2. Insiemi

2.1 Generalità

Un **insieme** è una collezione distinguibile di oggetti, detti elementi dell'insieme.
Quando un elemento a **appartiene** ad un insieme A si scrive $a \in A$.
Nel caso in cui a sia un elemento **non appartenente** all'insieme A si scrive $a \notin A$.
Gli insiemi finiti si possono rappresentare elencando uno per uno tutti gli elementi contenuti.
Ad esempio se l'insieme A è costituito dagli interi compresi fra 1 e 5 si scriverà $A = \{1,2,3,4,5\}$
L'insieme che non contiene nessun elemento si chiama **insieme vuoto** e si indica con $\emptyset$. Si ha $\emptyset = \{\}$

2.2 Relazioni e operazioni tra insiemi

La **relazione di inclusione** è una relazione che sussiste fra due insiemi quando ogni elemento del primo insieme appartiene anche al secondo.
In simboli, se $\forall a \in A \Rightarrow a \in B$, allora si scrive $A \subseteq B$ (o alternativamente $B \supseteq A$), e si dice che A è un *sottoinsieme* di B.

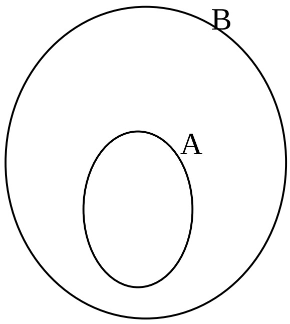

Figura 2.1. A sottoinsieme di B

Si parla di **inclusione stretta** fra due insiemi quando ogni elemento del primo insieme appartiene anche al secondo, ma i due insiemi sono diversi, ovvero esistono elementi del secondo insieme non appartenenti al primo.
Se $\forall a \in A \Rightarrow a \in B$ e $A \neq B$, ossia se $\exists b \in B$ tale che $b \notin A$, allora si scrive $A \subset B$ ($B \supset A$), e si dice che A è un *sottoinsieme proprio* di B.

Due insiemi A e B sono **uguali** se contengono esattamente gli stessi elementi. In formule

$$A = B \Leftrightarrow \forall x (x \in A \Leftrightarrow x \in B) \text{ oppure } A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$$

L'**unione** tra insiemi è un operatore fra due insiemi, A e B, che restituisce l'insieme contenente sia gli elementi di A sia gli elementi di B. La definizione di unione insiemistica si appoggia sull'operatore logico OR (inclusivo), il cui simbolo è $\vee$:

$$A \cup B = \{a : a \in A \vee a \in B\}$$

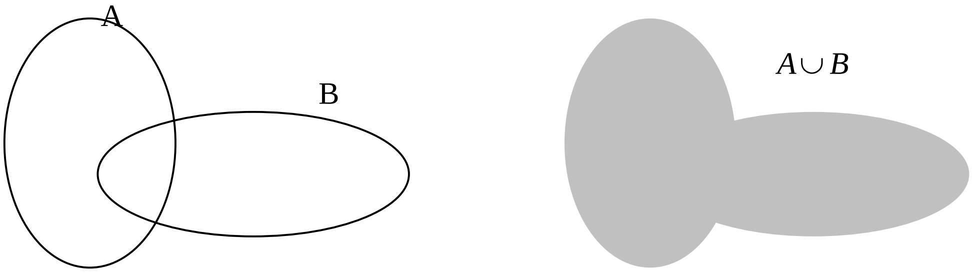

Figura 2.2. In grigio A unito B

L'**intersezione** tra insiemi è un operatore fra due insiemi, A e B, che restituisce l'insieme degli elementi appartenenti contemporaneamente sia ad A che a B. L'operatore intersezione viene definito formalmente facendo uso dell'operatore logico AND, il cui simbolo è $\wedge$:

