

CAPITOLO 2

[indice](#)

STRUTTURE ALGEBRICHE E RELAZIONALI

1. Esempi di strutture algebriche: gruppi, reticoli ed algebre di Boole

Prima di entrare nel merito della logica matematica è necessario ricordare alcune nozioni elementari di matematica senza le quali non sarebbe possibile andare avanti. Principalmente dovremo definire la nozione generale di struttura matematica e di isomorfismo tra strutture. Cominciamo con il ricordare alcuni tipi di strutture algebriche che si incontrano frequentemente: i semigrupp, i monoidi, i gruppi, gli anelli, i reticoli.

Definizione 1. Chiamiamo *semigrupp* ogni struttura algebrica $(G, \#)$ verificante la proprietà associativa

$$(x\#y)\#z = x\#(y\#z) \quad (\text{proprietà associativa})$$

Prende il nome di *monoide* ogni struttura algebrica $(G, \#, e)$ tale che $(G, \#)$ è un semigrupp ed in cui e è elemento neutro

$$x\#e = x \quad ; \quad e\#x = x \quad (e \text{ è elemento neutro}).$$

Definizione 2. Si chiama *grupp* ogni struttura algebrica $(G, \#, inv, e)$ tale che $(G, \#, e)$ è un monoide e inv è una funzione inverso, cioè

$$x \# inv(x) = e \quad ; \quad inv(x) \# x = e.$$

Nel caso in cui l'operazione $\#$ sia commutativa, cioè se per ogni $x, y \in G$ risulta $x\#y = y\#x$, il semigrupp (il monoide, il grupp) viene detto *commutativo*.

Per i gruppi a volte si usa la notazione moltiplicativa a volte quella additiva. Nel primo caso si usa un punto \cdot per denotare l'operazione binaria, si scrive x^{-1} al posto di $inv(x)$ e si usa il simbolo 1 per l'elemento neutro. Pertanto gli assiomi si scrivono al modo seguente:

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \quad (\text{proprietà associativa})$$

$$x \cdot x^{-1} = 1 \quad ; \quad x^{-1} \cdot x = 1$$

$$x \cdot 1 = x \quad ; \quad 1 \cdot x = x. \quad (1 \text{ è elemento neutro}).$$

Inoltre x^{-1} prende il nome di *inverso* di x . Quando invece si usa la notazione additiva si denota con $+$ l'operazione binaria, con $-$ l'operazione unaria e con 0 l'elemento neutro. In tale caso gli assiomi si scrivono

$$(x+y) + z = x + (y+z) \quad (\text{proprietà associativa})$$

$$x + (-x) = 0 \quad ; \quad (-x) + x = 0$$

$$x + 0 = x \quad ; \quad 0 + x = x \quad (0 \text{ è elemento neutro}).$$

Si noti che esistono operazioni in cui la proprietà associativa non è verificata. Ad esempio se $\#$ è l'elevazione a potenza allora

$$(2\#3)\#2 = 2^3 \cdot 2^3 = 2^6 \text{ mentre } 2\#(3\#2) = 2\#(3^2) = 2^9.$$

Per i gruppi commutativi si preferisce usare la notazione additiva.

Ulteriori strutture sono le seguenti.

Definizione 3. Chiamiamo *anello unitario commutativo* ogni struttura algebrica $(D, +, \cdot, 0, 1)$ tale che:

1) $(D, +, 0)$ è un grupp commutativo

2) $(D, \cdot, 1)$ è una operazione associativa e commutativa con 1 come elemento neutro

3. vale la proprietà distributiva cioè

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

Un anello unitario commutativo $(D, +, \cdot, 0, 1)$ è chiamato *campo* se $(D - \{0\}, \cdot, 1)$ è un grupp.

In ogni anello unitario commutativo risulta che:

i) $x \cdot 0 = 0$.

ii) $x \cdot (-y) = -x \cdot y$.

iii) $x \cdot (-1)$ è l'opposto di x .

iv) $(-1)^2 = 1$.

Infatti, per provare i) osserviamo che per la proprietà distributiva $x \cdot 0 = x \cdot (0+0) = x \cdot 0 + x \cdot 0$ da cui, sottraendo da entrambi i membri $x \cdot 0$, si ricava che $0 \cdot x = 0$. Per provare ii) osserviamo che $x \cdot (-y) + x \cdot y = x \cdot (-y+y) = x \cdot 0 = 0$. Le rimanenti proprietà sono ovvie.

Un'altra importante classe di strutture algebriche è quella dei reticoli e delle algebre di Boole.

Definizione 4. Chiamiamo *reticolo limitato*, o semplicemente, *reticolo*, una struttura algebrica $L = (L, \vee, \wedge, 0, 1)$ tale che, per ogni $x, y, z \in L$

(i) $x \vee y = y \vee x$; $x \wedge y = y \wedge x$ (proprietà commutativa)

(ii) $x \vee (y \vee z) = (x \vee y) \vee z$; $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ (proprietà associativa)

(iii) $0 \vee x = x$; $1 \wedge x = x$ (0 ed 1 sono elementi neutri)

(v) $x \vee x = x$; $x \wedge x = x$ (idempotenza).

Il reticolo è detto *distributivo* se

(iv) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$; $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ (proprietà distributiva).

Esempio 1. Sia L l'intervallo $[0,1]$ e poniamo

$$x \vee y = \max\{x, y\}, \quad x \wedge y = \min\{x, y\}$$

Allora $([0,1], \wedge, \vee, 0, 1)$ è un reticolo distributivo.

Esempio 2. Sia S un insieme e sia L l'insieme delle parti di S che o sono finite o coincidono con S o coincidono con \emptyset . Allora è subito visto che $(L, \cup, \cap, \emptyset, S)$ è un reticolo distributivo.

Esempio 3. La classe degli aperti di uno spazio topologico è un reticolo rispetto alle operazioni di unione e di intersezione.

Molti reticoli sono dotati di una ulteriore operazione 1-naria. Ad esempio poniamo D uguale all'insieme $\mathcal{P}(S)$ delle parti di un dato insieme S , allora è naturale considerare anche l'operazione unaria di complemento ed ottenere in tale modo la struttura $(\mathcal{P}(S), \cup, \cap, -, \emptyset, S)$. Strutture di tale tipo rientrano in una importante classe di strutture algebriche: le algebre di Boole.

Definizione 5. Chiamiamo *algebra di Boole* un reticolo distributivo L con una ulteriore operazione unaria $- : L \rightarrow L$ tale che

(v) $x \vee -x = 1$; $x \wedge -x = 0$ (terzo escluso e principio di non contraddizione)

Il principale esempio di algebra di Boole si ottiene ponendo

$$D = \{0,1\}, \quad x \vee y = \max\{x, y\}, \quad x \wedge y = \min\{x, y\}, \quad -x = 1-x.$$

Indicheremo con il simbolo **2** tale algebra.

Un altro esempio si ottiene fissando un insieme S e considerando la struttura $(\{0,1\}^S, \vee, \wedge, -, f_0, f_1)$ dove

- $f_0 : S \rightarrow \{0,1\}$ è la funzione costantemente uguale a 0,

- $f_1 : S \rightarrow \{0,1\}$ è la funzione costantemente uguale a 1

- le operazioni $\vee, \wedge, -$ sono definite ponendo, per ogni f e g in $\{0,1\}^S$

$$(f \wedge g)(x) = \min\{f(x), g(x)\}, \quad (f \vee g)(x) = \max\{f(x), g(x)\}, \quad (-f)(x) = 1-f(x).$$

Possiamo anche considerare la struttura $(\mathcal{P}(S), \cup, \cap, -, \emptyset, S)$ che anche è una algebra di Boole.

Dato un sottoinsieme X di S , chiamiamo *funzione caratteristica* di X la funzione $c_X : S \rightarrow \{0,1\}$ definita ponendo

$$c_X(x) = \begin{cases} 1 & \text{se } x \in X \\ 0 & \text{se } x \notin X \end{cases}$$

Allora è immediato provare che tale corrispondenza è un isomorfismo tra la struttura $(\mathcal{P}(S), \cup, \cap, -, \emptyset, S)$ e la struttura $(\{0,1\}^S, \vee, \wedge, -, f_0, f_1)$.

2. La nozione generale di struttura algebrica e di omomorfismo

Dopo avere ricordato alcuni esempi di strutture algebriche vogliamo fornire la nozione generale di struttura algebrica. Dato un insieme D , chiamiamo *operazione n -aria* in D ogni funzione h del prodotto cartesiano D^n in D (in breve scriveremo anche $h:D^n \rightarrow D$). Il numero di variabili a cui si applica l'operazione prende il nome di *arietà* della operazione. In generale si considerano solo operazioni binarie (come l'addizione, la moltiplicazione, l'unione, l'intersezione) oppure 1-arie (come "invertire un numero" oppure "il complemento di un insieme"). In generale si scrive $h(d_1, \dots, d_n)$ per indicare il valore assunto dall'operazione h negli elementi d_1, \dots, d_n (notazione *infissa*). Per le operazioni binarie si utilizza invece la notazione *infissa* in cui il simbolo di operazione viene messo in mezzo come ad esempio quando si scrive $3 \cdot 5$ oppure $3+4$.

