

Corso di ALGEBRA (M-Z)

2015-16

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 $a \triangleleft b$. 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 $f: P_1 \rightarrow P_2$ 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. $(P_1 \times P_2, \leq)$ 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. $\{(P_i, \leq_i)\}_{i \in I}$, l'*insieme p.o. prodotto* $(\prod_{i \in I} P_i, \leq)$ è definito da:

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

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

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

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

Reticoli come insiemi 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 $f: (L, \leq) \rightarrow (L', \leq)$ 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 :

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:

$$(I1) : (x \wedge y) \wedge x = (x \wedge x) \wedge y = x \wedge y \Rightarrow x \wedge y \leq x \text{ e analogamente } x \wedge y \leq y$$

$$(I2) : \text{ sia } z \leq x \text{ e } z \leq y \text{ allora } z \wedge x = z = z \wedge y \text{ e quindi } (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y \Rightarrow z \leq (x \wedge y) .$$

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:

$$(S1) \quad x \leq x \vee y \text{ e } y \leq x \vee y$$

$$(S2) \quad \text{ se } z \in L, \quad x \leq z \text{ e } y \leq z \text{ allora } x \vee y \leq z.$$

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

□

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*:

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

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 disuguaglianze distributive per ogni $x, y, z \in L$:

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

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

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 $\mathcal{C}(n)$, poiché catene della stessa lunghezza risultano isomorfe. Ogni catena è ovviamente un reticolo.

1. La catena dei numeri naturali \mathbb{N} ordinati dalla relazione naturale.

2. Il reticolo $(\mathbf{N}^*, |)$ dei numeri interi positivi ordinati dalla relazione di divisibilità.

La relazione $|$ è definita da:

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

Risulta:

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

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

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

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

Risulta :

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

Dim . i). Sia $\mathbf{R} = \{1, \dots, r\}$. L'isomorfismo $\phi : \mathcal{M}(\mathbf{R}) \rightarrow \mathbf{N}^r$ è definito da: $\phi(M) = (M(1), \dots, M(r))$

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

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

□

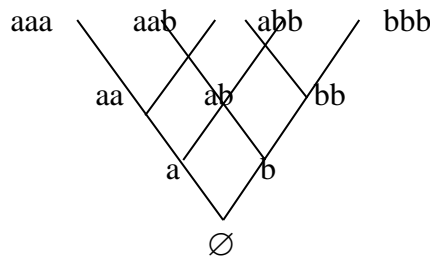


Fig.3.1: diagramma di Hasse di $\mathcal{M}(\{a,b\})$

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

Sia \mathbf{R} un insieme non vuoto, l'insieme $\mathcal{B}(\mathbf{R})$ di tutti i sottoinsiemi finiti di \mathbf{R} risulta un sottoreticolo del reticolo $(2^{\mathbf{R}}, \subseteq)$ dei sottoinsiemi di \mathbf{R} , dove l'operazione di \inf è l'intersezione e quella di \sup è l'unione. Se $|\mathbf{R}| = r < \infty$, allora $\mathcal{B}(\mathbf{R}) \cong \mathcal{C}(1)^r$ dove $\mathcal{C}(1)$ denota il reticolo prodotto di r copie delle catena $\mathcal{C}(1)$. Infatti, ordinati gli elementi di $\mathbf{R} = \{x_1, \dots, x_r\}$, l'applicazione ϕ che ad ogni sottoinsieme A associa la r -pla $\phi(A) = (\phi_A(x_1), \dots, \phi_A(x_r))$ determinata dalla ϕ_A , funzione caratteristica di A , è un isomorfismo di reticoli. L'algebra booleana di rango r è il reticolo $\mathcal{B}(r)$ 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 $(\pi), (\sigma)$ 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 $u_1, \dots, u_k \in A$ tali che $u_1 = a$ e $u_k = b$ e per ogni $i = 1, \dots, k-1$ $u_i(\pi)u_{i+1}$ oppure $u_i(\sigma)u_{i+1}$.

Si indichi con $\mathcal{R}(A)$ 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 $\mathcal{R}(n)$ di ordine n ($< \infty$).

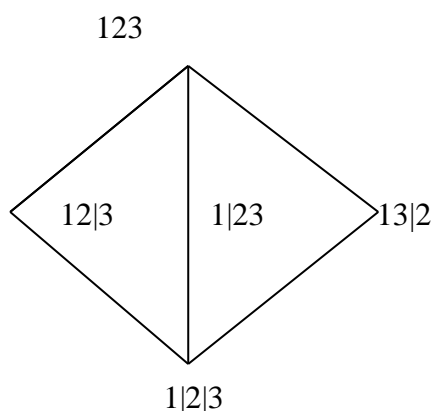


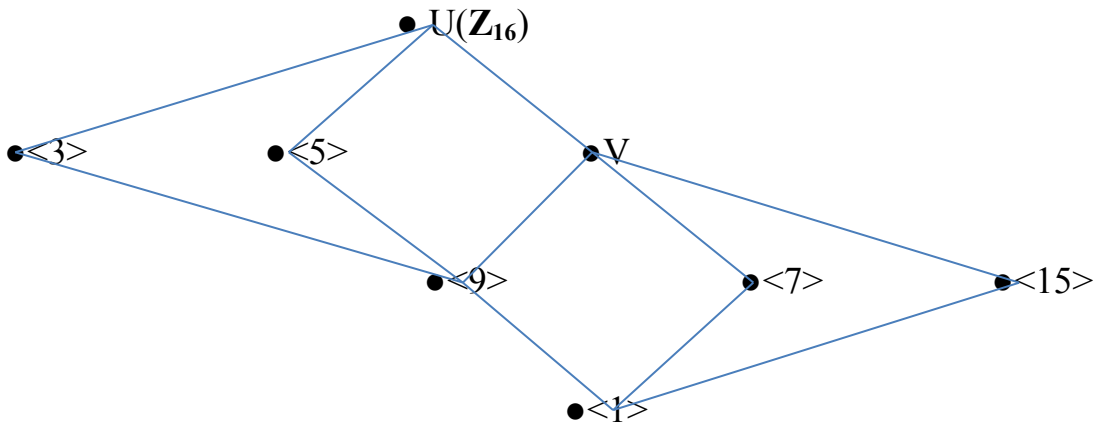
Fig.3.2: Il reticolo $\mathcal{R}(3)$

Teorema.(Pudlák-Tůma). Ogni reticolo finito è isomorfo ad un sottoreticolo del reticolo delle partizioni $\mathcal{R}(n)$.

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

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

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 $(A, +, \cdot)$.

La relazione d'ordine è l'inclusione. Dati due sottoanelli S, R allora $S \wedge R$ 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 $S \cup R$.