$$A \cap B = \{a : a \in A \wedge a \in B\}$$

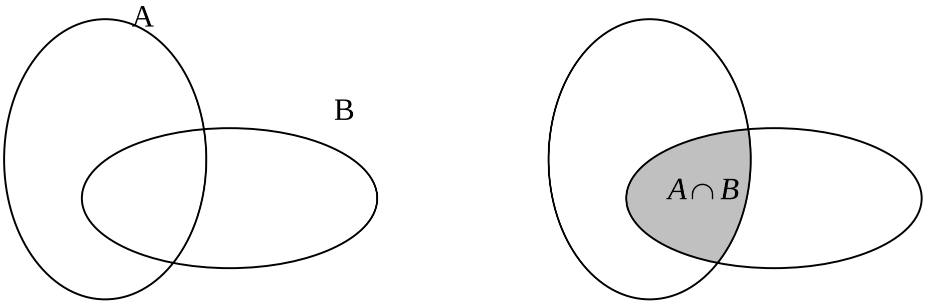

Figura 2.3. In grigio A intersezione B

La **differenza** fra due insiemi A e B, restituisce l'insieme contenente gli elementi che appartengono ad A e che contemporaneamente non appartengono a B.

$$A \setminus B = \{a : a \in A \wedge a \notin B\}$$

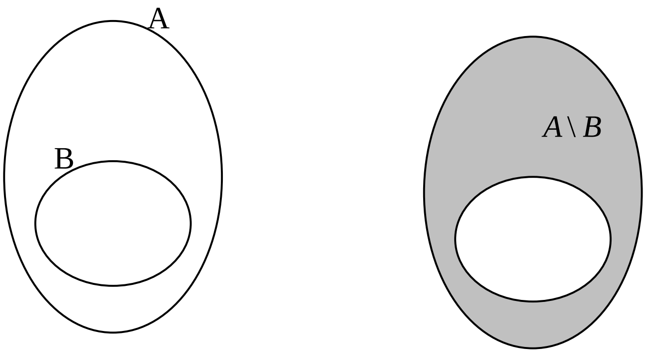

Figura 2.4. In grigio l'insieme differenza tra A e B

La **differenza simmetrica** fra due insiemi coincide con l'insieme degli elementi appartenenti ad uno dei due insiemi di partenza ma non ad entrambi contemporaneamente. Pertanto la differenza simmetrica è, per certi versi, analoga all'operatore OR esclusivo.

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

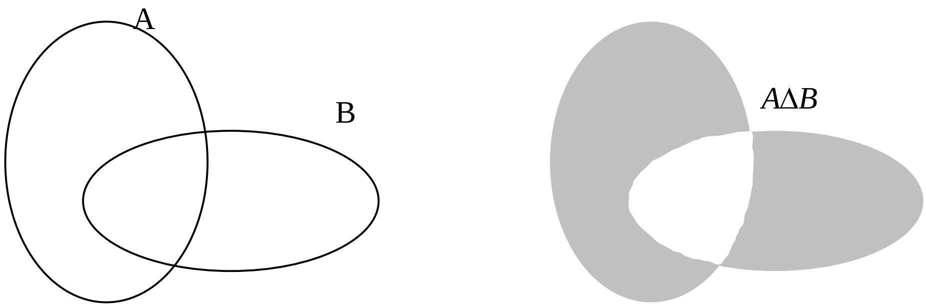

Figura 2.5. In grigio la differenza simmetrica tra A e B

L'operazione di **complementare** richiede uno spazio ambiente, ovvero l'insieme a cui appartengono *tutti* gli elementi esistenti. Se X è lo spazio ambiente e A è un suo sottoinsieme ($A \subseteq X$) allora il complementare di A, rispetto a X , è l'insieme di tutti gli elementi (di X) che non appartengono ad A:

