STRUTTURE ALGEBRICHE

Def. Si dice *struttura algebrica* una coppia $<A,\Omega>$ formata da un insieme A, chiamato sostegno della struttura, e da un insieme non vuoto e finito di leggi di composizione interne Ω che possono godere di particolari proprietà. Gli elementi di A si dicono elementi della struttura. La struttura si dice finita se è finito il suo sostegno

Di seguito elenchiamo alcune importanti strutture algebriche.

- Si dice *semigruppo* $<A,\cdot>$ un insieme A fornito di una legge di composizione interna binaria associativa.

  Esempi.

  L'insieme delle matrici quadrate di ordine n ad elementi positivi rispetto all'usuale prodotto di matrici è un semigruppo.

  Dato un insieme finito Σ, detto alfabeto, si dice *parola* su Σ una sequenza finita di simboli di Σ.
  Si indichi con Σ^+ l'insieme delle parole su Σ e si consideri su Σ^+ la legge di composizione interna binaria data dalla concatenazione di parole, ovvero considerate $u=a_{i_1}a_{i_2}\dots a_{i_n}$, $v=a_{j_1}a_{j_2}\dots a_{j_m}$ si indichi con uv la parola $a_{i_1}a_{i_2}\dots a_{i_n}a_{j_1}a_{j_2}\dots a_{j_m}$. L'insieme Σ^+ rispetto alla concatenazione di parole è un semigruppo, che si dice *semigruppo libero* sull'alfabeto Σ.

- Si dice *monoide* un semigruppo $<A,\cdot>$ dotato di elemento neutro rispetto all'operazione binaria $\cdot$.

  Esempi.

  L'insieme delle matrici quadrate di ordine n ad elementi interi, o razionali, o reali, rispetto all'usuale prodotto di matrici, è un monoide.

  Dato un insieme finito Σ, si indichi con Σ^* l'insieme $\Sigma^+\cup\{\varepsilon\}$ dove ε è un simbolo non appartenente a Σ, detto parola vuota, e si consideri su Σ^* la legge di composizione interna binaria data dalla concatenazione di parole con la convenzione che $u\varepsilon=\varepsilon u=u$ per ogni $u\in\Sigma^*$. Σ^* rispetto a tale operazione è un monoide detto *monoide libero* su Σ.

  Poiché come sappiamo l'unità di un monoide è unica, il monoide può essere visto come una struttura algebrica con due operazioni, un'operazione binaria $\cdot$ associativa ed una operazione 0-aria f che corrisponde alla scelta dell'elemento neutro ed associa ad ogni elemento b uno stesso elemento e, legata a $\cdot$ dalla relazione $a\cdot e=e\cdot a=a$ per ogni a nell'insieme sostegno.
  Un monoide viene di conseguenza spesso indicato con la notazione $<A,\cdot,e>$ per mettere in risalto la presenza di tale operazione di arità 0.

- Si dice *gruppo* un monoide $<A,\cdot,e>$ in cui ogni elemento ammette inverso rispetto all'operazione $\cdot$.

In altre parole un gruppo è un insieme A con una legge di composizione binaria $\cdot$ associativa , che soddisfa le seguenti condizioni:

1) esiste un $e\in A$ tale che, per ogni $a\in A$, si ha $a\cdot e=e\cdot a=a$
2) per ogni $a\in A$, esiste un $b\in A$ tale che $a\cdot b=b\cdot a=e$; tale b viene solitamente indicato col simbolo a^{-1}.

Esempi

L'insieme delle matrici quadrate non singolari di ordine n ad elementi razionali, o reali, rispetto all'usuale prodotto di matrici, è un gruppo.

L'insieme delle funzioni biettive di un insieme A in sé, rispetto alla usuale composizione di funzioni, è un gruppo.

