Corso di ALGEBRA (M-Z)

2012-13

INSIEMI PARZIALMENTE ORDINATI E RETICOLI

Sia P un insieme non vuoto. Una relazione d'ordine $\leq$ su P è una relazione riflessiva, antisimmetrica e transitiva. La coppia $(P,\leq)$ si dice *insieme parzialmente ordinato (p.o.).* Il *duale* di $(P,\leq)$ è l'insieme p.o. $(P,\geq)$, dove $\geq$ è la relazione duale di $\leq$ che è anch'essa una relazione d'ordine. Due elementi x,y di P si dicono *confrontabili* se risulta $x \leq y$ oppure $y \leq x$, in particolare $x \leq y$ e $x \neq y$ sarà indicato con $x< y$. Un insieme parzialmente ordinato tale che ogni coppia di suoi elementi sia confrontabile si dice *totalmente ordinato* o *catena,* la *lunghezza di una catena* è il numero dei suoi elementi diminuito di una unità.

L'insieme $[a,b] = \{x\in P : a \leq x \leq b\}$ si dice *intervallo di estremi a,b*; se l'intervallo $[a,b]$ $(a\neq b)$ è costituito solo da *a* e *b* si dice che *b copre a* (o che *a è coperto da b*), in simboli $a <\bullet\ b$. Dati $x, y\in P$, si definisce *estremo inferiore di* x e y l'elemento inf(x,y) di P tale che

(I1) $\inf(x,y) \leq x$ e $\inf(x,y) \leq y$,

(I2) se $z\in P$, $z \leq x$ e $z \leq y$ allora $z \leq \inf(x,y)$.

Si definisce *estremo superiore di* x e y l'elemento sup(x,y) di P tale che

(S1) $x \leq \sup(x,y)$ e $y \leq \sup(x,y)$,

(S2) se $z\in P$, $x \leq z$ e $y \leq z$ allora $\sup(x,y) \leq z$.

Ovviamente l'estremo inferiore di x e y, se esiste, è unico, come pure è unico l'estremo superiore.

Siano $(P_1,\leq_1)$ e $(P_2,\leq_2)$ insiemi p.o., un *morfismo di insiemi p.o.* (o *funzione monotona*) è una applicazione f: $P_1 \to P_2$ tale che se $x \leq_1 y$ allora $f(x) \leq_2 f(y)$, quando il morfismo è biiettivo (*isomorfismo*) i due insiemi p.o. si dicono *isomorfi.*

Un insieme parzialmente ordinato $(P,\leq)$ con 0 può essere rappresentato graficamente attraverso un diagramma (*diagramma di Hasse*) i cui punti corrispondono biunivocamente agli elementi di P in modo che per ogni coppia (x,y) di elementi distinti si abbia:

i) se $x \leq y$ allora il punto x è più in basso del punto y ,

ii) se y copre x allora i punti x ed y sono uniti da un segmento.

Il *prodotto* di due insiemi parzialmente ordinati $(P_1,\leq_1)$ e $(P_2,\leq_2)$ è l'insieme p.o $(P_1xP_2,\leq)$ dove la relazione d'ordine è definita da:

$$(x_1,x_2) \leq (y_1,y_2) : \text{se e solo se } x_1 \leq_1 y_1 \text{ e } x_2 \leq_2 y_2.$$

In generale data una famiglia di insiemi p.o $\{(P_i,\leq)\}_{i\in I}$, l' *insieme p.o. prodotto* $(\Pi_{i\in I} P_i,\leq)$ è definito da:

$$\{x_i\}_{i\in I}, \{y_i\}_{i\in I} \in \Pi_{i\in I} P_i,\ \{x_i\}_{i\in I} \leq \{y_i\}_{i\in I}: \text{ se e solo se } x_i \leq y_i \text{ per ogni } i \in I.$$

