che possono esistere casi particolari nei quali la suddetta legge valga; l'aritmetica dei numeri cardinali transfiniti è diversa da quella dei numeri cardinali finiti).

Consideriamo pertanto l'insieme $\mathbb{N}$ dei numeri naturali e siano $\mathbb{D}$ e $\mathbb{P}$, rispettivamente, il s.i. dei numeri dispari ed il s.i. dei numeri pari (disgiunti). Si ha $\mathbb{N} = \mathbb{P} \cup \mathbb{D}$. Ora $|\mathbb{N}| = |\mathbb{P}|$ (l'applicazione $f : n \in \mathbb{N} \longrightarrow 2n \in \mathbb{P}$ è una biiezione) ed $|\mathbb{N}| = |\mathbb{D}|$ (l'applicazione $g : n \in \mathbb{N} \longrightarrow 2n + 1 \in \mathbb{D}$ è una biiezione). Per definizione di somma di potenze, si ha:

$$|\mathbb{N}| = |\mathbb{P}| + |\mathbb{D}| = |\mathbb{N}| + |\mathbb{N}|, \text{ cioè } 0 + |\mathbb{N}| = |\mathbb{N}| + |\mathbb{N}|.$$

Se valesse la legge di cancellazione, sarebbe $0 = |\mathbb{N}|$, ma 0 è la potenza di $\emptyset$ ed $\mathbb{N} \neq \emptyset$, quindi non vale la legge di cancellazione.

Esercizio 3.4.9. *Si provi che non vale la legge di cancellazione per il prodotto di numeri cardinali*

Dim. Ricordiamo che la legge di cancellazione del prodotto è espressa da

$$xy = xz \Rightarrow y = z$$

(ed è vera per il prodotto in $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$). Proveremo l'affermazione fornendo un controesempio. Siano n, m due cardinali finiti, $m, n \neq 0$, e sia α un qualunque cardinale transfinito ($|A| = \alpha$). Risulta allora

$$n\alpha = |A^n| = |A| = \alpha,$$

$$m\alpha = |A^m| = |A| = \alpha,$$

(cfr. es. 3.3.21). Pertanto,

$$n\alpha = m\alpha \not\Rightarrow n = m.$$

Analogamente, se α, β, γ sono cardinali transfiniti, e $\beta, \gamma \leq \alpha$, si ha

$$\alpha\beta = \alpha, \quad \alpha\gamma = \alpha,$$

onde

$$\alpha\beta = \alpha\gamma$$

senza che sia, necessariamente, $\beta = \gamma$.

Esercizio 3.4.10. *Siano $S_1, S_2, \ldots, S_n$, $n \geq 2$, insiemi aventi la potenza del continuo e non necessariamente a due a due disgiunti. Si provi che $\bigcup_{j=1}^{n} S_j$ ha la potenza del continuo.*

Dim. Si può provare la tesi estendendo l'argomentazione svolta nel corso della dimostrazione dell'es. 3.3.20, oppure nel modo seguente. Siano $\{1\}, \{2\}, \ldots, \{n\}$, n insiemi distinti; si considerino gli insiemi $S_j \times \{j\}$, $j = 1, 2, \ldots, n$. Le applicazioni

$$f_j : S_j \longrightarrow S_j \times \{j\}, \text{ definite da } \forall x \in S_j, f_j(x) = \{x, j\},$$

sono manifestamente biiezioni. Pertanto (cfr. es. 3.3.19),

$$\bigcup_{j \in \{1,2,\ldots,n\}} S_j \times \{j\}$$

ha la potenza del continuo, essendo unione di un numero finito di insiemi a due a due disgiunti, ciascuno dei quali ha la potenza del continuo.

D'altra parte, l'applicazione

$$f : \bigcup_{j=1}^{n} S_j \times \{j\} \longrightarrow \bigcup_{j=1}^{n} S_j \text{ definitia da } f\big|_{S_j \times \{j\}} = f_j^{-1}$$

è un'applicazione su, ma non iniettiva (infatti, se $x \in S_h \cap S_k$, $f^{-1}(x) = \{(x, h), (x, k)\}$): si può allora individuare una restrizione sul dominio di f che sia biiettiva ed $\bigcup S_j$ è immergibile in $\bigcup S_j \times \{j\}$. Pertanto,

$$\big|\bigcup S_j\big| = \big|\bigcup S_j \times \{j\}\big|.$$

Ma $S_j \leq \bigcup S_j$, ed ha la potenza del continuo, quindi $\bigcup S_j$ ha la potenza del continuo, per il teorema di Schroeder-Bernstein.

Esercizio 3.4.11. *Siano α, β due cardinali qualsiasi, tali che $\alpha \leq \beta$; si provi che, per ogni cardinale γ risulta*

$$\alpha + \gamma \leq \beta + \gamma, \quad \alpha\gamma \leq \beta\gamma.$$

Dim. Se $\gamma \leq \alpha$, $\alpha+\gamma = \alpha$, $\beta+\gamma = \beta$, onde l'asserto. Se $\gamma \geq \beta$, $\gamma+\beta = \gamma$ e quindi l'affermazione è vera. Sia ora $\alpha \leq \gamma \leq \beta$; allora $\alpha+\gamma = \gamma,\ \beta+\gamma = \beta$ e quindi $\gamma \leq \beta \Rightarrow \alpha+\gamma \leq \beta+\gamma$. Analogamente si prova la seconda affermazione.

Esercizio 3.4.12. *Si provi che, se A, B, C sono tre insiemi qualsiasi, risulta*

$$|A^B|^{|C|} = |A^{B\times C}|.$$

Dim. Basterà provare che esiste una biiezione di $A^{C\times B}$ su $(A^B)^C$ (si tenga presente che $|C \times B| = |B \times C|$; (cfr. es. 3.2.6). Ciascuna $f \in A^{C\times B}$ è un'applicazione di $C \times B$ in A, cioè, per ogni $\{c, b\} \in C \times B$, $f((c, b)) \in A$. Fissata $f \in A^{C\times B}$, $\forall c \in C$, c fissato, questa individua un'applicazione di B in A. Consideriamo l'applicazione

$$\phi : A^{C\times B} \longrightarrow (A^B)^C, \text{ definitia da } \phi(f) = g,\ \forall f \in A^{C\times B}.$$

tale che, per ogni $c \in C$ fissato, $\phi(f_c) = g(c)$ (e quindi, per ogni $b \in B$, $f_c(b) = g(c)(b)$). Proviamo che ϕ è una biiezione, cioè che phi è iniettiva e su. Dire che phi è iniettiva significa

$$\phi(f) = \phi(f') \Rightarrow f = f'$$

si ha

$$\phi(f) = \phi(f') \Rightarrow g = g' \Rightarrow \forall c \in C, g(c) = g'(c) \Rightarrow$$
$$\Rightarrow \forall b \in B, g(c)(b) = g'(c)(b) \Rightarrow f_c(b) = f'_c(b) \Rightarrow f = f',$$

quindi ϕ è iniettiva. Proviamo che ϕ è su, cioè che

$$\forall g \in (A^B)^C,\ \exists f \in A^{C\times B} \text{ tale che } \phi(f) = g.$$

Si ha

$$g \in (A^B)^C \Rightarrow g(c) \in A^B \Rightarrow f_c = g(c) \Rightarrow \exists f_c \in A^B \Rightarrow \exists f \in A^{C\times B},$$

onde ϕ è su. Ne segue l'asserto.