$$A^c = C_A = \overline{A} = X \setminus A = \{x : x \in X \wedge x \notin A\}$$

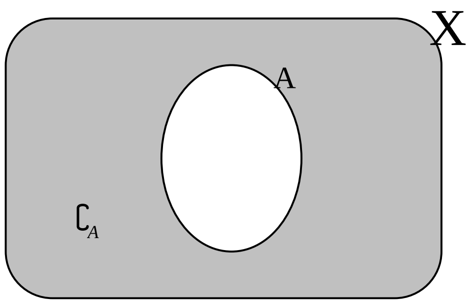

Figura 2.6. In grigio il complementare di A rispetto all'insieme ambiente X

L'**insieme potenza**, o **insieme delle parti**, di un insieme A è l'insieme che ha per elementi tutti i sottoinsiemi di A.

$$\wp(A) = \{X : X \subseteq A\}$$

Nota che $\varnothing \in \wp(A)$ e $A \in \wp(A)$.

Se l'insieme A è formato da n elementi, l'insime delle parti $\wp(A)$ è formato da 2^n elementi.

Il **prodotto cartesiano** fra due insiemi, A e B, restituisce l'insieme di tutte le coppie *ordinate*, tali per cui il primo elemento della coppia appartiene ad A ed il secondo a B.

$$A \times B = \{(a,b) : a \in A \wedge b \in B\}$$

Nota che se $A \neq B$ allora $A \times B \neq B \times A$.

Si usa anche la notazione $A \times A = A^2$.

Proprietà degli operatori insiemistici

$A \cap \varnothing = \varnothing$	$\varnothing$ è l'elemento assorbente dell'intersezione
$A \cup \varnothing = A$	$\varnothing$ è l'elemento neutro rispetto all'unione
$A \setminus \varnothing = A$	$\varnothing$ è l'elemento neutro (a destra) rispetto alla differenza insiemistica
$A \subseteq A$	proprietà riflessiva dell'inclusione
$A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$	proprietà transitiva dell'inclusione

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

Se X è l'insieme universo, allora $X^c = \varnothing$, $\varnothing^c = X$, $A^c \cap A = \varnothing$, $A^c \cup A = X$ (leggi di complementazione).

$A \cap B = A \setminus B^c$ proprietà del complementare rispetto all'intersezione
$A \setminus B = A \cap B^c$ proprietà del complementare rispetto alla differenza
$A \times (B \cup C) = (A \times B) \cup (A \times C)$ proprietà distributiva del prodotto cartesiano rispetto all'unione
$A \times (B \cap C) = (A \times B) \cap (A \times C)$ proprietà distributiva del prodotto cartesiano rispetto all'intersezione
$(A \setminus B) \times C = (A \times C) \setminus (B \times C)$ proprietà distributività del prodotto cartesiano rispetto alla differenza insiemistica
$(A \cap B)^c = A^c \cup B^c$, $(A \cup B)^c = A^c \cap B^c$ leggi di De Morgan

Una **relazione** fra n insiemi, $X_1, X_2, \ldots, X_n$ è un sottoinsieme del prodotto cartesiano $X_1 \times X_2 \times \ldots \times X_n$. Una relazione di questo genere è detta anche n-aria.

Una **relazione binaria** fra due insiemi A e B è un sottoinsieme del prodotto cartesiano $A \times B$. Se accade che $A = B$, si dice che una relazione binaria su A è un sottoinsieme del prodotto cartesiano $A \times A$.

Relazione iniettiva. Sia $\Re \subseteq A \times B$ una relazione binaria fra due insiemi. Si dice che $\Re$ è iniettiva se e soltanto se elementi distinti di A corrispondono a elementi distinti di B secondo la relazione $\Re$, cioè se e soltanto se dati $(a_1, b_1) \in \Re$ e $(a_2, b_2) \in \Re$ risulta

$$\forall a_1, a_2 \in A, b_1 = b_2 \Rightarrow a_1 = a_2 .$$

Relazione suriettiva. Sia $\Re \subseteq A \times B$ una relazione binaria fra due insiemi. Si dice che $\Re$ è suriettiva se e soltanto se $\forall b \in B \; \exists a \in A : (a,b) \in \Re$.