Si osservi che, se $(P, \leq)$ è un insieme p.o. e $X =\{x_1,\ldots,x_n\}$ un insieme con n elementi, è possibile definire una relazione d'ordine sull'insieme P^X delle funzioni da X in P ponendo:

$$f \leq g : \text{se e solo se } (f(x_1),\ldots,f(x_n)) \leq (g(x_1),\ldots,g(x_n)) \text{ nell'insieme prodotto } (P^n, \leq).$$

Pertanto la funzione $F : (2^X,\subseteq) \to (\{0,1\}^X,\leq)$ che ad ogni sottoinsieme A di X associa la sua funzione caratteristica ϕ_A (per ogni $i = 1,\ldots,r$, $\phi_A(x_i) = 0$ se $x_i \notin A$, $\phi_A(x_i) = 1$ se $x_i\in A$) è un isomorfismo di insiemi p.o.

Reticoli come insieme parzialmente ordinati. Un reticolo $(L,\leq)$ è un insieme p.o. tale che ogni coppia di elementi ha un estremo inferiore ed un estremo superiore.

Un morfismo di reticoli è una funzione monotona $f : (L,\leq) \to (L', \leq)$ tale che :

$$f(\inf(x,y)) = \inf (f(x),f(y)) \text{ e } f(\sup(x,y)) = \sup (f(x), f(y)), \text{ per ogni } x,y \in L$$

Due reticoli si dicono isomorfi se è possibile definire tra di essi un morfismo di reticoli biiettivo (*isomorfismo di reticoli*).

Si osservi che l'insieme p.o. $(L, \geq)$, duale di un reticolo, è anch'esso un reticolo in quanto, ponendo per ogni x,y in L : $\inf^*(x,y) = \sup(x,y)$ e $\sup^*(x,y) = \inf(x,y)$, si ha :

(I1) $\inf^*(x,y) \geq x$ e $\inf^*(x,y) \geq y$,
(I2) se $z \in P$, $z \geq x$ e $z \geq y$ allora $z \geq \inf^*(x,y)$.
(S1) $x \geq \sup^*(x,y)$ e $y \geq \sup^*(x,y)$,
(S2) se $z \in P$, $x \geq z$ e $y \geq z$ allora $\sup^*(x,y) \geq z$..
In un reticolo $(L,\leq)$ è possibile definire due operazioni: *l'operazione di inf* $\wedge$ definita da: $x \wedge y = \inf(x,y)$ e *l'operazione di sup* $\vee$ definita da: $x \vee y = \sup(x,y)$. Tali operazioni hanno le seguenti proprietà fondamentali:

(L1) idempotenza : $x \wedge x = x$ $x \vee x = x$
(L2) commutativa : $x \wedge y = y \wedge x$ $x \vee y = y \vee x$
(L3) associativa : $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ $x \vee (y \vee z) = (x \vee y) \vee z$
(L4) assorbimento $x \wedge (x \vee y) = x = x \vee (x \wedge y)$

Inoltre le operazioni di inf e sup risultano isotone, ossia :

se $x, y, z \in L$ e $y \leq z$ allora: $x \wedge y \leq x \wedge z$ e $x \vee y \leq x \vee z$

Si osservi che ogni proprietà (Li) è espressa da uguaglianze di stringhe $E(\wedge,\vee)$ nelle quali compaiono solo elementi del reticolo e i simboli: $\wedge$, $\vee$, (,),= . La stringa $E^*(\vee, \wedge)$ duale di $E(\wedge,\vee)$ è quella ottenuta da $E(\wedge,\vee)$ scambiando $\wedge$ con $\vee$ e $\vee$ con $\wedge$. Pertanto se nella proprietà (Li) si sostituisce ad ogni stringa la sua duale si ottiene ancora la proprietà stessa. Questo fatto si esprime affermando che le proprietà fondamentali sono auto-duali, quindi se $I(\wedge,\vee)$ è una identità che consegue dalle proprietà fondamentali allora è necessariamente vera anche l'identità $I^*(\vee, \wedge)$ sua duale. Nei reticoli vale più in generale il