Poiché, come abbiamo visto in un gruppo l'elemento neutro è unico ed ogni elemento ammette un unico inverso (ricordarsi quanto detto per una legge di composizione interna associativa), un gruppo può essere visto come una struttura algebrica con tre operazioni, un'operazione binaria $\cdot$ associativa, una operazione 0-aria f, che corrisponde alla scelta dell'elemento neutro e ed un'operazione 1-aria g che corrisponde al passaggio all'inverso tale che per ogni elemento a si abbia $a\cdot g(a)=g(a)\cdot a = e$.
Per mettere in risalto l'esistenza di queste due operazioni, per un gruppo si usa spesso la notazione $<A,\cdot,^{-1},e>$

Ci sono definizioni equivalenti di gruppo; sussiste infatti la seguente
Proposizione. Sia A un insieme con una legge di composizione interna binaria associativa. Sono equivalenti:

(i) A è un gruppo

(ii) esiste un $e\in A$ tale che, per ogni $a\in A$, si ha $a\cdot e =a$ $(e\cdot a=a)$ e per ogni $a\in A$ esiste un $b\in A$ tale che $a\cdot b =e$ $(b\cdot a=e)$, cioè in A ci sono elemento neutro a destra ed inverso destro di ogni elemento (oppure in A ci sono elemento neutro a sinistra ed inverso sinistro di ogni elemento)

(iii) per ogni $a,b\in A$, le equazioni $a\cdot x=b$, $x\cdot a=b$ ammettono ciascuna una e una sola soluzione in A.

Dim:
(i) implica (iii). Ci è già noto
(iii) implica (ii). Si consideri l'equazione $x\cdot b=b$ e sia e la sua unica soluzione, si ha allora $e\cdot b=b$; sia poi d la soluzione dell'equazione $a\cdot x=a$, da $a\cdot d=a$ segue $a\cdot(d\cdot b)=a\cdot b$, dall'unicità della soluzione dell'equazione $a\cdot x=a\cdot b$ si deduce $d\cdot b=b=e\cdot b$ e dunque $d=e$; esiste quindi un e tale che per ogni $a\in A$ si ha $a\cdot e=a$. La soluzione dell'equazione $a\cdot x=e$ risulta poi essere un elemento b di A tale che $a\cdot b=e$.
(ii) implica (i). Poiché in A esiste per ipotesi unità destra e ed ogni elemento ammette inverso destro, dobbiamo dimostrare che ogni elemento ammette inverso sinistro e che e risulta unità sinistra. Sia $a\cdot b=e$ e $b\cdot c=e$, allora $b\cdot a=(b\cdot a)\cdot e=(b\cdot a)\cdot(b\cdot c)= ((b\cdot a)\cdot b)\cdot c= (b\cdot(a\cdot b))\cdot c= (b\cdot e)\cdot c= b\cdot c=e$, cioè b è anche inverso sinistro di a. Si ha poi $a= a\cdot e= a\cdot(b\cdot a)=(a\cdot b)\cdot a=e\cdot a$, allora e è anche unità sinistra.

La precedente proposizione mette in luce che nella definizione di gruppo le condizioni (1) e (2) possono essere sostituite con la condizione (iii) oppure possono essere indebolite come indicato dalla condizione (ii), notare bene che non basta provare che A un insieme A con una legge di composizione interna binaria associativa ammetta elemento neutro a destra ed inverso sinistro di ogni elemento oppure elemento neutro a sinistra ed inverso destro di ogni elemento per concludere che è un gruppo.

Notazione. A volte si usa per la legge di composizione la notazione additiva a+b, in tal caso l'elemento neutro è chiamato 0, l'inverso di a è chiamato opposto di a ed indicato col simbolo -a e la potenza n-esima di a è indicata con na.

Un gruppo in cui la legge di composizione binaria gode della proprietà commutativa si dice *gruppo abeliano*.

Le strutture appena elencate sono le principali strutture con una sola legge di composizione binaria interna. Passiamo ora alle strutture con 2 leggi di composizioni binarie.

- Si dice *anello* una struttura algebrica $\langle A,\Omega\rangle$ con due operazioni binarie denotate da **+** e $\cdot$, tali che:
    1) $\langle A,+\rangle$ è un gruppo abeliano detto gruppo additivo dell'anello,
    2) $\langle A,\cdot\rangle$ è un semigruppo detto semigruppo moltiplicativo dell'anello,
    3) valgono le proprietà distributive di $\cdot$ rispetto a +, cioè per ogni $a,b,c\in A$ si ha
    $$a\cdot(b+c)=a\cdot b+a\cdot c \qquad , \qquad (a+b)\cdot c=a\cdot c+b\cdot c.$$

Esempi.

