Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Matematica

Reticoli distributivi, reticoli modulari e reticoli geometrici.

Relatore:
Chiar.ma Prof.ssa
MARILENA BARNABEI

Presentata da:
MELISSA ZUCCONI

III Sessione
Anno Accademico 2019/2020

Introduzione

I reticoli possono essere definiti sia come strutture algebriche astratte che soddisfano determinate proprietà; sia come insiemi parzialmente ordinati in cui ogni coppia di elementi possiede un unico estremo superiore ed un unico estremo inferiore.

E' possibile dunque contestualizzare la Teoria dei reticoli all'interno della Teoria dell'ordine; per questo motivo nel primo capitolo viene introdotta tale teoria.

In questo elaborato verranno presentati principalmente tre classi di reticoli: i reticoli distributivi, i reticoli modulari ed i reticoli geometrici.

Un reticolo distributivo è un reticolo nel quale le operazioni di inf e di sup sono distributive l'una rispetto all'altra. Gli esempi più banali di una tale struttura sono dati dalle catene, dalle Algebre di Boole e dai reticoli con al più quattro elementi. Nello studiare i reticoli distributivi è giusto soffermarsi su dei particolari elementi, chiamati sup-irriducibili, che in un tale reticolo permettono di decomporre in modo unico ogni elemento. La proprietà appena descritta risulta fondamentale perchè permette di caratterizzare un qualsiasi reticolo distributivo in modi differenti: grazie ai teoremi di Birkhoff esso può essere rappresentato come reticolo degli ideali d'ordine, può essere rappresentato come prodotto di catene oppure può essere descritto attraverso identità soddisfatte dalla sua funzione rango.

A seguire vengono poi presentati i reticoli modulari, i quali sono una generalizzazione di quelli distributivi. Esempi tipici su cui ci si è soffermati sono il reticolo costituito dai sottogruppi normali di un gruppo ed il reticolo costituito dai sottospazi di uno spazio vettoriale. Il risultato principale che si dimostra in questo capitolo è il teorema di isomorfismo canonico che fornisce condizioni necessarie e sufficienti affinchè un reticolo sia modulare. A differenza di ciò che accade nei reticoli distributivi, l'unicità della decomposizione in sup-irriducibili nei reticoli modulari non è più garantita, ma si dimostra che il numero di elementi che compaiono nella decomposizione è sempre lo stesso. I reticoli semimodulari sono una generalizzazione dei reticoli modulari. Il reticolo delle partizioni di un insieme che contiene più di tre elementi è un esempio di reticolo che è semimodulare ma non modulare. Il capitolo si conclude dimostrando che sia i reticoli modulari che quelli semimodulari possiedono una funzione rango che li caratterizza.

I reticoli geometrici sono reticoli con catene finite, atomici e semimodulari. Le algebre di Boole, i reticoli di sottospazi di uno spazio vettoriale di dimensione finita e i reticoli di partizioni di un insieme finito sono degli esempi. Si definiscono poi la matroide degli indipendenti e la matroide della chiusura.

Dimostreremo il teorema di Brirkhoff Whitney il quale caratterizza i reticoli geometrici attraverso il reticolo dei chiusi della matroide costruita sull'insieme degli atomi del reticolo geometrico dato. Un'ultima caratterizzazione dei reticoli geometrici è fornita dai reticoli relativamente complementati, che sono una generalizzazione dei reticoli complementati. Tutte e tre le classi di reticoli analizzati sono dotate di una funzione rango. Nell'ultimo capitolo vengono ripresi alcuni esempi già precedentemente citati, e per ognuno di essi vengono classificati gli elementi in base al rango.

Indice

Capitolo 1

Premesse

1.1 Insieme parzialmente ordinato

Definizione 1.1.1. *Sia P un insieme non vuoto e $\leq$ una relazione binaria che soddisfi le seguenti proprietà:*

1. *$x \leq x$ per ogni $x \in P$ (riflessività);*
2. *se $x \leq y$ e $y \leq x$ allora $x = y$ per ogni $x, y \in P$ (antisimmetria)*
3. *se $x \leq y$ e $y \leq z$ allora $x \leq z$ per ogni $x, y, z \in P$ (transitività)*

In tal caso diremo che $\leq$ è una relazione d'ordine parziale su P e la coppia $(P; \leq)$ prende il nome di insieme parzialmente ordinato o poset. L'insieme P è detto sostegno dell'insieme parzialmente ordinato.

