ALGEBRA (Parte I)

Nel seguito diamo per note le notazioni, le definizioni di inclusione, uguaglianza e operazioni su insiemi e le relative proprietà.

Relazioni

Ricordiamo che si chiama prodotto cartesiano degli n insiemi $A_1, A_2, \ldots, A_n$, l'insieme

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

Notiamo che gli elementi del prodotto cartesiano sono n-uple ordinate ed è quindi rilevante l'ordine in cui si considerano gli insiemi.
Per convenzione, se $n = 1$ il prodotto cartesiano si riduce ad A_1.

Si chiama relazione R (n-aria o di arità n) fra gli n insiemi $A_1, A_2, \ldots, A_n$ un qualsiasi sottoinsieme di $A_1 \times A_2 \times \ldots \times A_n$.

Siano ora $R \subseteq A_1 \times A_2 \times \ldots \times A_n$ e $T \subseteq A_1 \times A_2 \times \ldots \times A_n$ due relazioni fra gli n insiemi $A_1, A_2, \ldots, A_n$. Dalle definizioni insiemistiche si ha:

$R \subseteq T$ sse per ogni $(a_1, a_2, \ldots, a_n) \in R$ si ha $(a_1, a_2, \ldots, a_n) \in T$.
$R = T$ sse $R \subseteq T$ e $T \subseteq R$.
$R \subset T$ sse $R \subseteq T$ ed esiste almeno una n-upla $(a'_1, a'_2, \ldots, a'_n) \in T$ tale che $(a'_1, a'_2, \ldots, a'_n) \notin R$
$R \cap T = \{(a_1, a_2, \ldots, a_n) \mid (a_1, a_2, \ldots, a_n) \in R \text{ e } (a_1, a_2, \ldots, a_n) \in T\}$
$R \cup T = \{(a_1, a_2, \ldots, a_n) \mid (a_1, a_2, \ldots, a_n) \in R \text{ o } (a_1, a_2, \ldots, a_n) \in T\}$.

Come è ben noto dalle nozioni sulla teoria degli insiemi, le definizioni di intersezione ed unione si possono estendere ad una famiglia arbitraria di relazioni fra gli n insiemi $A_1, A_2, \ldots, A_n$. Pertanto se consideriamo una famiglia di relazioni $\{R_i \mid i \in I\}$ fra $A_1, A_2, \ldots, A_n$, dove l'indice i varia in un qualsiasi insieme I, usiamo le seguenti notazioni

$$\bigcap_{i \in I} R_i = \{(a_1, a_2, \ldots, a_n) \mid \forall i \in I \quad (a_1, a_2, \ldots, a_n) \in R_i\}$$
$$\bigcup_{i \in I} R_i = \{(a_1, a_2, \ldots, a_n) \mid \exists i \in I \quad (a_1, a_2, \ldots, a_n) \in R_i\}$$

Le operazioni fra relazioni godono ovviamente delle proprietà ben note per le operazioni insiemistiche.

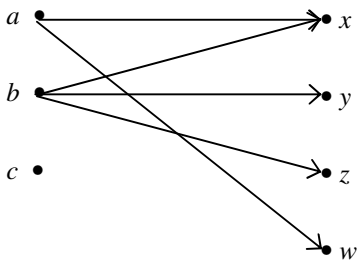
Relazioni binarie

Consideremo nel seguito il caso $n = 2$, cioè le relazioni binarie o di arità 2.
Se R è una relazione binaria la notazione $a_1 R a_2$ ha lo stesso significato della scrittura $(a_1, a_2) \in R$.

Nel caso in cui gli insiemi A_1 ed A_2 con cui lavoriamo contengano un *numero finito di elementi* (indicheremo rispettivamente con $|A_1|$ e $|A_2|$ tali numeri), una relazione $R \subseteq A_1 \times A_2$ potrà essere utilmente rappresentata attraverso:

- il grafo di incidenza.
  Un *grafo (orientato)* è una coppia di insiemi (V,E), V è l'insieme dei vertici, E è l'insieme degli archi, ogni arco può essere pensato come una coppia di vertici, il primo elemento della coppia si dice vertice iniziale dell'arco, il secondo vertice finale.
  Un grafo si può disegnare rappresentando i suoi vertici come punti ed i suoi archi come frecce dal vertice iniziale al vertice finale.
  In particolare se partiamo da una relazione $R \subseteq A_1 \times A_2$ si dice *grafo di incidenza* di R il grafo il cui insieme di vertici è $A_1 \cup A_2$ e il cui insieme di archi è R.

  Esempio: Siano $A_1=\{a,b,c\}$, $A_2=\{x,y,z,w\}$, $R=\{(a,x),(a,w),(b,x),(b,y),(b,z)\}$, il grafo di incidenza di R è



- la matrice di incidenza.
  Dopo aver fissato un ordine fra gli $|A_1|$ elementi di A_1 e fra gli $|A_2|$ elementi di A_2 (ad esempio quello in cui vengono elencati gli elementi in ciascun insieme) la *matrice di incidenza* di R è una matrice con $|A_1|$ righe ed $|A_2|$ colonne, con elementi in $\{0,1\}$, tale che il suo elemento di posto (i,k) è 1 se e solo se la coppia costituita dall'i-esimo elemento di A_1 e dal j-esimo elemento di A_2 appartiene ad R.

  Facendo riferimento all'esempio precedente (usando come ordine degli elementi dei due insiemi quello alfabetico) la matrice di incidenza di R è

$$M_R = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Osserviamo che, date le matrici di incidenza M_R, M_T di due relazioni binarie $R,T \subseteq A_1 \times A_2$, si possono immediatamente ottenere la matrice di incidenza di $R \cap T$ (facendo il prodotto elemento per elemento di M_R con M_T) e quella di $R \cup T$ (facendo la somma di M_R con M_T e ponendo uguale ad 1 tutti gli elementi della somma maggiori di 0).

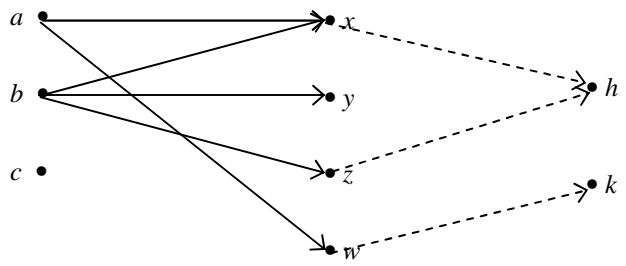
Siano ora date le relazioni $R \subseteq A_1 \times A_2$ e $T \subseteq A_2 \times A_3$. Si chiama prodotto delle due relazioni la relazione $R \cdot T \subseteq A_1 \times A_3$ così definita:

$$R \cdot T = \{(a_1,a_3) \mid \exists\, a_2 \colon (a_1,a_2) \in R \text{ e } (a_2,a_3) \in T\}$$

(ovviamente, per come sono definite le relazioni R e T, $(a_1,a_2) \in R$ e $(a_2,a_3) \in T$ implicano $a_1 \in A_1$, $a_2 \in A_2$, $a_3 \in A_3$). Notare la somiglianza col prodotto di matrici.

Nel caso in cui gli insiemi siano finiti, la definizione può essere resa più chiara con un esempio che utilizza anche la rappresentazione delle relazioni tramite grafi o matrici di incidenza.

Esempio: Siano $A_1=\{a,b,c\}$, $A_2=\{x,y,z,w\}$, $A_3=\{h,k\}$, $R=\{(a,x),(a,w),(b,x),(b,y),(b,z)\}$, $T=\{(x,h),(z,h),(w,k)\}$.
Calcoliamo $R\cdot T$, si ha
$(a,h)\in R\cdot T$ in quanto esiste x tale che $(a,x)\in R$ e $(x,h)\in T$,
$(a,k)\in R\cdot T$ in quanto esiste w tale che $(a,w)\in R$ e $(w,k)\in T$,
$(b,h)\in R\cdot T$ in quanto esiste x tale che $(b,x)\in R$ e $(x,h)\in T$,
nessuna altra coppia appartiene ad $R\cdot T$.
Usando i grafi delle due relazioni (sovrapponendo i vertici di ugual nome) abbiamo il seguente diagramma:



dove le frecce a tratto continuo rappresentano la relazione R e quelle tratteggiate rappresentano la T.
Dalla definizione risulta che una coppia di vertici appartiene alla relazione $R\cdot T$ se e solo se si può andare dal primo elemento della coppia al secondo percorrendo prima un arco a tratto continuo (relazione R) e poi un arco tratteggiato (relazione T).

Se consideriamo invece le matrici di incidenza abbiamo

$$M_R=\begin{bmatrix}1&0&0&1\\1&1&1&0\\0&0&0&0\end{bmatrix},\qquad M_T=\begin{bmatrix}1&0\\0&0\\1&0\\0&1\end{bmatrix}$$

si può effettuare il prodotto di matrici e si ottiene la matrice $\begin{bmatrix}1&1\\2&0\\0&0\end{bmatrix}$ che, con la solita convenzione di porre uguale ad 1 tutti gli elementi maggiori di 0, è proprio la matrice di incidenza di $R\cdot T$, infatti l'elemento di posto (i,k) di questa matrice è diverso da 0 se e solo se esiste un j tale che l'elemento di posto (i,j) di M_R e l'elemento di posto (j,k) di M_T siano entrambi non nulli.
Notiamo anche che la presenza di un $t>1$ nel posto (i,k) della matrice prodotto significa che ci sono t diversi elementi dell'insieme A_2 che possono servire da "collegamento" nel prodotto (nel nostro caso abbiamo 2 nel posto (2,1) perché esistono sia x sia z che possono servire da collegamento infatti $bR\,x$ e $x\,T\,h$, $b\,R\,z$ e $z\,T\,h$).

Il prodotto di relazioni gode delle seguenti proprietà:

- *è associativo*, cioè per ogni R, T, S tali che $R\subseteq A_1\times A_2$, $T\subseteq A_2\times A_3$, $S\subseteq A_3\times A_4$, si ha $(R\cdot T)\cdot S = R\cdot(T\cdot S)$.
  E' facile osservare che entrambe le relazioni $(R\cdot T)\cdot S$, $R\cdot(T\cdot S)$ sono contenute in $A_1\times A_4$.
  Dobbiamo allora provare che
  $(R\cdot T)\cdot S\subseteq R\cdot(T\cdot S)$
  cioè che $(a_1,a_4)\in(R\cdot T)\cdot S$ implica $(a_1,a_4)\in R\cdot(T\cdot S)$.

Per definizione $(a_1,a_4) \in (R\cdot T)\cdot S$ implica che esiste un a_3 tale che
$(a_1,a_3) \in R\cdot T$ e $(a_3,a_4) \in S$.
Ancora per definizione $(a_1,a_3) \in R\cdot T$ implica che esiste un a_2 tale che
$(a_1,a_2) \in R$ e $(a_2,a_3) \in T$.
Ora, $(a_2,a_3) \in T$ e $(a_3,a_4) \in S$ implicano $(a_2,a_4) \in T\cdot S$ e questa con $(a_1,a_2) \in R$ implica
$(a_1,a_4) \in R\cdot(T\cdot S)$.
Analogamente si prova che $R\cdot(T\cdot S) \subseteq (R\cdot T)\cdot S$ cioè che $(a_1,a_4) \in R\cdot(T\cdot S)$ implica $(a_1,a_4) \in (R\cdot T)\cdot S$.

