Matematica Generale

Sonia L'Innocente

Corso di Laurea

Informatica-Informatica digitale

Prima parte

Insiemi, Numeri e ralazioni

Outline

Insiemi

Introduciamo, cercando di evitare per ora troppe astrazioni, il concetto di insieme come segue:

Definizione

Chiamiamo *insieme* una qualunque collezione di oggetti o, come anche diremo, di *elementi*. Così la collezione dei numeri

$$0, 1, 2, 3, \ldots$$

forma l'insieme $\mathbb{N}$ dei **numeri naturali**, e la collezione

$$\ldots, -3, -2, -1, 0, +1, +2, +3, \ldots$$

costituisce l'insieme $\mathbb{Z}$ dei **numeri interi**;
-1 è elemento di $\mathbb{Z}$ ma non di $\mathbb{N}$.

Notazione.

1. In genere le lettere maiuscole $A, B, C, \ldots$ denotano gli insiemi; le minuscole $a, b, c, \ldots$ gli elementi.
2. $a \in A$ significa a **è elemento di** A, cioè che a appartiene ad A; $a \notin A$ significa che a **non è elemento di** A, ovvero che a non appartiene ad A.
3. Scriviamo $A = \{a, b, c, \ldots\}$ per dire che gli elementi di A sono $a, b, c, \ldots$
4. Scriviamo poi $A = \{a : \ a \text{ soddisfa } P\}$ per intendere che A è l'insieme degli elementi a che soddisfano la condizione P.
5. Una rappresentazione grafica degli insiemi un pò rudimentale, ma forse utile in questa prima fase, è quella che si ottiene attraverso i cosidetti *diagrammi di Eulero–Venn*.

Con il diagramma di Eulero–Venn, l'insieme $A = \{a, b, c, d \ldots\}$, viene descritto come segue:

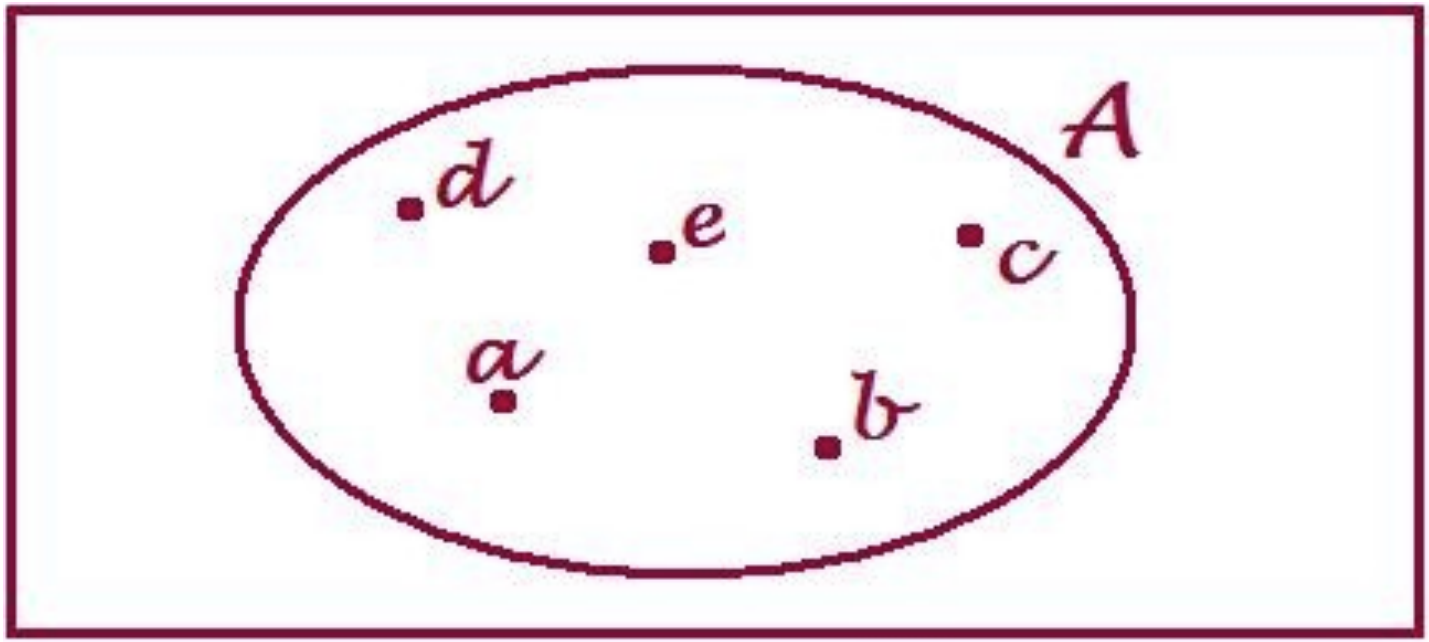


Figure: Diagramma di Eulero–Venn

Esempi

1. $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ è l'insieme dei numeri naturali.
2. $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, +1, +2, +3, \ldots\}$ è, invece, l'insieme dei numeri interi.
3. $\mathbb{Q} = \{\frac{m}{n} : \ m, n \in \mathbb{Z}, n > 0, \ m, n \text{ primi tra loro}\}$ è l'insieme dei numeri razionali (come $\frac{2}{3}$, $\frac{1}{2}$, $-\frac{4}{3}$, $\frac{2}{1}$ – da identificare con 2 – e così via).
4. $\mathbb{R}$ è l'insieme dei numeri reali.
5. $\mathbb{C}$ è l'insieme dei numeri complessi.

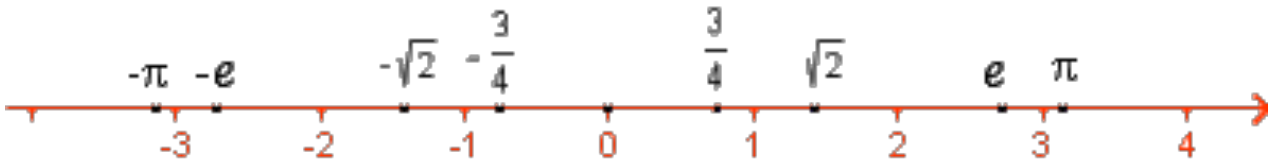
Un cenno sui reali e sui complessi

• Se consideriamo un retta r, vi fissiamo due punti distinti O e I e assegnamo loro, rispettivamente, le ascisse 0 e 1, allora si può convenire che i numeri reali corrispondono esattamente alle possibili ascisse di tutti i punti di r. Essi includono allora i razionali

$$\frac{1}{2} = 0,5, \quad \frac{1}{3} = 0,3333\cdots$$

con i loro allineamenti decimali finiti o infiniti e periodici; ma anche altri numeri (detti *irrazionali*) con rappresentazioni decimali anche infinite aperiodiche

$$\sqrt{2} = 1,41\cdots, \quad \pi = 3,14\cdots.$$



• I numeri complessi si ottengono dai reali aggiungendo il numero immaginario i (con la proprietà $i^2 = -1$) e tutti quei numeri della forma $a + ib$ con a, b reali.

Consideriamo ancora insiemi $A, B, C, \ldots$, che immaginiamo sottoinsiemi di un insieme S così "grande" da contenere tutti gli insiemi

Diciamo allora che due insiemi A e B sono **uguali** se hanno gli stessi elementi.

L'insieme non vuoto

Un insieme è **vuoto** se non ha elementi e si indica con il simbolo $\emptyset$.

Definizione.

Siano A, B insiemi. Diciamo

- A **sottoinsieme** di B, e scriviamo $A \subseteq B$, se ogni elemento di A è anche in B;
- A **sottoinsieme proprio** di B, e scriviamo $A \subsetneq B$, se $A \subseteq B$ ma $A \neq B$ (dunque ogni elemento di A è in B, ma esiste un elemento di B che non è in A).

Esempi

Siano $B = \mathbb{N}$, A l'insieme dei naturali pari, cioè $A = \{0, 2, 4, 6, \ldots\}$. Allora $A \subsetneq B$ (infatti $A \subseteq B$, ma $1 \notin A$).

Siano A, B, C insiemi. Allora si può facilmente osservare quanto segue.

1. $A \subseteq A$.
2. Se $A \subseteq B$ e $B \subseteq A$, allora $A = B$: infatti ogni elemento di A è in B e, viceversa, ogni elemento di B è in A; così $A = B$.
3. Se $A \subseteq B$ e $B \subseteq C$, allora $A \subseteq C$.

$A \not\subseteq B$ significa che A non è sottoinsieme di B, e quindi che c'è qualche elemento in A e non in B. $\not\subseteq$ è quindi da distinguere da $\subsetneq$.

Esempi.

1. Siano A l'insieme dei numeri naturali pari, B l'insieme dei naturali multipli di 3. Allora
   - $A \nsubseteq B$ perché $2 \in A$ ma $2 \notin B$.
   - $B \nsubseteq A$ perché $3 \in B$ ma $3 \notin A$.
2. Siano A l'insieme dei naturali pari, B l'insieme dei naturali dispari. Come nell'esempio 1, $A \nsubseteq B$ e $B \nsubseteq A$; anzi, nessun elemento di A è in B (e nessun elemento di B è in A).