Definizione 1. Prende il nome di *struttura algebrica* ogni struttura del tipo $(D, h_1, \dots, h_t, e_1, \dots, e_h)$ dove h_1, \dots, h_t sono operazioni in D ed e_1, \dots, e_h sono elementi in D .

In generale in una struttura si elencano quegli elementi e_1, \dots, e_h che per qualche motivo si ritiene debbano giocare un ruolo privilegiato. Ad esempio si dice che un gruppo è una struttura del tipo $(G, \cdot, {}^{-1}, 1)$ per evidenziare la presenza dell'elemento neutro 1. Per comodità di esposizione a volte gli elementi e_i sono chiamati *operazioni 0-arie* e prendono il nome di *costanti*. In questo caso possiamo indicare con (D, h_1, \dots, h_n) una struttura algebrica salvo poi specificare che alcune delle operazioni sono 0-arie. Assumiamo la convenzione di elencare le operazioni in ordine decrescente rispetto l'arietà.

Definizione 2. Chiamiamo *tipo* di una struttura algebrica (D, h_1, \dots, h_t) la t -pla (n_1, \dots, n_t) dove n_j è l'arietà dell'operazione h_j e dove $n_1 \geq \dots \geq n_t$.

Ad esempio, in accordo con le definizioni date nel paragrafo 9,

- i semigrupp hanno tipo (2),
- i monoidi tipo (2,0),
- i gruppi (2,1,0)
- gli anelli unitari hanno il tipo (2,2,0,0) poiché sono forniti di un prodotto, di una somma e di costanti 0 ed 1
- i reticoli hanno tipo (2,2,0,0).

Definizione 3. Siano S ed S' due strutture dello stesso tipo, chiamiamo *omomorfismo* di S in S' ogni funzione $f: D \rightarrow D'$ tale che:

- (1) $f(h_i(x_1, \dots, x_n)) = h'_i(f(x_1), \dots, f(x_n))$ ¹
- (2) $f(e_i) = e'_i$.

Diciamo che f è un *isomorfismo* se è invertibile.

In particolare diciamo che

- f è una *immersione* se è un omomorfismo iniettivo
- f è un *epimorfismo* se è suriettivo,
- f è un *endomorfismo* se è un omomorfismo di S in se stesso
- f è un *automorfismo* se è un isomorfismo di S in se stesso.

Da notare che non ha senso parlare di omomorfismi tra strutture di tipo diverso. Ad esempio non ha senso parlare di omomorfismo di un anello in un gruppo.

Problema. Dimostrare che l'inverso di un isomorfismo è ancora un isomorfismo. Dimostrare che la classe degli automorfismi di una data struttura costituisce un gruppo rispetto all'operazione di composizione.

¹ In altri termini l'immagine del composto (tramite l'operazione h_i) coincide con il composto (tramite l'operazione h'_i) delle immagini. A volte si dice anche che f *conserva* le operazioni.

Se D' è un sottoinsieme di D allora indichiamo con h/D' la restrizione di h a D' . Perché ciò abbia senso, naturalmente D' deve essere una *parte stabile* rispetto ad h , cioè deve accadere che:

$$d_1, \dots, d_n \in D' \Rightarrow h(d_1, \dots, d_n) \in D'.$$

Definizione 4. Una *sottostruttura* di una struttura algebrica $S = (D, h_1, \dots, h_n, e_1, \dots, e_n)$ è una struttura $S' = (D', h'_1, \dots, h'_n, e'_1, \dots, e'_n)$, dello stesso tipo di S , tale che:

- i) $D' \subseteq D$
- ii) $h'_i = h_i/D'$
- iii) $e'_i = e_i$.

Pertanto una sottostruttura di S si ottiene fissando una parte D' di D che sia stabile rispetto a tutte le operazioni e che contenga le costanti. Appare ancora una volta perché sia tanto importante elencare con precisione le operazioni e le costanti che si ritengono importanti nel definire una struttura. Infatti la nozione di parte stabile dipende dalle operazioni e dalle costanti che sono state esplicitate. Ad esempio indichiamo con R l'insieme dei numeri reali e consideriamo le strutture $(R, +)$, $(R, +, 0)$, $(R, +, -, 0)$. Tali strutture sono diverse tra loro poiché hanno tipi diversi. La loro diversità emerge quando si guarda alla nozione di sottostruttura. Infatti

- $([5, \infty), +)$ è una sottostruttura di $(R, +)$ ma non di $(R, +, 0)$
- $([0, \infty), +, 0)$ è una sottostruttura di $(R, +, 0)$ ma non di $(R, +, -, 0)$.

3. Esempi di strutture relazionali: relazioni d'ordine e di pre-ordine

Passiamo ora ad un altro tipo di strutture matematiche, le strutture relazionali.

Definizione 1. Siano D_1, \dots, D_n insiemi non vuoti, chiamiamo *relazione n-aria* tra gli insiemi D_1, \dots, D_n ogni sottoinsieme \mathcal{R} del prodotto cartesiano $D_1 \times \dots \times D_n$. Il numero n viene detto *arità* della relazione.

Noi siamo interessati solo al caso in cui tutti gli insiemi D_1, \dots, D_n coincidono con un unico insieme D . Le relazioni di arità 1 coincidono con i sottoinsiemi di D ed esprimono proprietà di elementi di D . Ad esempio sono relazioni unarie in N $\{n : n \text{ è pari}\}$, $\{n : n \text{ è primo}\}$ che corrispondono alla proprietà di essere pari o di essere primo. Le relazioni di arità due vengono dette *relazioni binarie*. Sono relazioni binarie $\{(n, m) \in N \times N : n \text{ è un multiplo di } m\}$, $\{(n, m) \in N \times N : n \text{ è primo con } m\}$. Un esempio di relazione di arità 3 è dato da $\{(m, x, y) \in N \times N : m = x + y/2\}$ che corrisponde alla proprietà "m è il valor medio tra x ed y". Tuttavia, come avviene per le operazioni, in genere in matematica si studiano solo le relazioni di arità 1 oppure 2. Per le relazioni binarie si usa la *notazione infissa*, cioè si scrive $x\mathcal{R}y$ per denotare che $(x, y) \in \mathcal{R}$, cioè per denotare che x ed y sono nella relazione \mathcal{R} .

Esistono diversi tipi di operazioni tra relazioni ed esiste un vero e proprio *calcolo delle relazioni*². Una operazione importante è quella di composizione che estende quella più nota di composizione di due funzioni.

Definizione 2. Date due relazioni binarie $\mathcal{R}_1 \subseteq D \times D$ e $\mathcal{R}_2 \subseteq D \times D$ chiamiamo *composizione* di \mathcal{R}_1 e \mathcal{R}_2 la relazione $\mathcal{R}_1 \circ \mathcal{R}_2 \subseteq D \times D$ definita ponendo

$$\mathcal{R}_1 \circ \mathcal{R}_2 = \{(x, z) \mid \exists y \in D \text{ tale che } x\mathcal{R}_1y \text{ e } y\mathcal{R}_2z\}.$$

Supponiamo che \mathcal{R}_1 e \mathcal{R}_2 siano relazioni funzionali. Allora fissato $x \in D$ esiste un solo y tale che $x\mathcal{R}_1y$ e d'altra parte esiste un solo $z \in D$ tale che $y\mathcal{R}_2z$. Pertanto dato x esiste un solo z tale che $(x, z) \in \mathcal{R}_1 \circ \mathcal{R}_2$. In definitiva la composizione di due relazioni funzionali è ancora una relazione funzionale.

Definizione 3. Data una relazione binaria $\mathcal{R} \subseteq X \times Y$ chiamiamo *inversa* di \mathcal{R} la relazione binaria $\mathcal{R}^{-1} \subseteq Y \times X$ definita ponendo

² Il "calcolo delle relazioni" costituisce la base teorica per un importante settore dell'informatica che si occupa dei database relazionali.

$$\mathcal{R}^{-1} = \{(y,x) \mid x\mathcal{R}y\}.$$

Di particolare importanza è la *relazione identità* $Diag(D) \subseteq D^2$ definita da

$$Diag(D) = \{(x,x) \mid x \in D\}.$$

Tale relazione viene detta anche *diagonale di D* e si comporta come elemento neutro rispetto alla composizione. Infatti è immediato che se \mathcal{R} è una relazione in D , allora

$$\mathcal{R} \circ Diag(D) = \mathcal{R} \quad ; \quad Diag(D) \circ \mathcal{R} = \mathcal{R}$$

Definizione 4. Sia \mathcal{R} una relazione binaria su di un insieme D , allora diciamo che

- \mathcal{R} è *riflessiva* se $x\mathcal{R}x \quad \forall x \in D$
- \mathcal{R} è *simmetrica* se $x\mathcal{R}y \Rightarrow y\mathcal{R}x \quad \forall x,y \in D$
- \mathcal{R} è *transitiva* se $x\mathcal{R}y$ e $y\mathcal{R}z \Rightarrow x\mathcal{R}z \quad \forall x,y,z \in D$
- \mathcal{R} è *asimmetrica* se $x\mathcal{R}y$ e $y\mathcal{R}x \Rightarrow x = y \quad \forall x,y \in D$
- \mathcal{R} è *antisimmetrica* se $x\mathcal{R}y \Rightarrow \text{non } y\mathcal{R}x \quad \forall x,y \in D$
- \mathcal{R} è *totale* o *lineare* se $x\mathcal{R}y$ oppure $y\mathcal{R}x \quad \forall x,y \in D$.