Sia $\leq$ una relazione d'ordine su un dato insieme P; due elementi $a, b \in P$ si dicono confrontabili (secondo la relazione $\leq$) se risulta $a \leq b$ oppure $b \leq a$. In caso contrario, a e b si dicono inconfrontabili. In generale non è detto che due elementi qualunque di P siano sempre confrontabili.

Esempio 1.1.1. *La relazione di divisibilità $|$ sull'insieme $\mathbb{Z}^+$ dei numeri interi positivi è una relazione d'ordine. Si noti che non tutti gli elementi del poset sono tra loro confrontabili, infatti $2 \nmid 3$ e $3 \nmid 2$.*
Si noti inoltre che, se indichiamo con $\leq$ l'usuale ordinamento tra i numeri naturali, le coppie $(\mathbb{Z}^+, \leq)$ e $(\mathbb{Z}^+, |)$ sono due differenti insiemi parzialmente ordinati, che hanno lo stesso sostegno.

Esempio 1.1.2. *Sia U un insieme; la relazione $\subseteq$ di inclusione tra i sottoinsiemi di U è una relazione d'ordine su $\mathcal{P}(U)$, cioè l'insieme delle parti di U. L'insieme parzialmente ordinato $(\mathcal{P}(U), \subseteq)$ viene detto Algebra di Boole dei sottoinsiemi di U, e denotato con $\mathcal{B}(U)$. Anche in questo caso, se la caridinalità di U è maggiore o uguale a 2, non tutti gli elementi sono confrontabili: per esempio se $U = \{a, b, c\}$ allora $\{a\} \nsubseteq \{b, c\}$ e $\{b, c\} \nsubseteq \{a\}$*
Si noti che, nel caso in cui U sia l'insieme vuoto, $\mathcal{P}(U) = \{\emptyset\}$ allora $\mathcal{B}(U)$ è un insieme parzialmente ordinato il cui sostegno è costituito da un solo elemento.

Definizione 1.1.2. *Se $(P;\leq)$ è un poest, si dice che:*

- *$(P;\leq)$ è una catena e $\leq$ è un ordine lineare (o totale) su P se*

$$\text{per ogni } x, y \in P, \text{ se } x \not\leq y \text{ allora } y \leq x.$$

- *$(P;\leq)$ è un'anticatena se*

$$\text{per ogni } x, y \in P, \text{ se } x \leq y \text{ allora } x = y.$$

In una catena tutti gli elementi sono tra loro confrontabili, come in $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$ dotati dell'ordine usuale; al contrario in un'anticatena ogni elemento è confrontabile solo con se stesso mentre tra elementi distinti non intercorre alcuna relazione.

Definizione 1.1.3. *Se $(P;\leq)$ è un poset e Q un sottoinsieme non vuoto di P, la restrizione a Q della relazione $\leq$ viene detta ordine indotto da $\leq$ su Q, e il poset $(Q;\leq)$ si dice sottoordine di $(P;\leq)$.*

Esempio 1.1.3. *Consideriamo il poset $(\mathbb{Z}^+,|)$. Posto $Q = \{1,3,9,27,81\}$ abbiamo che l'ordine indotto da $|$ su Q coincide con l'ordinamento usuale $\leq$ tra i numeri naturali, e quindi il sottoordine $(Q;|)$ è una catena.*

Esempio 1.1.4. *Un sottoinsieme di $\mathbb{Z}^+$ costituito da numeri due a due primi tra loro è un'anticatena del poset $(Z^+,|)$.*

Definizione 1.1.4. *Sia $(P;\leq)$ un poset e siano $x, y \in P$ tali che $x \leq y$. Si dice intervallo in P di estremi x e y l'insieme parzialmente ordinato il cui sostegno è il seguente sottoinsieme di P:*

$$[x;y] = \{z \in P \mid x \leq z \leq y\}$$

e l'ordine è quello indotto. Si noti che, in generale, un intervallo in P non è una catena.