Siano ancora A, B due insiemi in S, costruiamo nuovi sottoinsiemi di S attraverso le seguenti operazioni.

- L'**intersezione** di A e B, che si denota $A \cap B$, si definisce come $\{a \in S : \ a \in A \text{ e } a \in B\}$: è dunque l'insieme degli elementi che stanno tanto in A quanto in B.
- L'**unione** di A e B, che si denota $A \cup B$, si definisce come $\{a \in S : \ a \in A \text{ o } a \in B\}$: è quindi l'insieme degli elementi che appartengono ad A o a B, eventualmente ad entrambi.
- La **differenza** di A e B, che si denota $A - B$, si definisce come $\{a \in S : \ a \in A \text{ e } a \notin B\}$: è formata allora dagli elementi di A che non stanno in B.
- Il **complemento** di A (in S), che si denota A', si definisce come $\{a \in S : \ a \notin A\} = S - A$: si compone di tutti gli elementi (di S) fuori di A.

Esempi.

1. Siano $S = \mathbb{N}$, A l'insieme dei naturali pari, B l'insieme dei naturali multipli di 3, C l'insieme dei naturali dispari. Allora:
   - $A \cap C = \emptyset$, $A \cup C = \mathbb{N}$, $A - C = A$, $C - A = C$, $A' = C$,
   - $A \cap B$ è l'insieme dei naturali multipli di 6,
   - $B \cap C = B - A$.
2. Poniamo adesso $S = \mathbb{Z}$. Siano A l'insieme degli interi ≥ 10 e multipli di 3, $B = \{\ldots, -4, -2, 0, +2, +4, \ldots\}$ l'insieme degli interi pari, $C = \{0, \pm 1, \pm 2, \pm 3, \ldots, \pm 10\}$ l'insieme degli interi che hanno valore assoluto ≤ 10. Allora
   - l'insieme degli interi dispari è B',
   - $C - B = \{-9, -7, -5, -3, -1, +1, +3, +5, +7, +9\}$,
   - $A \cap B = \{12, 18, 24 \ldots\}$.

Definizione

Due insiemi A e B si dicono **disgiunti** se $A \cap B = \emptyset$.

Esercizi Siano A, B, C sottoinsiemi di un insieme S. Si mostri che

1.
   - $A \cap B = B \cap A$,
   - $(A \cap B) \cap C = A \cap (B \cap C)$ (entrambi coincidono con l'insieme $\{x \in S : x \in A \text{ e } x \in B \text{ e } x \in C\}$),
   - $A \cap \emptyset = \emptyset$, $A \cap A = A$, $A \cap A' = \emptyset$.
2.
   - $A \cup B = B \cup A$,
   - $(A \cup B) \cup C = A \cup (B \cup C)$ (entrambi coincidono con l'insieme $\{x \in S : x \in A \text{ o } x \in B \text{ o } x \in C\}$)
   - $A \cup \emptyset = A$, $A \cup A = A$, $A \cup A' = S$,
   - $A - A = \emptyset$, $A - \emptyset = A$, $A - B = A \cap B'$.
3. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

È possibile definire, per $A, B, C \subseteq S$,

- $A \cap B \cap C$ come $(A \cap B) \cap C$ o equivalentemente come $A \cap (B \cap C)$, in ogni caso come l'insieme degli elementi di S che stanno in A e in B e in C;
- $A \cup B \cup C$ allo stesso modo come $(A \cup B) \cup C$ o come $A \cup (B \cup C)$, in ogni caso come l'insieme degli $x \in S$ che stanno in A o in B o in C.

Più in generale, per $A_0, A_1, \ldots, A_n$ sottoinsiemi di S, possiamo costruire senza confusione

$$A_0 \cap A_1 \cap \cdots \cap A_n = \{x \in S : \ x \in A_0 \text{ e } x \in A_1 \text{ e } \cdots \text{ e } x \in A_n\},$$

$$A_0 \cup A_1 \cup \cdots \cup A_n = \{x \in S : \ x \in A_0 \text{ o } x \in A_1 \text{ o } \cdots \text{ o } x \in A_n\}.$$

In modo più compatto, possiamo indicare $A_0 \cap A_1 \cap \cdots \cap A_n$ come

$$\bigcap_{i=0}^{n} A_i$$

e $A_0 \cup A_1 \cup \cdots \cup A_n$ come

$$\bigcup_{i=0}^{n} A_i.$$

Anzi, introducendo anche le abbreviazioni $\forall, \exists$ a significare, rispettivamente, **per ogni**, **esiste**, possiamo scrivere

$$\bigcap_{i=0}^{n} A_i = \{x \in S : \forall i = 0, \ldots, n,\ x \in A_i\},$$

$$\bigcup_{i=0}^{n} A_i = \{x \in S : \exists i = 0, \ldots, n \text{ tale che } x \in A_i\}.$$

Esercizi.

1. Per ogni naturale $n \geq 2$, sia A_n l'insieme dei numeri naturali multipli di n, cioè dei prodotti $q \cdot n$ con $q \in \mathbb{N}$. Dunque $A_n = \{0, n, 2n, 3n, \ldots\}$. Si costruiscano

$$\bigcap_{n \geq 2} A_n, \quad \bigcup_{n \geq 2} A_n.$$

2. Per ogni naturale n, sia $B_n = \{x \in \mathbb{N} : \ x \leq n\}$. Si determinino

$$\bigcap_{n \in \mathbb{N}} B_n, \quad \bigcup_{n \in \mathbb{N}} B_n.$$

3. Finalmente, per ogni $n \in \mathbb{N}$, sia $C_n = \{n\}$. Di nuovo, si determinino

$$\bigcap_{n \in \mathbb{N}} C_n, \quad \bigcup_{n \in \mathbb{N}} C_n.$$

Insieme delle Parti

Definizione

Sia A un insieme (in S). Si dice **insieme delle parti** di A, e si denota con $\mathcal{P}(A)$, l'insieme dei sottoinsiemi di A.

Gli elementi di $\mathcal{P}(A)$ sono i sottoinsiemi di A. In particolare $\emptyset \in \mathcal{P}(A)$, $A \in \mathcal{P}(A)$.

Esempi.

1. Se $A = \emptyset$, allora $\mathcal{P}(A) = \{\emptyset\}$ ha $2^0 = 1$ elemento;
2. se $A = \{0\}$, allora $\mathcal{P}(A) = \{\emptyset, A\}$ ha $2^1 = 2$ elementi;
3. se $A = \{0, 1\}$, allora $\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, A\}$ ha $2^2 = 4$ elementi;
4. se $A = \{0, 1, 2\}$, allora $\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, A\}$ ha $2^3 = 8$ elementi,

Teorema

Se A è un insieme finito e $|A| = n$, allora $|\mathcal{P}(A)| = 2^n$.

Dimostrazione.

Utilizziamo un argomento basato su quello che si chiama **principio di induzione**, che afferma:

Un sottoinsieme di naturali, che contiene 0 ed è chiuso rispetto all'addizione con 1 *(nel senso che, se contiene un certo naturale n, allora include anche* $n + 1$*), coincide forzatamente con* $\mathbb{N}$*.* Per provare il teorema per ogni naturale n, ci basta mostrare che esso è vero per $n = 0$ e che, se è vero per n, è vero anche per $n + 1$.

Caso $n = 0$**:** allora $A = \emptyset$ e $\mathcal{P}(A) = \{\emptyset\}$ ha $1 = 2^0$ elementi. **Caso** $n + 1$**:** Procediamo ora col passo "*induttivo*", da n a $n + 1$. Ammettiamo la tesi vera per insiemi di cardinalità
n, e la mostriamo per quelli di cardinalità $n + 1$. Sia dunque $A = \{a_1, a_2, \ldots, a_n, a_{n+1}\}$ con $a_1 \neq a_2 \neq \cdots \neq a_n \neq a_{n+1}$. Allora

$$\mathcal{P}(A) = \{B \subseteq A : \ a_{n+1} \notin B\} \cup \{B \subseteq A : \ a_{n+1} \in B\}.$$

Denotiamo per semplicità $P = \{B \subseteq A : \ a_{n+1} \notin B\}$,
$Q = \{B \subseteq A : \ a_{n+1} \in B\}$. Anzitutto si osservi che $P \cap Q = \emptyset$. Inoltre:

- P ha 2^n elementi perché $P = \mathcal{P}(\{a_1 \ldots, a_n\})$ e il teorema è supposto vero per insiemi con n elementi come $\{a_1, \ldots, a_n\}$;
- anche Q ha 2^n elementi perché gli elementi di Q si ottengono aggiungendo a_{n+1} a quelli di P.