Problema. Sia D l'insieme dei numeri naturali: dire di che tipo sono le seguenti relazioni:

- $\mathcal{R} = \{(n,m) \mid n + m \leq 100\}$; $\mathcal{R} = \{(n,m) \mid n+m \leq 3100\}$;
- $\mathcal{R} = \{(n,m) \mid n+m \text{ è divisibile per } 10\}$; $\mathcal{R} = \{(n,m) \mid n-m \text{ è divisibile per } 10\}$
- $\mathcal{R} = \{(n,m) \mid |n-m| \leq 100\}$; $\mathcal{R} = \{(n,m) \mid n \text{ è un divisore di } m\}$;
- $\mathcal{R} = \{(n,m) \mid n \text{ è un multiplo di } m\}$; $\mathcal{R} = \{(n,m) \mid n^2 \leq m^2\}$.

E' possibile caratterizzare le diverse proprietà di una relazione utilizzando le operazioni tra relazioni che abbiamo definito.

Proposizione 5. Sia \mathcal{R} una relazione binaria su D , allora:

- i) \mathcal{R} riflessiva $\Leftrightarrow \mathcal{R} \supseteq Diag(D)$
- ii) \mathcal{R} simmetrica $\Leftrightarrow \mathcal{R} = \mathcal{R}^{-1}$
- iii) \mathcal{R} transitiva $\Leftrightarrow \mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$
- iv) \mathcal{R} asimmetrica $\Leftrightarrow \mathcal{R} \cap \mathcal{R}^{-1} \subseteq Diag(D)$
- v) \mathcal{R} antisimmetrica $\Leftrightarrow \mathcal{R} \cap \mathcal{R}^{-1} = \emptyset$
- vi) \mathcal{R} totale se $\mathcal{R} \cup \mathcal{R}^{-1} = D \times D$.

Dim. Si lascia come esercizio. □

Definizione 6. Una relazione binaria è chiamata:

- *pre-ordine* se è riflessiva e transitiva
- *ordine* se è una relazione di pre-ordine asimmetrica
- *ordine stretto* se è una relazione transitiva e antisimmetrica
- *ordine lineare* se è una relazione di ordine totale.

4. Equivalenze, partizioni e quozienti

Tra le relazioni binarie rivestono particolare importanza le relazioni d'ordine e le relazioni di equivalenza.

Definizione 1. Una relazione binaria \mathcal{R} su di un insieme D è chiamata *equivalenza* se è riflessiva, simmetrica e transitiva.

Una relazione di equivalenza si indica in genere con il simbolo \equiv che ricorda il simbolo di eguaglianza. L'importanza di tale nozione deriva dal fatto che è strettamente legata al processo di astrazione cioè al processo per cui si astrae da una particolare proprietà degli oggetti che si esaminano. Ciò comporta che vengono considerati "praticamente uguali", cioè equivalenti, due oggetti che si distinguono solo per tale proprietà. Ad esempio se non si considerano importanti le dimensioni di una fotografia ma solo le immagini che essa contiene, allora il considerare equivalenti una foto ed un suo ingrandimento equivale a fare astrazione dalle dimensioni. Se ci riferiamo all'insieme dei triangoli e non si interessa la particolare posizione occupata da un triangolo, allora saremo portati a considerare equivalenti due triangoli che siano sovrapponibili tramite un movimento.

Problema. Nell'insieme dei numeri reali poniamo $x\mathcal{R}_1y$ se x differisce da y per meno di un decimo. Poniamo poi $x\mathcal{R}_2y$ se x ed y hanno la stessa parte intera. Dire se le due relazioni ora definite sono relazioni di equivalenza.

Problema. Sia Tr l'insieme dei triangoli del piano e consideriamo le seguenti relazioni:

- $x\mathcal{R}_1y$ se i due triangoli x ed y hanno lo stesso perimetro
- $x\mathcal{R}_2y$ se i due triangoli x ed y hanno la stessa area
- $x\mathcal{R}_3y$ se x ha i vertici sopra i lati di y
- $x\mathcal{R}_4y$ se i due triangoli hanno gli stessi angoli (sono simili)
- $x\mathcal{R}_5y$ se esiste una traslazione che porta x in y
- $x\mathcal{R}_6y$ se le relative aree differiscono di un millimetro quadrato.

Dire quali di tali relazioni sono relazioni di equivalenza.

La nozione di equivalenza è strettamente collegata a quella di partizione.

Definizione 2. Una classe Π di sottoinsiemi di S è detta una *partizione* di S se:

- gli elementi di Π sono a due a due disgiunti,
- l'unione degli elementi di Π coincide con S .

Gli elementi di Π vengono anche chiamati *classi*.

In altre parole Π è una partizione di S se rappresenta un modo di dividere gli elementi di S in tante parti separate. Ad esempio se S è l'insieme dei numeri interi, P è l'insieme dei numeri pari e D è l'insieme dei numeri dispari, allora una partizione di S si ottiene ponendo $\Pi = \{P, D\}$.

Teorema 3. Sia \equiv una relazione di equivalenza in un insieme S ed indichiamo, per ogni $z \in S$, con $[z]$ la classe $\{z' \in S \mid z' \equiv z\}$, cioè l'insieme degli elementi equivalenti a z . Allora l'insieme $\Pi = \{[z] \mid z \in S\}$ è una partizione. Viceversa, sia Π una partizione di S e definiamo la relazione binaria \equiv ponendo $x \equiv y$ se e solo se x ed y appartengono allo stesso elemento in Π . Allora \equiv è una relazione di equivalenza.

Dim. Supponiamo che \equiv sia una relazione di equivalenza. Per la proprietà riflessiva $z \in [z]$ e ciò prova che ogni elemento di S appartiene ad una classe in Π . Se poi $[z]$ e $[z']$ sono due classi e $[z] \neq [z']$, allora non può esistere un elemento x comune a tali classi. Infatti in tale caso risulterebbe che $z \equiv x$ e $z' \equiv x$ e quindi per la proprietà simmetrica $z \equiv x$ e $x \equiv z'$ e quindi per la proprietà transitiva $z \equiv z'$ (in contrasto con l'ipotesi $[z] \neq [z']$).

Sia Π una partizione. Che \equiv sia riflessiva deriva dal fatto che per ogni x esiste $X \in \Pi$ tale che $x \in X$. Pertanto $x \equiv x$. La proprietà simmetrica è immediata. Per provare la proprietà transitiva supponiamo che $x \equiv y$ e $y \equiv z$, cioè che esistono X_1 ed X_2 in Π tali che $x, y \in X_1$ e $y, z \in X_2$. Allora X_1 ed X_2 hanno in comune l'elemento y . Poiché due elementi distinti di Π sono disgiunti, ciò comporta che $X_1 = X_2$ è quindi che x e z appartengono ad uno stesso elemento di Π . Allora $x \equiv z$ e pertanto \equiv è una relazione di equivalenza. \square

Ogni classe $[z]$ è chiamata *classe completa di equivalenza* e z viene chiamato *elemento rappresentativo* di tale classe, la partizione Π è chiamata *quoziente di S modulo \equiv* e si indica con S/\equiv .

Equivalenza e processo di astrazione. Il significato della proposizione ora dimostrata è che il processo di astrazione (a cui è associata una data relazione di equivalenza) induce ad identificare oggetti che prima si ritenevano diversi e quindi a costruirsi un nuovo mondo, il quoziente, popolato da "oggetti astratti". Ogni oggetto astratto rappresenta, in un certo senso, una intera classe di oggetti equivalenti tra loro. Nell'esempio delle fotografie di cui si è parlato prima si dirà che la stessa fotografia f è apparsa su giornali diversi e ciò significa che si è costruito un nuovo ente astratto che è diverso dalle singole fotografie presenti sui singoli giornali.