3.5 Gli assiomi di Peano. Definizione insiemistica di numero naturale

Finora abbiamo 'usato' i numeri naturali senza definirli, assumendoli cioè come concetto acquisito e sfruttando al loro proprietà più elementare, definizione che si può esprimere, in termini tutt'altro che rigorosi, dicendo che i numeri naturali sono quegli enti che servono per contare. Vogliamo ora dare una definizione assiomatica dei numeri naturali.

Riporteremo quindi gli assiomi di Peano, cioè un sistema assiomatico formale atto a definire i numeri naturali.

Precisiamo che un sistema assiomatico formale non specifica gli oggetti sui quali opera; questi possono venire concretizzati di volta in volta dando luogo ad un modello o ad un altro del sistema in questione. Inoltre, un sistema assiomatico formale si dice categorico se ammette un solo modello, cioè definisce esattamente un unico insieme di oggetti che soddisfi gli assiomi dati. Gli assiomi di Peano costituiscono un esempio di sistema assiomatico formale categorico per i numeri naturali, nel senso che definiscono soltanto i numeri naturali.

Enunciamo dunque gli assiomi di Peano:

I. Zero è un numero

II. Ogni numero ammette un successore (o successore immediato) che è un numero (e si denota con n^+ se n è il numero).

III. Lo zero non è successore di alcun numero.

IV. Se i successori (immediati) di due numeri sono eguali, i due numeri sono eguali: $n^+ = m^+ \Rightarrow n = m$.

V. Principio di *induzione matematica*: sia $p(n)$ una proposizione dipendente dal naturale n; se $p(0)$ è vera, e $p(n)$ vera $\Rightarrow$ $p(n^+)$ vera, allora $p(n)$ è vera per ogni naturale n. (Simbolicamente ciò si esprime con la scrittura: $[p(0)$ e $[p(n) \Rightarrow p(n^+)]] \Rightarrow p(n), \forall n \in \mathbb{N}$).

Quindi l'aritmetica di Peano è fondata su tre nozioni: zero, numero e successore. Osserviamo che la prima formulazione degli assiomi di Peano escludeva lo zero, onde l'assioma I era: 1 è un numero (con la sostituzione di 1 a 0 si ottiene tale prima formulazione).

Il principio di induzione matematica si può anche generalizzare nella forma seguente: sia $p(n)$ una proprietà dipendente dal naturale n; se $p(k)$ è vera e per $n \geq k,\ p(n) \Rightarrow p(n^+)$, allora $p(n)$ è vera $\forall n \in \mathbb{N},\ n \geq k$.

Come conseguenza degli assiomi di Peano si ottengono tutte le proprietà dei numeri naturali, ed inoltre è possibile introdurre in $\mathbb{N}$ le familiari operazioni di addizione e moltiplicazione.

Comunque, non utilizzeremo la formulazione originaria degli assiomi di Peano, precedentemente riportata in quanto gli assiomi stessi risultano sovrabbondanti ed il suddetto sistema di assiomi si può sostituire con un sistema equivalente, costiuito da tre assiomi soltanto. Precisamente, diamo la seguente

Definizione 3.5.1. *L'insieme dei numeri naturali naturali è un insieme* $\mathbb{N}$ *che soddisfa i seguenti assiomi (postulati):*

N1. $\mathbb{N}$ *è costituito da un elemento, denotato con* 0*, e da almeno un altro elemento diverso da* 0*; sia* M *il s.i. (proprio) di* $\mathbb{N}$ *costituito da tutti gli elementi diversi da* 0*.*

N2. Esiste una biiezione di $\mathbb{N}$ *su* M*,* $f : \mathbb{N} \longrightarrow M$*.*

N3. Ogni sottoinsieme S *di* $\mathbb{N}$ *tale che:*

(a) $0 \in S$

(b) $f(n) \in S$ *ogni qualvolta* $n \in S$ *(*$n \in \mathbb{N}$*), coincide con* $\mathbb{N}$*.*

$N3$ è quindi il cosiddetto postulato di induzione.

Per semplicità possiamo porre $f(0) = 1, f(1) = 2, f(2) = 3, \dots$ quindi l'insieme $\{0, 1, 2, \dots\}$ è un insieme di numeri naturali e, dato l'assioma $N3$, coincide con $\mathbb{N}$.

Inoltre, $\forall n \in \mathbb{N}$, $f(n)$ prende il nome di *successore* di n; poichè f è una biiezione, 0 non è successore di alcun numero (che è quanto afferam il III assioma di Peano). Ancora dal fatto che f è una biiezione segue

$$f(n) = f(m) \Rightarrow n = m$$

(cioè il IV postulato).

Il postulato di induzione (N_3) (che equivale a quanto stabilito dal V. assioma di Peano) permette di dimostrare il primo ed il secondo principio di induzione matematica; questi vengono applicati nelle cosiddette dimostrazioni per induzione.

Proposizione 3.5.2 (Primo principio di induzione matematica)**.** *Sia* $\mathcal{A}$ *un insieme di affermazioni (enunciati) ciascuna delle quli può essere vera o falsa (ma non entrambe) ed esista un'applicazione suriettiva* $g : \mathbb{N} \longrightarrow \mathcal{A}$*. Posto* $g(n) = A_n \in \mathcal{A}$*, se*

1) A_0 *è vera, e*

2) $A_{f(n)}$ *è vera ogniqualvolta* A_n *è vera,*

allora A_n *è vera per ogni* $n \in \mathbb{N}$*.*

Dimostrazione. Sia $V = \{m \in \mathbb{N} : A_m \text{ è vera}\}$. Per la 1), $0 \in V$, dato che A_0 è vera; inoltre, $f(n) \in V$ ogniqualvolta $n \in V$, per la 2). Segue allora da $N3$ che $V = \mathbb{N}$. □

Enunceremo e proveremo in seguito il secondo principio di induzione matematica, in quanto è opportuno introdurre prima le consuete operazioni di $+$ e $\cdot$ su $\mathbb{N}$; ciò verrà fatto utilizzando quella che prende il nome di *definizione ricorsiva*. Precisamente, si dice che una proprietà (nozione, concetto, ecc.) è definita *ricorsivamente* se quale che sia il naturale n, essa è definita per $f(n)$ ogniqualvota è definita per n.

Introdurre le operazioni di $+$ e $\cdot$ su $\mathbb{N}$ a questo punto, senza aver prima definito, in generale, cosa si intenda per operazione su un insieme, sembra poco opportuno. Pertanto, rinviamo la trattazione al cap. II, dove verranno anche provate rigorosamente le ben note proprietà delle operazioni suddette e verrà introdotto in maniera formale il consueto ordinamento naturale, $\leq$, su $\mathbb{N}$, che già è stato utilizzato. Comunque, faremo ancora uso di questa relazione d'ordine e delle sue proprietà ben note in alcune delle considerazioni che seguono.