Principio di dualità. Se in un reticolo $(L, \leq)$ è vero un enunciato $\mathscr{E}$ su stringhe composte solo da elementi del reticolo e dai simboli $\wedge$, $\vee$, (,), allora è vero anche l'enunciato duale $\mathscr{E}^*$ che si ottiene sostituendo ad ogni stringa $E(\wedge, \vee)$ di $\mathscr{E}$ la sua duale $E^*(\vee, \wedge)$ e ad ogni relazione $E_i \leq E_j$ la relazione $E_j{}^* \leq E_i{}^*$.

Reticoli come strutture algebriche. Le proprietà (L1), (L2), (L3), (L4) caratterizzano i reticoli, ossia:

Teorema. Data una struttura algebrica $(L, \wedge, \vee)$ dove le operazioni $\wedge$, $\vee$ hanno le proprietà (L1), (L2), (L3), (L4), è possibile definire su L una relazione d'ordine $\leq$ tale che $(L,\leq)$ sia un reticolo e che per ogni x, y di L si abbia $\inf(x,y) = x \wedge y$ e $\sup(x,y) = x \vee y$. Viceversa dato un reticolo $(L,\leq)$, le operazioni $\wedge$, $\vee$ definite su L rispettivamente da $x \wedge y = \inf(x,y)$ e $x \vee y = \sup(x,y)$ determinano una struttura algebrica $(L, \wedge, \vee)$ verificante le proprietà (L1), (L2), (L3), (L4).

Dim. Sia $(L, \wedge, \vee)$ una struttura algebrica verificante le proprietà (L1), (L2), (L3), (L4). La relazione $\leq$ definita da :

(3.1.) $x \leq y$: se e solo se $x \wedge y = x$

è una relazione d'ordine su L. Infatti è riflessiva per (L1). Inoltre se $x \leq y$ e $y \leq x$, per (L2) si ha:

$$x = x \wedge y = y \wedge x = y,$$

quindi la relazione è antisimmetrica. Infine se $x \leq y$ e $y \leq z$, per (L3) si ha:

$$x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x ,$$

e dunque $x \leq z$.

Si osservi che si ha: $x \wedge y = x$ se e solo se $x \vee y = y$. Infatti se $x \wedge y = x$ allora $x \vee y = (x \wedge y) \vee y = y$ per L4.

Rimane da dimostrare che per ogni $x,y \in L$ si ha :

$$\inf(x,y) = x \wedge y \text{ e } \sup(x,y) = x \vee y.$$

Infatti:
(I1) : $(x \wedge y) \wedge x = (x \wedge x) \wedge y = x \wedge y \Rightarrow x \wedge y \leq x$ e analogamente $x \wedge y \leq y$
(I2) : sia $z \leq x$ e $z \leq y$ allora $z \wedge x = z = z \wedge y$ e quindi $(x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y \Rightarrow z \leq (x \wedge y)$.
Inoltre:

Lemma. Si ha: $x \leq y$ se e solo se $(x \vee y) = y$.

Dim. Sia $x \leq y$. Allora per L4 $y = y \vee (x \wedge y) = y \vee x$. Viceversa se $y = x \vee y$, si ha $x = x \wedge (x \vee y) = x \wedge y$ e quindi $x \leq y$.

Tenendo conto del lemma e ripercorrendo le dimostrazioni fatte per l'inf, si ha:
(S1) $x \leq x \vee y$ e $y \leq x \vee y$
(S2) se $z \in L$, $x \leq z$ e $y \leq z$ allora $x \vee y \leq z$..
e quindi $\sup(x,y) = x \vee y$.