L'insieme delle matrici quadrate di ordine n ad elementi interi è un anello rispetto agli usuali somma e prodotto di matrici.

L'insieme degli interi relativi rispetto agli usuali somma e prodotto è un anello.

I polinomi a coefficienti reali nell'indeterminata x, rispetto alle usuali operazioni di somma e prodotto sono un anello.

Un anello il cui semigruppo moltiplicativo sia un monoide si dice *anello con unità*; un anello in cui il semigruppo moltiplicativo sia commutativo si dice *anello commutativo*. Il primo esempio è dunque un anello con unità, gli altri sono anelli commutativi con unità.

In un anello lo zero (elemento neutro rispetto a +) è unico e ogni elemento ammette un unico opposto. Pertanto un anello può essere visto come una struttura algebrica con due operazioni binarie **+** e $\cdot$, una operazione 0-aria (scelta dello zero), una operazione 1-aria (passaggio all'opposto), legate opportunamente tra loro. Un anello viene quindi spesso denotato da $\langle A,+,\cdot,0,-\rangle$.

Proposizione. In un anello $\langle A,+,\cdot,0,-\rangle$ si ha
$a\cdot 0=0\cdot a=0$ per ogni $a\in A$,
$a\cdot(-b)=(-a)\cdot b = -a\cdot b$ per ogni $a,b\in A$.
Dim.
Usando la proprietà distributiva si ha $a\cdot b=a\cdot(b+0)=a\cdot b+a\cdot 0$, ma è anche $a\cdot b=a\cdot b+0$, dunque $a\cdot b+a\cdot 0=a\cdot b+0$, da cui per la cancellatività rispetto alla + si ottiene $a\cdot 0=0$. Analogamente si prova $0\cdot a=0$. Da $0=a\cdot 0= a\cdot(b+(-b))= a\cdot b+a\cdot(-b)$, si ottiene poi che $a\cdot(-b)$ è l'opposto di $a\cdot b$. Analogamente si prova che $(-a)\cdot b$ è l'opposto di $a\cdot b$.

Un anello $\langle A,+,\cdot,0,-\rangle$ si dice *privo di divisori dello 0* se non esistono $a,b\in A$ e diversi da 0 tali che $a\cdot b=0$.
In un anello $\langle A,+,\cdot,0,-\rangle$ valgono le *leggi di cancellazione* se ognuna delle relazioni $a\cdot b=a\cdot c$ e $b\cdot a=c\cdot a$ con $a,b,c\in A$ ed $a\neq 0$ implica $b=c$.

Proposizione. Un anello <A,+,·,0,-> è privo di divisori dello zero se e solo se in esso valgono le leggi di cancellazione.

Dim.

Sia <A,+,·,0,-> privo di divisori dello zero e sia $a \cdot b = a \cdot c$ con $a,b,c \in A$ ed $a \neq 0$, allora si ha $a \cdot b + (-a \cdot c) = 0$ cioè $a \cdot (b + (-c)) = 0$, pertanto $b + (-c) = 0$ altrimenti a e $b+(-c)$ sarebbero divisori dello 0. Analogamente si prova che $b \cdot a = c \cdot a$ con $a \neq 0$ implica $b = c$.

Viceversa, sia <A,+,·,0,-> un anello in cui valgono le leggi di cancellazione e supponiamo $a \cdot b = 0$ con $a \neq 0$, allora essendo $a \cdot b = a \cdot 0$, per cancellazione si ottiene $b = 0$, per cui a,b non sono divisori dello 0.

Riflettete sulla possibilità di cancellare nell'anello Z degli interi relativi rispetto alle usuali somma e prodotto e su quanto avviene nell'anello delle matrici quadrate di un dato ordine n rispetto a somma e prodotto di matrici.

- Si dice *corpo* un anello in cui gli elementi diversi dallo 0 formano gruppo rispetto a ·.