Diamo ora un esempio di applicazione del primo principio di induzione matematica, provando che la somma s_n dei primi n termini di una progressione geometrica $< a_1, a_2, \ldots, a_n, \cdots >$ di ragione q è data da

$$s_n = a_1 \frac{1-q^n}{1-q};$$

si ha

$$s_1 = a_1 \frac{1-q}{1-q} = a_1, \text{ onde } s_1 \text{ è vera}$$

(per quanto osservato, si può partire da 1 invece che da 0 nel postulato di induzione).

Proviamo che s_n vera $\Rightarrow$ s_{n+1} vera:

$$s_{n+1} = s_n + a_{n+1} = s_n + a_1 q^n = a_1 \frac{1-q^n}{1-q} + a_1 q^n =$$

$$= a_1 \frac{1-q^n+q^n(1-q)}{1-q} = a_1 \frac{1-q^{n+1}}{1-q}$$

(si ricordi che, per definizione di progressione geometrica, $a_2 = a_1 q, a_3 = a_2 q = a_1 q^2, \ldots$).

Come altro esempio di applicazione del principio di induzione matematica, proviamo che la somma, s_n, dei primi n numeri naturali (zero escluso) è data da

$$s_n = \frac{n(n+1)}{2}.$$

Si ha

$$s_1 = \frac{1 \cdot 2}{2} = 1, \text{ onde } s_1 \text{ è vera.}$$

Proviamo che s_n vera $\Rightarrow$ s_{n+1} vera.

In base alla definizione, si ha:

$$s_{n+1} = s_n + (n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1)+2(n+1)}{2} =$$

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

che si ottiene da $s_n = \frac{n(n+1)}{2}$ ponendo $n+1$ in luogo di n, onde l'asserto.

Infine, come altro esempio, dimostriamo che la somma dei primi n numeri dispari, cioè degli elementi dell'insieme $A = \{1, 3, 5, \ldots, 2n-1\}$ è data da

$$s_n = n^2.$$

Si osservi innanzitutto che l'insieme A si può anche scrivere come

$$A = \{2k - 1 : k \in \underline{n}\}.$$

Si ha quindi

$$s_1 = 1^2 = 1 \ (= 2 \cdot 1 - 1),$$

onde s_1 è vera (dato che la somma del solo primo elemento dell'insieme dato è l'elemento stesso).

Si deve provare che

$$s_k = k^2 \text{ vera } \Rightarrow s_{k+1} = (k+1)^2 \text{ vera.}$$

Si ha:

$$s_{k+1} = s_k + 2(k+1) - 1 = s_k + 2k + 1 = k^2 + 2k + 1 = k^2 + 2k + 1 = (k+1)^2$$

cioè l'asserto.

Osserviamo che l'assioma $N3$ si può anche enunciare nella forma seguente: Sia S un s.i. dell'insieme $\mathbb{N}$ dei naturali, tali che

1) $1 \in S$;

2) $n \in S \Rightarrow f(n) \in S$

allora $S = \mathbb{N}$.

Qualora si ammetta come noto il buon ordinamento di $\mathbb{N}$, si può dimostrare che tale principio è conseguenza del fatto che l'insieme $\mathbb{N}$ è ben ordinato (cfr. n. **??** ed es. **??**) ed in questo ordine il principio di induzione matematica si generalizza nel cosidetto

Principio di induzione transfinita: Sia A un insieme ben ordinato e sia S un s.i. di A con le seguenti proprietà:

1) $a_0 \in S, a_0$ essendo il primo elemento di A;

2) $s(a) \in S \Rightarrow a \in S$, dove $s(a) = \{x \in A : x < a\}$ è il segmento iniziale di a.

Allora $S = A$.

Dimostrazione. Supponiamo che sia $S \neq A$, quindi $A \setminus S = T \neq \emptyset$. Poichè A è ben ordinato, T ha un primo elemento, sia esso t_0. Se consideriamo $s(t_0)$, ciascun $x \in s(t_0)$ precede t_0 e, pertanto, non può appartenere a T, quindi appartiene ad S. Ne segue che $s(t_0) \subset S$. Per la 2), $t_0 \in S$. Ciò non

contraddice $t_0 \in A \setminus S$, onde l'affermazione $S \neq A$ non è vera; ne segue $S = A$. Si noti che la 1) è, di fatto, conseguenza della 2), dato che $\emptyset = s(a_0)$ è un s.i. di S e perciò $a_0 \in S$.

□

Analogamente si generalizza la nozione di successore immediato: un elemento b di un insieme ben ordinato A si dice *successore immediato* di $a \in A$ (ed a si dice *predecessore immediato* di b) se $a < b$ e non esiste alcun $x \in A$ tale che $a < x < b$. (Si confronti con la nozione di copertura in un insieme parzialmente ordinato, data nel n.**??**).

Osserviamo che nell'insieme $\mathbb{Q}$ dei numeri razionali nessun elemento ha un successore (o predecessore) immediato; infatti

$$a, b \in \mathbb{Q},\ a < b \Rightarrow \frac{a+b}{2} \in \mathbb{Q} \text{ e } a < \frac{a+b}{2} < b.$$

Invece ogni elemento, tranne l'ultimo, di un insieme ben ordinato ha un successore immediato. Tale affermazione non è però vera per i predecessori immediati; infatti, esistono elementi di un insieme ben ordinato, oltre al primo, che non hanno un predecessore immediato. Ad esempio, siano

$$\mathbb{D} = \{1, 3, 5, 7, \dots\} \text{ e } \mathbb{P} = \{2, 4, 6, \dots\}$$

rispettivamente gli insiemi ben ordinati dei dispari e dei pari.

Definiamo

$$\{\mathbb{D}, \mathbb{P}\} = \{1, 3, 5, \dots; 2, 4, 5, \dots\},$$

cioè $\{\mathbb{D}, \mathbb{P}\}$ è $\mathbb{D} \cup \mathbb{P}$ ordinato parzialmente da sinistra a destra ed ogni elemento di $\mathbb{D}$ precede ogni elemento di $\mathbb{P}$ (elementi nello stesso insieme conservano il medesimo ordine); 1 e 2,allora, non hanno predecessori immediati.

Non intendiamo approfondire altre questioni legate a quanto detto, stanti i limiti che ci siamo proposti.

Passiamo dunque all'introduzione dei numeri naturali per via insimiestica.

Consideriamo pertanto l'insieme vuoto e poniamo (simbolicamente):

$$0 = \emptyset.$$

Ricordando poi che $\{\emptyset\}$ contiene un solo oggetto, poniamo

$$1 = \{\emptyset\} = \{0\} \text{ (usando il simbolo già introdotto);}$$

di conseguenza chiameremo

$$2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\} \text{ (dato che } \emptyset \neq \{\emptyset\} \text{)}$$

e quindi, in maniera analoga

$$3 = \{0, 1, 2\}$$

$$4 = \{0, 1, 2, 3\}$$

$$\dots$$

$$n = \{0, 1, 2, 3, \dots, n-1\}.$$

Ne segue che ogni naturale n si identifica con l'insieme $\{0, 1, \dots, n-1\}$ dei naturali che lo precedono.