- *è compatibile con l'inclusione*, cioè se $R \subseteq T \subseteq A_1\times A_2$, $S \subseteq A_2\times A_3$, $V \subseteq A_4\times A_1$ si ha
  $R\cdot S \subseteq T\cdot S$ e $V\cdot R \subseteq V\cdot T$.
  Da questo si deduce anche che se $R \subseteq T \subseteq A_1\times A_2$, $S \subseteq U \subseteq A_2\times A_3$ si ha
  $R\cdot S \subseteq T\cdot U$.
  Si osservi che se $R \subset T \subseteq A_1\times A_2$, $S \subseteq A_2\times A_3$, possiamo solo concludere che $R\cdot S \subseteq T\cdot S$ e non che $R\cdot S \subset T\cdot S$; analogamente se $R \subset T \subseteq A_1\times A_2$, $V \subseteq A_4\times A_1$ possiamo solo concludere che $V\cdot R \subseteq V\cdot T$ e se $R \subset T \subseteq A_1\times A_2$, $S \subset U \subseteq A_2\times A_3$ possiamo solo concludere che $R\cdot S \subseteq T\cdot U$ (*fare per esercizio*).

Il prodotto di relazioni *non è commutativo*, infatti date $R \subseteq A_1\times A_2$ e $T \subseteq A_2\times A_3$, $R\cdot T$ è sempre definito, mentre $T\cdot R$ è definito solo se gli insiemi A_1 e A_3 coincidono ed in tal caso $R\cdot T \subseteq A_1\times A_1$ e $T\cdot R \subseteq A_2\times A_2$, quindi $R\cdot T$ e $T\cdot R$ sono relazioni fra la stessa coppia di insiemi se e solo se anche gli insiemi A_1 e A_2 coincidono, ma anche in questo caso in genere $R\cdot T \neq T\cdot R$. Basta a tale scopo considerere $A_1=\{a,b\}$, $R=\{(a,b)\}$, T=$\{(b,b)\}$, si ha $R\cdot T=\{(a,b)\}$ e $T\cdot R=\varnothing$.
Se $R\cdot T = T\cdot R$, le relazioni T ed R si dicono *permutabili*.

Si dice relazione inversa di $R \subseteq A_1\times A_2$ la relazione $R^{-1} \subseteq A_2\times A_1$ definita da $R^{-1}=\{(a_2,a_1) \mid (a_1,a_2)\in R\}$.
Nel caso in cui A_1, A_2 siano finiti, il grafo di incidenza di R^{-1} si ottiene da quello di R invertendo la direzione delle frecce e la matrice di incidenza di R^{-1} è la trasposta di quella di R.

La relazione $I_{A_1}=\{(a_1,a_1)|a_1\in A_1\}$ è detta relazione identica su A_1, osserviamo che si ha
$I_{A_1}\cdot R = R$ per ogni $R \subseteq A_1\times A_2$
ed analogamente considerata la relazione identica su A_2, $I_{A_2} = \{(a_2,a_2)|a_1\in A_2\}$, si ha
$R\cdot I_{A_2} = R$ per ogni $R \subseteq A_1\times A_2$.

In generale si ha però $R\cdot R^{-1} \neq I_{A_1}$ ed $R^{-1}\cdot R \neq I_{A_2}$.

Relazioni binarie su un insieme *A*

Consideriamo di seguito il caso particolare in cui gli insiemi A_1 e A_2 coincidono, ci occupiamo quindi delle relazioni $R \subseteq A_1\times A_1$, che chiamiamo relazioni binarie su A_1 (nel seguito elimineremo l'indice *1*).

Tra le relazioni binarie su A ci sono la relazione vuota, indicata con $\varnothing$, la relazione identica su A, indicata con I_A e la relazione $A\times A$, detta relazione universale su A ed indicata con ω_A.

Data una relazione binaria R su A, in virtù delle definizione di prodotto e della proprietà associative del prodotto, possiamo definire le potenze ad esponente positivo di R ponendo

$$R^m = R \cdot R \cdot \ldots \cdot R \qquad (m \text{ volte}).$$

Per convenzione poniamo anche $R^0 = I_A$.

Per la proprietà associativa del prodotto e per il fatto che $I_A \cdot R = R \cdot I_A = R$ per ogni $R \subseteq A \times A$, continuano a sussistere, per esponenti interi non negativi, le proprietà formali delle potenze:

- $R^m \cdot R^n = R^{m+n} = R^n \cdot R^m$,
- $(R^m)^n = R^{mn}$.

Poiché abbiamo parlato di relazione inversa potrebbe venir spontaneo definire R^m ($m<0$) come $R^m = R^{-1} \cdot R^{-1} \cdot \ldots \cdot R^{-1}$ ($-m$ volte), va notato che essendo in generale $R \cdot R^{-1} \neq I_A$ ed $R^{-1} \cdot R \neq I_A$, la proprietà $R^m \cdot R^n = R^n \cdot R^m = R^{m+n}$ non vale in generale per esponenti interi (cioè per esponenti anche negativi).

Esercizio: Cosa succede di tale proprietà se m ed n sono entrambi negativi? Cosa succede della seconda proprietà per m,n interi generici?

Le relazioni binarie su un insieme A finito, possono essere facilmente rappresentate col grafo e con la matrice di incidenza (che sarà una matrice quadrata). Nel grafo di incidenza l'insieme dei vertici è A ($= A \cup A$) e quindi tra gli archi ci possono essere degli autoanelli basati su un vertice a, per indicare che $(a,a) \in R$, e delle frecce bidirezionali fra due vertici a_1 e a_2 per indicare che entrambe le coppie (a_1,a_2) e (a_2,a_1) stanno in R.

Le relazioni binarie su un insieme A possono godere di interessanti proprietà; per le applicazioni successive, considereremo in particolare le seguenti:

- proprietà seriale
  Si dice che una relazione R gode della proprietà seriale (o semplicemente è seriale) se per ogni $a \in A$ esiste (almeno) un $a_1 \in A$ tale che $(a,a_1) \in R$.
  In termini di grafo di incidenza una relazione è seriale se e solo se da ogni vertice parte almeno un arco, in termini di matrice di incidenza una relazione è seriale se e solo se in ogni riga della matrice c'è almeno un 1.
  I_A e ω_A sono relazioni seriali.

- proprietà riflessiva
  Si dice che una relazione R gode della proprietà riflessiva (o semplicemente è riflessiva) se per ogni $a \in A$ si ha $(a,a) \in R$.
  Si può facilmente provare che una relazione è riflessiva se e solo se $I_A \subseteq R$.
  In termini di grafo di incidenza una relazione è riflessiva se e solo se da ogni vertice parte un autoanello, in termini di matrice di incidenza una relazione è riflessiva se e solo se la diagonale principale è tutta fatta di 1.
  I_A e ω_A sono relazioni riflessive.

- proprietà simmetrica
  Si dice che una relazione R gode della proprietà simmetrica (o semplicemente è simmetrica) se per ogni $a_1, a_2 \in A$, $(a_1,a_2) \in R$ implica $(a_2,a_1) \in R$.
  Si può facilmente provare che una relazione è simmetrica se e solo se $R^{-1} \subseteq R$.

In termini di grafo di incidenza una relazione è simmetrica se e solo se ogni arco ha la doppia freccia (notare che gli autoanelli possono sempre essere pensati come archi con doppia freccia), in termini di matrice di incidenza una relazione è simmetrica se e solo se la matrice d'incidenza coincide con la propria trasposta (ovvero è una matrice simmetrica).
$\varnothing$, I_A e ω_A sono relazioni simmetriche.

- proprietà antisimmetrica
  Si dice che una relazione R gode della proprietà antisimmetrica (o semplicemente è antisimmetrica) se per ogni $a_1,a_2 \in A$, $(a_1,a_2) \in R$ ed $(a_2,a_1) \in R$ implicano $a_1 = a_2$.
  Si può facilmente provare che una relazione è antisimmetrica se e solo se $R \cap R^{-1} \subseteq I_A$.
  In termini di grafo di incidenza una relazione è antisimmetrica se e solo se i soli archi con doppia freccia sono gli eventuali autoanelli, in termini di matrice di incidenza una relazione è antisimmetrica se e solo se la somma della matrice d'incidenza con la sua trasposta non ha alcun 2 fuori dalla diagonale principale, in altri termini se e solo se ogni volta che nel posto (i,k) con $i \neq k$ c'è 1, l'elemento di posto (k,i) è 0.
  $\varnothing$ ed I_A sono relazioni antisimmetriche.

- proprietà transitiva
  Si dice che una relazione R gode della proprietà transitiva (o semplicemente è transitiva) se per ogni $a_1,a_2,a_3 \in A$, $(a_1,a_2) \in R$ ed $(a_2,a_3) \in R$ implicano $(a_1,a_3) \in R$.
  Si può facilmente provare che una relazione è transitiva se e solo se $R^2 \subseteq R$.
  In termini di grafo di incidenza una relazione è transitiva se e solo se, ogni volta che si può andare da un vertice a_1 ad un vertice a_2 seguendo due frecce consecutive, c'è un arco che collega a_1 ad a_2; in termini di matrice di incidenza una relazione è transitiva se e solo se tutte le volte che sia l'elemento di posto (i,k) sia l'elemento di posto (k,j) sono 1 anche l'elemento di posto (i,j) è 1.
  $\varnothing$, I_A e ω_A sono relazioni transitive.