Esempio 1.1.5. *Sia U un insieme non vuoto; consideriamo l'Algebra di Boole dei sottoinsiemi di U. Fissati due sottoinsiemi A e B di U, con $A \subseteq B$, l'intervallo $[A;B]$ è l'insieme parzialmente ordinato il cui sostegno è la sottofamiglia di insiemi $\{X \subseteq U \mid A \subseteq C \subseteq B\}$ e l'ordine è quello indotto. Si osservi che se $A = \emptyset$, l'intervallo $[A,B]$ coincide con l'Algebra di Boole $\mathcal{B}(B)$.*

Definizione 1.1.5. *Siano $(P;\leq_P)$ e $(Q;\leq_Q)$ sono due insiemi parzialmente ordinati, il loro prodotto è l'insieme parzialmente ordinato il cui sostegno è il prodotto cartesiano $P \times Q$, e la relazione d'ordine è definita come segue:*

$$(a,b) \leq (c,d) \iff a \leq_P c,\ b \leq_Q d.$$

Il prodotto di tre o più poset si definisce in modo analogo.

1.1.1 Copertura e diagramma di Hasse

Definizione 1.1.6. *Sia $(P;\leq)$ un insieme parzialmente ordinato, e siano $x, y \in P$ tali che $x < y$. Si dice che x è coperto da y (oppure che y copre x) se risulta $[x;y] = \{x, y\}$, cioè se l'intervallo di estremi x e y si riduce alla catena formata dai due punti x e y. In questo caso si scrive che $x \prec y$; ovvero*

$$x \prec y \iff x < y \text{ e per ogni } z \in P \text{ tale che } x < z \leq y \text{ allora } z = y.$$

L'insieme $\{(x, y) \mid x, y \in P, x \prec y\}$ è una relazione in P, quindi la relazione di copertura è un particolare sottoinsieme della relazione d'ordine definita su P.

Esempio 1.1.6. *Nell'insieme parzialmente ordinato $(\mathbb{N};\leq)$ dove $\leq$ è l'ordinamento naturale, x è coperto da y se e solo se $y = x + 1$.*

Esempio 1.1.7. *Nel poset $(\mathbb{Z}^+, |)$ il numero x è coperto dal numero y se e solo se esiste un numero primo p tale che $y = p \cdot x$.*

Esempio 1.1.8. *Sia U un insieme non vuoto; nell'Algebra di Boole $\mathcal{B}(U)$ l'insieme A è coperto dall'insieme $B \iff$ esiste $x \in U \setminus A$ tale che $B = A \cup \{x\}$*

Proposizione 1.1.1. *Se $(P;\leq)$ è un poset finito la relazione di copertura determina completamente la relazione d'ordine $\leq$ su P.*

Dimostrazione. Definiamo la relazione d'ordine $\leq'$ su P come:

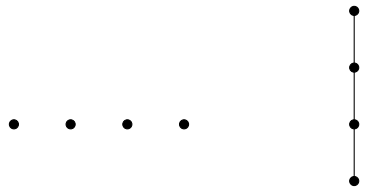
- per ogni $x \in P$, $x \leq' x$
- per ogni $x, y \in P$ con $x \neq y$, $x \leq' y$ se esistono $a_1, \ldots, a_n \in P$ tali che $x = a_1, y = a_n$ e valga $a_1 \prec a_2 \prec \cdots \prec a_n$