Relazione biunivoca. Sia $\Re \subseteq A \times B$ una relazione binaria fra due insiemi. Si dice che $\Re$ è una relazione biunivoca se e soltanto se è contestualmente iniettiva e suriettiva.

Proprietà delle relazioni

Sia $\Re \subseteq A \times A$ una relazione binaria su A.

Proprietà riflessiva. La relazione $\Re$ si dice riflessiva se e soltanto se $(a,a) \in \Re \quad \forall a \in A$.

Proprietà transitiva. La relazione $\Re$ si dice transitiva se e soltanto se per ogni terna $a,b,c \in A$ vale $(a,b) \in \Re \wedge (b,c) \in \Re \Rightarrow (a,c) \in \Re$.

Proprietà simmetrica. La relazione R si dice simmetrica se e soltanto se per ogni coppia $a,b \in A$ vale $(a,b) \in \Re \Rightarrow (b,a) \in \Re$.

Proprietà antisimmetrica. La relazione $\Re$ si dice antisimmetrica se e soltanto se per ogni coppia $a,b \in A$ vale $(a,b) \in R \wedge (b,a) \in R \Rightarrow a = b$.

Una **relazione di equivalenza** è una relazione binaria $\Re$ su un insieme A che rispetta le proprietà riflessiva, simmetrica e transitiva.

Esempio: la relazione di uguaglianza $=$ su $\mathbb{R}$ (insieme dei numeri reali) è una relazione di equivalenza.

Una **relazione d'ordine** è una relazione binaria $\Re$ su un insieme A se e soltanto se rispetta le proprietà riflessiva, antisimmetrica e transitiva.
*Esempio***:** la relazione $\leq$ su $\mathbb{R}$ (Insieme dei numeri reali) è una relazione d'ordine.

Una **partizione** di un insieme X è una suddivisione di X in sottoinsiemi $X_1, X_2, ...X_n$ tali che:

- l'unione di tutti i sottoinsiemi è l'insieme X stesso, cioè $X_1 \cup X_2 \cup ... \cup X_n = X$;
- due qualsiasi sottoinsiemi della partizione sono disgiunti, cioè $X_i \cap X_j = \varnothing \quad \forall i, j \in \{1, 2, ...n\}$, con $i \neq j$;
- nessun sottoinsime è vuoto, cioè $X_i \neq \varnothing \quad \forall i \in \{1, 2, ..., n\}$.

Ogni relazione di equivalenza $\Re$ su un insieme A determina una partizione di A, costituita da sottoinsiemi formati da elementi equivalenti fra di loro secondo la relazione $\Re$. Ognuno di questi sottoinsiemi prende il nome di **classe di equivalenza**; l'insieme delle classi di equivalenza forma l'**insieme quoziente**, che si indica con il rimbolo $A/\Re$.

2.3 Funzione

Funzione. Una corrispondenza univoca, o applicazione, o anche funzione, f da A in B, associa a ogni elemento $a \in A$ uno, e uno solo, elemento $b \in B$. Per indicare una funzione si usa il simbolo $f : A \to B$.

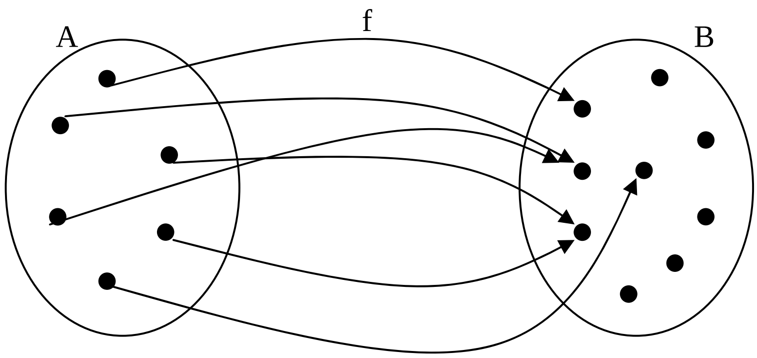

Figura 2.7. Rapresentazione di una funzione o corrispondenza univoca; a ogni elemento di A è associato un solo elemento di B.