Siano R, T relazioni binarie su A, osserviamo che
- se R è seriale anche ogni relazione che contiene R (e quindi anche $R \cup T$) è seriale;
- se R e T sono seriali anche $R \cdot T$ è seriale;
- anche se R e T sono seriali, $R \cap T$ in generale non è seriale: basta prendere $A = \{a,b\}$, $R = \{(a,b),(b,b)\}$, $T = \{(a,a),(b,a)\}$;
- anche se R è seriale, R^{-1} in generale non è seriale: basta prendere $A = \{a,b\}$, $R = \{(a,b),(b,b)\}$;
- se R è riflessiva anche ogni relazione che contiene R (e quindi anche $R \cup T$) è riflessiva;
- se R è riflessiva anche R^{-1} è riflessiva;
- se R e T sono riflessive anche $R \cdot T$ è riflessiva;
- se R e T sono riflessive anche $R \cap T$ è riflessiva;
- se R è simmetrica, anche R^{-1} è simmetrica;
- se R e T sono simmetriche anche $R \cap T$ è simmetrica;
- se R e T sono simmetriche anche $R \cup T$ è simmetrica;
- anche se R e T sono simmetriche $R \cdot T$ in generale non è simmetrica: basta prendere $A = \{a,b,c\}$, $R = \{(a,b),(b,a)\}$, $T = \{(b,c),(c,b)\}$, R e T sono simmetriche ma $R \cdot T = \{(a,c)\}$ non è simmetrica;
- se R e T sono simmetriche, $R \cdot T$ è simmetrica se e solo se R e T sono permutabili;
- se R è antisimmetrica anche ogni relazione contenuta in R (e quindi anche $R \cap T$) è antisimmetrica;
- se R è antisimmetrica anche R^{-1} è antisimmetrica;
- anche se R e T sono antisimmetriche, $R \cup T$ in generale non è antisimmetrica: basta prendere $A = \{a,b\}$, $R = \{(a,b)\}$, $T = \{(b,a)\}$;

- anche se R e T sono antisimmetriche, $R \cdot T$ in generale non è antisimmetrica: basta prendere $A = \{a,b,c\}$, $R = \{(a,b),(c,b)\}$, $T = \{(b,a),(b,c)\}$, R e T sono antisimmetriche ma $R \cdot T = \{(a,a),(a,c),(c,a),(c,c)\}$ non è antisimmetrica;
- se R è transitiva anche R^{-1} è transitiva;
- se R e T sono transitive anche $R \cap T$ è transitiva;
- se R e T sono transitive $R \cup T$ in generale non è transitiva: basta prendere $A = \{a,b,c\}$, $R = \{(a,b)\}$, $T = \{(b,c)\}$;
- se R e T sono transitive $R \cdot T$ in generale non è transitiva: basta prendere $A = \{a,b,c,d\}$, $R = \{(a,b),(c,d)\}$, $T = \{(b,c),(d,d)\}$, R e T sono transitive ma $R \cdot T = \{(a,c),(c,d)\}$ non è transitiva;
- se R e T sono transitive e permutabili anche $R \cdot T$ è transitiva.

Riassumendo, per quanto riguarda le inclusioni le proprietà si conservano in accordo alla seguente tabella, se $T \subset R \subset S$

T	R	S
no	seriale	sì
no	riflessiva	sì
no	simmetrica	no
sì	antisimmetrica	no
no	transitiva	no

Per quanto riguarda le operazioni di intersezione, unione, prodotto, passaggio alla relazione inversa le proprietà si conservano in accordo alla seguente tabella

R	T	$R \cap T$	$R \cup T$	$R \cdot T$	R^{-1}
seriale	seriale	no	sì	sì	no
riflessiva	riflessiva	sì	sì	sì	sì
simmetrica	simmetrica	sì	sì	no	sì
antisimmetrica	antisimmetrica	sì	no	no	sì
transitiva	transitiva	sì	no	no	sì

Consideriamo ora un insieme P di proprietà di cui le relazioni binarie possono godere.
Sia $R \subseteq A \times A$ una relazione binaria su A, chiamiamo chiusura di R rispetto a P o P-chiusura di R una relazione $T \subseteq A \times A$ tale che:

1) $R \subseteq T$;
2) T gode di tutte le proprietà in P;
3) se $S \subseteq A \times A$ è una relazione che gode di tutte le proprietà in P e contiene R, allora contiene anche T.

In altre parole la P-chiusura di R, se esiste, è la minima relazione che contiene R e ha tutte le proprietà in P.

La P-chiusura di R se esiste è unica.
Supponiamo infatti che T ed S siano due P-chiusure di R; dovendo soddisfare la 1) e la 2) entrambe contengono R e godono di tutte le proprietà in P, ma allora per la 3) si ha $T \subseteq S$ ed $S \subseteq T$, cioè $T = S$.

La P-chiusura di R può coincidere con R? E se sì, quando? (esercizio)

Osserviamo che se

- esiste almeno una relazione che gode di tutte le proprietà in P e che contiene R e
- l'intersezione di relazioni che godono di tutte le proprietà in P gode ancora di tutte quelle proprietà,

possiamo garantire che esiste la P-chiusura di R.
Infatti l'insieme X delle relazioni che contengono R e godono delle proprietà in P non è vuoto , l'intersezione T di tutte le relazioni appartenenti ad X è una relazione che contiene ancora R ed ha tutte le proprietà in P. Inoltre T, per come è costruita, è contenuta in tutte le relazioni che contengono R e godono delle proprietà in P (che sono elementi di X).

Possiamo allora concludere che *esistono la chiusura riflessiva, la chiusura simmetrica e la chiusura transitiva di una qualsiasi relazione* R.

In generale invece *non esiste la chiusura seriale* di una relazione R, basta considerare $A = \{a,b\}$, $R=\{(a,b)\}$, per trovare una relazione seriale che contenga R dobbiamo aggiungere ad R una coppia il cui primo elemento sia b, quindi (b,a) o (b,b). Nel primo caso otteniamo $T = \{(a,b),(b,a)\}$, nel secondo $S = \{(a,b),(b,b)\}$. Le relazioni T e S sono entrambe seriali e contengono entrambe R ma né $T \subseteq S$ nè $S \subseteq T$.

In generale *non esiste* neppure *la chiusura antisimmetrica* di una relazione R, infatti se R non è antisimmetrica, nessuna relazione che contenga R può essere antisimmetrica.

Vogliamo ora dare un metodo per costruire la chiusura riflessiva, la chiusura simmetrica e la chiusura transitiva di R:

- la chiusura riflessiva di R è la relazione $R \cup I_A$;
- la chiusura simmetrica di R è la relazione $R \cup R^{-1}$;
- la chiusura transitiva di R è la relazione $\bigcup_{n>0} R^n$ (ovviamente n è un intero)

Verifichiamo come esempio l'ultima di queste affermazioni (le altre sono quasi ovvie).

Dobbiamo provare che la relazione $T = \bigcup_{n>0} R^n$

1) contiene R e questo è immediato;
2) è transitiva, infatti se $(a_1,a_2) \in T$ ed $(a_2,a_3) \in T$ esistono due interi $m,n>0$ tali che $(a_1,a_2) \in R^n$ ed $(a_2,a_3) \in R^m$ e dunque $(a_1,a_3) \in R^{n+m} \subseteq T$.
3) è contenuta in ogni relazione transitiva che contenga R; infatti sia S una relazione transitiva che contenga R, si ha $R^2 \subseteq S^2$ perché il prodotto di relazioni è compatibile con l'inclusione, inoltre $S^2 \subseteq S$ per la transitività di S, dunque $R^2 \subseteq S$. Di nuovo per la compatibilità del prodotto con l'inclusione e per la transitività di S si ha $R^3 \subseteq S^2 \subseteq S$ e ripetendo lo stesso ragionamento (formalizzare bene con l'induzione per esercizio) si ottiene $R^n \subseteq S$ per ogni $n > 0$ e dunque $T \subseteq S$.

Notare bene che in genere non basta fare $R \cup R^2$ per trovare la chiusura transitiva di R, a tal proposito basta considerare $A = \{a,b,c,d\}$, $R = \{(a,b),(b,c),(c,d)\}$. Risulta $R^2 = \{(a,c),(b,d)\}$, quindi $R \cup R^2 = \{(a,b),(b,c),(c,d),(a,c),(b,d)\}$ non è transitiva. Per avere una relazione transitiva bisogna aggiungere ad R la coppia (a,d) che appartiene ad R^3. In questo caso quindi la chiusura transitiva di R è $R \cup R^2 \cup R^3$ (le potenze successive di R sono infatti vuote).

In generale il procedimento di unire nuove potenze di R finisce quando non si introducono più nuovi 1.

Cosa succede se consideriamo P come costituito da almeno due proprietà?
Le stesse considerazioni fatte per provare che in genere non esiste la chiusura antisimmetrica di una relazione si possono usare anche quando P non è costituito da una sola proprietà ma contiene la proprietà antisimmetrica. Analogamente le considerazioni sulla non esistenza della chiusura seriale, si possono usare quando P contiene la proprietà seriale (a meno che non capiti che la presenza di altre proprietà porti la serialità ad essere riflessività come accade quando si considera l'insieme delle proprietà seriale, riflessiva e transitiva).

Escludendo queste due proprietà, consideriamo:
- P = {riflessività, simmetria }
- P = {riflessività, transitività}
- P = {simmetria, transitività}
- P = {simmetria, riflessività, transitività}

Per tutti questi P esistono le P-chiusure di una relazione $R \subseteq A \times A$ perché ω_A gode delle proprietà P e contiene R, l'intersezione di relazioni che hanno le proprietà di P è una relazione che gode delle proprietà P e come già visto questo basta a garantire l'esistenza della P-chiusura di R.

Vediamo allora di costruire queste P chiusure:

- la chiusura riflessiva e simmetrica di R è la relazione $R \cup I_A \cup R^{-1}$;
- la chiusura riflessiva e transitiva di R è la relazione $\bigcup_{n\geq 0} R^n$;
- la chiusura simmetrica e transitiva di R è la relazione $\bigcup_{n>0} \left(R \cup R^{-1}\right)^n$;
- la chiusura riflessiva, simmetrica e transitiva di R è la relazione $\bigcup_{n>0} \left(R \cup I_A \cup R^{-1}\right)^n$;

Verifichiamo come esempio l'ultima di queste affermazioni (le altre si provano con tecniche del tutto analoghe).

Dobbiamo provare che la relazione $T = \bigcup_{n>0} \left(R \cup I_A \cup R^{-1}\right)^n$

1) contiene R e questo è immediato perché $R \subseteq R \cup I_A \cup R^{-1} \subseteq T$,
2) è riflessiva e questo segue immediatamente da $I_A \subseteq R \cup I_A \cup R^{-1} \subseteq T$;
   è simmetrica e questo segue dal fatto che $R \cup I_A \cup R^{-1}$ è simmetrica ed anche tutte le sue potenze ad esponenti positivi sono simmetriche (prodotto di relazioni simmetriche fra loro permutabili) e quindi T è simmetrica perché unione di relazioni simmetriche;
   è transitiva, infatti se $(a_1,a_2) \in T$ ed $(a_2,a_3) \in T$ allora esistono due interi $m, n > 0$ tali che $(a_1,a_2) \in (R \cup I_A \cup R^{-1})^n$ ed $(a_2,a_3) \in (R \cup I_A \cup R^{-1})^m$ e dunque $(a_1,a_3) \in (R \cup I_A \cup R^{-1})^{n+m} \subseteq T$.
3) è contenuta in ogni relazione riflessiva, simmetrica, transitiva che contenga R; infatti sia S una relazione riflessiva, simmetrica, transitiva che contenga R, per la riflessività S contiene anche I_A ed essendo simmetrica se contiene R deve anche contenere R^{-1}, pertanto $R \cup I_A \cup R^{-1} \subseteq S$. Inoltre S in quanto contiene $R \cup I_A \cup R^{-1}$ ed è transitiva deve anche contenere la chiusura transitiva di $R \cup I_A \cup R^{-1}$ che è proprio T.

Esempio: Dati $A = \{a,b,c,d\}$ ed $R = \{(a,a),(a,b),(b,d),(c,d)\}$ costruire la chiusura transitiva di R.
Risulta $R^2 = \{(a,a),(a,b),(a,d)\}$ ed $R^3 = R^2 = \{(a,a),(a,b),(a,d)\}$, quindi la chiusura transitiva di R è la relazione $\{(a,a),(a,b),(b,d),(c,d),(a,d)\}$ (le potenze di esponente maggiore di 2 non possono infatti aggiungere nuove coppie in questo caso).
Il tutto poteva facilmente essere ottenuto con considerazioni sulla matrice di incidenza di R.