Così $\mathcal{P}(A)$ ha $2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$ elementi. □

Prodotto cartesiamo

Per $a, b \in S$, possiamo formare la coppia ordinata (a, b). Si noti subito che (a, b) non va confusa con l'insieme $\{a, b\}$ costituito da a, b

$$\{a, b\} \neq (a, b);$$

infatti in (a, b) l'ordine con cui i due elementi compaiono è importante, in $\{a, b\}$ no. Così

$$(1, 2) \neq (2, 1) \text{ ma } \{1, 2\} = \{2, 1\}.$$

Per $a, a', b, b' \in S$, si pone quindi

$$(a, b) = (a', b') \text{ se e solo se } a = a' \text{ e } b = b'.$$

Definizione

Per A, B insiemi ($\subseteq S$), si dice **prodotto cartesiano** di A e B, e si denota con $A \times B$, l'insieme

$$\{(a, b) : \ a \in A, \ b \in B\}.$$

A^2 abbrevia $A \times A$.

Esempi. Siano $A = \{1, 2\}$, $B = \{2, 3, 4\}$. Allora

$$A \times B = \{(1,2), (1,3), (1,4), (2,2), (2,3), (2,4)\},$$

$$B \times A = \{(2,1), (2,2), (3,1), (3,2), (4,1), (4,2)\},$$

$$A^2 = \{(1,1), (1,2), (2,1), (2,2)\},$$

$$B^2 = \{(2,2), (2,3), (2,4), (3,2), (3,3), (3,4), (4,2), (4,3), (4,4)\}.$$

Teorema

Siano A, B insiemi finiti. Allora $|A \times B| = |A| \cdot |B|$.

Dimostrazione.

Vi sono $|A|$ possibilità di scegliere un elemento di A come prima componente di una coppia ordinata in $A \times B$, e, per ognuna di queste possibilità, $|B|$ opportunità di scegliere un elemento di B come seconda componente della coppia. Complessivamente si ottengono $|A| \cdot |B|$ possibilità. □

Ulteriori esempi

1. Siano $A = B = \mathbb{R}$, così $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$. Le coppie ordinate di reali sono usate in geometria analitica per rappresentare, rispetto ad un fissato riferimento cartesiano, i punti del piano.
2. Se consideriamo gli insiemi
   - $\{\mathbf{0}, \mathbf{A}, \mathbf{B}, \mathbf{AB}\}$ dei gruppi sanguigni;
   - $\{+, -\}$ che segnala la presenza o meno del fattore Rhesus,

   il loro prodotto cartesiano è l'insieme dei possibili tipi di sangue

$$\{(\mathbf{0}, +), (\mathbf{0}, -), (\mathbf{A}, +), (\mathbf{A}, -), (\mathbf{B}, +), (\mathbf{B}, -), (\mathbf{AB}, +), (\mathbf{AB}, -)\}.$$

Si puoò estendere l'ambito delle coppie ordinate (a, b) a sequenze più lunghe (terne, quadruple, e così via). In generale, per n naturale ≥ 2 e per $A_1, \ldots, A_n$ insiemi, possiamo considerare n-uple ordinate $(a_1, a_2, \ldots, a_n)$ con $a_i \in A_i$ per ogni $i = 1, 2, \ldots, n$.
Per $a_1, b_1 \in A_1, a_2, b_2 \in A_2, \ldots, a_n, b_n \in A_n$, si pone

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$$

se e solo se

$$a_1 = b_1,\ a_2 = b_2, \ldots, a_n = b_n.$$

L'insieme di queste n-uple si dice il prodotto cartesiano di $A_1, A_2, \ldots, A_n$ e si indica

$$A_1 \times A_2 \times \cdots \times A_n,$$

o, in modo più stringato,

$$\prod_{i=1}^{n} A_i.$$

A^n abbrevia il prodotto cartesiano di n insiemi uguali ad A.

Relazioni.

Definizione

Siano A, B insiemi. Si chiama **relazione** di A e B un sottoinsieme R di $A \times B$.

Per $A = B$ si parla di relazione binaria su A. Talora si preferisce scrivere aRb invece di $(a, b) \in R$ e $a\not{R}b$ invece di $(a, b) \notin R$. Intuitivamente una relazione di A e B si può pensare come un criterio di selezione di certe coppie ordinate (a, b) di $A \times B$ (con la conseguente esclusione delle altre).

Esempi.

1. Siano $A = B = \mathbb{Z}$, $R = \{(a,b) \in \mathbb{Z}^2 : \ a+b \text{ è dispari}\}$. Allora

$$(1,1) \notin R,\ (1,2) \in R,\ (1,4) \in R.$$

2. Siano $A = B = \mathbb{N}$, $R = \{(a,b) \in \mathbb{N}^2 : \ a \text{ divide } b\}$ la relazione di divisibilità ("a divide b" significa che esiste $q \in \mathbb{N}$ tale che $b = a \cdot q$). Così

$$(2,10) \in R,\ (2,7) \notin R,$$

perché 2 divide 10, ma non 7.
Solitamente la relazione di divisibilità R si denota con $|$. In particolare si scrive $2|10$, $2 \nmid 7$.
La relazione di divisibilità si definisce formalmente allo stesso modo tra gli interi, cioè per $A = B = \mathbb{Z}$. In questo ambito si ha, ad esempio, $2|-2$ perchè $-2 = 2 \cdot (-1)$.

3. Siano $A = B = \mathbb{N}$, $R = \{(a, b) \in \mathbb{N}^2 : \ a \text{ è minore o uguale a} b\}$ ("a minore o uguale a b" significa in $\mathbb{N}$ che esiste $d \in \mathbb{N}$ tale che $b = a + d$). Così
$$(2, 3) \in R, \ (3, 2) \notin R.$$
R si indica con $\leq$. Scriviamo allora $2 \leq 3$, $3 \not\leq 2$. $<$ denota invece la relazione $\{(a, b) \in \mathbb{N} : \ a \leq b \text{ e } a \neq b\}$. In modo analogo si recuperano in $\mathbb{N}$ le ben note relazioni $\geq$ e $>$ (" maggiore o uguale", " maggiore" rispettivamente). Anche $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ hanno la loro relazione di ordine $\leq$.
4. Per $A = B = \mathbb{Z}$, sia $R = \{(a, b) \in \mathbb{Z}^2 : \ a = 3 \cdot b\}$. Così $(3, 1) \in R$, ma non c'è nessuna coppia in R la cui prima componente è 1.
5. Ancora per $A = B = \mathbb{Z}$, sia $R = \{(a, b) \in \mathbb{Z}^2 : \ a = b^4\}$. Allora $(16, 2) \in R$ e $(16, -2) \in R$: così ci sono due coppie in R la cui prima componente è 16 (ma nessuna coppia in R ha come prima componente -1).

Possiamo poi immaginare relazioni tra tre o più insiemi, o relazioni 3-arie, 4-arie, ... sullo stesso insieme. Ne accenniamo brevemente.
Per $A_1, \ldots, A_n$ insiemi (e $n \geq 2$), una *relazione n-aria* tra $A_1, \ldots, A_n$ è un sottoinsieme R del prodotto cartesiano $A_1 \times \cdots \times A_n$, dunque (intuitivamente) un criterio di selezione di n-uple $(a_1, \ldots, a_n)$ in $A_1 \times \cdots \times A_n$.
Quando $A_1 = \cdots = A_n = A$, R si dice relazione n-aria su A.

Esempio.

$R = \{(x, y, z) \in \mathbb{N}^3 : x + y + z = 3\}$ è una relazione 3-aria su $\mathbb{N}$, e si compone delle seguenti terne di naturali:

$$(3,0,0),\ (0,3,0),\ (0,0,3),\ (2,1,0),\ (2,0,1),$$

$$(1,2,0),\ (0,2,1),\ (1,0,2),\ (0,1,2),\ (1,1,1).$$

Funzioni

Definizione

Si dice **funzione** o *applicazione* di A in B una relazione f di $A \times B$ tale che,

$$\forall a \in A, \text{ esiste uno e un solo } b \in B \text{ per cui } afb.$$

Notazione.

Per $a \in A$, $b \in B$, afb, si scrive $b = f(a)$, a sottolineare che b è l'unico elemento di B per cui afb; b si dice l'**immagine** di a, a una **retroimmagine** di b. Si scrive $f : A \to B$ a significare che f è una funzione di A in B. A si dice il **dominio** di f. Si pone poi:

- per $X \subseteq A$, $f(X) = \{f(a) : a \in X\} \subseteq B$,
- per $Y \subseteq B$, $f^{-1}(Y) = \{a \in A : f(a) \in Y\} \subseteq A$.

$f(A) = \{f(a) : a \in A\}$ è un sottoinsieme di B, ed è chiamato l'*immagine* di f.

Esempi.