Mostriamo che per ogni $x, y \in P, x \leq' y \iff x \leq y$.
Per $x = y$ è banalmente vero per definizione, supponiamo quindi $x \neq y$. Se $x \leq' y$ esistono $a_1 \ldots a_n$ come sopra e per la proprietà transitiva di $\leq$ si ha $x \leq y$. Viceversa supponiamo che $x < y$; se non esiste $a \in P$ tale che $x < a < y$ allora ponendo $a_1 = x, a_2 = y$ si ha che $x \leq' y$; in caso contrario si considera la catena $x < a < y$, se non esistono nè b_1 nè b_2 tali che $x < b_1 < a$ e $a < b_2 < y$ allora il processo termina, in caso contrario si procede come prima. Tale algoritmo deve necessariamente terminare perchè ad ogni passo la lunghezza della catena tra x e y aumenta e non può essere più lunga di un certo intero n (che è la lunghezza del poset P che per ipotesi è finita). Dunque rinominando opportunamente gli a_i si ha che $x \leq' y$. □

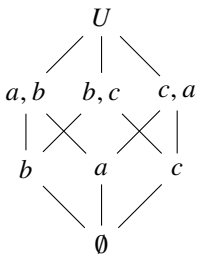
Per visualizzare graficamente un poset non è possibile rappresentare tutte le coppie della relazione $\leq$ perchè tale processo porterebbe, anche per poset molto piccoli, a rappresentazioni molto complicate. Tuttavia se abbiamo a che fare con un Poset finito possiamo rappresentare quest'ultimo limitandoci alla rappresentazione delle coppie della relazione di copertura associata. Tracciamo un grafo in modo tale che tutte le volte che l'elemento x è coperto da y, il punto corrispondente all'elemento x si trovi più

in basso rispetto al punto relativo all'elemento y. Con questa convenzione, possiamo disegnare i lati del grafo come segmenti anzichè come frecce. Il grafo così disegnato prende il nome di diagramma di Hasse delle relazione $\leq$. La relazione d'ordine $\leq$ può quindi essere ricostruita come nella dimostrazione precedente, ovvero due elementi sono confrontabili se e solo se fra l'uno e l'altro sale un percorso di segmenti che li collegano.

Esempio 1.1.9. *Di seguito vengono riportati i diagrammi di Hasse di una catena e di un'anticatena*



Esempio 1.1.10. *Sia $U = \{a, b, c\}$, il diagramma di Hasse dall'algebra di Boole $\mathcal{B}(U)$ è:*



1.1.2 Dualità

Definizione 1.1.7. *Sia $(P; \leq)$ un poset, si definisce l'ordinamento duale di $\leq$ e si indica con $\leq^*$ la seguente relazione d'ordine definita su P:*

$$\forall a, b \in P,\ a \leq^* b \iff b \leq a$$

Il poset $(P; \leq^*)$ è il poset duale di $(P; \leq)$.

Il fatto che l'inversa di una relazione d'ordine sia ancora una relazione d'ordine permette di formulare il principio di dualità. Se (t) è una proposizione espressa nei termini della teoria dei poset, si definisce la sua proposizione duale, e la si indica con (t^*), la proposizione ottenuta da (t) scambiando il termine "minore o uguale" con il termine "maggiore o uguale". Tale processo viene chiamato dualizzazione.

Teorema 1.1.1 (Principio di dualità)**.** *Se un teorema (t) della teoria degli insiemi parzialmente ordinati è vero, anche il suo duale (t*) è vero, e una dimostrazione di (t*) si ottiene dualizzando quella di (t).*

Esempio 1.1.11. *consideriamo la seguente affermazione:*

(t) In una catena ogni elemento è coperto al più da un elemento.

Una dimostrazione di questa affermazione è la seguente:
supponiamo che l'elemento $x$sia coperto da altri due elementi y e z; dato che questi ultimi due devono essere confrontabili, sarà ad esempio $y \leq z$; ma, poichè z deve coprire x, ciò implica $y = z$.
L'affermazione duale di t:

(t) In una catena ogni elemento copre al più un altro elemento.*

è automaticamente vera.

1.1.3 Morfismo d'ordine

Definizione 1.1.8. *Siano $(P; \leq_P)$ e $(Q; \leq_Q)$ due poset. Una funzione $f : P \to Q$ si dice morfismo d'ordine se*

$$\forall x, y \in P, x \leq_P y \implies f(x) \leq_Q f(y)$$

Un esempio banale di morfismo di poset è l'identità insiemistica.