Si ha $M_R=\begin{bmatrix}1&1&0&0\\0&0&0&1\\0&0&0&1\\0&0&0&0\end{bmatrix}$ e quindi $M_{R^2}=(M_R)^2=\begin{bmatrix}1&1&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix}$ da cui $M_{R\cup R^2}=\begin{bmatrix}1&1&0&1\\0&0&0&1\\0&0&0&1\\0&0&0&0\end{bmatrix}$, ora poiché

$M_{R^3}=(M_R)^3=\begin{bmatrix}1&1&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix}$ si ottiene $M_{R\cup R^2\cup R^3}=M_{R\cup R^2}=M_{R\cup R^2\cup R^3\cup R^4\cup\ldots}$.

Calcoliamo la chiusura simmetrica e transitiva di R. Si ha
$R\cup R^{-1}=\{(a,a),(a,b),(b,d),(c,d),(b,a),(d,b),(d,c)\}$,
da cui
$(R\cup R^{-1})^2=\{(a,a),(a,b),(a,d),(b,b),(b,c),(c,b),(c,c)\}$ e
$(R\cup R^{-1})^3=\{(a,a),(a,b),(a,d),(a,c),(b,b),(b,c),(c,b),(c,c)\}$.

Osservando il modo in cui queste chiusure si presentano, la prima è la chiusura riflessiva della chiusura simmetrica di R, la seconda è la chiusura riflessiva della chiusura transitiva di R, tuttavia avremmo ottenuto lo stesso risultato se avessimo fatto rispettivamente la chiusura simmetrica della chiusura riflessiva e la chiusura transitiva della chiusura riflessiva.
La chiusura simmetrica e transitiva di R è la chiusura transitiva della chiusura simmetrica di R, in questo caso va notato che facendo la chiusura simmetrica della chiusura transitiva di R, calcolando cioè $\bigcup_{n>0}R^n\cup\left(\bigcup_{n>0}R^n\right)^{-1}$, non avremmo in generale ottenuto la relazione cercata, infatti la relazione $\bigcup_{n>0}R^n\cup\left(\bigcup_{n>0}R^n\right)^{-1}$ può non essere transitiva (ricordarsi che l'unione di relazioni transitive non è necessariamente transitiva).
A tal scopo basta considerare $A=\{a,b,c\}$, $R=\{(a,b),(b,c)\}$; risulta $\bigcup_{n>0}R^n=\{(a,b),(b,c),(a,c)\}$ e dunque $\bigcup_{n>0}R^n\cup\left(\bigcup_{n>0}R^n\right)^{-1}=\{(a,b),(b,c),(a,c),(b,a),(c,b),(c,a)\}$ che non è transitiva.
Analogamente la chiusura riflessiva, simmetrica e transitiva di R è la chiusura transitiva della chiusura riflessiva e simmetrica di R, se avessimo fatto la chiusura simmetrica della chiusura riflessiva e transitiva di R in generale non avremmo trovato il risultato voluto (avremmo potuto perdere la transitività).

Esercizio: Facendo la chiusura riflessiva della chiusura simmetrica e transitiva di R, otteniamo la chiusura riflessiva, simmetrica e transitiva di R?

Relazioni di equivalenza

Una relazione binaria R su A che goda delle proprietà riflessiva, simmetrica e transitiva si chiama relazione di equivalenza su A.

Esempi

- La relazione di uguaglianza sull'insieme N dei numeri naturali è una delle prime relazioni di equivalenza che si incontrano;
- La relazione di similitudine tra i triangoli di un piano è una relazione di equivalenza ben nota;

- Siano Z l'insieme degli interi relativi ed n un intero maggiore di 1 fissato. La relazione $R \subseteq Z \times Z$ definita ponendo $(r,s) \in R$ se e solo se n divide $r - s$ (nel seguito scriveremo $r \equiv s \pmod{n}$ per indicare che $(r,s) \in R$ e scriveremo $n \mid m$ per dire che n divide m, cioè che esiste k appartenente ad N tale che m = k n) è una relazione di equivalenza, detta <u>*relazione di congruenza*</u> modulo n.
  Infatti per ogni $r \in Z$ si ha $r \equiv r \pmod{n}$ perché $n \mid 0 = r - r$, quindi la relazione è riflessiva;
  se $r \equiv s \pmod{n}$, cioè se $n \mid r - s$, questo significa che esiste un $h \in Z$ tale che $r - s = h \cdot n$ e quindi $s - r = (-h) \cdot n$, cioè $n \mid s - r$ da cui $s \equiv r \pmod{n}$, quindi la relazione è simmetrica;
  se $r \equiv s \pmod{n}$ e $s \equiv t \pmod{n}$, cioè se n divide $r - s$ ed n *divide* $s - t$, allora esistono $h, k \in Z$ tali che $r - s = h \cdot n$ e $s - t = k \cdot n$. Sommando membro a membro queste due uguaglianze si ottiene $r - t = (h + k)\, n$, ovvero $n \mid r - t$ da cui $r \equiv t \pmod{n}$, quindi la relazione è transitiva.
- Ricordiamo che due matrici A, B quadrate di ordine n (a coefficienti reali) si dicono simili se esiste una matrice P (quadrata di ordine n e non singolare) tale che $A = P^{-1}BP$ (riguardare gli appunti di Geometria ed Algebra Lineare). La relazione di similitudine è una relazione di equivalenza nell'insieme delle matrici quadrate di ordine n (a coefficienti reali). Verifichiamo che la relazione di similitudine gode della proprietà riflessiva, dobbiamo cioè trovare per ogni matrice A quadrata di ordine n una matrice P tale che $A = P^{-1}AP$ (facile in quanto $P = I_n$, matrice identica di ordine n). Verifichiamo che la relazione di similitudine gode della proprietà simmetrica, dobbiamo cioè provare che se A è simile a B, cioè se esiste una matrice P tale che $A = P^{-1}BP$, allora B è simile ad A, cioè esiste una matrice Q tale che $B = Q^{-1}AQ$. Per far ciò, moltiplichiamo primo e secondo membro di $A = P^{-1}BP$ entrambi per P e P^{-1}, otteniamo $PAP^{-1} = P(P^{-1}BP)P^{-1} = (PP^{-1})B(PP^{-1}) = B$, da cui, ricordando che $P = (P^{-1})^{-1}$, abbiamo anche $B = (P^{-1})^{-1}AP^{-1}$ e quindi ricaviamo che B è simile ad A (basta prendere $Q = P^{-1}$). Verifichiamo infine che la relazione di similitudine gode della proprietà transitiva, dobbiamo cioè provare che se A è simile a B e B è simile a C, cioè se esistono due matrici P e Q tali che $A = P^{-1}BP$ e $B = Q^{-1}CQ$, allora A è simile a C, cioè esiste una matrice D tale che $A = D^{-1}CD$. Per far ciò, sostituiamo in $A = P^{-1}BP$ al posto della matrice B la matrice $Q^{-1}CQ$, otteniamo allora $A = P^{-1}(Q^{-1}CQ)P = (P^{-1}Q^{-1})C(QP) = B$, da cui ricordando che $(P^{-1}Q^{-1}) = (QP)^{-1}$ abbiamo che $A = (QP)^{-1}C(QP)$ è simile a C (porre $D = QP$).
- Nell'insieme di tutti gli uomini la relazione che associa due uomini se e solo se essi sono nati nello stesso anno è una relazione di equivalenza.

Osserviamo che la chiusura riflessiva, simmetrica e transitiva di una relazione R è una relazione d'equivalenza ed è la minima relazione di equivalenza che contiene R, tale relazione viene anche chiamata chiusura di equivalenza di R o più comunemente *relazione d'equivalenza generata da* R.

Nel seguito denoteremo le relazioni di equivalenza con le lettere minuscole dell'alfabeto greco.

<u>Esercizi</u>

L'intersezione di relazioni di equivalenza è una relazione d'equivalenza?

L'unione di relazioni di equivalenza è una relazione d'equivalenza?

Il prodotto di relazioni di equivalenza è una relazione d'equivalenza?

La relazione inversa di una relazione di equivalenza è una relazione d'equivalenza?

Giustificare brevemente le risposte positive e fornire un controesempio nel caso di risposta negativa.

Data una relazione di equivalenza ρ su un insieme A, per ogni $a \in A$, chiamiamo classe di equivalenza (rispetto a ρ) avente come rappresentante a, o più semplicemente ρ-classe di a, l'insieme $\rho_a = \{x \in A | (a,x) \in \rho\}$ (denotata anche con $[a]_\rho$).

Esempi

- Si consideri l'insieme N e sia ρ la relazione d'uguaglianza su N; la ρ-classe di un intero naturale n è costituita dal solo elemento n.
- Si consideri l'insieme di tutti i triangoli del piano e sia ρ la relazione di similitudine fra triangoli. Riferito il piano ad un sistema di coordinate cartesiane, sia T il triangolo avente vertici $O = (0,0)$, $A = (1,0)$, $B = (0,1)$; la ρ-classe di T è l'insieme di tutti i triangoli isosceli e rettangoli.
- Sull'insieme Z sia ρ la relazione di congruenza modulo 2, la ρ-classe di 0 è l'insieme di tutti gli interi pari, la ρ-classe di 1 è l'insieme di tutti gli interi dispari. Cosa è la ρ-classe di 4?
- Sull'insieme delle matrici reali quadrate di ordine 2, sia ρ la relazione di similitudine fra matrici. Sia $A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$. La ρ-classe di A è l'insieme delle matrici cui A è simile, cioè è l'insieme delle matrici B tali che $A = P^{-1}BP$ per qualche matrice non singolare P, cioè anche l'insieme delle matrici simili ad A, (come appreso dal corso di Geometria ed Algebra lineare, una matrice si dice diagonalizzabile se è simile ad una matrice diagonale, una matrice con tutti gli autovalori distinti è sempre diagonalizzabile e matrici simili hanno gli stessi autovalori) quindi la ρ-classe di A è l'insieme di tutte e sole le matrici che hanno come autovalori 1 e 2 (infatti ogni matrice simile ad A ha gli stessi autovalori di A, cioè 1 e 2, viceversa ogni matrice che abbia come autovalori 1 e 2 è diagonalizzabile e quindi simile ad una matrice diagonale che abbia sulla diagonale 1 e 2). Come sono fatte le ρ-classi della matrice identica e della matrice nulla?
- Sull'insieme di tutti gli uomini si consideri la relazione ρ che associa due uomini se e solo se sono nati nello stesso anno. La ρ-classe del prof. Giacconi (Nobel per la fisica nel 2004) è l'insieme formato da tutti gli uomini nati nel 1931.

Si dice partizione di A un insieme $\{B_i \mid i \in I\}$ di sottoinsiemi di A tale che sia $\bigcup_{i \in I} B_i = A$ e $B_i \cap B_j \neq \varnothing$ implichi $B_i = B_j$.