- Un corpo in cui · gode della proprietà commutativa si dice *campo*.

Esempi.

I numeri razionali, reali e complessi rispetto alle usuali operazioni di somma e prodotto sono campi.

L'insieme {0,1,2} rispetto alla somma e al prodotto definiti da

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

•	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

è un campo finito.

Non esistono corpi finiti che non siano campi. Sussiste infatti l'importante teorema: *ogni corpo finito è un campo.*

Un esempio di corpo che non sia campo è il seguente: si consideri come sostegno del corpo l'insieme C di tutti gli elementi della forma $a\underline{i}+b\underline{j}+c\underline{k}+d$ dove a,b,c,d sono numeri reali qualsiasi, si definisca la somma di due elementi di questo tipo come la somma di polinomi nelle variabili $\underline{i},\underline{j},\underline{k}$, si definisca il prodotto di due elementi di questo tipo in questo modo: dopo aver effettuato il prodotto come se fosse il prodotto di polinomi, si ponga nel prodotto così ottenuto $\underline{i}^2=\underline{j}^2=\underline{k}^2=-1$ e $\underline{ij}=\underline{k}$, $\underline{jk}=\underline{i}$, $\underline{ki}=j$, $\underline{ji}=-\underline{k}$, $\underline{kj}=-\underline{i}$, $\underline{ik}=-j$. C rispetto alla somma e al prodotto così definiti è un corpo detto *corpo dei quaternioni*.

- Si dice *reticolo* un insieme A con due operazioni binarie $\wedge$ e $\vee$, dette rispettivamente intersezione ed unione che godano entrambe delle proprietà commutativa ed associativa e per le quali valgano le leggi di assorbimento:

  $a\wedge(a\vee b)=a \qquad a\vee(a\wedge b)=a$ per ogni $a,b\in A$

Esempi.

L'insieme degli interi naturali con le operazioni di intersezione ed unione definite da $a\wedge b$=M.C:D.(a,b) e $a\vee b$=m.c.m.(a,b) è un reticolo.

L'insieme delle parti di un insieme A rispetto alle usuali operazione di intersezione ed unione insiemistica è un reticolo

Riflettere sul fatto che abbiamo già dato una definizione di reticolo come insieme parzialmente ordinato in cui ogni coppia di elementi ammette inf e sup.
Vedremo più avanti come le due definizioni si equivalgano.

Sottostrutture di una struttura algebrica

Data una struttura algebrica $<A,\Omega>$, un sottoinsieme non vuoto di H di A si dice *sottostruttura* di $<A,\Omega>$ se risulta essere una struttura dello stesso tipo di A rispetto alle operzioni di Ω.

Ad esempio, se $<A,\cdot>$ è un semigruppo, un sottoinsieme H di A tale che per ogni $a,b\in H$ si abbia $a\cdot b\in H$ si dice *sottosemigruppo* di $<A,\cdot>$.
Se $<A,\cdot,e>$ è un monoide (di elemento neutro e), un sottoinsieme H di A tale che $e\in H$ e, per ogni $a,b\in H$, si abbia $a\cdot b\in H$ si dice *sottomonoide* di $(A, \cdot,e)$.
Se $(A,\cdot,^{-1},e)$ è un gruppo, un sottoinsieme H di A tale che $e\in H$ e, per ogni $a,b\in H$, si abbia $a\cdot b\in H$ ed $a^{-1}\in H$ si dice *sottogruppo* di $(A,\cdot,^{-1},e)$.
Se $<A,+,\cdot,0,->$ è un anello, un sottoinsieme H di A tale che $0\in H$ e, per ogni $a,b\in H$, si abbia $a\cdot b\in H$, $a+b\in H$ e $-a\in H$ si dice *sottoanello* di $<A,+,\cdot, 0,->$
Se $<A,\wedge,\vee>$ è un reticolo, un sottoinsieme H di A tale che per ogni $a,b\in H$, si abbia $a\wedge b\in H$ e $a\vee b\in H$ si dice *sottoreticolo* di $<A, \wedge,\vee>$.