Il **dominio** della funzione f è l'insieme A; il **codominio** è l'insieme B. L'elemento $b = f(a)$ si dice **immagine** di a, mentre a si dice **controimmagine** di b. L'**insieme immagine** di f è l'insieme $f(A) = \{b \in B : \exists a \in A / f(a) = b\}$.

Funzione suriettiva. Una funzione si dice suriettiva quando $f(A) = B$.

Funzione iniettiva. Una funzione si dice iniettiva se ad elementi distinti di A associa elementi distinti di B, in simboli $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.

Esempio 1: $A = \{1, 2, 3\}$, $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $f : A \to B$ associa a un elemento di A il suo quadrato. Questa funzione non è sureittiva poiché $f(A) = \{1, 4, 9\} \subset B$. La funzione f è iniettiva perché ad elementi distinti di A associa elementi distinti in B.

Esempio 2: $C = \{-1, 0, +1, +2\}$, $D = \{0, 1, 2, 3, 4\}$, $g : C \to D$ associa a un elemento di C il suo quadrato. Questa funzione non è iniettiva poiché $f(-1) = f(+1) = 1$.

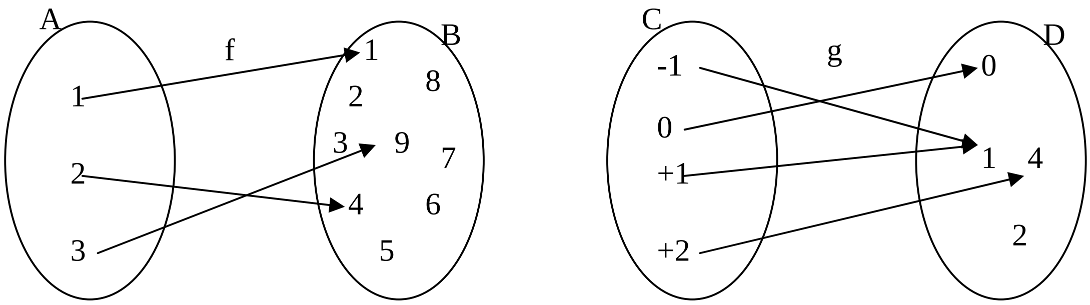

Figura 2.8. La funzione $f: A \to B$ è iniettiva; la funzione $g: C \to D$ non è iniettiva.

Funzione biettiva. Una funzione si dice biettiva se è iniettiva e suriettiva.
Funzione inversa. Si dice funzione inversa di una funzione biettiva $f: A \to B$ la funzione, indicata con f^{-1} che associa a ogni elemento $b \in B$ l'unica controimmagine $a \in A$ tale che $f(a) = b$.
Funzione composta. Date due funzioni $f: A \to B$ e $g: B \to C$ risulta definita una terza funzione $h: A \to C$ che ad un elemento di A associa un elemento di C ottenuto applicando f ad a e poi applicando g ad $f(a)$. Questa funzione si dice funzione composta di f e g e si indica con $h = g \circ f$, oppure $h = g(f(x))$.