Un esempio di carattere più matematico si ottiene interpretando i numeri interi come passi da effettuare, a partire da una posizione iniziale, lungo un percorso ed in una data direzione. Ad esempio il numero 5 rappresenta il fare 5 passi avanti, il numero -5 il fare 5 passi indietro. Allora se si suppone che i passi di tale percorso vengano fatti sui vertici di un pentagono appare naturale identificare due numeri che rappresentano cammini in cui si giunge alla stessa posizione. Ad esempio il fare 5 passi equivale a fare 0 passi, il fare 9 passi equivale a fare 4 passi, e così via. In definitiva, se x e y differiscono per un multiplo di 5, facendo x passi si perviene alla stessa posizione che facendo y passi. Allora nell'insieme dei numeri interi relativi Z introduciamo una relazione di equivalenza \equiv definita da:

$$x \equiv y \Leftrightarrow x-y \text{ è un multiplo di } 5.$$

Ad esempio $0 \equiv 5$, $1 \equiv 6$, $2 \equiv 7$, . . . Tale relazione è chiamata *congruenza modulo 5*. Il relativo quoziente viene indicato con $Z/5$ e contiene solo cinque classi. Infatti è immediato che $[0]$, $[1]$, $[2]$, $[3]$, $[4]$ sono classi distinte ma che $[5] = [0]$, $[6] = [1]$, $[7] = [2]$ e così via. Gli elementi di tale classe vengono anche chiamati interi modulo 5. È chiaro che se si tenesse conto anche di fattori diversi da quelli della posizione raggiunta, ad esempio dell'energia o del tempo occorrenti ad eseguire n passi, allora una tale identificazione non sarebbe giustificata. Il quoziente ottenuto è proprio il frutto del fatto che si è fatto astrazione da tali aspetti.

Un modo per ottenere relazioni di equivalenza è quello di chiamare equivalenti due oggetti o persone che hanno in comune alcune proprietà. Ad esempio se la proprietà è avere una certa altezza possiamo chiamare equivalenti due persone che hanno la stessa altezza. Se oltre l'altezza consideriamo anche il sesso allora possiamo considerare equivalenti due persone che abbiano la stessa altezza e lo stesso sesso e così via. Se indichiamo con $f(x)$ le proprietà di cui gode x e con $f(y)$ le proprietà di cui gode y allora viene definita la relazione

$$x \equiv y \Leftrightarrow f(x) = f(y).$$

Questo fatto suggerisce la seguente proposizione.

Proposizione 4. Sia $f: D \rightarrow D'$ una funzione di un insieme D in un insieme D' , allora la relazione \equiv_f definita ponendo

$$x \equiv_f y \Leftrightarrow f(x) = f(y)$$

è una relazione di equivalenza che viene detta il *nucleo* di f . Il quoziente di D modulo tale relazione è equipotente al codominio di f .

È anche interessante osservare che ogni relazione di equivalenza può essere considerata come ottenuta in tale modo.

Proposizione 5. Sia D un insieme, \equiv una relazione di equivalenza in D e D' il relativo quoziente. Allora la funzione $f: D \rightarrow D'$ definita ponendo $f(x) = [x]$ è una funzione il cui nucleo coincide con \equiv .

5. Nozione generale di struttura relazionale

Siamo ora pronti a dare la nozione generale di struttura relazionale.

Definizione 1. Chiamiamo *struttura relazionale* una struttura $(D, \mathcal{R}_1, \dots, \mathcal{R}_m, e_1, \dots, e_h)$ dove $\mathcal{R}_1, \dots, \mathcal{R}_m$ sono relazioni in D ed e_1, \dots, e_h sono elementi di D .

Anche per le strutture relazionali si parlerà di *tipo* inteso come lista delle arità delle relazioni.

Ad esempio dato un insieme S , $(P(S), \subseteq, \emptyset, S)$ è una struttura relazionale del tipo $(2,0,0)$.

Definizione 2. Siano S ed S' due strutture relazionali dello stesso tipo, chiamiamo *omomorfismo* di S in S' ogni funzione $f: D \rightarrow D'$ tale che:

- (1) $f(e_i) = e'_i$;
- (2) $(x_1, \dots, x_n) \in \mathcal{R}_i \Rightarrow (f(x_1), \dots, f(x_n)) \in \mathcal{R}'_i$.

Inoltre diciamo che

- f è un *omomorfismo pieno* se vale anche la converso di (2), cioè

- (3) $(x_1, \dots, x_n) \in \mathcal{R}_i \Leftrightarrow (f(x_1), \dots, f(x_n)) \in \mathcal{R}'_i$.

- f è una *immersione* se è un omomorfismo pieno iniettivo

- f è un *isomorfismo* se è invertibile ed il suo inverso è ancora un omeomorfismo.

La nozione di omomorfismo “pieno” non viene data per le strutture algebriche. Nel seguito vedremo perché invece per le strutture relazionali tale nozione è importante. Si noti anche la differenza tra i due tipi di strutture anche per quanto riguarda la nozione di immersione e di isomorfismo. Come per le strutture algebriche, abbiamo anche le seguenti definizioni:

- f è un *epimorfismo* se è suriettivo,

- f è un *endomorfismo* se è un omomorfismo di S in se stesso

- f è un *automorfismo* se è un isomorfismo di S in se stesso.

Proposizione 3. Le seguenti asserzioni sono equivalenti:

- a) f è un isomorfismo
- b) f è un omomorfismo pieno invertibile.

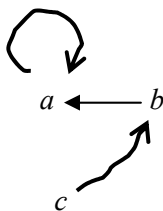
Dim. Sia f un isomorfismo, e supponiamo che $(f(x_1), \dots, f(x_n)) \in \mathcal{R}'_i$. Allora, essendo f^{-1} un omomorfismo, sarà anche $(f^{-1}f(x_1), \dots, f^{-1}f(x_n)) \in \mathcal{R}_i$ e quindi $(x_1, \dots, x_n) \in \mathcal{R}_i$. Pertanto, valendo (4), f è un omomorfismo pieno.

Supponiamo ora che f sia un omomorfismo pieno invertibile e che $(y_1, \dots, y_n) \in \mathcal{R}'_i$. Allora il fatto che f sia suriettiva assicura l'esistenza di x_1, \dots, x_n in D tali che $f(x_i) = y_i$. Pertanto sappiamo che $(f(x_1), \dots, f(x_n)) \in \mathcal{R}'_i$. Per la (4) da ciò si ricava che $(x_1, \dots, x_n) \in \mathcal{R}_i$ e quindi che $(f^{-1}(y_1), \dots, f^{-1}(y_n)) \in \mathcal{R}_i$. In conclusione f^{-1} è un omomorfismo e quindi f è un isomorfismo. \square

Si osservi che l'ipotesi di pienezza è essenziale poiché esistono omomorfismi invertibili che non sono isomorfismi. Per esaminare il fenomeno consideriamo strutture relazionali che hanno una semplice rappresentazione grafica.

Definizione 4. Una struttura relazionale (D, \mathcal{R}) con \mathcal{R} relazione binaria viene detta *grafo*.

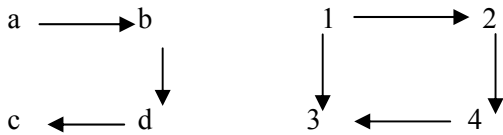
Un grafo si rappresenta sul piano euclideo fissando per ogni elemento di D un punto e tracciando, per ogni coppia di punti p_1 e p_2 una freccia che parte da p_1 e raggiunge p_2 ogni volta che la coppia (p_1, p_2) corrisponde a due elementi di D che stanno nella relazione \mathcal{R} . Ad esempio, se $D = \{a, b, c\}$ ed $\mathcal{R} = \{(a, a), (b, a), (c, b)\}$, allora rappresentiamo il grafo al modo seguente:



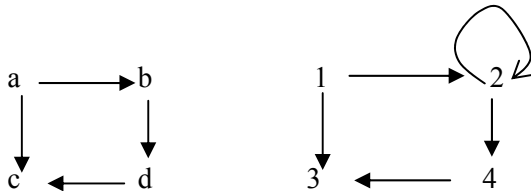
Consideriamo ora i due grafi



e sia f la funzione invertibile definita da $f(a) = 1, f(b) = 2, f(c) = 3, f(d) = 4$. Allora è immediato che f è un isomorfismo. Proviamo ora a togliere una coppia, cioè una freccia al primo grafo ottenendo



E' evidente che f pur continuando ad essere un omomorfismo, non è più pieno e quindi non è un isomorfismo. Ciò in quanto pur essendo $f(a) = 1$ in relazione con $f(c) = 3$ non risulta che a è in relazione con c . Similmente proviamo ad aggiungere la coppia $(2,2)$ al secondo grafo. Si ottiene la coppia di grafi



Anche in tale caso la funzione f pur essendo un omomorfismo non è un omomorfismo pieno e quindi non è un isomorfismo. Infatti $f(b) = 2$ ma pur essendo 2 in relazione con 2, b non è in relazione con b .

Più in generale se si considerano due grafi (S_1, \mathcal{R}_1) e (S_2, \mathcal{R}_2) e se $f : S_1 \rightarrow S_2$ è un omomorfismo allora:

- a) se si sottraggono coppie, cioè frecce, al grafo (S_1, \mathcal{R}_1) f continua ad essere un omomorfismo
- b) se si aggiungono coppie, cioè frecce, al grafo (S_2, \mathcal{R}_2) , f continua ad essere un omomorfismo.