Criteri per i sottogruppi.
Sia $<A,\cdot,^{-1},e>$ un gruppo, un sottoinsieme H di A è un sottogruppo di $<A,\cdot,^{-1},e>$ se e solo se per ogni $a,b\in H$ si ha $a\cdot b\in H$ ed $a^{-1}\in H$
o equivalentemente se e solo se per ogni $a,b\in H$ si ha $a\cdot b^{-1}\in H$.
Nel caso A sia finito un sottoinsieme H di A è un sottogruppo di $<A,\cdot,^{-1},e>$ se e solo se per ogni $a,b\in H$ si ha $a\cdot b\in H$.
(esercizio)

Criterio per i sottoanellli.
Sia $<A,+,\cdot,0,->$ un anello, un sottoinsieme H di A è un sottoanello di $<A,+,\cdot,0,->$ se e solo se per ogni $a,b\in H$ si ha $a-b\in H$, $a\cdot b\in H$.

Relazioni di congruenza e strutture quozienti

Def. Si considerino un insieme A, una legge di composizione interna ω di arità n su A ed una relazione di equivalenza ρ su A.
La relazione ρ si dice *compatibile con* ω se per ogni $a_1,a_2,...,a_n;b_1,b_2,...,b_n\in A$, $(a_1,b_1)\in\rho$, $(a_2,b_2)\in\rho,..., (a_n,b_n)\in\rho$ implicano $(\omega(a_1,a_2,...,a_n),\omega(b_1,b_2,...,b_n))\in\rho$.
Data una struttura algebrica $<A, \Omega>$ una relazione di equivalenza ρ su A si dice *relazione di congruenza* su A se è compatibile con ogni $\omega\in\Omega$.

Esempi.

Si consideri la struttura $<Z,+,\cdot>$, la relazione di congruenza modulo 3 è una relazione di congruenza nel senso della definizione precedente, infatti sappiamo già che è una relazione di equivalenza, inoltre se $n\equiv m \pmod 3$ ed $r\equiv s \pmod 3$ esistono $h,k\in$ tali che

n-m =3h ed
r-s=3k
e quindi sommando membro a membro le due uguaglianze si ha n+r-(m+s)=3(h+k), cioè (n+r,m+s)$\in\rho$
inoltre moltiplicando entrambi i membri della prima uguaglianza per r ed entrambi i membri della seconda per m e sommando poi membro a membro si ottiene
nr-ms=3(hr+km), cioè (nr,ms)$\in\rho$.

Si consideri la struttura <Z,+,·>, la relazione di equivalenza ρ indotta dalla partizione di Z in interi positivi che indicheremo con POS, 0, interi negativi che indicheremo con NEG, non è una relazione di congruenza, infatti risulta compatibile con il prodotto, ma non con la somma (ad esempio $(3,7)\in\rho$, $(-4,-2)\in\rho$ e $(3+(-4),7+(-2))\notin\rho$).

Osservazione Data una struttura algebrica <A, Ω>, è facile provare che l'intersezione di un numero qualsiasi di congruenze di A è una congruenza di A, inoltre la relazione universale è una congruenza, dunque, data una qualsiasi relazione binaria ρ su A, esiste sempre la minima congruenza di A contenente ρ che si dice *congruenza generata da* ρ su A. Tale congruenza risulta essere l'intersezione di tutte le congruenze su A contenenti ρ.

Consideriamo ora la struttura <Z,+,·>, la relazione di congruenza modulo 3 e l'insieme quoziente Z_3 di Z rispetto alla congruenza modulo 3, notiamo che possiamo introdurre in modo semplice una somma ed un prodotto su Z_3 definendo come somma di due classi di resti modulo 3 la classe che ha come rappresentante la somma dei rappresentanti e come prodotto di due classi di resti la classe che ha come rappresentante il prodotto dei rappresentanti.
Se consideriamo invece nella stessa struttura la relazione di equivalenza indotta dalla partizione in NEG, 0 e POS, non possiamo in modo naturale definire una operazione di somma tra questi tre classi , infatti se dicessimo la somma di due classi è la classe che ha come rappresentante la somma dei rappresentanti, non definiremmo correttamente un'operazione perché se prendiamo come rappresentante di NEG –1 e come rappresentante di POS 1 la somma NEG+POS darebbe 0, ma se scegliessimo 3 come rappresentante di POS la somma darebbe POS. Questo dipende dal fatto che la relazione non è compatibile con la somma.