Tenendo presente una terminologia già introdotta, possiamo identificare n con il segmento iniziale di n (il che è lecito in quanto $\mathbb{N}$ è ben ordinato), cioè

$$n = s(n) = \{x \in \mathbb{N} : x < n\}.$$

In questo modo ogni naturale si identifica con un numero cardinale finito, precisamente con quello dell'insieme che lo definisce (ovvero del suo segmento iniziale); in altri termini ha significato la

Definizione 3.5.3. *Per ogni $n \in \mathbb{N}$, si dice che un insieme S ha n elementi se e solo se è equipotente al numero naturale n.*

In questo ordine di idee risultano allora intuitivamente evidenti le seguenti affermazioni:

- Un insieme è finito se e solo se è equipotente ad un numero naturale.

- Ogni numero naturale è un insieme finito.

Proviamo ora la

Proposizione 3.5.4. *Un insieme S è infinito se e solo se, $\forall n \in \mathbb{N}$, contiene un sottoinsieme equipotente ad n.*

Dimostrazione. Supponiamo che S sia infinito. Allora S o è numerabile o contiene un sottoinsieme A numerabile. Nel primo caso, $|S| = |\mathbb{N}|$, cioè esiste $f : \mathbb{N} \to S$, f biiezione. Poichè $n \in \mathbb{N}$ si identifica con $\{0, 1, \ldots, n-1\}$, $f(n) \in S$, essendo f una biiezione, si identifica con $\{f(0), f(1), \ldots, f(n-1)\}$, onde l'asserto. Nel secondo caso, si ripete il ragionamento per A, ed è $|A| = |\mathbb{N}|$, quindi $A \subseteq S \Rightarrow S$ infinito.
Viceversa, supponiamo che, $\forall n \in \mathbb{N}$, S contenga un sottoinsieme equipotente ad n; allora S contiene tutto $\mathbb{N}$, cioè è infinito e l'affermazione è provata. □

Osserviamo che, mentre da un lato l'introduzione insiemistica dei naturali presenta degli indubbi vantaggi, in particolare ai fini della teoria della potenza, l'introduzione di $\mathbb{N}$ mediante gli assiomi di Peano, o, meglio, mediante gli assiomi N_1, N_2, N_3 (ad essi equivalenti) permette invece una formalizzazione molto più utile.
Evidentemente, anche pensando i naturali come insiemi, restano verificati gli assiomi di Peano (ovvero N_1, N_2, N_3); infatti, è sufficiente sostituire gli oggetti che chiamiamo numeri naturali con insieme rigorosamente costruiti.
La verifica della validità degli assiomi di Peano, quando i naturali sono considerati insiemi, è immediata. Infatti

- N_1 è vero, in quanto, ammessa l'esistenza di $\emptyset$, esiste $\{\emptyset\}$ (si ricordi che nella teoria assiomatica degli insiemi si postula la esistenza di $\emptyset$ e dell'insieme delle parti di un insieme).

- N_2 è vero, dato che $f : \mathbb{N} \to M$, definita da $\emptyset = 0 \to \{\emptyset\} = 1$, $1 \to \{0, 1\} = \{\emptyset, \{\emptyset\}\}$, e così via, è manifestamente una biiezione.

- N_3 è vero, dato che $0 \in S$, $n \in S \Rightarrow n + 1 \in S \Rightarrow S = \mathbb{N}$ per costruzione.

Con tale definizione insiemistica dei numeri naturali è immediato introdurre l'ordinamento $\leq$ in $\mathbb{N}$. Precisamente

$$n \leq m \Leftrightarrow n \subseteq m$$

cioè

$$n \leq m \Leftrightarrow \{0, 1, \ldots, n-1\} \subseteq \{0, 1, \ldots, m-1\}.$$

In altri termini la relazione d'ordine $\leq$ viene dedotta dall'inclusione insiemistica dei sottoinsiemi finiti di $\mathbb{N}$.
Non è altrettanto immediato introdurre le relazioni $+$ e $\cdot$ in $\mathbb{N}$ da questo punto di vista, ma tale argomento non sarà trattato.

Esercizi

Esercizio 3.5.1. *Si provi che*

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} = 2^n - 1$$

applicando il principio di induzione matematica.

Sol. Posto

$$s_n = 1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} = 2^n - 1,$$

si ha

$$s_1 = 1 = 2^1 - 1,$$

cioè s_1 è vera.
Proviamo che s_n vera $\Rightarrow$ s_{n+1} vera. In base alla definizione,

$$s_{n+1} = 1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} + 2^n = s_n + 2^n =$$

$$= 2^n - 1 + 2^n = 2 \cdot 2^n - 1 = 2^{n+1} - 1,$$

cioè l'asserto.

Esercizio 3.5.2. *Si provi che la somma dei quadrati dei primi n numeri naturali è*

$$\frac{n \cdot (n+1) \cdot (2n+1)}{6}.$$

Sol. Posto

$$s_n = 1^2 + 2^2 + 3^2 + \cdots + n^2,$$

occorre provare che è $s_n = \frac{n \cdot (n+1) \cdot (2n+1)}{6}$. Applichiamo il principio di induzione matematica, e calcoliamo dapprima s_1. Si ha

$$s_1 = 1^2 = \frac{1 \cdot (2) \cdot (3)}{6},$$

cioè s_1 è vera. Proviamo allora che s_n vera $\Rightarrow$ s_{n+1} vera. Si ha

$$s_{n+1} = 1^2 + 2^2 + 3^2 + \cdots + n^2 + (n+1)^2 = s_n + (n+1)^2 =$$

$$= \frac{n \cdot (n+1) \cdot (2n+1)}{6} + (n+1)^2 =$$

$$= \frac{n+1}{6}\big[n(2n+1) + 6n + 6\big] = \frac{n+1}{6}(2n^2 + 7n + 6) =$$

$$= \frac{(n+1) \cdot (n+2) \cdot (2n+3)}{6},$$

che si ottiene dalla espressione di s_n sostituendo ad n il valore $n+1$, onde l'asserto.

Esercizio 3.5.3. *Si provi che la somma dei cubi dei primi n numeri naturali è*

$$\left[\frac{n\cdot(n+1)}{2}\right]^2.$$

Sol. Poniamo

$$s_n = 1^3 + 2^3 + 3^3 + \cdots + n^3;$$

occorre provare che s_n vale $\left[\frac{n\cdot(n+1)}{2}\right]^2$. Applichiamo il principio di induzione matematica. Si ha

$$s_1 = 1^3 = 1 = \left[\frac{1\cdot 2}{2}\right]^2 = 1,$$

cioè s_1 è vera. Proviamo ora che s_n vera $\Rightarrow$ s_{n+1} vera. Si ha:

$$s_{n+1} = 1^3 + 2^3 + 3^3 + \cdots + n^3 + (n+1)^3 = s_n + (n+1)^3 =$$

$$\left[\frac{n(n+1)}{2}\right]^2 + (n+1)^3 = (n+1)^2\left[\frac{n^2}{4} + (n+1)\right] =$$

$$(n+1)^2\left[\frac{n^2+4n+4}{4}\right] = \frac{(n+1)^2(n+2)^2}{4} =$$

$$= \left[\frac{(n+1)(n+2)}{2}\right]^2,$$

cioè l'asserto.

Esercizio 3.5.4. *Si provi che*

$$1\cdot 2 + 2\cdot 3 + 3\cdot 4 + \cdots + n\cdot(n+1) = \frac{n\cdot(n+1)\cdot(n+2)}{3}$$

applicando il principio di induzione matematica.