Esempio. Dato un insieme finito S , consideriamo gli insiemi ordinati $(P(S), \subseteq, \emptyset)$ e $(N, \leq, 0)$. Allora la funzione $f : (P(S), \subseteq, \emptyset)$ che associa ad ogni $X \in P(S)$ il numero dei suoi elementi è un omomorfismo di $(P(S), \subseteq, \emptyset)$ in $(N, \leq, 0)$. Tale omomorfismo non è pieno. Infatti se X ha meno elementi di Y non è detto che X sia contenuto in Y .

Esempio. Consideriamo i voti che possono essere assegnati all'università e la corrispondente struttura ordinata $(\{1,2,\dots,30\}, \leq, 18, 30)$. Gli elementi 18 e 30 sono stati esplicitati in quanto giocano un ruolo particolare. Consideriamo i voti che possono essere assegnati a scuola e la corrispondente struttura ordinata $(\{1,2,\dots,10\}, \leq, 6, 10)$. Allora la funzione $f(n) = 3 \cdot n$ è un omomorfismo di $(\{1,2,\dots,10\}, \leq, 6, 10)$ in $(\{1,2,\dots,30\}, \leq, 18, 30)$ poiché

$$n \leq m \Rightarrow f(n) \leq f(m)$$

$$f(6) = 18$$

$$f(10) = 30.$$

6. Congruenze e quozienti in una struttura algebrica.

Se si considera una relazione di equivalenza \equiv in una struttura algebrica $S = (D, h_1, \dots, h_n, e_1, \dots, e_k)$ è possibile tentare di costruire una nuova struttura algebrica sull'insieme quoziente $D' = D/\equiv$ semplicemente operando sulle classi. Ad esempio consideriamo l'anello $(Z, +, \cdot, -, 0, 1)$ dell'anello degli interi e, dato un intero m , esaminiamo la congruenza modulo m che si ottiene ponendo

$$x \equiv y \Leftrightarrow x - y \text{ è un multiplo di } m.$$

Detto Z/m l'insieme delle classi di equivalenza, è possibile definire la somma di due classi X ed Y negli interi modulo m al modo seguente

- si prenda un elemento x in X
- si prenda un elemento y in Y
- si consideri la classe Z contenente $x+y$.

La classe Z ottenuta in tale modo viene chiamata *somma* di X ed Y . In altre parole si può porre

$$[x]+[y]=[x+y].$$

Ora non è detto che un tale modo di procedere sia corretto. Infatti potrebbe accadere che se scelgo in X ed in Y due elementi x' ed y' diversi da x ed y , allora $x'+y'$ dia luogo ad una classe X' diversa da X . In tale caso il risultato dell'operazione dipenderebbe dal modo come viene eseguita. Fortunatamente in questo esempio ciò non accade poiché si prova che

$$x \equiv x' \text{ e } y \equiv y' \Rightarrow x+y \equiv x'+y'$$

Infatti se $x-x'$ è dei tipo $n \cdot m$, $y-y'$ è del tipo $n' \cdot m$, allora

$$(x+y)-(x'+y') = x-x'+y-y' = n \cdot m + n' \cdot m = (n+n') \cdot m$$

e quindi $x+y \equiv x'+y'$. Quando è verificata l'implicazione sopra data si dice che \equiv è compatibile con $+$.

Definizione 1. Una relazione di equivalenza \equiv in un insieme D si dice *compatibile* con una operazione n -aria h se

$$x_1 \equiv x'_1, \dots, x_n \equiv x'_n \Rightarrow h(x_1, \dots, x_n) \equiv h(x'_1, \dots, x'_n).$$

Una *congruenza* in una struttura algebrica $S = (D, h_1, \dots, h_m, e_1, \dots, e_h)$ è una relazione di equivalenza compatibile con tutte le operazioni in tale struttura.

Esercizio. Consideriamo in $(Z, +, -, \cdot, 0, 1)$ la relazione \equiv definita al modo seguente:

$$x \equiv y \Leftrightarrow x \text{ ed } y \text{ hanno gli stessi divisori primi.}$$

Dimostrare che tale relazione è di equivalenza. Dire se è compatibile con la somma ed il prodotto.

Esercizio. Sia $ass : Z \rightarrow Z$ la funzione "valore assoluto" e consideriamo la struttura algebrica in $(Z, +, -, \cdot, ass, 0, 1)$. Dire se l'equivalenza modulo m è una congruenza di tale struttura.

Definizione 2. Sia \equiv una congruenza in S , allora il *quoziente modulo \equiv* di S si definisce come la struttura $(D', h'_1, \dots, h'_n, e'_1, \dots, e'_h)$ dello stesso tipo di S tale che

- D' è uguale al quoziente di D modulo \equiv ,
- $h'_i([x_1], \dots, [x_i]) = [h_i(x_1, \dots, x_i)]$,
- $e'_j = [e_j]$.

Riferendoci ad un esempio precedente, assumiamo che $\mathcal{A} = (Z, +, 0)$ e che \equiv sia la congruenza modulo 5. Allora il quoziente è costituito dall'insieme $Z/\equiv = \{[0], \dots, [4]\}$, dall'operazione di somma di classi e dalla costante $[0]$.

Teorema 3. (Primo teorema di omomorfismo). Sia \equiv una congruenza nella struttura algebrica S e sia S' il relativo quoziente. Allora l'applicazione $cl : D \rightarrow D/\equiv$ che associa ad ogni $x \in D$ la classe $cl(x) = [x]$ è un epimorfismo di S su S' (detto *epimorfismo canonico*).

Dim. Per provare che cl è un omomorfismo osserviamo che

$$h'_i(cl(a_1), \dots, cl(a_n)) = h'_i([a_1], \dots, [a_n]) = [h_i(a_1, \dots, a_n)] = cl(h_i(a_1, \dots, a_n)).$$

Inoltre $c'_j = [c_j] = cl(c_j)$. E' evidente che cl è suriettivo. □

Teorema 4. (Secondo teorema di omomorfismo). Sia f un omomorfismo della struttura algebrica S nella struttura algebrica S' . Allora

- a) $f(D)$ è una parte stabile e quindi definisce una sottostruttura S_f di S'
- b) il nucleo di f è una congruenza in S che indichiamo con \equiv_f
- c) la funzione $g : D/\equiv_f \rightarrow S'$ definita dal porre $g([x]) = f(x)$ è una immersione del quoziente S/\equiv_f in S'
- d) la funzione $g : D/\equiv_f \rightarrow f(D)$ è un isomorfismo tra S/\equiv_f ed S_f .

Dim. a) Sia h_i' una operazione in S' e y_1, \dots, y_n elementi di $f(D)$. Allora esistono x_1, \dots, x_n in D tali che $f(x_i) = y_i$. Pertanto

$$h_i'(y_1, \dots, y_n) = h_i'(f(x_1), \dots, f(x_n)) = f(h_i(x_1, \dots, x_n))$$

dove h_i è l'operazione in S corrispondente ad h_i' . Ciò prova che $h_i'(y_1, \dots, y_n) \in f(D)$.

b) Supponiamo che $x_1 \equiv_f y_1, \dots, x_n \equiv_f y_n$, cioè che $f(x_1) = f(y_1), \dots, f(x_n) = f(y_n)$. Allora

$$f(h_i(x_1, \dots, x_n)) = h_i'(f(x_1), \dots, f(x_n)) = h_i'(f(y_1), \dots, f(y_n)) = f(h_i(y_1, \dots, y_n)).$$

Ciò prova che $h_i(x_1, \dots, x_n) \equiv_f (h_i(y_1, \dots, y_n))$. La rimanente parte del teorema si dimostra similmente. \square

Nota: Algebra Universale. Diremo che una nozione o un teorema è *di carattere universale* se si riferisce a tutte le possibili strutture. Il ramo della matematica che si occupa delle nozioni di carattere universale prende il nome di *Algebra universale*. Per fare un esempio, la nozione di sottogruppo normale non è di carattere universale in quanto la sua definizione richiede la nozione di inverso che è tipica dei gruppi. Tuttavia in teoria dei gruppi si vede che tale nozione è equivalente a quella di congruenza che invece è di carattere universale. Naturalmente è preferibile, fino a quando è possibile, procedere con nozioni e risultati di carattere universale in modo che i risultati ottenuti si possano applicare a tutti i tipi di strutture.