Dati un insieme A, una legge di composizione interna ω di arità n su A ed una relazione di equivalenza ρ su A compatibile con ω, la funzione ω': $A/\rho\times A/\rho\times\ldots\times A/\rho$ (n volte)$\rightarrow A/\rho$ definita da $\omega'(\rho_{a_1},\rho_{a_2},\ldots,\rho_{a_n})=\rho_{\omega(a_1,a_2,\ldots,a_n)}$ è una legge di composizione interna ω' di arità n su A/ρ, detta *operazione indotta* da ω. Dobbiamo ovviamente verificare che la definizione di ω'è ben posta ovvero che $\omega'(\rho_{a_1},\rho_{a_2},\ldots,\rho_{a_n})$ non dipende dai rappresentanti scelti per le ρ-classi. Supponiamo infatti $\rho_{a_1}=\rho_{b_1}$, $\rho_{a_2}=\rho_{b_2}$,..., $\rho_{a_n}=\rho_{b_n}$ e calcoliamo $\omega'(\rho_{b_1},\rho_{b_2},\ldots,\rho_{b_n})$. Essendo ρ compatibile con ω si ha $(\omega(a_1,a_2,\ldots,a_n),\omega(b_1,b_2,\ldots,b_n))\in\rho$ e quindi $\omega'(\rho_{b_1},\rho_{b_2},\ldots,\rho_{b_n})=\rho_{\omega(b_1,b_2,\ldots,b_n)}=\rho_{\omega(a_1,a_2,\ldots,a_n)}=\omega'(\rho_{a_1},\rho_{a_2},\ldots,\rho_{a_n})$.

Def. Data una struttura algebrica <A, Ω> ed una relazione di congruenza ρ su A si dice *struttura quoziente* di A rispetto a ρ, la struttura <A/ρ, Ω'> avente come sostegno l'insieme quoziente di A rispetto a ρ e come insieme di operazioni l'insieme delle operazioni ω' indotte dalle operazioni ω di Ω.

Esempio
Se su Z_n, insieme delle classi di resti modulo n, si definisce la somma di due classi ponendo $\{r\}+\{s\}=\{r+s\}$ ed il prodotto di due classi ponendo $\{r\}\cdot\{s\}=\{r\cdot s\}$ si ottiene una struttura quoziente di $<Z,+,\cdot>$, che indicheremo con $<Z_n,+,\cdot>$; vogliamo sottolineare il fatto che le operazioni fra classi , pur essendo indicate con gli stessi segni utilizzati per le operazioni su Z sono le operazioni indotte dalle operazioni su Z.

Verificare che $<Z_n,+,\cdot>$ è un anello commutativo e con unità.
Verificare inoltre che se n non è un numero primo in tale anello ci sono dei divisori dello 0.
Verificare che $<Z_n,+,\cdot>$ è un campo se e solo se n è un numero primo (ricordarsi che dati due interi naturali r,s, esistono due interi relativi h,k tali che M.C.D(r,s)=hr+ks)

Le regole di calcolo in $<Z_n,+,\cdot>$ fanno parte della cosiddetta aritmetica modulare.
Facciamo ora alcune osservazioni sulla soluzione di equazioni a coefficienti in $<Z_n,+,\cdot>$.
Una equazione del tipo $\{a\}x+\{b\}=\{c\}$ con a primo con n ammette sempre una ed una sola soluzione. Infatti ogni classe $\{a\}$ con 1=M.C.D(a,n), ha inverso (1=M.C.D(a,n)=ha+kn per qualche intero h,k implica $\{1\}=\{h\}\{a\}+\{k\}\{n\}=\{h\}\{a\}$) e perciò risulta $x=\{a\}^{-1}\{c-b\}$.
Una equazione del tipo $\{a\}x+\{b\}=\{c\}$ con a non primo con n o non ammette soluzioni o ne ammette più di una. Infatti ogni classe $\{a\}$ con M.C.D(a,n)>1, è un divisore dello 0, cioè esiste una classe $\{d\}$ diversa da $\{0\}$ tale che $\{a\}\{d\}=\{0\}$, dunque se $\{r\}$ è una soluzione dell'equazione anche $\{r\}+\{d\}$ lo è (perché?)