Sol. Posto

$$s_n = 1\cdot 2 + 2\cdot 3 + 3\cdot 4 + \cdots + n\cdot(n+1),$$

occorre provare che $s_n = \frac{n\cdot(n+1)\cdot(n+2)}{3}$. Si ha

$$s_1 = 1\cdot 2 = 2 = \frac{1\cdot(2)\cdot(3)}{3} = \frac{6}{3} = 2,$$

onde s_1 è vera. Proviamo ora che s_n vera $\Rightarrow$ s_{n+1} vera. Si ha:

$$s_{n+1} = 1\cdot 2 + 2\cdot 3 + 3\cdot 4 + \cdots + n\cdot(n+1) + (n+1)(n+2) =$$

$$= s_n + (n+1)(n+2) = \frac{n\cdot(n+1)\cdot(n+2)}{3} + (n+1)(n+2) =$$

$$= \frac{(n+1)}{3}\big[n(n+2)+3n+6\big] = \frac{n+1}{3}(n^2+3n+2n+6) =$$
$$= \frac{n+1}{3}(n^2+5n+6) = \frac{n+1}{3}(n+2)(n+3),$$

cioè l'asserto.

Esercizio 3.5.5. *Si provi che*

$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$$

applicando il principio di induzione matematica.

Sol. Posto

$$s_n = \frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2n-1)(2n+1)},$$

occorre provare che $s_n = \frac{n}{2n+1}$. Si ha

$$s_1 = \frac{1}{1\cdot 3} = \frac{1}{3} = \frac{1}{2\cdot 1+1} = \frac{1}{3},$$

onde s_1 è vera. Proviamo che s_n vera $\Rightarrow$ s_{n+1} vera. Si ha

$$s_{n+1} = \frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2n-1)(2n+1)}+\frac{1}{(2n+1)(2n+3)} =$$
$$= s_n + \frac{1}{(2n+1)(2n+3)} = \frac{1}{(2n+1)} + \frac{1}{(2n+1)(2n+3)} =$$
$$= \frac{n(2n+3)+1}{(2n+1)(2n+3)} = \frac{2n^2+3n+1}{(2n+1)(2n+3)} = \frac{(n+1)(2n+1)}{(2n+1)(2n+3)} = \frac{n+1}{2n+3},$$

cioè l'asserto.

Esercizio 3.5.6. *Sia S un qualunque insieme infinito e sia $A \neq \emptyset$ un qualunque insieme finito. Si provi che $|S^A| = |S|$.*

Dim. Sia $|A| = n$. Se $n = 1$, $S^A = S$ (cfr. es. 3.2.3) onde l'affermazione è vera. Se $n = 2$, S^2 è l'insieme delle applicazioni di $\{0,1\}$ in S, quindi l'insieme delle coppie ordinate di elementi di S; pertanto $|S^2| = |S|$. Supponiamo vera l'affermazione per $|A| = n-1$ e proviamola per $|A| = n$. Se $|S^{n-1}| = |S|$, si ha $|S^{n-1} \times S| = |S \times S| = |S|$, onde l'asserto.

Esercizio 3.5.7. *Si provi che l'insieme di tutti i sottoinsiemi finiti di un insieme numerabile è numerabile.*

Dim. Si può provare l'affermazione sull'insieme $\mathbb{N}$. Tenendo presente che ogni sottoinsieme finito di $\mathbb{N}$ è un naturale n e che l'insieme di tutti i naturali n è proprio $\mathbb{N}$, l'affermazione è provata.

Esercizio 3.5.8. *Siano A e B due insiemi qualsiasi; si provi che uno dei due insiemi è equipotente ad un sottoinsieme dell'altro.*

Dim. L'affermazione è banalmente vera se A e B sono entrambi finiti, in quanto $\mathbb{N}$ è totalmente ordinato ed ogni insieme finito è equipotente ad un naturale (cfr. def. 3.5.3). Analogamente è vera se uno dei due insiemi è finito (cfr. prop. 3.5.4).
In generale, per il teorema di Schroeder-Bernstein, vale la legge di tricotomia per i numeri cardinali; pertanto, se $|A| = |B|$, ciascuno dei due insiemi è equipotente ad un sottoinsieme dell'altro (teorema di Cantor-Bernstein). Se $|A| \neq |B|$, o è $|A| < |B|$ e quindi A è equipotente ad un sottoinsieme di B (per definizione di disuguaglianza tra potenze, cfr. prop. 3.2.1), oppure $|B| < |A|$ e B è equipotente ad un sottoinsieme di A. Ne segue l'asserto.

Esercizio 3.5.9. *Sia $n \in \mathbb{N}$, $n \neq \emptyset$, un qualunque naturale; tenendo presente che $n = \{0, 1, 2, \ldots, n-1\}$, si provi che*

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

Dim. L'applicazione $f : \mathbb{N} \times n \to \mathbb{N}$, definita da

$$f((m, j)) = n \cdot m + j, \quad \forall (m, j) \in \mathbb{N} \times n,$$

è una biiezione. Infatti

$$f((m,j)) = f((m',j')) \Rightarrow n \cdot m + j = n \cdot m' + j' \Rightarrow n(m - m') = j' - j \Rightarrow$$

$$\Rightarrow n|(j' - j) \Rightarrow j' - j = 0 \Rightarrow n(m - m') = 0 \Rightarrow m = m' \Rightarrow$$

$$\Rightarrow (m, j) = (m', j')$$

(si è tenuto conto che, se n divide il primo membro di $n(m - m') = j' - j$, deve dividere anche il secondo, e che $j', j \in n \Rightarrow j', j \leq n-1 \Rightarrow |j'-j| < n$), cioè f è biiettiva.
Inoltre, $\forall s \in \mathbb{N}$, esistono e sono unici i naturali m, j tali che $s = n \cdot m + j$: essi sono quoziente e resto della divisione di s per n (onde $0 \leq j \leq n - 1$), quindi f è su.
È evidente poi che $|n \times \mathbb{N}| = |\mathbb{N} \times n|$ (cfr. es. 3.2.6).

3.6 Assioma di scelta. Postulato di Zermelo. Lemma di Zorn.

Abbiamo già citato il postulato di Zermelo (cfr. n. **??**); vogliamo ora dare alcune precisazioni sulle formulazioni equivalenti del medesimo.
Introduciamo dapprima la nozione di funzione di scelta.

Sia $(A_i : \ i \in I)$ una famiglia di sottoinsiemi non vuoti di un insieme S. Una applicazione

$$f : (A_i : \ i \in I) \longrightarrow S$$

prende il nome di *funzione di scelta* se

$$\forall i \in I, \quad f(A_i) \in A_i$$

(cioè l'immagine di ogni insieme della famiglia è un elemento dell'insime stesso).
In altri termini, fissata una famiglia di insiemi, una funzione di scelta "sceglie" un elemento di ciascun insieme della famiglia. In base a questa nozione, il prodotto cartesiano di una famiglia non vuota di insiemi non vuoti (cfr. n. **??**) è l'insieme di tutte le funzioni di scelta definite sulla famiglia $(A_i : \ i \in I)$.
Osserviamo che, sebbene una funzione di scelta sia stata definita per una famiglia di sottoinsiemi di un insieme, la definizione è del tutto generale, in quanto ogni famiglia di insiemi si può considerare come famiglia di sottoinsiemi della sua unione.
Siamo ora in grado di enunciare lo

Assioma di scelta: Esiste una funzione di scelta per una famiglia non vuota di insiemi non vuoti.