1. Sia $f : \mathbb{Z} \to \mathbb{Z}$ tale che, $\forall x \in \mathbb{Z}$, $f(x) = x^4$; in altre parole, $f = \{(x, y) \in \mathbb{Z}^2 : y = x^4\}$. Allora $f(1) = 1$, $f(2) = 16$, 2 non è nell'immagine di f.
2. Sia $f : \mathbb{Z} \to \mathbb{Z}$ tale che, $\forall x \in \mathbb{Z}$, $f(x) = 3x$, cioè $f = \{(x, y) \in \mathbb{Z}^2 : y = 3x\}$. Allora $f(1) = 3$, $f(2) = 6$, 1 non appartiene all'immagine di f.
3. Sia A un insieme. L'**identità** di A è la funzione $id_A : A \to A$ tale che, $\forall x \in A$, $id_A(x) = x$. Talora quando A è chiaro dal contesto la indicheremo più rapidamente id.
4. Siano A, B insiemi, $b \in B$, $f : A \to B$ tale che, $\forall x \in A$, $f(x) = b$. f si dice una **funzione costante**.
5. Siano $A \subseteq B$ insiemi, $i : A \to B$ tale che, $\forall a \in A$, $i(a) = a$. i si dice una **immersione** di A in B. Ovviamente, per $A = B$, i è l'identità di A. Ma può anche essere $A \neq B$.

6. Siano S un insieme, $A \subseteq S$. Definiamo

$$f_A : S \to \{0, 1\}$$

ponendo, $\forall x \in S$,

$$f_A(x) = \begin{cases} 1 & \text{se } x \in A, \\ 0 & \text{se } x \notin A. \end{cases}$$

Così f_A è una funzione "*test*" per l'appartenenza ad A di un elemento di S: l'immagine $f_A(x)$ di x chiarisce se x è o no in A tramite i valori distinti 1 e 0. f_A si dice la **funzione caratteristica** di A (in S).

7. Sia $A = \mathbb{N}$. L'addizione è una funzione da $\mathbb{N}^2$ a $\mathbb{N}$: trasforma cioè coppie ordinate di naturali in naturali, ad esempio $(2, 3)$, o $(1, 4)$ in $5 = 2 + 3 = 1 + 4$. La si chiama allora **operazione binaria** su $\mathbb{N}$. Anche la moltiplicazione è un'operazione binaria su $\mathbb{N}$, trasforma cioè coppie ordinate di naturali in naturali, $(2, 3)$ in $6 = 2 \cdot 3$, $(1, 4)$ in $4 = 1 \cdot 4$.

7. In generale per ogni insieme A e per ogni intero positivo n si chiama operazione n-aria su A una funzione da A^n in A. Così $+$, $\cdot$ sono operazioni binarie anche su $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e

$$f(a, b, c) = (a + b) \cdot c$$

definisce un'operazione ternaria su $\mathbb{N}$ (ma anche in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$).

8. Sia A un insieme ($\subseteq S$). Una funzione a di $\mathbb{N}$ in A si dice una **successione** in A. a si può identificare con la sequenza delle immagini dei naturali in A

$$(a(0), a(1), a(2), \ldots, a(n), \ldots).$$

Una successione a in A si rappresenta dunque come sequenza di naturali

$$(a_0, a_1, a_2, \ldots, a_n, \ldots) = (a_n)_{n \in \mathbb{N}}$$

intendendo $a_n = a(n)$, $\forall n \in \mathbb{N}$.

8. Supponiamo che, $\forall n \in \mathbb{N}$, $A_n \subseteq A$. Possiamo indicare con

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

l'insieme delle successioni $(a_0, a_1, \ldots, a_n, \ldots) = (a_n)_{n\in\mathbb{N}}$ in A tali che, per ogni $n \in \mathbb{N}$, $a_n \in A_n$. Più in generale, sia I un insieme e, $\forall i \in I$, sia $A_i \subseteq A$. Denotiamo con

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

l'insieme delle sequenze $(a_i)_{i\in I}$ (cioè delle funzioni di I in A) tali che, $\forall i \in I$, $a_i \in A_i$.
La notazione richiama quella del prodotto cartesiano. Infatti $\prod_{i=1}^{n} A_i$ è stato definito come l'insieme delle n-uple $(a_1, \ldots, a_n)$ con $a_1 \in A_1, \ldots, a_n \in A_n$; ma una tale n-upla può anche intendersi come una funzione $a : \{1, \ldots, n\} \to \bigcup_{i=1}^{n} A_i$ che $\forall i = 1, \ldots, n$ associa un elemento $a_i \in A_i$ (e quindi costruisce complessivamente proprio $(a_1, \ldots, a_n)$).

Osservazione.

Due funzioni $f, g : A \to B$ sono uguali quando, per ogni $a \in A$, $f(a) = g(a)$

Definizione.

Una funzione f di A in B si dice

- **iniettiva** se, per ogni $b \in B$, esiste al massimo un $a \in A$ per cui $f(a) = b$ (in altre parole: $\forall a, a' \in A$, se $f(a) = f(a')$, allora $a = a'$);
- **suriettiva** se, per ogni $b \in B$, esiste almeno un $a \in A$ per cui $f(a) = b$;
- **biiettiva** (o *corrispondenza biunivoca*) se f è iniettiva e suriettiva: $\forall b \in B$, $\exists!$ (cioè, esiste uno e uno solo) $a \in A$ tale che $f(a) = b$.

Esempi.

1. Sia $f : \mathbb{Z} \to \mathbb{Z}$ tale che, $\forall x \in \mathbb{Z}$, $f(x) = x^4$. Notiamo $f(2) = f(-2) = 16$: così f non è iniettiva. Inoltre per nessun $x \in \mathbb{Z}$ si ha $-1 = x^4 = f(x)$: f non è neanche suriettiva.
2. Sia $f : \mathbb{Z} \to \mathbb{Z}$ tale che, $\forall x \in \mathbb{Z}$, $f(x) = 3x$. Chiaramente, $\forall x, x' \in \mathbb{Z}$, se $f(x) = f(x')$, cioè se $3x = 3x'$, deve essere $x = x'$: f è quindi iniettiva. Invece f non è suriettiva: nessun $x \in \mathbb{Z}$ soddisfa $1 = 3x = f(x)$.
3. Siano $S = \{1, 2, 3, 4, 5, 6\}$, $A = \{2, 4, 6\}$, f_A la funzione caratteristica di A. Così $f_A(1) = f_A(3) = f_A(5) = 0$, $f_A(2) = f_A(4) = f_A(6) = 1$. f_A è suriettiva, ma non iniettiva.
4. Sia $f : \mathbb{Z} \to \mathbb{Z}$ tale che, $\forall x \in \mathbb{Z}$, $f(x) = x + 1$. Allora, $\forall y \in \mathbb{Z}$, $\exists! x \in \mathbb{Z}$ per cui $y = f(x) = x + 1$, per la precisione $x = y - 1$. Così f è biiettiva.
5. L'addizione e la moltiplicazione in $\mathbb{N}$ sono suriettive, ma non iniettive. Infatti ogni naturale a si esprime come $a + 0$, o $a \cdot 1$. Ma $2 + 3 = 1 + 4 = 5$, $3 \cdot 4 = 2 \cdot 6 = 12$.

Esercizi

1. Sia f una funzione costante di A in B. In quali casi f è suriettiva? Iniettiva?
2. Si provi che, per ogni insieme A, id_A è biiettiva.
3. Sia $A \subseteq B$. Si provi che l'immersione di A in B è iniettiva. In quali casi è suriettiva?

Osservazione.

Sia $A = \{s_1, \ldots, s_n\}$ un insieme finito, e sia $f : A \to A$. Proviamo che

f è iniettiva se e solo se f è suriettiva.

Infatti, se f è iniettiva, $f(s_1) \neq \cdots \neq f(s_n)$ (per $s_1 \neq \cdots \neq s_n$). Così $f(s_1), \ldots, f(s_n)$ riempiono gli n posti in A, e f ùriettiva.
Si provi per esercizio il contrario: se f è suriettiva, f deve essere anche iniettiva.

Si noti che la precedente proprietà non è più vera per insiemi infiniti A.

Composizione di funzioni.

Definizione.

Siano $f : A \to B$, $g : B \to C$ funzioni. Si definisce **composizione** di f e g, e si indica con $g \circ f$, la funzione di A in C tale che, per ogni $a \in A$,

$$(g \circ f)(a) = g(f(a)).$$

Per definire $g \circ f$ è ovviamente essenziale che l'insieme B a cui f arriva (l'immagine) sia anche il dominio di g (o almeno vi sia contenuto).

Esempi.

Siano $f, g : \mathbb{Z} \to \mathbb{Z}$ tali che, $\forall x \in \mathbb{Z}$,

- $f(x) = x^2$
- $g(x) = x + 1$.

Allora, $\forall x \in \mathbb{Z}$,

$$(g \circ f)(x) = g(f(x)) = g(x^2) = x^2 + 1,$$

$$(f \circ g)(x) = f(g(x)) = f(x + 1) = (x + 1)^2 = x^2 + 2x + 1.$$

In particolare

$$(g \circ f)(2) = 5, \ (f \circ g)(2) = 9.$$

Così, è possibile comporre $g \circ f$ e $f \circ g$, ma $g \circ f \neq f \circ g$.