Esempi

- La suddivisione di Z nei due sottoinsiemi degli interi pari e degli interi dispari è una partizione di Z.
- La suddivisione di tutti gli uomini nei sottoinsiemi di coloro che sono coetanei (nati nello stesso anno) è una partizione dell'insieme degli uomini.

Osserviamo che data una relazione d'equivalenza ρ su un insieme A, le ρ-classi di A sono una partizione di A. Tale partizione si dice *partizione indotta* da ρ.

Infatti ogni $a \in A$ appartiene a ρ_a (per la proprietà riflessiva di ρ) quindi $\bigcup_{a \in A} \rho_a = A$. Inoltre se esiste $c \in \rho_a \cap \rho_b$ abbiamo $\rho_a = \rho_b$, infatti $c \in \rho_a \cap \rho_b$ implica $(a,c) \in \rho$ e $(b,c) \in \rho$, quindi, per la simmetria di ρ, $(c,b) \in \rho$ e, per la transitività di ρ, $(a,b) \in \rho$ e di nuovo per simmetria, $(b,a) \in \rho$. Sia ora $x \in \rho_a$ cioè $(a,x) \in \rho$, per transitività (essendo $(b,a) \in \rho$), si ottiene $(b,x) \in \rho$ cioè $x \in \rho_a$ quindi $\rho_a \subseteq \rho_b$. Analogamente si ottiene $\rho_b \subseteq \rho_a$ e quindi $\rho_a = \rho_b$.

Viceversa data una partizione di A è sempre possibile definire una relazione d'equivalenza ρ che induca su A la partizione data.

Si definisce ρ ponendo $(a,b) \in \rho$ se e solo se a,b stanno nello stesso elemento della partizione, il resto è quasi ovvio.

L'insieme delle ρ-classi di A si dice insieme quoziente di A rispetto a ρ e si indica con A/ρ. Dunque $A/\rho = \{\rho_a \mid a \in A\}$.

Esempi

- Determinare l'insieme quoziente di Z rispetto alla relazione di congruenza modulo 3. Osserviamo che la classe che contiene 0 è formata da tutti e soli gli interi m tali che $3 \mid m - 0$, cioè da tutti e soli i multipli di 3. Tale classe coincide con la classe che ha per rappresentante 3 (in quanto 3 appartiene sia alla classe che ha per rappresentante 0 sia alla classe che ha come rappresentante 3 e due classi che hanno un elemento comune coincidono); lo stesso argomento si può usare per provare che la classe che ha come rappresentante 0 coincide con ogni classe che abbia per rappresentante un intero della forma $3h$ con h intero relativo. La classe che contiene 1 è formata da tutti e soli gli interi m tali che $3 \mid m - 1$, cioè da tutti e soli i numeri della forma $3h+1$ con h intero relativo; la classe di 2 è formata da tutti e soli gli interi m tali che $3 \mid m - 2$, cioè da tutti e soli i numeri della forma $3h+2$ con h intero relativo. Queste 3 classi sono una partizione di Z e pertanto sono le sole classi distinte di Z rispetto alla relazione di congruenza modulo 3 e sono pertanto i 3 elementi dell'insieme quoziente di Z rispetto alla relazione di congruenza modulo 3; tale insieme viene di solito indicato con Z_3 e i suoi elementi vengono chiamati classi di resto modulo 3 e denotati con $\{0\},\{1\},\{2\}$ (si osservi che i possibili resti della divisione di un intero per 3 sono 0,1,2 e che un intero m sta nella classe $\{i\}$ se e solo se dividendo m per 3 si ottiene come resto i) Notiamo che l'insieme quoziente di Z rispetto alla relazione di congruenza modulo n viene di solito indicato con Z_n e i suoi elementi vengono chiamati *classi di resto modulo n*; con considerazioni analoghe alle precedenti si prova che ci sono n classi distinte $\{0\},\{1\},\{2\},...,\{n - 1\}$, dove la generica classe $\{r\}$ è formata dagli interi della forma $nh+r$.
- Siano $A = \{a,b,c,d,e\}$ ed $R = \{(a,b),(a,d),(c,e)\}$. Determinare la relazione d'equivalenza ρ generata da R e l'insieme A/ρ. Dobbiamo costruire la chiusura transitiva della chiusura riflessiva e simmetrica T di R, quindi $T = \{(a,b),(a,d),(c,e),(a,a),(b,b),(c,c),(d,d),(e,e),(b,a),(d,a),(e,c)\}$. Risulta $T^2 = \{(a,b),(a,d),(c,e),(a,a),(b,b),(c,c),(d,d),(e,e),(b,a),(d,a),(e,c),(b,d),(d,b)\}$ (aiutarsi col grafo o con la matrice di incidenza) e $T^2 = T^3$, quindi $\rho = T \cup T^2 = T^2$. Quindi si ha $\rho_a = \{a,b,d\}$ in quanto (a,a), (a,b), $(a,d) \in \rho$ mentre (a,c), $(a,e) \notin \rho$. Ovviamente $\rho_a = \rho_b = \rho_d$. Si ha poi $\rho_c = \{c,e\}$ in quanto $(c,e) \in \rho$. Dunque $A/\rho = \{\rho_a, \rho_c\}$.
- Determinare la relazione d'equivalenza ρ su Z che induce su Z la partizione nei due sottoinsiemi degli interi pari e degli interi dispari. Due interi sono associati in ρ se e solo se sono entrambi pari o entrambi dispari, cioè se e solo se la loro differenza è divisibile per 2. La relazione ρ è dunque la congruenza modulo 2.
- Determinare la relazione d'equivalenza ρ su $A = \{a,b,c,d,e\}$ che induce su A la partizione $\{\{a\},\{b,d,e\},\{c\}\}$.Ovviamente $\rho = \{(a,a),(b,b),(b,d),(b,e),(d,b),(d,d),(d,e),(e,b),(e,d),(e,e),(c,c)\}$. Si suggerisce di costruire sia il grafo sia la matrice di incidenza di ρ.

Relazioni d'ordine

Una relazione binaria R su A che goda delle proprietà riflessiva, antisimmetrica e transitiva si chiama relazione d'ordine su A. Inoltre, se per ogni coppia di elementi a, b di A si ha o $(a,b) \in R$ o $(b,a) \in R$, R si dice relazione d'ordine totale. Se invece esistono due elementi in A tali che né $(a,b) \in R$ né $(b,a) \in R$, tali elementi si dicono non confrontabili rispetto ad R.

Un insieme su cui sia data una relazione d'ordine si chiama insieme parzialmente ordinato o poset (da **p**artially **o**rdered **set**). Nel caso in cui la relazione sia totale e si voglia evidenziare questo fatto si parla di insieme totalmente ordinato.

Esempi.

- La usuale relazione $\leq$ è una relazione d'ordine totale su tutti gli insiemi numerici N, Z, Q, R.
- Considerato l'insieme delle parti di un insieme A, denotato con $\mathcal{P}(A)$, la relazione di inclusione debole $\subseteq$ è una relazione d'ordine su $\mathcal{P}(A)$ e non è totale, se A contiene almeno due elementi.
- La relazione di divisibilità "|" è una relazione d'ordine su N e non è totale.
- La relazione di divisibilità non è una relazione d'ordine sull'insieme dei numeri interi Z (esercizio).

Osserviamo che la proprietà riflessiva può sembrare una richiesta un po' forte in quanto richiedendo questa proprietà non sono chiamate relazioni d'ordine la usuale relazione $<$ in N (e in Z, Q, R, C) e l'inclusione forte $\subset$ di insiemi in $\mathcal{P}(A)$.
Alcuni testi quindi non richiedono la riflessività, ma in tal caso risulta essere una relazione d'ordine la relazione quella vuota $\varnothing$ rispetto alla quale però tutte le coppie di elementi sarebbero formate da elementi non confrontabili.
In genere nei testi di matematica è richiesta la proprietà riflessiva ed in quelli di informatica no.

Se R è una relazione d'ordine su A si usa per convenzione scrivere $a \leq b$ o $b \geq a$ per dire che $(a,b) \in R$.

Esercizi

L'intersezione di relazioni d'ordine è una relazione d'ordine?

L'unione di relazioni d'ordine è una relazione d'ordine?

Il prodotto di relazioni d'ordine è una relazione d'ordine?

La relazione inversa di una relazione d'ordine è una relazione d'ordine?

Giustificare brevemente le risposte positive e fornire un controesempio nel caso di risposta negativa.

Osserviamo che data una relazione R non esiste in genere una relazione d'ordine che contenga R perché se R non è antisimmetrica tutte le relazioni che contengono R non sono antisimmetriche.
Ci si potrebbe allora chiedere se una relazione antisimmetrica R possa sempre essere contenuta in una relazione d'ordine. Poiché una relazione d'ordine è riflessiva e transitiva, se esistesse una relazione d'ordine contenente R, questa conterrebbe la chiusura riflessiva e transitiva di R. Se tale chiusura non risulta antisimmetrica, allora non esiste una relazione d'ordine che contiene R. Se invece è antisimmetrica è anche una relazione d'ordine e quindi abbiamo trovato una relazione d'ordine che contiene R (che è tra l'altro la minima relazione d'ordine che contiene R).

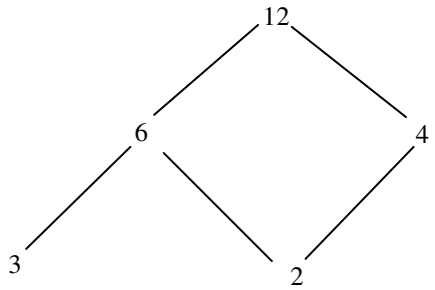
Quando si lavora con relazioni d'ordine $\leq$ su un insieme finito A, si utilizza spesso una versione semplificata del grafo di incidenza di $\leq$, detto diagramma di Hasse.
Questo diagramma si ottiene dal grafo di incidenza usando alcune convenzioni:

- non si rappresentano gli autoanelli (perché su ogni vertice ce n'è uno);
- non si mette la freccia sugli archi (perché ogni arco ha una sola freccia), ma si assume che ogni arco vada dal vertice che sta più in basso a quello che sta più in alto nel disegno;

- se c'è un arco che va dal vertice a al vertice b ed uno che va dal vertice b al vertice c, si evita di disegnare l'arco (sicuramente presente nel grafo per la transitività della relazione) che va dal vertice a al vertice c.

Esempio

Sia $A=\{2,3,4,6,12\}$ e si consideri su A la relazione definita ponendo $a \leq b$ sse a divide b.
Abbiamo $2\leq 2$, $2\leq 4$, $2\leq 6$, $2\leq 12$, $3\leq 3$, $3\leq 6$, $3\leq 12$, $4\leq 4$, $4\leq 12$, $6\leq 6$, $6\leq 12$, $12\leq 12$ mentre tutte le altre coppie di elementi di A sono formate da elementi non confrontabili.
Il diagramma di Hasse è allora



Disegnare il grafo di incidenza e vedere quanto è più complesso.

Si consideri ora un insieme parzialmente ordinato A (e indichiamo con $\leq$ la sua relazione d'ordine).