Tenendo conto dell'osservazione fatta a proposito del prodotto cartesiano di una famiglia di insiemi, l'assioma di scelta può essere formulato anche nel modo seguente:

Assioma di scelta: Il prodotto cartesiano di una famiglia non vuota di insiemi non vuoti è non vuoto.

Come proveremo, l'assioma di scelta è equivalente al postulato di Zermelo (cfr. n. **??**), che si può anche enunciare nella forma seguente:

Postulato di Zermelo: Se $(A_i : \ i \in I)$ è una qualunque famiglia non vuota di insiemi non vuoti disgiunti, esiste un sottoinsieme M di $\bigcup(A_i : \ i \in I)$ tale che l'intersezione di M e di ciascun A_i contenga esattamente un elemento.

Osserviamo che nel postulato di Zermelo gli insiemi sono disgiunti, mentre nell'assioma di scelta possono anche essere non disgiunti.
Proviamo dunque:

Proposizione 3.6.1. *L'assioma di scelta è equivalente al postulato di Zermelo.*

Dimostrazione. Sia $(A_i : i \in I)$ una famiglia non vuota di insiemi non vuoti disgiunti e sia f una funzione di scelta su $(A_i : i \in I)$. Consideriamo l'insieme $M = \{f(A_i) : i \in I\}$. L'insieme $A_i \cap M = \{f(A_i)\}$ contieme esattamente un elemento, dato che gli A_i sono disgiunti ed f è una funzione di scelta. Quindi l'assioma di scelta implica il postulato di Zermelo.
Viceversa, sia $(A_i : i \in I)$ una qualunque famiglia non vuota di insiemi non vuoti, non necessariamente disgiunti. Consideriamo, $\forall i \in I$, l'insieme $A_i^* = A_i \times \{i\}$; $(A_i^* : i \in I)$ è una famiglia di insiemi disgiunti, dato che $i \neq j \Rightarrow A_i \times \{i\} \neq A_j \times \{j\}$, anche se $A_i = A_j$ (si considera la formulazione generale di famiglia di insiemi, cfr. n. **??**). Per il postulato di Zermelo, esiste un sottoinsieme di M di $\bigcup(A_i^* : i \in I)$ tale che $M \cap A_i^* = \{(a_i, i)\}$ contenga esattamente un elemento. Ne segue che $a_i \in A_i$ e, pertanto, la funzione f su $(A_i : i \in I)$, definita da $f(A_i) = a_i$ è una funzione di scelta. Quindi il postulato di Zermelo implica l'assioma di scelta e l'equivalenza è completamente provata. □

Un'altra conseguenza dell'assioma di scelta e, per quanto ora provato, del postulato di Zermelo è il lemma di Zorn.
Prima di enunciarlo, diamo due definizione che ritroveremo nel seguito. Se $\langle S; \leq \rangle$ è un insieme parzialmente ordinato ed $M \subseteq S$, un elemento $a \in S$ si dice *estremo* (o *confine*) *superiore* di M se $\forall h \in M$, $h \leq a$, e b si dice *minimo confine superiore* o *sup* di M se $b \leq a$, per ogni estremo superiore a di M.
Inoltre, un elemento $m \in S$ si dice *massimale* se $\forall x \in S,\ m \leq x \Rightarrow m = x$.
Enunciamo ora il
Lemma di Zorn: Sia $S \neq \emptyset$ un insieme parzialmente ordinato in cui ogni sottoinsieme totalmente ordinato ammette un estremo superiore in S. Allora S contiene almeno un elemento massimale.
Osserviamo che il lemma di Zorn stabilisce l'esistenza di certi tipi di elementi, ma non fornisce alcun procedimento costruttivo per determinarli.
Si può provare che

Proposizione 3.6.2. *Il lemma di Zorn è equivalente all'assioma di scelta.*

(Omettiamo la dimostrazione di questa proposizione perchè non è molto semplice e trascende i limiti che ci siamo proposti).
Il lemma di Zorn sarà ampiamente utilizzato nel seguito.
Notiamo infine che un'osservazione analoga a quella fatta a proposito del lemma di Zorn si potrebbe fare riguardo all'esistenza dei sottoinsiemi di un insieme, dando per scontata l'esistenza di sottoinsiemi (uno almeno, cioè l'isieme vuoto).
Si può ovviare a questo inconveniente ammettendo il cosiddetto
Assioma di specificazione: Se $a(x)$ è una qualunque affermazione (enunciato) dipendente dall'oggetto (elemento) x ed S è un qualunque insieme, esiste un insieme tale che

$$M = \{y \in S : a(y) \text{ è vera}\}.$$

In tal modo resta garantita l'esistenza di sottoinsiemi di un insieme e, in particolare, è lecito affermare che l'insieme vuoto è un sottoinsieme di un qualunque insieme.

3.7 I classici paradossi della teoria cantoriana degli insiemi ed alcune osservazioni sulla stessa.

Abbiamo già accennato al fatto che la teoria cantoriana degli insiemi conduce a paradossi od antinomie; riteniamo pertanto opportuno riportare con qualche dettaglio due dei paradossi più noti, precisamente quello di Cantor e quello di Russel (non citeremo, invece, il paradosso di Burali-Forti, perchè in esso intervengono i numeri ordinali, la trattazione dei quali trascende i limiti di questa esposizione).

Paradosso di Cantor: Sia Σ l'"insieme" di tutti gli insiemi. Allora ogni sottoinsieme di Σ è anche elemento di Σ; quindi l'insieme delle parti di Σ, $P(\Sigma)$, è un sottoinsieme di Σ, cioè $2^\Sigma \subset \Sigma$. Ne segue che $2^\Sigma \subset \Sigma \Rightarrow |2^\Sigma| \leq |\Sigma|$. D'altra parte, per il teorema di Cantor (cfr. prop. 3.2.5), $|\Sigma| < |2^\Sigma|$.
Pertanto, il concetto di "insieme di tutti gli insiemi" conduce ad una contraddizione. (Questa contraddizione è quella che "ingenuamente" si supera considerando la classe di tutti gli insiemi).

Paradosso di Russel: Sia S l'insieme di tutti gli insiemi che non contengono se stessi come elementi, cioè

$$S = \{A : \ A \notin A\}.$$

Si pone allora la questione di decidere se S appartiene a se stesso oppure no. Se S non appartiene a se stesso, allora, per definizione di S, $S \in S$. D'altra parte, se $S \in S$, per definizione di S, $S \notin S$. Quindi, in entrambi i casi, si ottiene una contraddizione.