Esercizi

1. Siano $f : A \to B$, $g : B \to C$. Si provi che:
   - se g, f sono iniettive, anche $g \circ f$ lo è;
   - se g, f sono suriettive, anche $g \circ f$ lo è;
   - se g, f sono biiettive, anche $g \circ f$ lo è.
2. Siano $f : A \to B$, $g : B \to C$, $h : C \to D$. Si provi
$$(h \circ g) \circ f = h \circ (g \circ f).$$
3. Sia $f : A \to B$. Si provi
$$f \circ id_A = f, \quad id_B \circ f = f.$$

Definizione.

Sia R una relazione di A e B. La relazione inversa R^{-1} di R è la relazione di B e A così definita: $\forall b \in B$, $\forall a \in A$,

$$(b, a) \in R^{-1} \text{ se e solo se } (a, b) \in R.$$

Esempio.

Sia $A = B = \mathbb{N}$, $R = \leq$. Allora $R^{-1} = \geq$. Si osservi inoltre che $(R^{-1})^{-1} = R$.

Ci chiediamo: sia f una funzione di A in B; allora f^{-1} è una funzione di B in A?

1. Sia $f : \mathbb{Z} \to \mathbb{Z}$ tale che, $\forall x \in \mathbb{Z}$, $f(x) = x^4$. Allora f^{-1} non è una funzione da $\mathbb{Z}$ a $\mathbb{Z}$, infatti $f(2) = f(-2) = 16$ e $(16, 2), (16, -2) \in f^{-1}$ (in altre parole, non sappiamo come definire l'eventuale $f^{-1}(16)$). Inoltre $-1 \notin f(\mathbb{Z})$; nessuna coppia in f^{-1} ha -1 come prima componente (e dunque non sappiamo come definire l'eventuale $f^{-1}(-1)$).
2. Sia $f : \mathbb{Z} \to \mathbb{Z}$ tale che, $\forall x \in \mathbb{Z}$, $f(x) = 3x$. Nessuna coppia in f^{-1} ha 1 come prima componente perché $1 \notin f(\mathbb{Z})$. Così f^{-1} non è una funzione.
3. Sia $f : \mathbb{Z} \to \mathbb{Z}$ tale che, per ogni $x \in \mathbb{Z}$, $f(x) = x + 1$. Allora f^{-1} è una funzione. Infatti f è biiettiva: $\forall y \in \mathbb{Z}$, esiste uno e un solo $x \in \mathbb{Z}$, $x = y - 1$, tale che $f(x) = y$, cioè $(y, x) \in f^{-1}$. Allora si può porre $f^{-1}(y) = y - 1$ $\forall y \in \mathbb{Z}$.

Teorema.

Sia f una funzione di A in B. Allora f^{-1} è una funzione di B in A se e solo se f è biiettiva. Inoltre, in tal caso, anche f^{-1} è biiettiva.

Dimostrazione.

f^{-1} è una funzione di B in A se e solo se, per ogni $b \in B$, esiste uno e un solo $a \in A$ tale che $(b, a) \in f^{-1}$, ovvero $(a, b) \in f$, ovvero $f(a) = b$, cioè se e solo se f è biiettiva. In tal caso, siccome f è una funzione, per ogni $a \in A$, esiste uno e un solo $b \in B$ per cui $(a, b) \in f$, ovvero $(b, a) \in f^{-1}$: quindi f^{-1} è biiettiva. □

Si osservi che, se $f : A \to B$ è biiettiva,

- $f^{-1} \circ f = id_A$: infatti, per ogni $a \in A$, $(f^{-1} \circ f)(a) = f^{-1}(f(a)) = a$;
- $f \circ f^{-1} = id_B$: infatti, per ogni $b \in B$, $(f \circ f^{-1})(b) = f(f^{-1}(b)) = b$.

Relazioni di equivalenza

Definizione.

Sia $A \neq \emptyset$. Una relazione binaria E su A si dice di **equivalenza** se valgono le seguenti proprietà:

(i) per ogni $a \in A$, aEa (proprietà riflessiva);

(ii) per ogni scelta di $a, b \in A$, se aEb, allora bEa (proprietà simmetrica),

(iii) per ogni scelta di $a, b, c \in A$, se aEb e bEc, allora aEc (proprietà transitiva).

Esempi.

1. Sia A l'insieme delle rette del piano. Per $r, s \in A$, poniamo
$$r // s \text{ se e solo se } r \text{ è parallela a } s$$
(cioè $r = s$ oppure r, s non hanno punti in comune): $//$ è una relazione di equivalenza in A. Infatti:
   - ogni retta è parallela a se stessa,
   - se una retta è parallela ad un'altra, la seconda lo è alla prima,
   - se due rette sono parallele ad una terza, allora lo sono anche tra loro.
2. Sia $A \neq \emptyset$. La relazione di uguaglianza in A, quella formata dalle coppie (a, b) con $a = b$, è una relazione di equivalenza. Infatti:
   - ogni elemento a di A è uguale a se stesso,
   - se $a, b \in A$ e $a = b$, allora anche $b = a$,
   - se $a, b, c \in A$, $a = b$ e $b = c$, allora $a = c$.

   Anche $E = A^2$ (l'insieme di tutte le coppie ordinate di elementi di A) è una relazione di equivalenza su A. Infatti qualunque coppia (a, b) in A^2 è accettata da E, il che rende banale la verifica delle tre proprietà riflessiva, simmetrica e transitiva.

3. Sia $A = \mathbb{R}$ e sia E la relazione binaria su $\mathbb{R}$ tale che, per ogni scelta di $x, y \in \mathbb{R}$,

$$xEy \text{ se e solo se } |x| = |y|,$$

cioè x, y hanno lo stesso valore assoluto (ricordiamo che $|x| = x$ se $x \geq 0$ mentre $x = -x$ se $x < 0$). Allora E è una relazione di equivalenza in $\mathbb{R}$, (controllare). Se intendiamo x, y come ascisse di punti di una retta rispetto a un fissato sistema di riferimento, xEy significa che i punti di ascissa x, y sono alla stessa distanza dall'origine O del sistema di riferimento.

4. Siano A un insieme, $A \neq \emptyset$, f una funzione di A in un insieme B: poniamo, per ogni scelta di $a, a' \in A$,

$$aEa' \text{ se e solo se } f(a) = f(a').$$

Allora E è una relazione di equivalenza su A .

5. Sia $A = \mathbb{Z}$. Fissiamo un intero positivo m e poniamo, per ogni scelta di $a, b \in \mathbb{Z}$ $a \equiv b\,(mod\, m)$ (da leggersi: a è **congruo** b **modulo** m) se e solo se $m|(a-b)$, cioè se e solo se esiste $q \in \mathbb{Z}$ tale che $m \cdot q = a - b$. Controlliamo nel dettaglio in questo caso le tre proprietà (i), (ii), (iii).

Dunque si ha:

(i) p$\forall a \in \mathbb{Z}$, $a \equiv a\,(mod\ m)$ perchè $a - a = 0 = m \cdot 0$;

(ii) $\forall a, b \in \mathbb{Z}$, se $a \equiv b\,(mod\ m)$, allora $b \equiv a\,(mod\ m)$: infatti, se $\exists q \in \mathbb{Z}$ tale che $m \cdot q = a - b$, l'intero $-q$ soddisfa $b - a = m \cdot (-q)$;

(iii) $\forall a, b, c \in \mathbb{Z}$, se $a \equiv b\,(mod\ m)$ e $b \equiv c\,(mod\ m)$, allora $a \equiv c\,(mod\ m)$: infatti se ammettiamo che esistano $q, p \in \mathbb{Z}$ tali che $m \cdot q = a - b$ e $m \cdot p = b - c$, sommando membro a membro si ottiene

$$m \cdot (q + p) = m \cdot q + m \cdot p = a - b + b - c = a - c.$$

Così $\equiv\ (mod\ m)$ è una relazione di equivalenza in $\mathbb{Z}$.

Definizione.

Siano $A \neq \emptyset$, E una relazione di equivalenza in A. Per $a \in A$, diciamo **classe di equivalenza** di a rispetto a E (e denotiamo $a|_E$)

$$\{b \in A : \ aEb\}.$$

Si noti che $a \in a|_E$ perché aEa. Diciamo poi *insieme quoziente* di A rispetto a E l'insieme delle classi di equivalenza di elementi di A rispetto a E

$$A|_E = \{a|_E : \ a \in A\}.$$

Una proprietà fondamentale delle classi di equivalenza è che due qualunque di esse, se distinte, sono anche disgiunte, prive cioè di elementi comuni.

Lemma.

Siano $a, b \in A$. Se aEb, allora $a|_E = b|_E$; altrimenti, se $a \not E b$, $a|_E \cap b|_E = \emptyset$.

Dimostrazione.