□

Si osservi che un morfismo di reticoli come strutture algebriche f: $(L, \wedge, \vee) \rightarrow (L', \wedge, \vee)$, ossia un'applicazione f tale che:

$$f(x \wedge y) = f(x) \wedge f(y) \text{ e } f(x \vee y) = f(x) \vee f(y),$$

è anche un morfismo di insiemi p.o., invece un morfismo di insiemi p.o, ossia una funzione monotona da L in L', non necessariamente è un morfismo di reticoli.

In ogni reticolo $(L, \wedge, \vee)$ è vera la *disuguaglianza modulare*:

(LM) Per ogni $x,z \in L$ con $x \leq z$ risulta : $x \vee (y \wedge z) \leq (x \vee y) \wedge z$.

Dim. $(x \vee y) \wedge z$ è un maggiorante sia di x che $(y \wedge z)$ e quindi è maggiore del loro estremo superiore $x \vee (y \wedge z)$.

□

Si osservi che l'enunciato (LM) è autoduale.
In ogni reticolo $(L, \wedge, \vee)$ valgono inoltre le disuaglianze distributive per ogni $x,y,z \in L$:

$(LD)_1$ $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$
$(LD)_2$ $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$

Dim. Le due disuguaglianze sono una duale dell'altra, pertanto basta dimostrare la $(LD)_1$. Poiché $x \vee (y \wedge z) = \sup(x, y \wedge z)$ basta dimostrare che:

$$x \leq (x \vee y) \wedge (x \vee z) \text{ e } (y \wedge z) \leq (x \vee y) \wedge (x \vee z).$$

Infatti $x \leq (x \vee y)$ e $x \leq (x \vee z)$ e quindi x è minore di $(x \vee y) \wedge (x \vee z)$. Inoltre $(y \wedge z) \leq y \leq (x \vee y)$ e $(y \wedge z) \leq z \leq (x \vee z)$ da cui $(y \wedge z)$ è minore di $(x \vee y) \wedge (x \vee z)$.

Alcuni reticoli fondamentali
Nel seguito una catena di lunghezza n, ossia una catena costituita da (n+1) elementi, sarà indicata con $\mathscr{C}(n)$, poiché catene della stessa lunghezza risultano isomorfe. Ogni catena è ovviamente un reticolo.

1. La catena dei numeri naturali N ordinati dalla relazione naturale.

2. Il reticolo (N*,|) dei numeri interi positivi ordinati dalla relazione di divisibilità.

La relazione | è definita da:

$$m \mid n \Leftrightarrow m \text{ divide } n : \Leftrightarrow \text{ esiste un intero positivo k tale che } n = km.$$

Risulta:

$$m \wedge n := \text{massimo comun divisore tra m e n} = MCD(m,n),$$
$$m \vee n := \text{minimo comune multiplo tra m ed n} = mcm(m,n).$$

3. Il reticolo $\mathscr{M}$(R) dei multinsiemi finiti di un insieme R.

Ricordiamo che un multinsieme di R è una applicazione M da R in **N.** Il reticolo $\mathscr{M}$(R) è un sottoreticolo del reticolo di tutti i multinsiemi di R, dove se M,M'sono multinsiemi di R, si ha:

$$M \leq M' : \Leftrightarrow M(x) \leq M'(x) \text{ per ogni } x \in R$$
$$M \wedge M'(x) := \inf (M(x),M'(x))$$
$$M \vee M'(x) := \sup(M(x),M'(x)).$$

Risulta :

i) Se $|R| = r < \infty$, il reticolo $\mathscr{M}$(R) è isomorfo al reticolo $\mathbf{N}^r$ ottenuto come prodotto di r copie della catena dei numeri naturali **N,** pertanto il reticolo dei multinsiemi di un r-insieme sarà indicato con $\mathscr{M}$(r), (fig.3.1).

ii) Se $|R| = |\mathbf{N}|$, il reticolo $\mathscr{M}$(R) dei multinsiemi finiti di R è isomorfo al reticolo (**N***,|) degli interi positivi ordinati dalla divisibilità.