7. Congruenze e quozienti nelle strutture relazionali.

Se si considera una relazione di equivalenza \equiv in un insieme D in cui è definita una relazione binaria \mathcal{R} , è possibile tentare di estendere tale relazione all'insieme quoziente $D' = D/\equiv$. Un modo per fare questo è definire \mathcal{R}' ponendo

$$([x_1], \dots, [x_t]) \in \mathcal{R}' \Leftrightarrow (x_1, \dots, x_t) \in \mathcal{R}.$$

In altre parole diciamo che le classi $[x_1], \dots, [x_t]$ sono nella relazione \mathcal{R}' se i relativi elementi rappresentativi x_1, \dots, x_t sono nella relazione \mathcal{R} . Perché una tale definizione vada bene, l'essere in relazione per le classi non deve dipendere dagli elementi rappresentativi che vengono scelti in ciascuna classe. In altre parole, deve succedere che

$$d_1 \equiv c_1, \dots, d_n \equiv c_n \Rightarrow (d_1, \dots, d_n) \in \mathcal{R} \text{ se e solo se } (c_1, \dots, c_n) \in \mathcal{R}.$$

Definizione 1. Una relazione di equivalenza \equiv è *compatibile con una relazione n-aria* \mathcal{R} se risulta:

$$d_1 \equiv c_1, \dots, d_n \equiv c_n \Rightarrow (d_1, \dots, d_n) \in \mathcal{R} \text{ se e solo se } (c_1, \dots, c_n) \in \mathcal{R}.$$

Una *congruenza* in una struttura relazionale $S = (D, \mathcal{R}_1, \dots, \mathcal{R}_m, e_1, \dots, e_h)$ è una relazione di equivalenza compatibile con tutte le relazioni in tale struttura.

Ad esempio consideriamo la struttura (Z, \leq) dove Z è l'insieme dei numeri interi ed \leq la relazione d'ordine usuale. Consideriamo in tale struttura la congruenza \equiv modulo 5. Allora $6 \equiv 1, 5 \equiv 5$ ma pur essendo $1 < 5$ non è vero che $6 < 5$. Pertanto la congruenza modulo 5 non è compatibile con l'ordinamento.

Definizione 2. Sia \equiv una congruenza in S , allora il *quoziente modulo* \equiv di S si definisce come la struttura $(D', \mathcal{R}'_1, \dots, \mathcal{R}'_m, c'_1, \dots, c'_h)$ dello stesso tipo di S tale che

- D' è uguale al quoziente di D modulo \equiv ,

- $\mathcal{R}'_i = \{([x_1], \dots, [x_r]) \mid (x_1, \dots, x_r) \in \mathcal{R}_i\}$

- $e'_j = [e_j]$.

Teorema 3. (Primo teorema di omomorfismo). Sia \equiv una congruenza nella struttura relazionale S e sia S' il relativo quoziente. Allora l'applicazione $cl : D \rightarrow D/\equiv$ che associa ad ogni $x \in D$ la classe $cl(x) = [x]$ è un epimorfismo pieno di S su S' (detto *epimorfismo canonico*).

Il nucleo di tale omomorfismo coincide con \equiv .

Dim. Per provare che f è un omomorfismo osserviamo che

$$c'_j = [c_j] = cl(c_j)$$

e

$$(cl(a_1), \dots, cl(a_n)) \in \mathcal{R}_i' \Leftrightarrow ([a_1], \dots, [a_n]) \in \mathcal{R}_i' \Leftrightarrow (a_1, \dots, a_n) \in \mathcal{R}_i.$$

E' evidente che cl è suriettivo. □

Teorema 4. (Secondo teorema di omomorfismo). Sia f un omomorfismo pieno della struttura relazionale S nella struttura relazionale S' . Allora

- a) il nucleo di f è una congruenza in S che indichiamo con \equiv_f
- b) la funzione $g : D/\equiv_f \rightarrow D'$ definita dal porre $g([x]) = f(x)$ è una immersione del quoziente S/\equiv_f in S'
- c) la funzione $g : D/\equiv_f \rightarrow f(D)$ è un isomorfismo tra S/\equiv_f ed S_f .

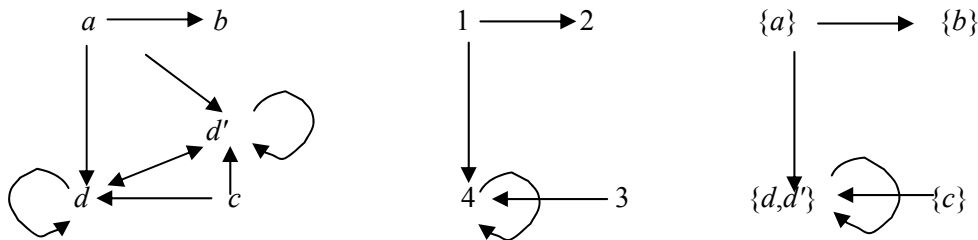
Dim. a) Siano \mathcal{R}_i e \mathcal{R}_i' due relazioni, allora

$$(x_1, \dots, x_n) \in \mathcal{R}_i \Leftrightarrow (f(x_1), \dots, f(x_n)) \in \mathcal{R}_i' \Leftrightarrow (f(y_1), \dots, f(y_n)) \in \mathcal{R}_i' \Leftrightarrow (y_1, \dots, y_n) \in \mathcal{R}_i.$$

La rimanente parte del teorema è ovvia. □

Ad esempio consideriamo i due grafi

$\mathcal{R}_1 = \{(a,b), (a,d'), (a,d), (d,d), (d',d'), (d',d), (d,d'), (c,d), (c,d')\}$ e $\mathcal{R}_2 = \{(1,2), (1,4), (3,4), (4,4)\}$ negli insiemi $D_1 = \{a,b,c,d,d'\}$ e $D_2 = \{1,2,3,4\}$ che rappresentiamo con le prime due figure seguenti



Sia $f: \{a, b, c, d, d'\} \rightarrow \{1,2,3,4\}$ la funzione definita ponendo:

$$\begin{aligned} f(a) &= 1, \\ f(b) &= 2, \\ f(c) &= 3, \\ f(d) &= f(d') = 4. \end{aligned}$$

E' immediato provare che tale funzione è un omomorfismo pieno. La congruenza indotta da f determina un quoziente tale che:

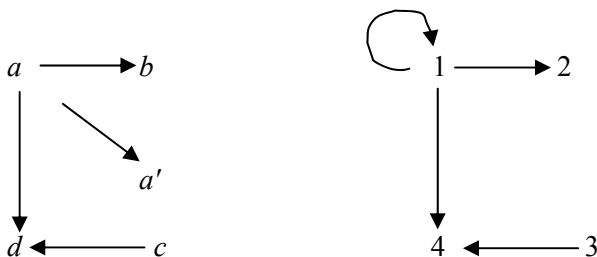
- il dominio coincide con l'insieme delle classi di equivalenza $D = \{\{a\}, \{b\}, \{c\}, \{d,d'\}\}$
- la relazione \mathcal{R} coincide con $\{(\{a\}, \{b\}), (\{a\}, \{d,d'\}), (\{d,d'\}, \{d,d'\}), (\{c\}, \{d,d'\})\}$.

Tale quoziente è rappresentato dalla terza figura ed è evidentemente isomorfo a (D_2, \mathcal{R}_2) .

Nota. L'ipotesi di pienezza è essenziale poiché esistono omomorfismi il cui nucleo non è una congruenza.

Ad esempio consideriamo i due grafi

$$\mathcal{R}_1 = \{(a,b), (a,a'), (a,d), (c,d)\} \text{ e } \mathcal{R}_2 = \{(1,1), (1,2), (1,4), (3,4)\}$$



e sia f la funzione definita da $f(a) = 1, f(a') = 1, f(b) = 2, f(c) = 3, f(d) = 4$. Allora è immediato che f è un omomorfismo. Tale omomorfismo non è pieno poiché $f(a) \in \mathcal{R}_2$ mentre a non è in relazione \mathcal{R}_1

con a . Inoltre risulta che $a \equiv_f a'$, $a \mathcal{R}_1 d$ mentre non è vero che $a' \mathcal{R}_1 d$. Pertanto il nucleo \equiv_f non è una congruenza. In altre parole, se dovessi definire il grafo quoziente nell'insieme $\{\{a, a'\}, \{b\}, \{c\}, \{d\}\}$ delle classi, non sarebbe determinato se mettere la classe $\{a, a'\}$ in relazione con $\{d\}$ (in quanto a è in relazione con d) oppure no (in quanto a' non è in relazione con d).

Esercizio. Dimostrare che $\{2, 4, 6, 8\}$ e $\{6, 8, 9, 10\}$ sono isomorfi rispetto la struttura d'ordine usuale.

8. Omomorfismi e congruenze nelle strutture d'ordine e nei reticoli.

Esiste una forte relazione tra

- la nozione di preordine
- la nozione d'ordine
- la nozione di ordine stretto
- la nozione di reticolo.

Infatti valgono le seguenti proposizioni.

Proposizione 1. Sia \leq una relazione di pre-ordine in un insieme S . Allora la relazione \equiv ottenuta ponendo

$$x \equiv x' \Leftrightarrow x \leq x' \text{ and } x' \leq x$$

è una congruenza in (S, \leq) . Il relativo quoziente è un insieme ordinato.