Diciamo minimo di A (se esiste) un $m \in A$ tale che per ogni $a \in A$ sia $m \leq a$.

Diciamo massimo di A (se esiste) un $m \in A$ tale che per ogni $a \in A$ sia $a \leq m$.

Diciamo elemento minimale di A (se esiste) un $m \in A$ tale che $a \in A$ ed $a \leq m$ implichino $a = m$ (in altre parole per ogni $a \in A$ si ha o a non confrontabile con m o $m \leq a$).

Diciamo elemento massimale di A (se esiste) un $m \in A$ tale che $a \in A$ ed $m \leq a$ implichino $a = m$ (in altre parole per ogni $a \in A$ si ha o a non confrontabile con m o $a \leq m$).

L'insieme parzialmente ordinato di cui abbiamo sopra disegnato il diagramma di Hasse ha 12 come massimo e 2, 3 come elementi minimali.

Osserviamo che:

- il minimo (massimo) se esiste è unico:
- se un insieme parzialmente ordinato è finito ed ha un unico elemento minimale (massimale) questo è un minimo (massimo).

Sia ora B un sottoinsieme dell'insieme parzialmente ordinato A.

Diciamo minorante di B (se esiste) un elemento $m \in A$ tale che per ogni $b \in B$ sia $m \leq b$.

Diciamo maggiorante di B (se esiste) un elemento $m \in A$ tale che per ogni $b \in B$ sia $b \leq m$.

Chiamiamo estremo inferiore di B e lo indichiamo con inf B il massimo, se esiste, dei minoranti di B (N.B. sempre rispetto alla relazione definita in A!)

Chiamiamo estremo superiore di B e lo indichiamo con sup B il minimo, se esiste, dei maggioranti di B (N.B. sempre rispetto alla relazione definita in A!)

Se consideriamo il sottoinsieme $B=\{2,3\}$ dell'insieme A dell'esempio precedente non esistono minoranti di B e quindi neppure inf B; 6,12 sono maggioranti di B e si ha sup $B=6$.

Osserviamo che:

- se B ha un minimo questo è un minorante di B ed è inf B;
- se B ha un massimo questo è un maggiorante di B ed è sup B;
- se un minorante di B appartiene a B, allora è il minimo di B ed è inf B;
- se un maggiorante di B appartiene a B, allora è il massimo di B ed è sup B.

Un insieme parzialmente ordinato tale che per ogni sua coppia di elementi a, b esistano inf $\{a,b\}$ e sup $\{a,b\}$ si dice reticolo.

Esempio

L'insieme dell'esempio precedente non è un reticolo, non esiste infatti inf $\{2,3\}$.

L'insieme $B=\{2,4,6,12\}$ rispetto alla relazione d'ordine definita ponendo $a \leq b$ sse a divide b è un reticolo (trovare inf e sup di ogni coppia di suoi elementi).

Funzioni

Una relazione $f \subseteq A \times B$ tale che

(*) per ogni $a \in A$ esiste uno ed un solo $b \in B$ tale che $(a,b) \in f$

si dice *funzione (o applicazione)* da A a B.

In tal caso si usa la più comune notazione $f : A \to B$ e l'unico elemento b associato ad a dalla relazione f viene indicato con $f(a)$ e chiamato *immagine* di a mediante f, l'elemento a viene invece detto *controimmagine* di b.
Si utilizzano anche le notazioni $f(A)$ per indicare l'insieme $\{f(a) |\ a \in A\}$ ed $f^{-1}(b)$ per indicare l'insieme $\{a \in A | f(a) = b\}$.

Se A e B sono insiemi finiti e si considera la rappresentazione di f tramite il suo grafo di incidenza, f è una funzione se e solo se c'è uno e un solo arco uscente da ogni vertice che rappresenta un elemento di A, se invece si rappresenta f tramite la matrice di incidenza f è una funzione se e solo se nella matrice di incidenza di f c'è uno ed un solo 1 su ogni riga.

Siano ora $f : A \to B$ e $g : B \to C$ due funzioni, è facile provare che il prodotto di f per g, pensate come relazioni, è una funzione $f \cdot g : A \to C$ definita da $f \cdot g\ (a) = g(f(a))$ per ogni $a \in A$.
Infatti sappiamo che $f \cdot g$ è seriale (essendo sia f sia g seriali) e quindi per ogni $a \in A$ esiste almeno un $c \in C$ tale che $(a,c) \in f \cdot g$. Supponiamo ora $(a,c) \in f \cdot g$ e proviamo che $c = g(f(a))$, da $(a,c) \in f \cdot g$ per definizione di prodotto esiste un b tale che $(a,b) \in f$ e $(b,c) \in g$ ma poiché f è una funzione l'elemento $b \in B$ tale che $(a,b) \in f$ è unico ed è $b = f(a)$ da cui $(f(a),c) \in g$ ma poiché g è una funzione anche c è unico e risulta $c = g(f(a))$.

La funzione $f \cdot g$ appena definita viene detta *prodotto* delle due funzioni f e g.

Il prodotto di funzioni è ovviamente associativo (essendo un prodotto di relazioni), in generale non è commutativo.

Osserviamo inoltre che la relazione identica su A, I_A, è una funzione da A ad A, che in questo contesto viene spesso indicata con $\imath_A$; si ha ovviamente che $\imath_A \cdot f = f = f \cdot \imath_B$.
Osserviamo invece che la relazione inversa f^{-1} di una funzione f non è in generale una funzione.

E' naturale la domanda: quando la relazione inversa f^{-1} di una funzione f è una funzione?

A tal scopo introduciamo le seguenti definizioni:

- Una funzione f è *iniettiva*
  se ogni $b \in B$ ha al più una controimmagine in A, o equivalentemente
  se $f(a_1) = f(a_2)$ implica $a_1 = a_2$, o equivalentemente
  se $a_1 \neq a_2$ implica $f(a_1) \neq f(a_2)$.

  Naturalmente per verificare che una relazione f è una funzione iniettiva si deve anche verificare la condizione (*).

  Rappresentando la relazione f tramite la sua matrice di incidenza (se possibile) si ha che f è una funzione iniettiva se e solo se su ogni riga della matrice c'è uno ed un solo 1 e su ogni colonna al più un 1.
  Rappresentando la relazione f tramite il suo grafo di incidenza (se possibile) si ha che f è una funzione iniettiva se e solo se da ogni vertice che rappresenta un elemento di A esce uno ed un solo arco e ad ogni vertice che rappresenta un elemento di B arriva al più un arco.

  E' immediato provare che

  - *il prodotto di due funzioni iniettive è una funzione iniettiva;*

  - *se il prodotto* $f \cdot g$ *delle funzioni* f *e* g *è iniettivo allora* f *è iniettiva.*
    Infatti se f non fosse iniettiva esisterebbero $a_1 \neq a_2$ tali che $f(a_1) = f(a_2)$, ma allora ovviamente si avrebbe anche $f \cdot g\,(a_1) = g(f(a_1)) = g(f(a_2)) = f \cdot g\,(a_2)$, contro l'iniettività di $f \cdot g$.

  La funzione g può essere non iniettiva anche se $f \cdot g$ è iniettiva, basta infatti considerare il seguente esempio: $A = \{a\}$, $B = \{b_1, b_2\}$, $C = \{c\}$, $f(a) = b_1$, $g(b_1) = g(b_2) = c$, $f \cdot g$ è ovviamente iniettiva, ma g non lo è.
  Il prodotto $f \cdot g$ di due funzioni può non essere iniettivo anche se f è iniettiva, basta infatti considerare il seguente esempio: $A = \{a_1, a_2\}$, $B = \{b_1, b_2\}$, $C = \{c\}$, $f(a_1) = b_1$, $f(a_2) = b_2$, $g(b_1) = g(b_2) = c$ si ha allora $f \cdot g\,(a_1) = f \cdot g\,(a_2)$ quindi $f \cdot g$ non è iniettiva, ma f lo è.

- Una funzione f è *suriettiva*
  se ogni $b \in B$ ha almeno una controimmagine in A, o equivalentemente
  se $f(A) = B$.

  Naturalmente per verificare che una relazione f è una funzione suriettiva va anche verificata la condizione (*).

  Rappresentando la relazione f tramite la sua matrice di incidenza (se possibile) si ha che f è una funzione suriettiva se e solo se su ogni riga della matrice c'è uno ed un solo 1 e su ogni colonna almeno un 1.
  Rappresentando la relazione f tramite il suo grafo di incidenza (se possibile) si ha che f è una funzione suriettiva se e solo se da ogni vertice che rappresenta un elemento di A esce uno ed un solo arco e ad ogni vertice che rappresenta un elemento di B arriva almeno un arco.

E' immediato provare che:

- *il prodotto di due funzioni suriettive è una funzione suriettiva;*
- *se il prodotto* f · g *delle funzioni* f *e* g *è suriettivo allora* g *è suriettiva.*

La funzione f può essere non suriettiva anche se $f\cdot g$ è suriettiva, basta infatti considerare il solito esempio: $A = \{a\}$, $B = \{b_1,b_2\}$, $C = \{c\}$, $f(a) = b_1$, $g(b_1) = g(b_2) = c$, $f\cdot g$ è ovviamente suriettiva, ma f non lo è.
Il prodotto $f\cdot g$ di due funzioni può non essere suriettivo anche se g è suriettiva, basta infatti considerare l'esempio: $A = \{a_1,a_2\}$, $B = \{b_1,b_2\}$, $C = \{c_1,c_2\}$, $f(a_1) = f(a_2) = b_2$, $g(b_1) = c_1$, $g(b_2) = c_2$ si ha allora $f\cdot g\ (a_1)= f\cdot g\ (a_2) = c_2$ quindi $f\cdot g$ non è suriettiva, ma g lo è.

- Una funzione f è *biunivoca (biettiva)* se è suriettiva ed iniettiva.

Naturalmente per verificare che una relazione f è una funzione biunivoca va anche verificata la condizione (*).

Rappresentando la f tramite la sua matrice di incidenza (se possibile), si ha che f è una funzione biunivoca se e solo se su ogni riga e su ogni colonna della matrice c'è uno ed un solo 1.
Rappresentando la f tramite il suo grafo di incidenza (se possibile), si ha che f è una funzione biunivoca se e solo se da ogni vertice che rappresenta un elemento di A esce uno ed un solo arco e ad ogni vertice che rappresenta un elemento di B arriva uno e un solo arco.

E' immediato provare che:

- *il prodotto di due funzioni biunivoche è una funzione biunivoca;*
- *se il prodotto* f·g *delle funzioni* f *e* g *è una funzione biunivoca allora* f *è iniettiva e* g *è suriettiva.*

Osserviamo ora che la relazione inversa f^{-1} di una funzione $f : A\to B$ è una funzione se e solo se f è biunivoca ed in tal caso si ha $f\cdot f^{-1} = \imath_A$ e $f^{-1}\cdot f = \imath_B$.