Esercizio. Supponiamo di essere nell'anello delle matrici quadrate di ordine 2 ad elementi interi positivi. Cosa possiamo dire a proposito dell'esistenza e del numerosi eventuali soluzioni di un'equazione matriciale della forma AX=B?

Strutture simili ed omomorfismi

Def. Due strutture algebriche $<A_1,\Omega_1>$, $<A_2,\Omega_2>$ si dicono *simili* se esiste una funzione biunivoca τ tra Ω_1 ed Ω_2 tale che ω_1 e $\tau(\omega_1)$ abbiano la stessa arità per ogni $\omega_1\in\Omega_1$.

Def. Date due strutture algebriche $<A_1,\Omega_1>$, $<A_2,\Omega_2>$ simili, si dice *omorfismo* di $<A_1,\Omega_1>$ in $<A_2,\Omega_2>$ una funzione f di A_1 in A_2 tale che per ogni $\omega_1\in\Omega_1$ di arità n, posto $\omega_2=\tau(\omega_1)$, sia, per ogni $a_1, a_2,..., a_n\in A_1$,

$$f(\omega_1(a_1, a_2,..., a_n))=\omega_2(f(a_1),f(a_2),...,f(a_n)).$$

In breve si dice che un omorfismo è una funzione f di A_1 in A_2 che conserva le operazioni.
Un omorfismo f si dice *monomorfismo* se f è una funzione iniettiva, si dice *epimorfismo* se f è suriettiva, si dice *isomorfismo* se f è biunivoca.

Esempi

Si considerino le due strutture simili (R,+) ed (R,.) e l'applicazione f che ad ogni numero reale r associa e^r, f è un monomorfismo di (R,+) in (R,.).

Si consideri l'insieme M_n delle matrici di ordine n ad elementi reali, rispetto al prodotto di matrici e l'insieme dei numeri reali R rispetto al prodotto, la corrispondenza che associa ad ogni matrice il suo determinante è un epimorfismo di $(M_n,.)$ su (R,.).

Cosa succede di tale funzione per le strutture $(M_n,+,.)$ su $(R,+,.)$? (esercizio)

Osservazione. Se si considerano tre strutture simili $<A_1,\Omega_1>$, $<A_2,\Omega_2>$, $<A_3,\Omega_3>$ e due omorfismi f e g di $<A_1,\Omega_1>$ in $<A_2,\Omega_2>$ e di $<A_2,\Omega_2>$ in $<A_3,\Omega_3>$ rispettivamente, allora la composizione $f\cdot g$, come funzione, dei due omorfismi è un omorfismo di $<A_1,\Omega_1>$ in $<A_3,\Omega_3>$. Se f è un isomorfismo di $<A_1,\Omega_1>$ in $<A_2,\Omega_2>$, le funzione inversa di f è un isomorfismo di $<A_2,\Omega_2>$ in $<A_1,\Omega_1>$.