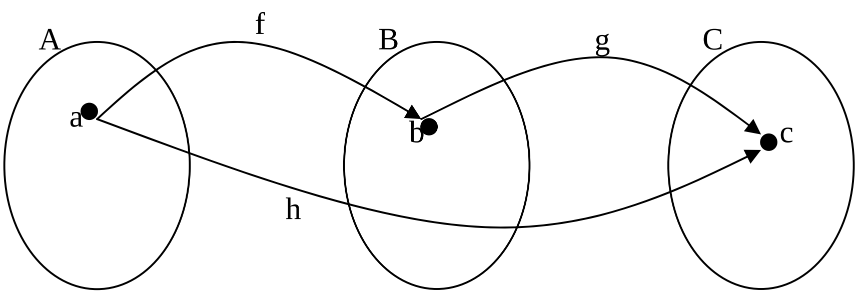

Figura 2.9. La funzione composta

La **funzione identica** o **identità** è l'applicazione $f: A \to A$ che lascia inalterati gli elementi di A e cioè tale che $f(a) = a \quad \forall a \in A$, solitamente indicata con $I(A)$ oppure $id(A)$.

2.4 Strutture algebriche

Una **legge di composizione interna binaria** è un'applicazione che associa ad ogni coppia ordinata di elementi a, b di A uno e un solo elemento c di A. In simboli

$$\begin{array}{c} f: A \times A \to A \\ (a,b) \mapsto c \end{array} \quad \text{oppure } a \otimes b = c$$

Una **struttura algebrica** è un insieme sul quale è definito una legge di composizione interna. Una struttura algebrica si indica come una coppia $(A, \otimes)$, dove A è l'insieme, $\otimes$ l'operazione interna.

Un **semigruppo** è una struttura algebrica $(A, \otimes)$ in cui l'operazione $\otimes$ è associativa, cioè

$(a \otimes b) \otimes c = a \otimes (b \otimes c) \quad \forall a,b,c \in A$.
Un **semigruppo abeliano** è un semigruppo nel quale l'operazione interna è anche commutativa, cioè $a \otimes b = b \otimes a, \quad \forall a,b \in A$.
Un **monoide** è un semigruppo che ha un elemento neutro u, tale che $u \otimes a = a \otimes u = a, \quad \forall a \in A$.
Un **gruppo** è una struttura algebrica $(A,\otimes)$ in cui l'operazione $\otimes$ è
- associativa: $(a \otimes b) \otimes c = a \otimes (b \otimes c) \quad \forall a,b,c \in A$
- dotata di elemento neutro u: $u \otimes a = a \otimes u = a, \quad \forall a \in A$
- ogni elemento ammette un simmetrico a^{-1} tale che $a \otimes a^{-1} = a^{-1} \otimes a = u, \quad \forall a \in A$.

Un **grupppo abeliano** è un gruppo la cui operazione è anche commutativa: $a \otimes b = b \otimes a, \quad \forall a,b \in A$.
Esempi: $\mathbb{Z}(+)$ forma un gruppo. $\mathbb{N}(+)$ non è un gruppo poiché non ci sono gli elementi simmetrici.
Un **anello** è una struttura algebrica con due operazioni $(A,\oplus,\otimes)$ per la quale
- $(A,\oplus)$ è un gruppo abeliano
- $(A,\otimes)$ è un semigruppo
- vale la proprietà distributiva dell'operazione $\otimes$ rispetto all'operazione $\oplus$, cioè: $a \otimes (b \oplus c) = (a \otimes b \oplus a \otimes c), \quad \forall a,b,c \in A$.

Un **anello commutativo** è un anello nel quale tutte e due le operazioni sono commutative.
Esempio: $\mathbb{Z}(+,\cdot)$ è un anello commutativo.
Un **anello unitario** è un anello $(A,\oplus,\otimes)$ nel quale c'è un elemento neutro per l'operazione $\otimes$, cioe $(A,\otimes)$ è un monoide.
Un **corpo** è un anello $(A,\oplus,\otimes)$ nel quale $A-\{u\}$, dove u è l'elemento neutro di $\otimes$, è un gruppo rispetto all'operazione $\otimes$.
Un **campo** è un corpo $(A,\oplus,\otimes)$ nel quale l'operazione $\otimes$ è commutativa.
Esempi: $\mathbb{Q}(+,\cdot)$, $\mathbb{R}(+,\cdot)$ sono campi.