Chiamiamo <u>funzione inversa</u> di una funzione $f : A\to B$, una funzione $g : B\to A$, se esiste, t.c. $f\cdot g = \imath_A$ e $g\cdot f = \imath_B$.
Una funzione h: $B\to A$ per cui si abbia $f\cdot h = \imath_A$ si dice <u>inversa destra</u> di f; una funzione $k : B\to A$ per cui si abbia $k\cdot f = \imath_B$ si dice <u>inversa sinistra</u> di f.

Sussistono i seguenti teoremi:

- *C.n.s affinché* f *ammetta inversa destra è che* f *sia iniettiva.*
  Se f ammette inversa destra h allora f è iniettiva in quanto $\imath_A = f\cdot h$ e $\imath_A$ è iniettiva. Viceversa se f è iniettiva costruiamo una sua inversa destra ampliando la relazione inversa di f. Infatti per ogni $b\in B$, se b ammette una controimmagine, che indichiamo con a_b, poniamo $h(b) = a_b$, mentre se b non ha controimmagini allora poniamo $h(b) = a$ per un fissato elemento di $a\in A$. La h è ovviamente una funzione ed è un'inversa destra di f, infatti per ogni $x\in A$ si ha $f\cdot h\ (x) = h(\ f(x)\ ) = x$, cioè $f\cdot h = \imath_A$.

- *C.n.s affinché* f *ammetta inversa sinistra è che* f *sia suriettiva* (la c.s utilizza il postulato della scelta).
  Se f ammette inversa sinistra k allora f è suriettiva in quanto $\imath_B = k\cdot f$ e $\imath_B$ è suriettiva. Viceversa se f è suriettiva costruiamo una sua inversa sinistra come relazione contenuta nella relazione inversa di f. Infatti

supponiamo di poter scegliere per ogni $b \in B$ nell'insieme delle controimmagini di b un elemento a_b e poniamo $k(b) = a_b$. La k è ovviamente una funzione ed è un'inversa sinistra di f perché per ogni $b \in B$ si ha $k \cdot f(b) = f(k(b)) = f(a_b) = b$, cioè $k \cdot f = \iota_B$.
(La scelta di un elemento fra le controimmagini di b, per ogni $b \in B$ è la scelta di un elemento in ciascun insieme di una partizione di A ed è un procedimento che si può facilmente effettuare se l'insieme A è numerabile, in generale però ammettere che tale scelta sia sempre effettuabile porta a conseguenze che non sembrano "troppo naturali", quando si utilizza questa possibilità di scelta si usa un postulato detto appunto postulato della scelta, e tale uso va dichiarato).

- *Se una funzione* f *ammette inversa sinistra e destra queste coincidono.*
  Siano h, k funzioni tali che $f \cdot h = \iota_A$ e $k \cdot f = \iota_B$. Abbiamo allora $k = k \cdot \iota_A = k \cdot (f \cdot h) = (k \cdot f) \cdot h = \iota_B \cdot h = h$ (notare che abbiamo usato, oltre le ipotesi, l'associatività del prodotto di funzioni e le proprietà delle funzioni identiche).

- *Una funzione* f *ammette funzione inversa (sinistra e destra) se e solo se è biunivoca; in tal caso l'inversa è unica e coincide con la relazione inversa di* f.
  Conseguenza immediata di quanto sopra.

Dalla costruzione delle inverse destre e sinistre, indicata nella dimostrazione, segue che se f ammette solo inversa sinistra o solo inversa destra queste non sono uniche.

Esempi:

Siano $A = \{a_1,a_2,a_3\}$, $B = \{b_1,b_2,b_3,b_4,b_5\}$, $f : A \to B$ definita da $f(a_i) = b_i$ per $i = 1,2,3$. La funzione f è iniettiva ma non suriettiva, dunque f ammette inversa destra. Una possibile inversa destra è la funzione h così definita:

$h(b_i) = a_i$ per $i = 1,2,3$,
$h(b_4) = h(b_5) = a_1$,

ma ovviamente è un'inversa destra anche una qualsiasi funzione che contenga la relazione inversa di f e che porti b_4 in un elemento di A e b_5 in un elemento di A; in totale quindi ho nove diverse inverse destre.

Siano $A=\{a_1,a_2,a_3,a_4,a_5\}$, $B=\{b_1,b_2,b_3\}$, $f : A \to B$ definita da $f(a_1) = f(a_2) = b_1$, $f(a_3) = f(a_4) = b_2$, $f(a_5) = b_3$. La funzione f è suriettiva ma non iniettiva dunque f ammette inversa sinistra. Una possibile inversa sinistra è la k così definita: $k(b_1) = a_1$, $k(b_2) = a_3$, $k(b_3) = a_5$, ma ovviamente è un'inversa sinistra anche una qualunque funzione che porti b_1 in uno degli elementi di $\{a_1,a_2\}$ (insieme delle controimmagini di b_1) e b_2 in uno degli elementi di $\{a_3,a_4\}$ (insieme delle controimmagini di b_2), quindi in totale abbiamo quattro possibili inverse sinistre di f.

Funzioni e relazioni di equivalenza.

Sia $f : A \to B$ una funzione. L'insieme $\{f^{-1}(b) | \ b \in B\}$ degli insiemi delle controimmagini degli elementi di B è una partizione di A e quindi è l'insieme delle classi di equivalenza di una relazione di equivalenza su A che chiamiamo $\ker f$.
E' facile notare che $\ker f$ è definita da $(a_1,a_2) \in \ker f$ sse $f(a_1) = f(a_2)$.
Se consideriamo una relazione di equivalenza ρ su A esiste sempre una funzione suriettiva h_ρ: $A \to A/\rho$ tale che $\ker h_\rho = \rho$. La h_ρ (detta anche proiezione canonica di A sul suo insieme quoziente A/ρ) è definita ponendo $h_\rho(a) = \rho_a$.

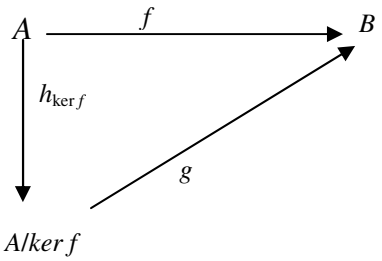
Il legame fra f: $A \to B$ e $h_{\ker f}$: $A \to A/\ker f$ è illustrato dal seguente teorema (I° teorema di fattorizzazione delle applicazioni):

- *Siano* f*:* A→B *una funzione e* $h_{\ker f}$*:* A→A/ker f *la proiezione canonica di* A *su* A/ker f. *Allora esiste un'unica funzione* g*:* A/ker f→B *tale che* $h_{\ker f}$·g = f. *Inoltre* g *è iniettiva. In particolare* f *è suriettiva se e solo se* g *è biunivoca*

Nel seguito indicheremo con $[a]$ la classe di equivalenza di a rispetto a ker f. Osserviamo che per avere $h_{ker\ f} \cdot g = f$, dobbiamo porre $g([a]) = f(a)$. La g così definita è una funzione infatti se $[a_1] = [a_2]$ abbiamo $(a_1,a_2) \in ker\ f$ e cioè $f(a_1) = f(a_2)$. La funzione g è unica per costruzione ed è iniettiva perché se $g([a_1]) = g([a_2])$, otteniamo subito $f(a_1) = f(a_2)$ e quindi $(a_1,a_2) \in ker\ f$ da cui $[a_1]=[a_2]$.

Questo teorema viene di solito enunciato dicendo:

- *Siano* f*:* A→B *una funzione e* $h_{\ker f}$*:* A→A/ker f *la proiezione canonica di* A *su* A/ker f. *Allora esiste un'unica funzione* g*:* A/ker f → B *che rende commutativo il seguente diagramma:*



Inoltre g *è una funzione iniettiva ed è biunivoca se e solo se* f *è suriettiva.*

(dire che un diagramma è commutativo significa che comunque ci muoviamo lungo le direzioni permesse da quel diagramma, quando arriviamo ad uno stesso punto otteniamo lo stesso risultato: quindi, nel nostro caso, se partiamo da $a \in A$ e ci muoviamo lungo la freccia etichettata da f arriviamo all'elemento $f(a) \in B$, se ci muoviamo lungo il cammino composto dalla frecce etichettate con $h_{ker\ f}$ e g otteniamo $g(h_{ker\ f}(a)) = h_{ker\ f} \cdot g(a)$, la commutatività del diagramma dice quindi che $h_{ker\ f} \cdot g = f$).

Osserviamo che come conseguenza del teorema di fattorizzazione si ottiene che $f(A)$ è in corrispondenza biunivoca con $A/ker\ f$.
Inoltre il teorema dice che una qualsiasi funzione f può essere pensata come il prodotto di una funzione suriettiva per una funzione iniettiva.

Osservazione: Nel corso di Geometria ed Algebra lineare avete probabilmente incontrato la nozione di ker di una applicazione lineare f da uno spazio vettoriale V ad uno spazio vettoriale V'. In tal caso ker f è l'insieme delle controimmagini dello 0 di V'. La definizione puo sembrare in questo momento molto diversa, ma possiamo notare che $(v_1,v_2) \in ker\ f$ secondo la definizione qui data di $ker\ f$ se e solo se $v_1 - v_2 \in ker\ f$ secondo la definizione data nel corso di Geometria ed Algebra lineare.

Cardinalità di un insieme

Diciamo che due insiemi A e B hanno la stessa cardinalità e scriviamo $|A| = |B|$ se esiste una corrispondenza biunivoca $f : A \to B$
(Osserviamo che poiché l'applicazione identica è biunivoca, l'inversa di una applicazione biunivoca è a sua volta biunivoca, il prodotto di applicazioni biunivoche è una funzione biunivoca e quindi si ha subito che:

$|A| = |A|$,

se $|A| = |B|$ allora $|B| = |A|$;

se $|A| = |B|$ e $|B| = |C|$ allora $|A| = |C|$).

Diciamo che A ha cardinalità inferiore a B e scriviamo che $|A|\leq|B|$ se esiste una applicazione iniettiva da A a B (il che equivale a dire che A è in corrispondenza biunivoca con un sottoinsieme di B).
(Osserviamo che l'antisimmetria della relazione ≤ appena definita non è ovvia).

Diciamo che A ha cardinalità strettamente inferiore a B e scriviamo $|A|<|B|$ se $|A|\leq|B|$ ma $|A|\neq|B|$ (cioè se esiste una funzione iniettiva da A a B ma non esiste una funzione biunivoca da A a B).

Diciamo che l'insieme A è *finito* ed ha cardinalità n se ha la stessa cardinalità di $\{1,2,\ldots,n\}$.

Diciamo che A è *infinito* se non è finito, ovvero se non ha cardinalità n per alcun n intero positivo.
Una caratterizzazione degli insiemi infiniti è la seguente:

- *Un insieme è infinito se e solo se può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio.*

Un insieme infinito ha la *potenza del numerabile* se ha la stessa cardinalità di N, ha la *potenza del continuo* se ha la stessa cardinalità di R. Ricordiamo che Z e Q sono numerabili.

Esistono insiemi con cardinalità superiore alla potenza del continuo? La risposta è data dal seguente teorema che nel nostro contesto è importante anche per la tecnica dimostrativa che utilizza.