Definizione 1.1.9. *La funzione $f : P \to Q$ si dice poi isomorfismo d'ordine se:*

1. *f è biettiva*
2. *f è un morfismo d'ordine*
3. *f^{-1} è un morfismo d'ordine*

o equivalentemente, se:

1. *f è biettiva*
2. *$\forall x, y \in P, x \leq_P y \iff f(x) \leq_Q f(y)$*

$(P; \leq_P)$ e $(Q; \leq_Q)$ sono isomorfi se esiste un isomorfismo d'ordine $f : P \to Q$.

1.2 Reticolo

Definizione 1.2.1. *Sia $(P; \leq)$ un poset; un elemento x di P si dice minimale se non esistono elementi in P strettamente minori di x, cioè se*

$$\forall y \in P,\ y \leq x \implies y = x.$$

Dualmente un elemento x di P si dice massimale se non esistono elementi in P strettamente maggiori di x, cioè se

$$\forall y \in P,\ x \leq y \implies x = y.$$

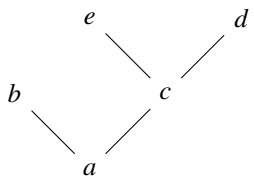
Notiamo che gli elementi minimali di un poset sono gli elementi massimale del duale e viceversa.
Se poi P possiede esattamente un elemento minimale, esso si dice minimo di P, e viene indicato con il simbolo 0.
Se P possiede esattamente un elemento massimale, esso si dice massimo di P, e viene indicato con il simbolo 1.

Esempio 1.2.1. *Sia U un insieme; l'algebra di Boole $\mathcal{B}(U)$ dei sottoinsiemi di U ha come minimo l'insieme vuoto e come massimo l'insieme U.*

Esempio 1.2.2. *Il poset $(\{a,b,c,d,e\};\leq)$ dove $\leq$ è l'insieme delle coppie*

$$\{(a;b),(a;c),(a;d),(a;e),(c;d),(c;e)\}$$

ha minimo, cioè a, ed ha tre elementi massimali, cioè b,e,d; di conseguenza non ha massimo.



Sia $(P;\leq)$ un poset, siano x e z due elementi di P. L'elemento z si dice maggiorante di x se è tale che $x \leq z$. Siano ora $x, y \in P$; l'insieme M dei maggioranti comuni di x ed y, cioè $M = \{z \in P \mid x \leq z, y \leq z\}$ è un sottoordine di P; se esso ammette minimo, tale minimo viene detto estremo superiore (o "sup") di x ed y, ed indicato con il simbolo $x \vee y$.
Dalla definizione è evidente che $x \vee y = y \vee x$, e che:

$$x \vee y = y \iff x \leq y.$$

Dualmente, un elemento t di P, si dice minorante di x se è tale che $t \leq x$. Se poi x e y sono due elementi di P, consideriamo l'insieme M' dei minoranti comuni di x ed y, $M' = \{z \in P \mid z \leq x, z \leq y\}$; se M' ammette massimo, tale massimo viene detto estremo inferiore di x ed y (o "inf"), e viene indicato con $x \wedge y$.
Anche in questo caso abbiamo che $x \wedge y = y \wedge x$ e che

$$x \wedge y = x \iff x \leq y$$

E' evidente che le nozioni di sup e di inf sono una duale dell'altra.

Definizione 1.2.2. *Sia $(P,\leq)$ un poset non vuoto. Si dice che P è un reticolo se per ogni coppia di elementi $x, y \in P$, esistono $x \vee y$ e $x \wedge y$.*

La nozione di reticolo è autoduale: di conseguenza, se un poset è un reticolo lo è anche il suo duale. In un reticolo $(L;\leq)$ possono quindi essere definite due funzioni binarie: l'estremo superiore e l'estremo inferiore:

$$\vee : L \times L \to L,\ (x, y) \mapsto x \vee y$$
$$\wedge : L \times L \to L,\ (x, y) \mapsto x \wedge y.$$

Esempio 1.2.3. *Il poset $(\mathbb{Z}^+; |)$ è un reticolo: infatti dati due interi positivi il loro sup coincide con il minimo comune multiplo e il loro inf con il massimo comune divisore.*