L'esame di questi paradossi, o meglio antinomie, mette chiaramente in luce il fatto che il punto debole della teoria intuitiva degli insiemi è, in un certo senso, insito nell'affermazione che ogni proprietà determina un insieme.
Osserviamo che la proprietà che definisce l'insieme S del paradosso di Cantor è soddisfatta da tutti gli oggetti che non sono insiemi, dato che tali oggetti possono essere privi di elementi ed in tal caso non possono essere elementi di se stessi. D'altra parte, la proprietà è soddisfatta dalla maggior parte degli insiemi: ad esempio, l'insieme dei numeri pari.
Non intendiamo affermare che i paradossi citati costituiscono dimostrazioni dell'affermazione che l'uso illimitato del principio di astrazione fornisca una teoria contraddittoria; invece, possiamo dire che, basandoci sulla logica ordinaria, i paradossi provano che è falso che in corrispondenza di ogni

proprietà esista un insieme di oggetti che gode di quella proprietà. Notiamo che anche il viceversa è falso, cioè è falso che ogni insieme abbia una proprietà che lo definisca (come dimostrato da Skolem, 1929).
Dunque la teoria intuitiva degli insiemi, con le sue antinomie, spinge ad un esame critico, con lo scopo di creare una teoria che sia al tempo stesso consistente e goda del maggior numero possibile di aspetti della teoria intuitiva. Ciò si raggiunge, in parte, con la teorie assiomatiche formali, che permettono di procedere essenzialmente come nella teoria intuitiva, ma evitano i paradossi. Ciò farebbe supporre che esse siano consistenti, anche se ciò non è stato provato per alcune di esse (Teorema di Goedel: se una teoria assiomatica formale è consistente, non esiste alcuna dimostrazione della sua consistenza che utilizza metodi formalizzabili entro la teoria stessa).
Per concludere questa parte di elementi di teoria degli insiemi, vogliamo sottolineare qualche altro limite della teoria cantoriana, nonchè mostrare che alcune delle definizioni date, anche se abbastanza intuitive, contengano qualcosa di più profondo, tanto che una giustificazione rigorosa richiede l'accettare un assioma ulteriore. Ciò sarà reso più chiaro dalle osservazioni che seguono.
La definizione di Dedekind (accettata da Cantor) di insieme finito non equipotente ad alcun sottoinsieme proprio, richiede l'assioma di scelta per provare che un insieme finito in tal senso è finito nel senso ordinario (cioè nel senso che contiene n elementi e quindi il procedimento di "contare" gli elementi dell'insieme stesso ha termine).
Comunque, esistono altre definizioni di insieme finito (che non necessitano dell'assioma di scelta per dimostrare che coincidono con quella intuitiva); a proposito cominciamo con il citare la definizione di Sierpinski (1918) nella versione modificata da Tarski:

Definizione 3.7.1. *Un insieme S è finito sse l'insieme S appartiene ad ogni insieme A tale che*

1) $\emptyset \in A$;

2) se $x \in S$, *allora* $\{x\} \in A$;

3) se $B \in A$ *e* $C \in A$, *allora* $B \cup C \in A$,

e la modifica di Kuratowski (1920) di tale definizione:

Definizione 3.7.2. *Un insieme S è finito sse l'insieme $P(S)$ è il solo insieme K che coddisfazione le condizioni*

1) $K \subseteq P(S)$;

2) $\emptyset \in K$;

3) se $x \in S$, *allora* $\{x\} \in K$;

4) se $B \in K$ e $C \in K$, allora $B \cup C \in K$.

Apparentemente più semplice è, invece, la definizione di Tarski (1924):

Definizione 3.7.3. *Un insieme S è finito sse ogni famiglia non vuota di sottoinsiemi di S ha un elemento minimale (x è un elemento minimale di S sse $x \in S$, e x è un insieme e $\forall B$, se $B \in S$, allora non è $B \subset x$):*

(Notiamo che in tutte queste definizioni, tipiche della teoria assiomatica degli insiemi, gli unici oggetti che si considerano sono insiemi, quindi anche gli "elementi" di un insieme sono insiemi).
Si può provare direttamente che un insieme finito nel senso di Tarski è finito nel senso di Dedekind (per provare il viceversa, come si è detto, è necessario l'assioma di scelta).
Non è privo di interesse citare la definizione di insieme finito di Staeckel (1907), dato che ha un contenuto intuitivo abbastanza immediato:

Definizione 3.7.4. *Un insieme S è finito sse può essere doppiamente ben ordinato, cioè sse esiste una relazione R tale che sia R, sia R^{-1}, definiscono un buon ordinamento su S (cfr. es.* **??***).*

Si può provare allora che S è finito nel senso di Tarski e nel senso ordinario (cioè di essere equipotente ad un numero naturale ed uno soltanto e viceversa).
Quanto ora detto mette in luce l'importanza dell'assioma di scelta; al riguardo, vogliamo pure osservare che la legge di tricotomia (cfr. n. 3.5) è equivalente all'assioma di scelta ed anche l'ipotesi del continuo generalizzata (nella seconda formulazione data, cfr. n. **??**) implica l'assioma di scelta (come è stato dimostrato da Sierpinski, 1947).
L'affermare, poi, che l'uso dell'assioma di scelta possa condurre a contraddizioni, è falso, nel senso che Goedel ha dimostrato che l'assioma di scelta si può aggiungere agli altri assiomi della teoria degli insiemi senza condurre a contraddizione, purchè gli assiomi stessi siano consistenti. D'altra parte, l'applicazione dell'assioma di scelta può condurre a risultati paradossali, come, ad esempio, il paradosso di Banach-Tarski (1924): usando tale assioma, una sfera di raggio assegnato può essere decomposta in un numero finito di parti e ricomposta in modo da formare due sferi aventi quel raggio.
Una discussione analoga a quella fatta per gli insiemi finiti nel senso di Dedekind si può fare per gli insiemi infiniti; ciò conduce, in particolare, a giustificare il cardinale transfinito contrapponendolo a quello di cardinale infinito.
Precisamente, α è un cardinale infinito se esiste un insieme infinito A tale che $|A| = \alpha$; α è un cardinale transfinito se esiste un insieme infinito (nel senso di Dedekind) A tale che $|A| = \alpha$ (e provare che i cardinali transfiniti coincidono con quelli infiniti richiede l'assioma dell scelta).

Naturalmente, ciò richiede una definizione di cardinale differente da quella che è stata data; d'altra parte, mediante l'assioma di scelta, si può provare che un cardinale è infinito sse è transfinito. Pertanto, una volta accettato l'assioma, le deduzioni tratte dalle definizioni di Dedekind restano perfettamente valide anche in un contesto più generale.
Accettando la definizione di Tarski di insieme finito, un insieme si dirà infinito sse non è finito e il numero cardinale di un insiene è un "oggetto" associato ad ogni elemento, soddisfacente la sola condizione

$$|A| = |B| \Longrightarrow A \text{ equipotente a } B.$$

Osserviamo pure che talune proprietà dei numeri naturali si trasferiscono ai cardinali (come è evidente se si tiene conto che i cardinali finiti coincidono con i naturali); ad esempio, si definisce il *successore di un cardinale* α al modo seguente:

Definizione 3.7.5. *Il successore α^+ di un cardinale α è tale che $\alpha^+ = \beta$ sse esiste un insieme A tale che $|A| = \alpha$ e $|A \cup \{A\}| = \beta$.*