Dim . i). Sia R = {1,…,*r*}. L'isomorfismo $\phi : \mathscr{M}(R) \to \mathbf{N}^r$ è definito da: $\phi(M) = (M(1),\ldots,M(r))$

Dim. ii). In questo caso R è numerabile e dunque si può supporre R = **N.** Ricordiamo che i numeri primi sono infiniti in quanto se per assurdo fossero in numero finito : $p_1,\ldots,p_h$, l'intero $n = (\prod p_i) +1$, primo con ogni p_i, non sarebbe primo. Sia dunque $\{p_i\}_{i\in N}$ la successione dei numeri primi. L'isomorfismo

$\phi : \mathscr{M}(R) \to$ (**N***,|) associa ad ogni multinsieme finito M il numero naturale $m = \prod_{i\in \mathbf{N}} p_i^{M(i)}$.

□

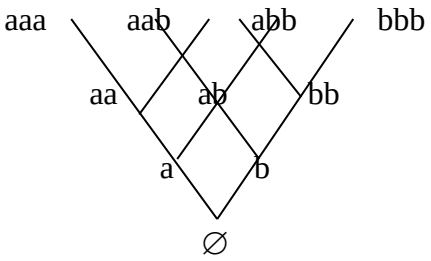


Fig.3.1: diagramma di Hasse di $\mathscr{M}$({a,b})

4. L'algebra booleana $\mathscr{B}$(r) di rango r.

Sia R un insieme non vuoto, l'insieme $\mathscr{B}$(R) di tutti i sottoinsiemi finiti di R risulta un sottoreticolo del reticolo $(2^R,\subseteq)$ dei sottoinsiemi di R, dove l'operazione di inf è l'intersezione e quella di sup è l'unione. Se $|R| = r < \infty$, allora $\mathscr{B}(R) \cong \mathscr{C}(1)^r$ dove $\mathscr{C}(1)^r$ denota il reticolo prodotto di r copie delle catena $\mathscr{C}$(1). Infatti, ordinati gli elementi di $R = \{x_1,\ldots,x_r\}$, l'applicazione ϕ che ad ogni sottoinsieme A associa la r-pla $\phi(A) = (\phi_A(x_1),\ldots,\phi_A(x_r))$ determinata dalla ϕ_A, funzione caratteristica di A, è un isomorfismo di reticoli. L'*algebra booleana di rango* r è il reticolo $\mathscr{B}$(r) dei sottoinsiemi di un insieme con r elementi.

5. Reticolo delle partizioni di un insieme.

Sia A un insieme non vuoto. L'insieme delle partizioni di A è ordinato dalla relazione di raffinamento definita come segue. Siano π, σ partizioni di A e (π), (σ) le relazioni di equivalenza da esse determinate, si ha:

$\pi \leq \sigma \ :\Leftrightarrow \ a(\pi)b$ implica $a(\sigma)b$, per ogni $a,b \in A \Leftrightarrow$ ogni blocco di π è contenuto in un blocco di σ
$\Leftrightarrow$ ogni blocco di σ è unione di blocchi di π.

Inoltre la partizione $\pi \wedge \sigma$ è determinata dalla relazione di equivalenza:

$$a(\pi \wedge \sigma)b :\Leftrightarrow a(\pi)b \text{ e } a(\sigma)b,$$

mentre la partizione $\pi \vee \sigma$ è determinata da:

$a(\pi \vee \sigma)b : \Leftrightarrow$ esistono $u_1,\ldots u_k \in A$ tali che $u_1 = a$ e $u_k = b$ e per ogni $i = 1,\ldots,k\text{-}1$ $u_i(\pi)u_{i+1}$ oppure $u_i(\sigma)u_{i+1}$.