Esempio 1.2.4. *Sia U un insieme; l'Algebra di Boole $\mathcal{B}(U)$ dei sottoinsiemi di U è un reticolo: dati due sottoinsiemi di U il sup coincide con l'unione dei due insiemi e l'inf coincide con l'intersezione dei due insiemi.*

Esempio 1.2.5. *Un poset che possiede due o più elementi minimali non è un reticolo perchè: se x e y sono due dei suoi elementi minimali, l'insieme dei minoranti comuni di x e y è vuoto, e quindi non possiede massimo. Dualmente, un poset che possiede due o più elementi massimali distinti non è un reticolo.*

Esempio 1.2.6. *Una qualunque catena C è un reticolo, dato che per ogni $x, y \in C$ risulta:*

$$x \leq y \implies x \vee y = y, \quad x \wedge y = x$$
$$\textit{oppure}$$
$$y \leq x \implies x \vee y = x, \quad x \wedge y = y.$$

Esempio 1.2.7. *$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ dotati dell'ordinamento usuale sono reticoli: il sup tra due elementi è il maggiore dei due, l'inf tra due elementi è il minore dei due.*

I reticoli possono essere caratterizzati come strutture algebriche che soddisfano determinate identità

Definizione 1.2.3. *Consideriamo una struttura algebrica $(L; \vee; \wedge)$ dove L è un insieme e $\wedge, \vee$ sono due operazioni binarie $\vee, \wedge : L \times L \to L$. Diciamo che L è un reticolo astratto se per ogni $x, y, z \in L$ sono verificate le seguenti identità:*

1. $x \vee x = x, x \wedge x = x$ *(idempotenza);*
2. $x \vee y = y \vee x, x \wedge y = y \wedge x$ *(commutativa);*
3. $(x \vee y) \vee z = x \vee (y \vee z)$ *(associativa di $\vee$);*
4. $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ *(associativa di $\wedge$);*
5. $x \vee (x \wedge y) = x = x \wedge (x \vee y)$ *(assorbimento).*

Si verifica poi usando la definizione data di sup e di inf che un reticolo $(P; \leq)$ è sempre un reticolo astratto.
Viceversa:
se $(L; \vee; \wedge)$ è un reticolo astratto, la relazione $\leq$ definita da

$$x \leq y \iff x \vee y = y$$

è una relazione d'ordine tale che nel poset $(L; \leq)$ il sup due elementi x, y in L è proprio $x \vee y$, e l'inf di x, y è $x \wedge y$.
Di conseguenza le nozioni di reticolo astratto e di reticolo coincidono.

1.2.1 Reticolo completo

Sia $(L; \vee; \wedge)$ un reticolo, e sia $S \subseteq L$, $S \neq \emptyset$. Consideriamo l'insieme M dei maggioranti comuni di tutti gli elementi di S, cioè:

$$M := \{z \in L \mid x \leq z, \text{ per ogni } x \in S\}.$$

Questo è un sottoordine di L; se esso ammette minimo, tale minimo è detto estremo superiore del sottoordine S, e indicato con $\bigvee S$.
Dualmente, sia M' l'insieme dei minoranti comuni di tutti gli elementi di S, cioè:

$$M' := \{z \in L \mid z \leq x, \text{ per ogni } x \in S\}.$$

Anche questo è un sottoordine di L; se esso ammette massimo, tale massimo viene chiamato estremo inferiore del sottoinsieme S, e indicato con $\bigwedge S$.

Definizione 1.2.4. *Un reticolo $(L; \vee; \wedge)$ si dice completo se esistono l'estremo superiore e l'estremo inferiore di ogni sottoinsieme non vuoto di L.*

Si noti che un reticolo completo è sempre dotato di minimo e di massimo; infatti l'elemento $\bigvee L$ è il minimo degli elementi massimali di L, e quindi il massimo di L; dualmente $\bigwedge L$ è il minimo di L.