Osservazione. Sia f una applicazione del gruppo $<A_1,\bullet,^{-1},e_1>$ nel gruppo $<A_2,*,^{-1},e_2>$ che conservi l'operazione binaria (che sia cioè un omorfismo fra i due semigruppi $<A_1,\bullet>$ e $<A_2,*>$) allora $f(e_1)=e_2$, $f(a^{-1})=f(a)^{-1}$. Infatti preso b in A_1 si ha $f(b)=f(b\bullet e_1)=f(b)*f(e_1)=f(b)*e_2$, da cui per le leggi di cancellazione si deduce $f(e_1)=e_2$. Inoltre per ogni $a\in A_1$ si ha $f(a)*f(a)^{-1}=e_2=f(e_1)=f(a\bullet a^{-1})=f(a)*f(a^{-1})$ e ancora per la legge di cancellazione $f(a^{-1})=f(a)^{-1}$.
Sia f una applicazione del monoide $<A_1,\bullet,e_1>$ nel monoide $<A_2,*,e_2>$ che conservi l'operazione binaria allora non è detto che sia $f(e_1)=e_2$. Basta considerare il monoide $<R^+,+,0>$ dei numeri reali non negativi rispetto alla somma ed il monoide $< R^+\cup\{e\},+,e>$ avente come sostegno l'insieme dei reali non negativi con l'aggiunta dell'elemento e, rispetto alla legge di composizione data dall'usuale somma se si compongono due numeri reali, e da $e+r=r+e=r, e+e=e$. L'applicazione identica è un omorfismo di semigruppi di $<R^+,+>$ in $< R^+\cup\{e\},+>$, ma non manda l'unità del primo monoide nell'unità del secondo, non è cioè un omorfismo di monoidi.
E' facile provare che ogni epimorfismo di semigruppo di un monoide su un altro monoide risulta invece un epimorfismo di monoidi (esercizio)

Si considerino due strutture simili $<A_1,\Omega_1>$, $<A_2,\Omega_2>$ e sia f un morfismo di $<A_1,\Omega_1>$ in $<A_2,\Omega_2>$, la relazione $\ker f =\{(x,y)\in A_1\times A_1 | f(x)=f(y)\}$ è una congruenza di $<A_1,\Omega_1>$
Sappiamo già che ker f è una relazione di equivalenza, dimostriamo che è compatibile con le operazioni; sia ω_1 una qualsiasi operazione di arità n in Ω_1, e siano $(a_1,b_1), (a_2,b_2),..., (a_n,b_n) \in \ker f$, si considerino $f(\omega_1(a_1,a_2,...,a_n))$ e $f(\omega_1(b_1,b_2,...,b_n))$. Per definizione di omorfismo, detta ω_2 l'operazione in Ω_2 associata a ω_1, si ha $f(\omega_1(a_1,a_2,...,a_n))= \omega_2(f(a_1), f(a_2),...,f(a_n))$ e $f(\omega_1(b_1,b_2,...,b_n))= \omega_2(f(b_1), f(b_2),...,f(b_n))$ e dunque $(a_1,b_1), (a_2,b_2),..., (a_n,b_n) \in \ker f$ implicano $\omega_2(f(a_1), f(a_2),...,f(a_n))= \omega_2(f(b_1), f(b_2),...,f(b_n))$ da cui si ha immediatamente $f(\omega_1(a_1,a_2,...,a_n))= f(\omega_1(b_1,b_2,...,b_n))$ ovvero $(\omega_1(a_1,a_2,...,a_n),\omega_1(b_1,b_2,...,b_n)) \in \ker f$, per definizione di ker f.

Una struttura $<A, \Omega>$ e una sua struttura quoziente $<S/\rho, \Omega'>$ sono sempre simili e la *proiezione canonica* p_ρ: $A\rightarrow A/\rho$ è un epimorfismo di $<A, \Omega>$ su $<S/\rho, \Omega'>$ e $\ker p_\rho= \rho$.

Siamo ora in grado di enunciare il primo teorema di fattorizzazione degli omorfismi
Teorema. Si considerino due strutture simili $<A_1,\Omega_1>$, $<A_2,\Omega_2>$. Siano: f un omorfismo di $<A_1,\Omega_1>$ in $<A_2,\Omega_2>$, $<A_1/\rho,\Omega_1'>$ la struttura quoziente di $<A_1,\Omega_1>$ rispetto alla congruenza $\rho=\ker f$, p_ρ l'epimorfismo canonico di $<A_1,\Omega_1>$ in $<A_1/\rho,\Omega_1'>$. Allora esiste unico un omorfismo g di $<A_1/\rho,\Omega_1'>$ in $<A_2,\Omega_2>$, tale che $f= p_\rho\cdot g$. Inoltre g è un monomorfismo ed f è un epimorfismo se e solo se g è un isomorfismo.
(provare a fare la dimostrazione per esercizio, ricordandosi come viene definita la funzione g nel teorema di fattorizzazione delle applicazioni).