Dim. Assumiamo che $x \equiv x'$ e $y \equiv y'$, dobbiamo provare che

$$x \leq y \Leftrightarrow x' \leq y'$$

Ora se $x \leq y$ poiché $x \equiv x'$ e $y \equiv y'$ implicano che $x' \leq x$ e $y \leq y'$ risulta che $x' \leq x \leq y \leq y'$. Pertanto per la proprietà transitiva $x' \leq y'$. Allo stesso modo si prova che $x' \leq y'$ implica $x \leq y$.

Il fatto che \equiv sia una congruenza permette di definire il quoziente S/\equiv in cui si pone

$$[x] \leq [y] \Leftrightarrow x \leq y.$$

Per provare che la relazione definita nel quoziente è una relazione d'ordine osserviamo che

$$[x] \leq [y] \text{ e } [y] \leq [x] \Rightarrow x \leq y \text{ e } y \leq x \Rightarrow x \equiv y \Rightarrow [x] = [y].$$

Proposizione 2. Dato una struttura d'ordine (S, \leq) è possibile definire una struttura d'ordine stretto $(S, <)$ "sottraendo la diagonale", cioè ponendo

$$x < y \Leftrightarrow x \leq y \text{ and } x \neq y.$$

Dato una struttura d'ordine stretto $(S, <)$ è possibile definire una struttura d'ordine (S, \leq) "aggiungendo la diagonale", cioè ponendo

$$x \leq y \Leftrightarrow x < y \text{ oppure } x = y.$$

Infine i reticoli coincidono con particolari insiemi ordinati. Infatti vale il seguente teorema di cui omettiamo la dimostrazione.

Teorema 3. Sia $(L, \vee, \wedge, 0, 1)$ un reticolo limitato e definiamo una relazione d'ordine ponendo

$$x \leq y \Leftrightarrow \text{se } x \wedge y = x.$$

Allora $(L, \leq, 0, 1)$ è un insieme ordinato tale che $\text{Inf}\{x, y\} = x \wedge y$ e $\text{Sup}\{x, y\} = x \vee y$ e dove 0 ed 1 sono rispettivamente il minimo ed il massimo elemento.

Viceversa, sia $(L, \leq, 0, 1)$ un insieme ordinato con un elemento minimo 0 ed un elemento massimo 1 e supponiamo che per ogni $x, y \in L$ esista l'estremo superiore $x \vee y$ e l'estremo inferiore $x \wedge y$. Allora $(L, \vee, \wedge, 0, 1)$ è un reticolo tale che

$$x \leq y \Leftrightarrow x \wedge y = x.$$

Esaminiamo ora le nozioni di congruenza e di omomorfismo in rapporto ai diversi modi di considerare un insieme ordinato. Ricordiamo che nel caso di relazioni d'ordine un omomorfismo di (S, \leq) in (S', \leq') è una funzione $f: S \rightarrow S'$ crescente, cioè

$$x \leq y \Rightarrow f(x) \leq f(y)$$

Un omomorfismo di $(S, <)$ e $(S', <')$ è una funzione $f: S \rightarrow S'$ strettamente crescente, cioè

$$x < y \Rightarrow f(x) < f(y).$$

Nel caso in cui tali insiemi ordinati siano anche reticoli, un omomorfismo di (S, \vee, \wedge) in (S', \vee, \wedge) è una funzione f tale che

$$f(x \wedge y) = f(x) \wedge f(y) \quad ; \quad f(x \vee y) = f(x) \vee f(y).$$

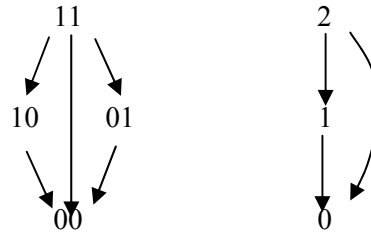
Consideriamo ad esempio l'insieme $P(\{a, b\})$ costituito dai quattro elementi $\emptyset, \{a\}, \{b\}, \{a, b\}$ in cui è definita la relazione di inclusione. Consideriamo anche l'insieme $\{0, 1, 2\}$ rispetto alla relazione d'ordine usuale. Nelle figure sotto indicate indichiamo il grafo di queste due strutture relazionali (relative all'ordine stretto) dove, per semplicità, abbiamo indicato con 00, 10, 01, 11, gli elementi $\emptyset, \{a\}, \{b\}, \{a, b\}$, rispettivamente. Inoltre consideriamo la funzione $f: \{00, 01, 10, 11\} \rightarrow \{0, 1, 2\}$ che associa ad ogni insieme il numero dei suoi elementi,

$$f(00) = 0, f(10) = 1, f(01) = 1, f(11) = 2$$

$$f(11) = 2$$

$$f(10) = 1, f(01) = 1$$

$$f(00) = 0$$



Allora risulta che f

- è un omomorfismo non pieno di $(P(\{a,b\}), \subseteq)$ in $(\{0,1,2\}, \subseteq)$ (non è pieno in quanto $f(10) \leq f(01)$ ma non è vero che $10 \subseteq 01$)
- è un omomorfismo pieno di $(P(\{a,b\}), \subseteq)$ in $(\{0,1,2\}, <)$ (pur non essendo iniettiva)
- non è un omomorfismo di $(P(\{a,b\}), \cup, \cap)$ in $(\{0,1,2\}, \vee, \wedge)$ (infatti $f(\{a\}) \wedge f(\{b\}) = 1 \neq 0 = f(\{a\} \cap \{b\})$).

Ne segue che il nucleo \equiv di f , che pone equivalenti 10 e 01.

- non è una congruenza di $(P(\{a,b\}), \subseteq)$
- non è una congruenza di $(P(\{a,b\}), \cup, \cap)$
- è una congruenza in $(P(\{a,b\}), \subseteq)$.

Il quoziente modulo \equiv definisce un ordine stretto nella partizione $\{00\}, \{10,01\}, \{11\}$ e tale ordine stretto è isomorfo a $(\{0,1,2\}, <)$.

Consideriamo invece la funzione $g : \{00, 01, 10, 11\} \rightarrow \{0,1,2\}$ definita dal porre

$$g(00) = 0, g(10) = 1, g(01) = 0, g(11) = 2.$$

Allora g

- è un omomorfismo non pieno di $(P(\{a,b\}), \subseteq)$ in $(\{0,1,2\}, \subseteq)$ (non è pieno in quanto $g(00) \geq g(01)$ pur non essendo $00 \supseteq 01$)
- non è un omomorfismo di $(P(\{a,b\}), \subseteq)$ in $(\{0,1,2\}, <)$ (in quanto $\emptyset \subset \{b\}$ ma non è vero che $g(\emptyset) < g(\{b\})$)
- è un omomorfismo di (D, \cup, \cap) in (D', \cup', \cap') (osserviamo solo che $g(10) \wedge g(01) = 0 = f(10 \cap 01)$).

Ne segue che il nucleo di g è una congruenza del reticolo $(P(\{a,b\}), \cup, \cap)$ in cui le classi sono $\{00,01\}, \{10\}, \{11\}$. Anche in questo caso il quoziente è isomorfo al reticolo $(\{0,1,2\}, \vee, \wedge)$.

Il fatto che f e g non sono omomorfismi pieni di $(P(\{a,b\}), \subseteq)$ rappresenta un fatto molto più generale. Infatti vale la seguente proposizione.

Proposizione 1. Nelle strutture con una relazione d'ordine \leq tutti gli omomorfismi pieni sono iniettivi e l'unica congruenza è l'identità. Sia nelle strutture con ordine stretto che nelle strutture di reticolo esistono omomorfismi pieni non iniettivi e quindi congruenze che non si riducono all'identità.

Dim. Siano (D, \leq) e (D', \leq') due insiemi ordinati e sia $f : D \rightarrow D'$ un omomorfismo pieno. Allora

$$f(x) = f(y) \Rightarrow f(x) \leq' f(y) \text{ e } f(y) \leq' f(x) \Rightarrow x \leq y \text{ e } x \geq y \Rightarrow x = y.$$

Supponiamo che \equiv sia una relazione di *equivalenza* in (D, \leq) compatibile con \leq . Allora

$$d_1 \equiv c_1, d_2 \equiv c_2 \Rightarrow d_1 \leq d_2 \Leftrightarrow c_1 \leq c_2$$

ed in particolare

$$x \equiv x', x \equiv x \Rightarrow x \leq x \Leftrightarrow x' \leq x.$$

Poiché risulta sempre che $x \equiv x$ e $x \leq x$,

$$x \equiv x' \Rightarrow x' \leq x$$

Per lo stesso motivo deve accadere anche che

$$x \equiv x' \Rightarrow x \leq x'$$

e quindi $x \equiv x' \Rightarrow x = x'$. Per la proprietà riflessiva delle equivalenze è anche evidente che $x = x' \Rightarrow x \equiv x'$ e ciò mostra che \equiv coincide con l'identità $=$.