Sia aEb (da cui anche bEa). Proviamo $a|_E \subseteq b|_E$ ($b|_E \subseteq a|_E$ segue allora da bEa, invertendo i ruoli di a e b; così si conclude $a|_E = b|_E$).
Sia $c \in a|_E$. Allora aEc; da bEa e dalla proprietà transitiva, bEc; segue $c \in b|_E$.
Sia ora $a \not E b$, cioè a non sia in relazione E con b. Se esiste $c \in a|_E \cap b|_E$, vale sia aEc che bEc, dunque aEb: assurdo. Cosdeve essere $a|_E \cap b|_E = \emptyset$. □

Definizione.

Si dice **partizione** di un insieme A un insieme P di sottoinsiemi di A non vuoti, disgiunti, aventi A come unione.

Per il lemma, le classi di equivalenza $a|_E = \{b \in A : \ aEb\}$ formano al variare di $a \in A$ una partizione di A: infatti

- $\forall a \in A$, $a|_E \neq \emptyset$ perché $a|_E$ contiene a;
- se $a, b \in A$ e $a|_E \neq b|_E$, $a|_E \cap b|_E = \emptyset$;
- $\forall a \in A$, $a \in a|_E$, e così $A = \bigcup_a a|_E$.

Viceversa, si può provare che ad ogni partizione P di A corrisponde una relazione di equivalenza E per cui

$$P = A|_E.$$

Consideriamo l'insieme A con una classe fi equivalenza E e la funzione $\pi : A \to A|_E$ che associa $\forall a \in A$ associa

$$\pi(a) = a|_E;$$

π si dice la **proiezione canonica** di A su $A|_E$. π è suriettiva perché, $\forall a \in A$, $a|_E = \pi(a)$. Inoltre, per $a, b \in A$,

$\pi(a) = \pi(b)$ se e solo se $a|_E = b|_E$, dunque se e solo se aEb.

La relazione di equivalenza suddivide gli elementi dell'insieme A in base a un qualche prefissato criterio; le classi di equivalenza che così si formano raggruppano gli elementi che manifestano lo stesso comportamento rispetto a questo criterio; l'insieme quoziente $A|_E$, che è formalmente l'insieme delle classi, rappresenta intuitivamente la lista dei possibili comportamenti degli elementi di A rispetto al criterio stabilito da E; la proiezione canonica associa ad ogni $a \in A$ la sua classe.

Esempi. Riprendiamo gli esempi precedenti.

1. $\forall r \in A$ (cioè per ogni retta del piano), $r|_{//} = \{s \in A : r//s\}$ può intendersi come la comune "direzione" di r e delle rette ad essa parallele. In questo senso, $A|_{//}$ l'insieme delle possibili direzioni delle rette del piano.
2. Consideriamo il caso di $=$. $\forall a \in A$, $a|_{=} = \{a\}$. La classe di a è formata dal solo a. Così $A|_{=} = \{\{a\} : a \in A\}$ si può identificare con con A. Nell'altro caso trattato nell'esempio, si ha che, per ogni $a \in A$, $a|_E = A$; tutti gli elementi condividono la stessa classe A, dunque $A|_E = \{A\}$ ha un solo elemento.

3. $\forall x \in \mathbb{R}$, $x|_E = \{x, -x\}$, infatti due elementi sono nella stessa classe se e solo se hanno lo stesso valore assoluto. Così $x|_E$ è individuata dal reale non negativo $|x|$ e in questo senso $\mathbb{R}|_E = \mathbb{R}^{\geq 0}$ (l'insieme dei reali ≥ 0, cioè dei possibili valori assoluti dei reali).
4. $\forall x, y \in \mathbb{R}$, $(x, y)|_E = \{(x', y') : x'^2 + y'^2 = x^2 + y^2\}$ è la circonferenza con centro $O(0, 0)$ e raggio $\sqrt{x^2 + y^2}$; quindi la classe $(x, y)|_E$ è individuata dalla comune distanza da O dei suoi elementi, e in questo senso $\mathbb{R}^2|_E = \mathbb{R}^{\geq 0}$ (inteso come l'insieme dei possibili raggi di queste circonferenze).
5. $\forall a \in A$, $a|_E = \{a' \in A : f(a) = f(a')\}$ è costituito dagli elementi di A che hanno la stessa immagine di a in f. Così $A|_E = f(A) \subseteq B$.

Grafi.

Definizione.

Un **grafo non orientato** (o, più semplicemente, *grafo*) è una coppia (V, R) dove V è un insieme non vuoto e R è una relazione binaria su V tale che

(i) $\forall v \in V$, $v \not R v$ (proprietà antiriflessiva);

(ii) $\forall u, v \in V$, se uRv, allora vRu (proprietà simmetrica).

Si noti che la proprietà antiriflessiva non è la negazione della proprietà riflessiva: quest'ultima chiede

$$\forall v \in V,\ vRv,$$

ed è dunque negata dicendo

$$\exists v \in V \text{ tale che } v \not R v.$$

Quindi la proprietà antiriflessiva è assai più forte.

I punti si V si dicono **vertici** (o *nodi*) del grafo, le coppie di R **lati** o *archi*.

Esempio.

Consideriamo il grafo avente

- vertici 0, 1, 2, 3, 4,
- lati $(0,1)$, $(1,2)$, $(2,4)$, $(4,0)$, $(0,3)$ (e $(1,0)$, $(2,1)$, $(4,2)$, $(0,4)$, $(3,0)$).

Un grafo orientato è da intendere come una coppia (V, R) con V insieme non vuoto e R relazione binaria su V.

Come per i grafi, anche i grafi orientati hanno una rappresentazione visiva, ma stavolta ogni lato (u, v) in R viene dotato di una freccia da u a v, a denotare l'ordine degli elementi della coppia. Naturalmente, non è escluso che quando uRv, si abbia talora anche vRu: si ha allora un lato da u a v, e un altro lato di ritorno da v ad u.

Relazioni d'ordine

Definizione.

Sia $A \neq \emptyset$. Una relazione binaria R su A si dice **di ordine parziale** se valgono le seguenti proprietà:

(i) riflessiva: $\forall a \in A$, aRa;

(ii) antisimmetrica: $\forall a, b \in A$, se aRb e bRa, allora $a = b$;

(iii) transitiva: $\forall a, b, c \in A$, se aRb e bRc, allora aRc.

Ricordiamo che la proprietà simmetrica afferma:

$$\forall a, b \in A, \text{ se } aRb, \text{ allora } bRa.$$

Così la sua negazione dice:

$$\exists^{\text{no}}\, a, b \in A \text{ tali che } aRb \text{ ma } b \not R\, a.$$

Dunque la proprietà antisimmetrica sopra enunciata è molto più forte di quest'ultima condizione.
Se R è una relazione di ordine parziale su A, scriveremo che (A, R) è un insieme **parzialmente ordinato** o anche che A è *parzialmente ordinato* da R.

Esempi.

a. Siano $A = \mathbb{Z}$, $R = \leq$. Allora (i), (ii), (iii) si verificano facilmente. Inoltre vale:

(iv) per ogni scelta di $a, b \in \mathbb{Z}$, $a \leq b$ oppure $b \leq a$.

Lo stesso vale per $A = \mathbb{N}$, $R = \leq$ (in $\mathbb{N}$).

b. Consideriamo $A = \mathbb{N}$, $R = |$ (la relazione di divisibilità: per $a, b \in \mathbb{N}$, $a|b$ se e solo se esiste $q \in \mathbb{N}$ tale che $b = a \cdot q$). Allora $|$ è una relazione di ordine parziale.

(i) $\forall a \in \mathbb{N}$, $a|a$: infatti $a = a \cdot 1$.

(ii) $\forall a, b \in \mathbb{N}$, se $a|b$ e $b|a$, allora $a = b$: infatti esistono $q, q' \in \mathbb{N}$ tali che $b = a \cdot q$, $a = b \cdot q'$, così $a = a \cdot q \cdot q'$ e $a \cdot (1 - q \cdot q') = 0$; se $a \neq 0$ deve essere $1 - q \cdot q' = 0$, da cui $q = q' = 1$ e $a = b$; se invece $a = 0$, anche $b = 0$ e dunque $a = b$.

(iii) $\forall a, b, c \in \mathbb{N}$, se $a|b$ e $b|c$, allora $a|c$. Infatti siano $q, q' \in \mathbb{N}$ tali che $b = a \cdot q$ e $c = b \cdot q'$, allora $c = a \cdot (q \cdot q')$.

Invece non vale (iv): ad esempio $2 \nmid 3$ e $3 \nmid 2$.

c. Siano S un insieme, $A = \mathcal{P}(S)$, $R = \subseteq$. Sappiamo che valgono (i), (ii), (iii). Invece, (iv) non vale (almeno se S ha almeno due elementi $s \neq t$: infatti $\{s\} \not\subseteq \{t\}$ e $\{t\} \not\subseteq \{s\}$).

