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 $\{f(a) | a \in A\}$ ed $f^{-1}(b)$ per indicare $\{a \in A | f(a)=b\}$.

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.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 è una funzione da A ad A, che in questo contesto viene spesso indicata con ι_A; si ha ovviamente : $\iota_A \cdot f = f = f \cdot \iota_B$.
Osserviamo invece che la relazione inversa di una funzione f non è in generale una funzione.

E' naturale la domanda: quando la relazione inversa 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 $f(a_1)=f(a_2)$ allora $a_1=a_2$, o equivalentemente
  se $a_1 \neq a_2$ allora $f(a_1) \neq f(a_2)$

  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·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·g.

La funzione g può essere non iniettiva anche se f·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·g è ovviamente iniettiva, ma g non lo è.
Il prodotto f·g di due funzioni può non essere iniettivo anche se f è iniettivo, 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·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 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·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·g è ovviamente suriettiva, ma f non lo è.
Il prodotto f·g di due funzioni può non essere suriettivo anche se g è suriettivo, 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·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 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→B è una funzione se e solo se f è biunivoca ed in tal caso si ha : $f\cdot f^{-1}= \iota_A$ e $f^{-1}\cdot f= \iota_B$.

Chiamiamo *funzione inversa* di una funzione f:A→B, una funzione g:B→A, se esiste, t.c. $f\cdot g=\iota_A$ e $g\cdot f=\iota_A$.
Una funzione h:B→A per cui si abbia $f\cdot h=\iota_A$ si dice *inversa destra* di f; una funzione k:B→A per cui si abbia $k\cdot f=\iota_b$ si dice *inversa sinistra* di f.

Sussistono i seguenti teoremi:

- *C.n.s affinché f ammetta inversa destra è che f sia iniettiva.*
  Se f ammette inversa destra f è iniettiva perché ι_A è iniettiva, viceversa se f è iniettiva costruiamo una sua inversa destra, ampliando la relazione inversa di f. Infatti per ogni b∈ B che ammetta una controimmagine, che indichiamo con a_b, poniamo $h(b)= a_b$, mentre se b non ha controimmagini poniamo h(b)=a per un fissato elemento di A. La h è ovviamente una funzione ed è inversa destra di f, infatti per ogni a∈ A si ha f·h (a)=g(f(a))=a, cioè $f\cdot h=\iota_A$.

- *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 f è suriettiva perché ι_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∈ 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 inversa sinistra infatti per ogni b∈ 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∈ 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 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→B definita da $f(a_i)=b_i$ per i=1,2,3. f è iniettiva ma non suriettiva, dunque f ammette inversa destra. Una possibile inversa destra è la h così definita: $h(b_i)=a_i$ per i=1,2,3, $h(b_4)=h(b_5)=a_1$, ma ovviamente è inversa destra anche una qualsiasi funzione che contenga la relazione inversa di f e porti b_4 in un elemento di A e b_5 in un elemento di A; in totale quindi ho 9 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 $f(a_1)= f(a_2)=b_1$, $f(a_3)= f(a_4)=b_2$, $f(a_5)= b_3$. 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 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 4 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 invece consideriamo una relazione di equivalenza ρ su A esiste sempre una funzione suriettiva $p_\rho:A\to A/\rho$ tale che $\ker p_\rho=\rho$. La p_ρ (detta anche proiezione canonica di A sul suo insieme quoziente A/ ρ) è definita ponendo $p_\rho(a)=\rho_a$.

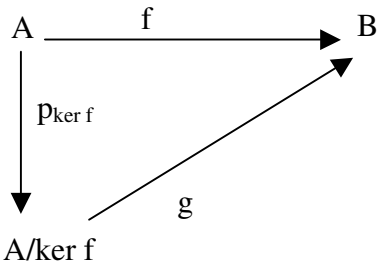
Il legame fra $f:A\to B$ e $p_{\ker f}:A\to A/\ker f$ è illustrato dal seguente teorema (I teorema di fattorizzazione delle applicazioni):

> *Siano $f:A\to B$ una funzione e $p_{ker\,f}:A\to A/ker\,f$ l'applicazione canonica di A si A/ker f. Esiste unica una funzione $g: A/ker\,f\to B$ tale che $p_{ker\,f}\cdot g=f$. Inoltre g è iniettiva.*

Nel seguito chiameremo [a] la classe di equivalenza di a rispetto a ker f. Osserviamo che per avere $p_{\ker f}\cdot g=f$, 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 $f:A\to B$ una funzione e $p_{ker\,f}:A\to A/ker\,f$ l'applicazione canonica di A si A/ker f. Esiste unica una funzione $g: A/ker\,f\to B$ che rende commutativo il seguente diagramma:*



> *Inoltre g è iniettiva.*

(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 $p_{\ker f}$ e g otteniamo $g(p_{\ker f}(a))= p_{\ker f}\cdot g(a)$, la commutatività del diagramma dice quindi che $p_{\ker f}\cdot g=f$).

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.

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→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 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, |A|≤|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 del ≤ appena definito non è ovvia)

Diciamo che A ha cardinalità inferiore a B, |A|<|B|, se |A|≤|B| ma |A|≠|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,…,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:
Un insieme è infinito se e solo se può essere messo in corrispondenza biunivoca con una sottoinsieme proprio.

Come già sapete 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.
Ricordo 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 .

Teorema di Cantor: Ogni insieme A ha cardinalità strettamente inferiore al suo insieme delle parti. P(A).
Dim.
Esiste ovviamente una applicazione iniettiva da A a P(A): basta considerare l'applicazione h che manda ogni a∈ A nell'insieme {a}∈ P(A).
Supponiamo per assurdo che esista una applicazione biunivoca g:A→ P(A).
Consideriamo l'insieme B={a∈ A | a∉ g(a)}, B∈ P(A) dunque ammette una controimmagine ã∈ A, si ha allora g(ã)=B. Supponiamo ora che ã∈ B allora per come è definito B abbiamo ã∉ g(ã)=B. Quindi ã∉ B=g(ã) e allora per come è definito B si ha ã∈ 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 $\mathtt{P}(A)$.

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

Leggi di composizione.

Dati gli insiemi $A_1, A_2,\ldots, A_n, A$, una applicazione $\omega: A_1\times A_2\times\ldots\times A_n\to A$ si dice *legge di composizione n-aria* (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 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 per stabilire le loro proprietà. Come avremmo potuto introdurre una definizione di potenza ad esponente positivo di a senza l'associatività?)
  (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 $e*a=a$, e si dice elemento neutro a sinistra, se invece si ha solo $a*e=a$, 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 e 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 $z*a=z$, z si dice zero a sinistra, se invece si ha solo $a*z=z$, 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 ad $*$ 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, se invece si ha solo $a*\tilde{a}=e$, $\tilde{a}$ si dice inverso a destra.
  Notiamo che se a ammette inverso $\tilde{a}$, l'inverso di $\tilde{a}$ è a.
  - Se $*$ 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 $*$ 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 $*$ 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 $*$ 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 $*$ è associativa ed a ammette inverso sinistro, $a*b= a*c$ implica $b=c$ (esercizio).
- Se $*$ è associativa ed a ammette inverso destro , $b*a= c*a$ implica $b=c$ (esercizio).
- Se $*$ 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 $(\tilde{a}_2* \tilde{a}_1)* (a_1*a_2)=e$.