Si indichi con $\mathscr{P}(A)$ il *sottoreticolo costituito dalle partizioni di* A *con un numero finito di blocchi*. Dati due insiemi finiti con la stessa cardinalità n, i rispettivi reticoli delle partizioni risultano isomorfi, pertanto è possibile definire il *reticolo delle partizioni* $\mathscr{P}(n)$ *di ordine* n $(< \infty)$.

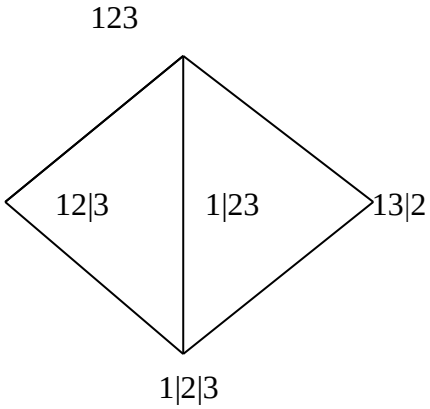


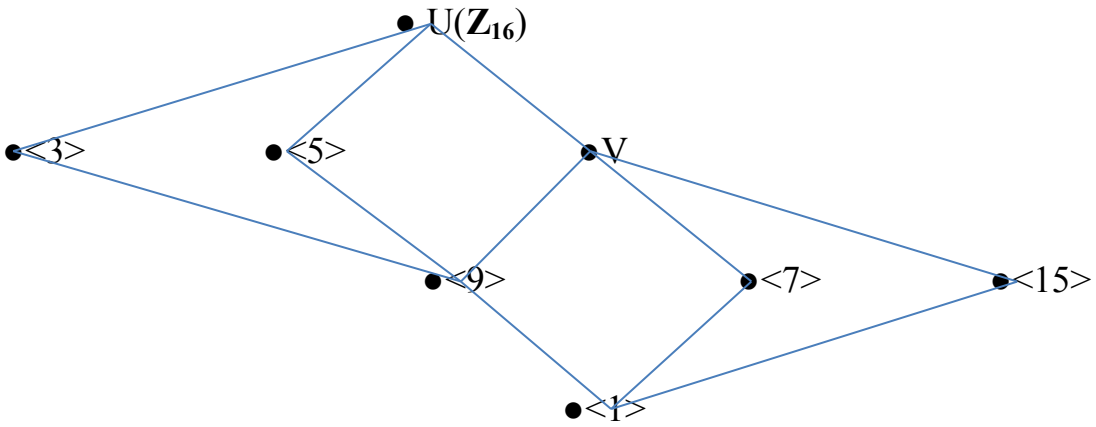
Fig.3.2: Il reticolo $\mathscr{P}(3)$

Teorema.(Pudlák-Tûma). Ogni reticolo finito è isomorfo ad un sottoreticolo del reticolo delle partizioni $\mathscr{P}(n)$.

Esempio 6. Reticolo dei sottospazi $\mathscr{L}(n,K)$ di uno spazio n-dimensionale su un campo K .

Esempio 7. Reticolo dei sottogruppi di un gruppo (G,•).

La relazione d'ordine è l'inclusione. Dati due sottogruppi H,K allora $H \wedge K$ è l'intersezione dei due sottogruppi. Il sottogruppo $H \vee K$ è il sottogruppo generato dall'unione $H \cup K$, ossia è l'intersezione di tutti i sottogruppi contenenti l'insieme $H \cup K$.



Il reticolo dei sottogruppi del gruppo $U(\mathbf{Z}_{16})$ degli elementi invertibili dell'anello $(\mathbf{Z}_{16},+,\cdot)$.

Esempio 8. Reticolo dei sottoanelli di un anello (A,+, •) .
La relazione d'ordine è l'inclusione. Dati due sottoanelli S,R allora $S \wedge S$ è l'intersezione dei due sottoanelli. Il sottoanello $S \vee R$ è il sottogruppo generato dall'unione $S \cup R$, ossia è l'intersezione di tutti i sottoanelli contenenti l'insieme $S \cup R$.