Sussistono allora proprietà analoghe a quelle stabilite dagli assiomi di Peano.
La nozione di successore di un cardinale permette pure di caratterizzare gli insiemi infiniti nel senso di Dedekind; precisamente, un insieme A è infinito nel senso di Dedekind sse A è equipotente ad $A \cup \{A\}$.
Inoltre, si prova che un insieme infinito nel senso di Dedekind è infinito.
Una caratterizzazione degli insiemi infiniti nel senso di Dedekind è fornito dalla

Proposizione 3.7.6. *Ogni insieme che contenga un sottoinsieme numerabile è infinito nel senso di Dedekind e viceversa.*

Esaminando le operazioni sui i cardinali transfiniti abbiamo osservato che risulta

$$\alpha + \beta = \alpha \cdot \beta$$

(cfr. n. 3.5); a rigore, si prova direttamente che $\alpha + \beta \leq \alpha \cdot \beta$; quando poi si fa uso dell'assioma di scelta, la disuguaglianza si precisa nell'uguaglianza.
Non intendiamo approfondire altre questioni analoghe, anche perchè ciò richiederebbe una trattazione sistematica non soltanto dei numeri ordinali, ma anche dgli insiemi ben ordinati, però vogliamo concludere dando qualche proprietà relativa alle funzioni di scelta; precisamente:

Proposizione 3.7.7. *Se S è un insieme ben ordinato, S ha una funzione di scelta.*

Proposizione 3.7.8. *Ogni insieme finito ha una funzione di scelta.*

Proposizione 3.7.9. *Ogni insieme S può essere ben ordinato (cioè esiste una relazione R su S che determina un buon ordinamento di S).*

Quanto ora accennato molto brevemente mostra che uno sviluppo completo e sistematico della teoria degli insiemi non si può raggiungere con la teoria cantoriana, ma richiede nozioni forse meno intuitive, ma indubbiamente meno generali, quali quelle che sono alla base di una teoria assiomatica, anche se gran parte delle precedenti osservazioni dovrebbero risultare intuitivamente accettabili e valide.

3.8 Sul concetto di numerazione in una data base. Numerazione in base 2

È ben noto che per poter scrivere i numeri (naturali) nel familiare sistema decimale, usiamo la scrittura posizionale, nella quale il significato delle cifre che compongono il numero dipende dalla posizione di queste. Tale posizione rappresenta l'esponente della potenza di 10 di cui la cifra è coefficiente. Ad esempio, $375 = 3 \cdot 10^2 + 7 \cdot 10^1 + 5 \cdot 10^0$.
Pertanto per avere un sistema di numerazione in una qualunque base b, b naturale, occorre e basta fissarne le cifre, che sono esattamente i numeri naturali $0,\ 1,\ 2, \ldots, b-1$. Tale insieme rappresenta, infatti, il naturale b (cfr. n.). queste cifre saranno i coefficienti della combinazione lineare ordinata delle potenze di b, crescenti da destra verso sinistra e senza omissioni di alcuna intermedia. Ad esempio, per $b = 3$, $201 = 2 \cdot 3^2 + \cdot 0 \cdot 3^1 + 1 \cdot 3^0$. Più precisamente si scrive $(201)_3$ per far notare quale sia la base.
Si noti che se $b > 10$, li elementi della base vengono di solito denotati con $0, 1, \ldots, 9$ ed alcune lettere dell'alfabeto, da convenirsi.
È consuetudine di indicare simbolicamente gli elementi di una base b con $\{r_0, r_1, \ldots, r_{b-1}\}$.
Evidentemente, se m è un qualunque naturale tale che $b^n \leq m < b^{n+1}$ si può scrivere

$$m = \sum_{j=0}^{n} r_j b^j, \quad r_j \in \{0, 1, \ldots, b-1\},$$

e quindi rappresentare m con la seguenza (ordinata) $r_n r_{n-1} \cdots r_1 r_0$ (e qui l'indice di r rappresenta la sua posizione nella scrittura posizionale di m, non il naturale che esso rappresenta quando si scrive la base).
Fissata b, è evidente che lo sviluppo in base b di un qualunque numero naturale è unico.
Per ottenere lo sviluppo in base b di un numero razionale, si considerano anche le potenze ad esponente negativo di b, e lo sviluppo è ancora unico.
È ben noto che in base 10 vi sono due tipi di "numeri con la virgola", quelli in cui le cifre dopo la virgola sono definitivamente zero, allineamento decimale aperiodico limitato, e quelli periodici. Il primo caso rappresenta lo sviluppo di una frazione decimale, ossia di un razionale $\frac{m}{n}$ con n potenza di 10, il secondo quello di ogni altro razionale.

Pertanto, dato il razionale $\frac{m}{n}$, se $n = b^h$, allora nel suo sviluppo in base b, le cifre dopo la virgola saranno definitivamente nulle. In ogni altro caso, a prescindere da un eventuale antiperiodo, si avrà un allineamento periodico.
In ogni base b si costruisce la frazione generatrice di un numero periodico esattamente come in base 10, sostituendo il 9 con $b-1$.
Si noti che nella base b, le potenze di b si rappresentano con un 1 seguito da tanti zeri quanto è l'esponente. Ad esempio, 25 in base 5 si scrive 100 e $\frac{3}{25}$ in base 5 si scrive $\frac{3}{100} = 0,03$.
È ben noto che oltre alla base 10, è molto usata la base 2. I Babilonesi, comunque, usavano la base 60, alcuni popoli primitivi usavano la base 20, e anche la base 12 ha una certa diffusione, come pure la base 5, usata dai Romani e dai Giapponesi. Nei calcolatori si usano anche le basi 8 e 16.
Il passaggio da una base ad un'altra richiede soltanto una seguenza di divisioni con resto. Infatti, $r_n r_{n-1} \cdots r_1 r_0$ è un numero x, diciamo nel sistema decimale, allora r_0 è il resto della divisione per 10, $x = 10q_0 + r_0$. Similmente, $q_0 = 10q_1 + r_1$, $q_1 = 10q_2 + r_2$, etc.
Lo stesso significato hanno le cifre nella scrittura posizionale in ogni base. Ad esempio, se vogliamo convertire in base 4 il decimale 126, avremo: $126 = 31 \cdot 4 + 2$, $31 = 7 \cdot 4 + 3$, $7 = 1 \cdot 4 + 3$, $1 = 0 \cdot 4 + 1$, per cui $(126)_{10} = (1332)_4$.
Osserviamo che l'algoritmo di divisione con resto è quello che consente la rappresentazione di un numero in una qualunque base e garantisce la unicità di tale rappresentazione.
Per quanto riguarda la base 2, osserviamo che soltanto i razionali che scritti in base 10 hanno per denominatore 2^h danno luogo ad un allineamento (di 0 e 1) limitato aperiodico dopo la virgola. Per ogni altro razionale si ha un allineamento periodico ed il periodo è costituito da almeno due cifre, dato che $0,\overline{1} = 1$. Diamo ora due esempi di frazioni generatrici di numeri periodici in base 2:

$$1,\overline{01} = \frac{101-1}{11} = \frac{100}{11}, \quad 101,10\overline{01} = \frac{1011001-10110}{1100} = \frac{1000011}{1100}.$$

Si noti che la classica tavola pitagorica in base 10 si scrive in qualunque base, e si può scrivere anche la tabella additiva.