<u>*Teorema di Cantor*</u>*: Ogni insieme* A *ha cardinalità strettamente inferiore al suo insieme delle parti* $\mathcal{P}$*(*A*).*
Dim.
Esiste ovviamente un'applicazione iniettiva da A a $\mathcal{P}(A)$: basta considerare l'applicazione h che manda ogni $a\in A$ nell'insieme $\{a\}\in \mathcal{P}(A)$.
Supponiamo per assurdo che esista una applicazione biunivoca $g : A\rightarrow \mathcal{P}(A)$ e consideriamo l'insieme $B = \{a\in A|\ a\notin g(a)\}$. Poiché $B\in \mathcal{P}(A)$, B ammette una controimmagine $\tilde{a}\in A$ cioè $g(\tilde{a}) = B$. Supponiamo ora che $\tilde{a}\in B$. Allora, per come è definito B, si ha che $\tilde{a}\notin g(\tilde{a}) = B$ che è assurdo in quanto stavamo supponendo che $\tilde{a}\in B$. Segue che $\tilde{a}\notin B$ con $B = g(\tilde{a})$. Allora si ha che $\tilde{a}\notin g(\tilde{a})$ e quindi, per come è definito B, segue che $\tilde{a}\in B$ che è assurdo in quanto stavamo supponendo che $\tilde{a}\notin B$. Abbiamo quindi un assurdo che dipende dall'ipotesi di esistenza di g.

Il teorema sostanzialmente afferma che c'è una sequenza infinita di infiniti.

Osserviamo che la cardinalità di R è la cardinalità dell'insieme delle parti di N. Non è noto se esistano insiemi con cardinalità compresa fra quella del numerabile e quella del continuo, e analogamente non è noto se, dato un insieme infinito A, esistano insieme con cardinalità compresa fra quella di A e quella di $\mathcal{P}(A)$.

L'ipotesi del continuo (generalizzata) assume che non ci siano insiemi di cardinalità compresa fra quella di N e quella di $\mathcal{P}(N)$ (fra quella di un qualsiasi insieme infinito A e quella del suo insieme delle parti).

<u>Leggi di composizione.</u>

Dati gli insiemi $A_1, A_2,\ldots, A_n, A,$ una funzione $\omega: A_1\times A_2\times\ldots\times A_n\rightarrow A$ si dice <u>*legge di composizione*</u> <u>n-*aria*</u> (o di arità n) di $A_1, A_2,\ldots, A_n$ a valori in A. Per ogni $(a_1,a_2,\ldots,a_n)\in A_1\times A_2\times\ldots\times A_n$ l'elemento

$a = \omega(a_1,a_2,\ldots,a_n)$ (che esiste ed è unico) è detto il risultato della composizione ω della n-upla $(a_1,a_2,\ldots,a_n)$.
Se $A_1 = A_2 = \ldots = A_n = A$, diremo che ω è una *legge di composizione* (o *operazione*) interna n-aria (o di arità n) su A.

Siamo interessati soprattutto alle operazioni interne n-arie con $n = 1$ (unarie) ed $n = 2$ (binarie).
Per le operazioni interne binarie su un insieme A useremo la notazione infissa, indicando il risultato della composizione $*$ di (a,a') con $a * a'$.

Se A è un insieme finito i risultati di una operazione binaria interna su A possono essere rappresentati tramite la tavola di composizione (detta spesso tavola di moltiplicazione) illustrata di seguito con un esempio (generalizzazione ovvia della tavola pitagorica)

Esempi
Il passaggio da un intero al suo opposto è una legge di composizione interna unaria in Z (perché non lo è in N?)
La ordinaria somma è un'operazione interna binaria su N, su Z, su Q,…
La differenza è un'operazione interna su Z, ma non è un'operazione interna su N (perché?)
Il prodotto righe per colonne di matrici quadrate reali d'ordine n è una legge di composizione interna binaria sull'insieme delle matrici quadrate reali di ordine n.
Il prodotto di relazioni binarie su A, che abbiamo precedentemente definito, è una legge di composizione interna sull'insieme delle relazioni binarie su A.
Il prodotto di funzioni da A ad A è una legge di composizione interna sull'insieme delle funzioni da A ad A.
Dato $A=\{a,b,c\}$ la seguente è un'operazione interna binaria su A: $a*a=b$, $a*b=c$, $a*c=a$, $b*a=a$, $b*b=b$, $b*c=c$, $c*a=b$, $c*b=a$, $c*c=a$ rappresentabile con la seguente tavola di composizione

	a	b	c
a	b	c	a
b	a	b	c
c	b	a	a

Introduciamo alcune proprietà delle operazioni binarie interne su A ponendo l'attenzione sul genere di calcoli che la presenza di queste proprietà rendono leciti.

Indichiamo di seguito con $*$ una generica operazione binaria interna su A:

- L'operazione $*$ è *commutativa* se per ogni $a, a' \in A$ si ha $a*a'=a'*a$
  La commutatività di $*$ appare evidente dalla sua tavola di composizione (se si può fare)
  Infatti tale tavola risulterà simmetrica rispetto alla diagonale che parte dal vertice in alto a sinistra.

- L'operazione $*$ è *associativa* se per ogni $a, a', a'' \in A$ si ha $a*(a'*a'')= (a*a')*a''$

Se l'operazione $*$ è associativa possiamo definire le potenze ad esponenti positivi di un qualsiasi elemento $a\in A$, ponendo $a^{(n)}= a*a*\ldots*a$ (n volte) e le potenze godono delle proprietà formali $a^{(n)} * a^{(m)}= a^{(n+m)}$, $(a^{(n)})^{(m)}= a^{(nm)}$.
(Notate bene che l'associatività non è indispensabile per definire le potenze ma lo è per stabilire le loro proprietà. Come avremmo potuto introdurre una definizione di potenza ad esponente positivo di $a\in A$ senza l'associatività della legge di composizione?)
(Cosa è la potenza quarta di 3 rispetto all'usuale somma di naturali?)

- Esiste un *elemento neutro* (identità) in A rispetto all'operazione $*$ se esiste un $e\in A$ tale che per ogni $a\in A$ risulta $e*a=a*e=a$. Se si ha solo $e*a=a$, per ogni $a\in A$, e si dice elemento neutro a sinistra, se invece si ha solo $a*e=a$, per ogni $a\in A$, e si dice elemento neutro a destra.
  - Se esiste l'elemento neutro, si può definire in A la potenza ad esponente 0 di un qualunque $a\in A$, ponendo $a^{(0)}=e$.
  - Se in A esistono elemento neutro a destra ed elemento neutro a sinistra rispetto all'operazione $*$, questi coincidono.

  Infatti se e è elemento neutro a sinistra ed f è elemento neutro a destra si ha $e*f=e$, se ci si ricorda che f è elemento neutro a destra, ed $e*f=f$, se ci si ricorda che e è elemento neutro a sinistra; quindi $e=f$.

  Di conseguenza
  - Se in A esiste elemento neutro questo è unico

  Sulla tavola di composizione di $*$, se è possibile farla, si possono facilmente identificare gli eventuali elementi neutri destri e sinistri (come?)
  Notare che se A ammette solo elemento neutro a destra (o a sinistra) rispetto all'operazione, questo non è necessariamente unico. Scrivere una tavola di composizione per un insieme A in modo che esistano due diverse unità sinistre.

- Esiste uno *zero* in A rispetto all'operazione $*$ se esiste uno $z\in A$ tale che per ogni $a\in A$ risulta $z*a=a*z=z$. Se si ha solo $z*a=z$, per ogni $a\in A$, z si dice zero a sinistra, se invece si ha solo $a*z=z$, per ogni $a\in A$, z si dice zero a destra
  - Se in A esistono zero a destra e zero a sinistra rispetto all'operazione $*$, questi coincidono. Di conseguenza se A ammette zero, tale zero è unico

  Sulla tavola di composizione di $*$, se è possibile farla, si possono facilmente identificare gli zeri destri e sinistri (come?)

- Se esiste in A un elemento neutro rispetto all'operazione $*$, diciamo che $a\in A$ ammette *inverso* (è invertibile) rispetto all'operazione $*$ se esiste un $\tilde{a}\in A$ tale che $\tilde{a}*a=a*\tilde{a}=e$. Se si ha solo $\tilde{a}*a=e$, $\tilde{a}$ si dice elemento inverso a sinistra di a, se invece si ha solo $a*\tilde{a}=e$, $\tilde{a}$ si dice inverso a destra di a.
  Notiamo che se a ammette inverso $\tilde{a}$, l'inverso di $\tilde{a}$ è a.
  - Se l'operazione $*$ è associativa ed a è invertibile, si possono definire in A le potenze ad esponente intero di un qualunque $a\in A$. Abbiamo già visto come definirla se $n\geq 0$, se $n<0$ poniamo $a^{(n)}= \tilde{a} *\tilde{a}*\ldots *\tilde{a}$ ($-n$ volte). Continuano a sussistere le proprietà formali delle potenze (esercizio).
  - Se l'operazione $*$ è associativa ed a ammette inverso sinistro a^s ed inverso destro a^d questi coincidono (esercizio). Quindi se $*$ è associativa ed a ammette inverso, questo inverso è unico
  - Se l'operazione $*$ è associativa ed a ammette inverso, ogni equazione del tipo $a*x=b$ ($b\in A$) ammette uno ed una soluzione della forma $\tilde{a}*b$.

Proviamo che $a*x=b$ ammette soluzione sostituendo $\tilde{a}*b$ al posto di x in $a*x$, abbiamo $a*(\tilde{a}*b)=(a*\tilde{a})*b=e*b=b$.
Supponiamo ora che $c\in A$ sia una soluzione di $a*x=b$, si avrà allora $a*c=b$, da cui moltiplicando a sinistra entrambi i membri per $\tilde{a}$ abbiamo $\tilde{a}*(a*c)=\tilde{a}*b$, ma $\tilde{a}*(a*c)=(\tilde{a}*a)*c=e*c=c$ e dunque $c=\tilde{a}*b$.

- Se l'operazione $*$ è associativa ed a ammette inverso ogni equazione del tipo $x*a=b$ $(b\in A)$ ammette uno ed una soluzione della forma $b*\tilde{a}$. (esercizio)
- Se l'operazione $*$ è associativa ed a ammette inverso sinistro, $a*b=a*c$ implica $b=c$ (esercizio).
- Se l'operazione $*$ è associativa ed a ammette inverso destro, $b*a=c*a$ implica $b=c$ (esercizio).
- Se l'operazione $*$ è associativa ed a_1, a_2 ammettono inversi $\tilde{a}_1$, $\tilde{a}_2$ allora a_1*a_2 ammette inverso e questo inverso è $\tilde{a}_2*\tilde{a}_1$.
  Infatti $(a_1*a_2)*(\tilde{a}_2*\tilde{a}_1)=(a_1*(a_2*\tilde{a}_2))*\tilde{a}_1=(a_1*e)*\tilde{a}_1=a_1*\tilde{a}_1=e$, analogamente si prova che $(\tilde{a}_2*\tilde{a}_1)*(a_1*a_2)=e$.