Definizione

Sia R una relazione di ordine parziale su A. R si dice una relazione di **ordine totale** (o *lineare*) se soddisfa l'ulteriore condizione:

(iv) per ogni scelta di $a, b \in A$, aRb o bRa.

In tal caso (A, R) si dice **totalmente ordinato** (o *linearmente ordinato*). Così $\leq$ è una relazione di ordine totale in $\mathbb{Z}$ (o, in $\mathbb{N}$ o $\mathbb{Q}$ o $\mathbb{R}$).

Da ora in poi, denoteremo con $\leq$ una generica relazione di ordine parziale. Inoltre, per $a, b \in A$,

$$a < b \text{ significherà } a \leq b \text{ e } a \neq b.$$

Definizione.

Sia (A, R) un insieme parzialmente ordinato. Un elemento $a \in A$ si dice

- **massimo** se, $\forall s \in A$, $a \geq s$,
- **minimo** se, $\forall s \in A$, aRs.

Esempi.

1. L'insieme S è un massimo e l'insieme $\emptyset$ è un minimo in $\mathcal{P}(S)$ rispetto a $\subseteq$.
2. 1 è un minimo in $\mathbb{N}$ rispetto alla relazione di divisibilità $|$ perché 1 divide ogni naturale; $(\mathbb{N}, |)$ ha anche un massimo 0, infatti ogni naturale a è divisore di 0, $0 = a \cdot 0$.

Osservazione.

- Un insieme parzialmente ordinato A può non avere massimo, o minimo: ad esempio, $(\mathbb{Z}, \leq)$ non ha né massimo né minimo, mentre l'insieme $\{a \in \mathbb{Q} : \ 0 < a \leq 1\}$ rispetto alla relazione $\leq$ tra i razionali ha massimo 1, ma non minimo (non cè infatti un minimo razionale positivo a: per ogni $a > 0$, $0 < \frac{a}{2} < a$). Invece $(\mathbb{N}, \leq)$ ha minimo 0, ma non massimo.
- Se A ha massimo, o minimo, esso è unico (con le notazioni $max\, A$, $min\, A$, rispettivamente). Infatti, se a, a' sono due massimi, $a \leq a'$ e $a' \leq a$, dunque $a = a'$ per l'antisimmetria. Lo stesso vale per i minimi.

Definizione.

Un elemento $a \in A$ si dice

- **massimale** se, $\forall s \in A$, quando aRs, allora $s = a$;
- **minimale** se, $\forall s \in A$, quando sRa, allora $s = a$.

Un elemento è massimale se non ne ha di più grandi, e minimale se non ne ha di più piccoli. È ammessa tuttavia l'eventualità di elementi che non gli sono confrontabili in $\leq$. Bisogna allora porre attenzione a distinguere

- *elementi massimali* da *massimi*,
- *elementi minimali* da *minimi*.

Esempio

Consideriamo l'insieme $\{1, 2, 3\}$ ordinato dalla divisibilità. Così

$$1|2, \ 1|3, \ 2 \nmid 3, \ 3 \nmid 2.$$

1 è minimo (e minimale), mentre $2, 3$ sono massimali, ma non massimi.

Definizione.

Una relazione di ordine totale $\leq$ in A si dice un ordine **denso** se, $\forall a, b \in A$ con $a < b$, $\exists c \in A$ tale che $a < c$ e $c < b$.

Esempi.

1. L'usuale relazione $\leq$ tra i razionali $\mathbb{Q}$ è densa; infatti per $a, b \in \mathbb{Q}$ con $a < b$, consideriamo l'elemento $c = \frac{a+b}{2}$. Allora $c \in \mathbb{Q}$ e $a = \frac{a+a}{2} < \frac{a+b}{2} < \frac{b+b}{2} = b$.
2. Analogo discorso vale per $(\mathbb{R}, \leq)$.

Un possibile controesempio è costituito da $(\mathbb{Z}, \leq)$. Esso non è denso: ad esempio $0 < 1$, ma non esiste alcun $x \in \mathbb{Z}$ tale che $0 < x < 1$.

Definizione.

Una relazione di ordine (parziale) $\leq$ in A si dice un **buon ordine** se ogni sottoinsieme non vuoto X di A ha un minimo rispetto a $\leq$. In tal caso $(A, \leq)$ si dice insieme **bene ordinato**.

Si osservi che un buon ordine è totale: infatti, per $a, b \in A$, l'insieme $\{a, b\}$ ha un minimo a o b, dunque $a \leq b$ o $b \leq a$.

Un esempio di buon ordine è rappresentato da $\mathbb{N}$ rispetto a $\leq$. In effetti in un insieme bene ordinato $(A, \leq)$ c'è un primo elemento a_0 (il minimo di A), poi un secondo elemento a_1 (il minimo di $A - \{a_0\}$), e così via, fino a elencare tutti gli elementi di A, proprio come accade per $\mathbb{N}$, i cui elementi si enumerano $0, 1, 2, \ldots$.

Qualche Calcolo

Ammettiamo di avere due insiemi **finiti** A e B, e di conoscere il numero degli elementi tanto di A quanto di B. Poniamo quindi $|A| = n$ e $|B| = m$, fissiamo $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_m\}$.Vogliamo contare quanti sono gli elementi di $A \cup B$, $A \cap B$, $A \times B$, $\mathcal{P}(A)$, $A - B$; o anche quante sono le funzioni di A in B; chiarire altre simili questioni di calcolo.

Ricordiamo:

- $|\mathcal{P}(A)| = 2^n$,
- $|A \times B| = n \cdot m$.

Consideriamo allora gli altri casi. Si ha anzitutto quanto segue.

Osservazione.

- $|A \cup B| = |A| + |B| - |A \cap B|$.

In particolare vale $|A \cup B| = |A| + |B|$ se e solo se A, B sono disgiunti. L'uguaglianza sopra enunciata si pu ò generalizzare opportunamente al caso di tre o pi ù insiemi: ad esempio si vede

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|.$$

Per gli elementi di $A \cup B \cup C$ si ottengono considerando prima quelli di A, poi quelli di B, infine quelli di C; ma in questo modo gli elementi che appartengono a una delle intersezioni $A \cap B$, $A \cap C$, $B \cap C$ sono contati due volte, e dunque vanno sottratti. Capita che gli elementi di $A \cap B \cap C$ siano sottratti tre volte; occorre dunque riaggiungerli per ottenere l'uguaglianza corretta.

1. $|A - B| = |A| - |A \cap B|$.
   In particolare $|A - B| = |A| - |B|$ se e solo se $B \subseteq A$.

Supponiamo di dover rispondere alle seguenti domande:

1. Quanti sono i numeri naturali con 5 cifre (nella usuale rappresentazione decimale)?
2. Quanti quelli con 5 cifre tutte diverse tra loro?
3. Quanti quelli con 5 cifre di cui almeno 2 uguali?

Ecco la rispettiva discussione.

1. La prima cifra puèessere scelta in 9 modi (da 1 a 9), le altre in 10 modi (da 0 a 9). Coì le possibili scelte di un numero di 5 cifre sono

$$9 \cdot 10^4$$

(si usa qui la legge per stabilire il numero degli elementi di un prodotto cartesiano).

2. Scelta la prima cifra, la seconda, per evitare ripetizioni, può essere presa solo in $10 - 1 = 9$ modi. Si hanno allora

$$9 \cdot 9 \cdot 8 \cdot 7 \cdot 6$$

numeri con 5 cifre, di cui mai due uguali.

3. I numeri che hanno 5 cifre di cui almeno due uguali sono, allora,

$$9 \cdot 10^4 - 9 \cdot 9 \cdot 8 \cdot 7 \cdot 6$$

si ottengono cioè da quelli con 5 cifre escludendo quelli che non hanno ripetizioni.

Contiamo adesso quante sono le possibili funzioni da A a B, e anche quante di queste funzioni sono iniettive o suriettive, o biiettive. Va osservato che non sempre esistono funzioni iniettive, o suriettive, o biiettive da A a B; in ragione di $|A|$ o $|B|$, queste funzioni possono, infatti, mancare.

Ad esempio, ammettiamo che A sia un insieme di n piccioni, B un insieme di m nicchie dove ogni piccione può trovare riparo. È allora facile convenire:

Principio della piccionaia. Se una piccionaia ha m nicchie e n piccioni, con $n > m$, allora almeno due piccioni finiscono nella stessa nicchia.
Tradotto in termini rigorosi, il principio sostiene che, se $n > m$, nessuna funzione di A in B è iniettiva.

Teorema.

Siano A, B insiemi finiti, con $|A| = n$ e $|B| = m$. Fissiamo, come sopra, $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_m\}$. Allora:

(i) esiste una funzione iniettiva di A in B se e solo se $n \leq m$,

(ii) esiste una funzione suriettiva di A in B se e solo se $n \geq m$,

(iii) esiste una funzione biiettiva di A in B se e solo se $n = m$.