Poiché le relazioni d'ordine sono tra le più considerate in matematica, tale proposizione mostra perché la nozione di congruenza in una struttura relazionale (e la conseguente nozione di quoziente) non viene usualmente considerata dai matematici (con esclusione di quelli che si occupano di teoria dei grafi).

Proposizione 3. Ogni omomorfismo di ordine stretto è anche un omomorfismo di ordine ma il viceversa non vale.

Dim. Sia f un omomorfismo di ordine stretto allora se $x \leq y$ due sono i casi: $x=y$ oppure $x < y$. Nel primo caso risulta che $f(x) = f(y)$ e quindi $f(x) \leq f(y)$. Nel secondo caso $f(x) < f(y)$ e quindi ancora $f(x) \leq f(y)$. Il viceversa non vale poiché se f è una funzione costante allora f è un omomorfismo d'ordine che non è un omomorfismo di ordine stretto.

Proposizione 4. Ogni omomorfismo di reticolo è anche un omomorfismo di ordine ma il viceversa non vale.

Dim. Sia f un omomorfismo di reticolo, allora

$$x \leq y \Rightarrow x \wedge y = x \Rightarrow f(x) \wedge f(y) = f(x \wedge y) = f(x) \Rightarrow f(x) \leq f(y).$$

Quindi f è anche un omomorfismo d'ordine.

Per mostrare che il viceversa non vale, basta vedere l'esempio della funzione f di $P(\{a,b\})$ in $\{0,1,2\}$ che è un omomorfismo d'ordine che non è un omomorfismo di reticolo .

Esercizio.

Dato l'insieme ordinato $([0,1], \leq, 0,1)$ ed una funzione $f: [0,1] \rightarrow [0,1]$ tale che $f(0) = 0, f(1) = 1$. Allora

f è un omomorfismo d'ordine $\Leftrightarrow f$ è crescente $\Leftrightarrow f$ è un omomorfismo di reticolo,

Infatti se $x \leq y$, poiché $f(x) \leq f(y)$, abbiamo che $f(x \wedge y) = f(x) = f(x) \wedge f(y)$ e $f(x \vee y) = f(y) = f(x) \vee f(y)$.

Da tali equivalenze si evidenzia che se si considera una qualunque funzione crescente non è lecito considerare il suo nucleo come congruenza rispetto alla struttura d'ordine ma è lecito considerarlo come congruenza della struttura di reticolo.

$$\begin{aligned} f \text{ è un omomorfismo d'ordine stretto} &\Leftrightarrow f \text{ è strettamente crescente} \Leftrightarrow \\ &f \text{ è un omomorfismo d'ordine pieno} \\ &\Leftrightarrow f \text{ è strettamente crescente} \Leftrightarrow f \text{ è una immersione di reticolo} \end{aligned}$$

9. Strutture del primo ordine.

Mettendo insieme la nozione di struttura algebrica e quella di struttura relazionale otteniamo la definizione generale di struttura del primo ordine.

Definizione 1. Una *struttura del primo ordine* è un oggetto matematico del tipo $(D, h_1, \dots, h_n, \mathcal{R}_1, \dots, \mathcal{R}_m, e_1, \dots, e_h)$ dove

- h_1, \dots, h_n sono operazioni in D ,
- $\mathcal{R}_1, \dots, \mathcal{R}_m$ relazioni in D
- e_1, \dots, e_h elementi di D .

Il campo ordinato dei numeri reali è un esempio di struttura in cui sono presenti sia operazioni che una relazione d'ordine.

Definizione 2. Due strutture del primo ordine

$$(D, h_1, \dots, h_n, \mathcal{R}_1, \dots, \mathcal{R}_m, e_1, \dots, e_k) \text{ e } (D', h_1', \dots, h_n', \mathcal{R}_1', \dots, \mathcal{R}_m', e_1', \dots, e_k')$$

si dicono *dello stesso tipo* se

- i) per ogni i , h_i ed h_i' hanno lo stesso numero di variabili
- ii) per ogni j , \mathcal{R}_j e \mathcal{R}_j' si applicano allo stesso numero di elementi.

Una *sottostruttura* di una struttura $S = (D, h_1, \dots, h_n, \mathcal{R}_1, \dots, \mathcal{R}_m, e_1, \dots, e_k)$

è una struttura $S' = (D', h_1', \dots, h_n', \mathcal{R}_1', \dots, \mathcal{R}_m', e_1', \dots, e_k')$, dello stesso tipo di S , tale che:

- i) $D' \subseteq D$
- ii) $h_i' = h_i/D'$
- iii) $\mathcal{R}_i' = \mathcal{R}_i/D'$
- iv) $e_i' = e_i$.

Pertanto una sottostruttura di S si ottiene fissando una parte D' di D che sia stabile rispetto alle operazioni h_1, \dots, h_n e che contenga le costanti e_1, \dots, e_k .

Definizione 3. Una *congruenza* in una struttura del primo ordine $S = (D, h_1, \dots, h_n, \mathcal{R}_1, \dots, \mathcal{R}_m, e_1, \dots, e_k)$ è una relazione di equivalenza compatibile con tutte le relazioni e le operazioni in tale struttura. Sia \equiv una congruenza in S , allora il *quoziente modulo* \equiv di S si definisce come la struttura $(D', h'_1, \dots, h'_n, \mathcal{R}'_1, \dots, \mathcal{R}'_m, c'_1, \dots, c'_k)$ dello stesso tipo di S tale che

- D' è uguale al quoziente di D modulo \equiv ,
- $h'_i([x_1], \dots, [x_l]) = [h_i(x_1), \dots, h_i(x_l)]$,
- $\mathcal{R}'_i = \{([x_1], \dots, [x_r]) \mid (x_1, \dots, x_r) \in \mathcal{R}_i\}$
- $e_j' = [e_j]$.

Riferendoci ad un esempio precedente, assumiamo che $\mathcal{A} = (Z, +, 0)$ e che \equiv sia la congruenza modulo 5. Allora il quoziente è costituito dalle cinque classi e la costante $[0]$ è costituita dalla classe dei multipli di 5.

Definizione 4. Siano S ed S' due strutture dello stesso tipo, chiamiamo *omomorfismo* di S in S' ogni funzione $f: D \rightarrow D'$ tale che:

- (1) $f(h_i(x_1, \dots, x_n)) = h'_i(f(x_1), \dots, f(x_n))$;
- (2) $f(e_i) = e_i'$;
- (3) $(x_1, \dots, x_n) \in \mathcal{R}_i \Rightarrow (f(x_1), \dots, f(x_n)) \in \mathcal{R}'_i$.

Inoltre diciamo che

- f è un *omomorfismo pieno* se vale anche la converso di (3), cioè
- (4) $(x_1, \dots, x_n) \in \mathcal{R}_i \Leftrightarrow (f(x_1), \dots, f(x_n)) \in \mathcal{R}'_i$.

- f è una *immersione* se è un omomorfismo pieno iniettivo
- f è un *epimorfismo* se è suriettivo,
- f è un *isomorfismo* se è invertibile ed il suo inverso è ancora un omomorfismo
- f è un *endomorfismo* se è un omomorfismo di S in se stesso
- f è un *automorfismo* se è un isomorfismo di S in se stesso.

Naturalmente nelle strutture algebriche non essendoci relazioni gli omomorfismi pieni coincidono con gli omomorfismi e le immersioni con gli omomorfismi iniettivi.

Proposizione 5. Le seguenti asserzioni sono equivalenti:

- a) f è un isomorfismo
- b) f è un omomorfismo pieno invertibile.

Se S è una struttura algebrica allora f è un isomorfismo se e solo se è un omomorfismo iniettivo.

Teorema 6. (Primo teorema di omomorfismo). Sia \equiv una congruenza nella struttura S e sia S' il relativo quoziente. Allora l'applicazione $cl: D \rightarrow D/\equiv$ che associa ad ogni $x \in D$ la classe $cl(x) = [x]$ è un epimorfismo pieno di S su S' (detto *epimorfismo canonico*).

Teorema 7. (Secondo teorema di omomorfismo). Sia f un omomorfismo pieno della struttura S nella struttura S' . Allora

- a) $f(D)$ è una parte stabile e quindi definisce una sottostruttura S_f di S'
- b) il nucleo di f è una congruenza in S che indichiamo con \equiv_f
- c) la funzione $g: D/\equiv_f \rightarrow D'$ definita dal porre $g([x]) = f(x)$ è una immersione del quoziente S/\equiv_f in S'
- d) la funzione $g: D/\equiv_f \rightarrow f(D)$ è un isomorfismo tra S/\equiv_f ed S_f .

NOTA. Anche se molti esempi di strutture studiate dai matematici sono strutture del primo ordine (i gruppi, gli anelli, i reticoli, gli insiemi ordinati, i campi ordinati ...) esistono anche moltissimi esempi di strutture matematiche che non rientrano in tale definizione. Ad esempio gli spazi topologici, gli spazi metrici.