Dimostrazione.
(i) Se $n \leq m$, ponendo $f(a_i) = b_i$ per ogni $i = 1, \ldots, n$, si definisce una funzione iniettiva di A in B. Viceversa, se $f : A \to B$ è iniettiva, $f(a_1), \ldots, f(a_n)$ sono elementi distinti di B, quindi $m \geq n$.

(ii) Se $n \geq m$, ponendo $f(a_i) = b_i$ per ogni $i = 1, \ldots, m$ e $f(a_{m+1}) = \cdots = f(a_n) = b_1$, si definisce una funzione suriettiva di A su B. Viceversa, se $f : A \to B$ è suriettiva, possiamo scegliere $x_1, \ldots, x_m \in A$ tale che $f(x_1) = b_1, \ldots, f(x_m) = b_m$; così $x_1, \ldots, x_m$ sono elementi distinti di A, e $m \leq n$.

(iii) Una funzione biiettiva di A su B, è anche iniettiva (il che implica $n \leq m$) e suriettiva (dunque $m \leq n$). Quindi $n = m$. Viceversa, se $n = m$, ponendo $f(a_i) = b_i$ per ogni $i = 1, \ldots, n$ si definisce una funzione biiettiva di A su B. □

Teorema

Siano A, B, n, m come nel Teorema precedente, con $n \leq m$ (così ci sono funzioni iniettive di A in B). Allora esistono $m \cdot (m-1) \cdot (m-2) \cdots (m-n+1)$ funzioni iniettive di A in B.

Ad esempio, per $|A| = 3$ e $|B| = 5$, ci sono $5 \cdot 4 = 20$ funzioni iniettive da A in B.

Dimostrazione. Sia $f : A \to B$ iniettiva. Ci sono m valori possibili per $f(a_1)$, $m-1$ valori per $f(a_2)$ (perché va escluso quello giù ottenuto da $f(a_1)$), $m-2$ valori per $f(a_3)$, e così via. □

Corollalio

Sia $n = m$ (ci sono corrispondenze biunivoche di A su B). Allora le corrispondenze biunivoche di A su B sono $n \cdot (n-1) \cdots 2 \cdot 1$.

Dimostrazione. Si ricordi che una funzione di A in B è biiettiva se e solo se è iniettiva. Si applichi allora il teorema precedente al caso $m = n$. □

Definizione.

$\forall n \in \mathbb{N}$, con $n > 0$, poniamo

$$n! = n \cdot (n-1) \cdots 2 \cdot 1;$$

$n!$ si legge n **fattoriale**. Si conviene poi $0! = 1$.

Ad esempio,

- $1! = 1$,
- $2! = 2 \cdot 1 = 2$,
- $3! = 3 \cdot 2 \cdot 1 = 6$,
- $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$,
- $5! = 120$.

Ovviamente, $\forall n \in \mathbb{N}$, $(n+1)! = (n+1) \cdot n!$.

Possiamo allora dire che, per $|A| = |B| = n$, ci sono $n!$ corrispondenze biunivoche di A su B. In particolare, per $|A| = n$, ci sono $n!$ corrispondenze biunivoche di A su A.

Teorema.

Siano A, B insieme finiti, con $|A| = m$, $|B| = n$. Le funzioni di A in B sono m^n.

Dimostrazione. Sia f una funzione di A in B. Esistono m possibili valori per ogni elemento $f(a_1), \ldots, f(a_n)$. La loro scelta determina f. Così vi sono $m \cdot m \cdots m = m^n$ funzioni di A in B. □

Passiamo adesso a contare i sottoinsiemi di un insieme A con n elementi. Sappiamo che il loro numero complessivo è 2^n. Ma può essere utile sapere quanto segue.

Teorema.

Sia $k \in \mathbb{N}$, $k \leq n$. Allora il numero dei sottoinsiemi di A con esattamente k elementi è

$$\frac{n!}{k! \cdot (n-k)!}.$$

Dimostrazione. Fissiamo $C \subseteq A$, $|C| = k$. $\forall C' \subseteq A$, $|C'| = k$ se e solo se esiste una corrispondenza biunivoca di C su C', cioè una funzione iniettiva f da C in A con $f(C) = C'$. Fissato C', possono esserci più funzioni iniettive di C in A con immagine C': esse, comunque, coincidono con le corrispondenze biunivoche di C su C', che sappiamo essere $k!$; dunque il numero delle funzioni iniettive da C in A è uguale al prodotto del numero s dei sottoinsiemi C' di A aventi k elementi per il numero $k!$ delle corrispondenze biunivoche di C su un tale C'.

Sappiamo che il numero complessivo delle funzioni iniettive di C in A è $n \cdot (n-1) \cdots (n-k+1)$. Ne deduciamo

$$s \cdot k! = n \cdot (n-1) \cdots (n-k+1).$$

Segue

$$s = \frac{n \cdot (n-1) \cdots (n-k+1)}{k!}.$$

Moltiplicando numeratore e denominatore per $(n-k)! = (n-k) \cdot (n-k-1) \cdots 2 \cdot 1$, otteniamo finalmente

$$s = \frac{n!}{k! \cdot (n-k)!}.$$

□

Definizione.

Siano $k, n \in \mathbb{N}$, $k \leq n$. Il numero $\frac{n!}{k! \cdot (n-k)!}$ appena determinato si indica

$$\binom{n}{k}$$

Osservazioni.

1. Per $k = 0$
$$\binom{n}{0} = \frac{n!}{0! \cdot n!} = 1;$$
del resto A ha un solo sottoinsieme con 0 elementi, cioè $\emptyset$. Analogamente
$$\binom{n}{n} = \frac{n!}{n! \cdot 0!} = 1,$$
infatti l'unico sottoinsieme di A con n elementi è A stesso.

2. Per $k \leq n$, si ha
$$\binom{n}{k} = \binom{n}{n-k}$$
infatti $n - (n - k) = k$. I sottoinsiemi di A con k elementi sono tanti quanti i loro complementi in A, cioè i sottoinsiemi con $n - k$ elementi.

3. Vale anche

Proposizione.

Siano $k, n \in \mathbb{N}$, $0 < k < n$. Allora

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Dimostrazione. Fissiamo $A = \{a_1, \ldots, a_n\}$ con $a_1 \neq \cdots \neq a_n$. I sottoinsiemi di A con k elementi si suddividono in due insiemi disgiunti:

- quelli non contenenti a_1, ovvero i sottoinsiemi di $\{a_2, \ldots, a_n\}$ con k elementi: ce ne sono $\binom{n-1}{k}$;
- quelli contenenti a_1, che si ottengono dai sottoinsiemi di $\{a_2, \ldots, a_n\}$ con $k-1$ elementi aggiungendo a_1: essi sono $\binom{n-1}{k-1}$.

Dunque

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Teorema binomiale.

Sia $n \in \mathbb{N}$. Allora, per ogni scelta di a, b,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k}.$$

Dimostrazione. Usiamo principio di induzione per $\mathbb{N}$: mostriamo cioè che il teorema è vero per $n = 0$ e che, se è valido per un certo n, allora si trasmette anche a $n+1$.

Per $n = 0$ si nota facilmente

$$(a+b)^0 = 1, \quad \binom{0}{0} a^0 \cdot b^0 = 1.$$

Operiamo adesso il passo induttivo: supponiamo cioè il risultato vero per n, e lo proviamo per $n+1$. La dimostrazione è svolta dalla seguente computazione:

$$(a+b)^{n+1} = (a+b)^n \cdot (a+b) = \left(\sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k}\right) \cdot (a+b) =$$

$$= \left(\binom{n}{0} b^n + \binom{n}{1} a \cdot b^{n-1} + \binom{n}{2} a^2 \cdot b^{n-2} + \cdots + \binom{n}{n-1} a^{n-1} \cdot b + \binom{n}{n} a^n\right) \cdot (a+b) =$$

$$= \binom{n}{0} b^{n+1} + \left(\binom{n}{0} + \binom{n}{1}\right) a \cdot b^n + \left(\binom{n}{1} + \binom{n}{2}\right) a^2 \cdot b^{n-1} + \cdots + \binom{n}{n} a^{n+1}$$

$$= \binom{n+1}{0} b^{n+1} + \binom{n+1}{1} a \cdot b^n + \binom{n+1}{2} a^2 \cdot b^{n-1} + \cdots$$

$$\cdots + \binom{n+1}{n+1} a^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k \cdot b^{n+1-k}.$$

Nel primo rigo si sfrutta l'ipotesi di induzione valida per n per rappresentare $(a+b)^n$. Si svolge poi il prodotto $(a+b)^n \cdot (a+b)$. Al penultimo rigo si usa la Proposizione precedente per scrivere, ad esempio, $\binom{n}{0} + \binom{n}{1}$, come $\binom{n+1}{1}$; si osserva poi che banalmente

$$\binom{n}{0} = 1 = \binom{n+1}{0},$$

$$\binom{n}{n} = 1 = \binom{n+1}{n+1}.$$

□