Esempio 1.2.8. *Per ogni insieme U, l'algebra di Boole $\mathcal{B}(U)$ è un reticolo completo, perchè si possono sempre determinare l'unione e l'intersezione di qualunque famiglia di sottoinsiemi di U.*

Esempio 1.2.9. *Il poset $(\mathbb{N}, \leq)$, dove $\leq$ è l'ordinamento naturale, è una catena, e quindi un reticolo; tuttavia, esso non è completo, perchè, ad esempio, non esiste il sup del sottoinsieme di $\mathbb{N}$ costituito dai numeri pari. Osserviamo che, invece, ogni sottoinsieme di $\mathbb{N}$ ammette estremo inferiore.*

Esempio 1.2.10. $(\mathbb{R}; \leq)$ *dove $\leq$ è l'ordinamento naturale, è anch'esso un reticolo non completo perchè per esempio non esiste il sup dell'insieme $\{x \in \mathbb{R} \mid x > 2\}$*

Teorema 1.2.1. *In un reticolo ogni sottoinsieme finito ammette sup e inf. Di conseguenza, un reticolo finito è sempre completo; in particolare è dotato di minimo e di massimo.*

1.2.2 Sottoreticolo; morfismo di reticoli

Definizione 1.2.5. *Un sottoinsieme non vuoto S di un reticolo L si dice sottoreticolo se è chiuso rispetto alle operazioni di inf e di sup definite su L; cioé se verifica la seguente condizione:*

$$\forall x, y \in S\text{: } x \vee y \in S,\ x \wedge y \in S.$$

Esempio 1.2.11. *Sia $(L; \vee; \wedge)$ un reticolo, e siano $x, y \in L$ tali che $x \leq y$; allora l'intervallo $[x; y]$ è un sottoreticolo: infatti $\forall z, t \in [x; y]$ risulta:*

$$x \leq z,\ t \leq y \implies x \leq z \vee t \leq y,\ x \leq z \wedge t \leq y$$

Definizione 1.2.6. *Siamo $(L; \vee; \wedge)$ e $(L'; \vee'; \wedge')$. Una funzione $f: L \to L'$ si dice morfismo di reticoli se verifica la seguenti condizioni: per ogni x,y $\in L$*

$$f(x \vee y) = f(x) \vee' f(y)$$
$$f(x \wedge y) = f(x) \wedge' f(y).$$

Osservazione 1.2.1. *E' immediato riconoscere che un morfismo di reticoli è anche un morfismo d'ordine, mentre il viceversa è falso: un morfismo d'ordine tra due reticoli può non essere un morfismo di reticoli.*

Esempio 1.2.12. *Sia U insieme finito non vuoto; la funzione*

$$f: \mathcal{P}(U) \to \mathbb{N} \text{ tale che } f(X) = |X|$$

è un morfismo d'ordine tra l'algebra di Boole $\mathcal{B}(U)$ e la catena $(\mathbb{N}, \leq)$, dove $\leq$ è l'ordinamento naturale; tuttavia f non è un morfismo di reticoli, perchè, se X, Y sono due sottoinsieme di U tali che $X \nsubseteq Y$ e $Y \nsubseteq X$ si ha:

$$f(X \cup Y) = |X \cup Y| \neq max\{|X|; |Y|\} = |X| \vee |Y|;$$

dato che in una catena il sup di due elementi coincide con il maggiore dei due.

Definizione 1.2.7. *Dati due reticoli L, L', una funzione $f: L \to L'$ si dice isomorfismo di reticoli se:*

1. *f è biettiva*
2. *f è un morfismo di reticoli.*

Si noti che se f verifica le due condizioni la funzione inversa f^{-1} risulta automaticamente un morfismo di reticoli.
Due reticoli si dicono isomorfi se esiste un isomorfismo di reticoli $f: L \to L'$.

Definizione 1.2.8. *Se a e b sono due elementi di un poset $(P;\leq)$ tali che $a \leq b$, per catena tra l'elemento a e l'elemento b si intende una catena dell'intervallo $[a,b]$.*
Una catena C tra a e b si dice massimale (o satura) se non esiste nessuna catena tra a e b che contenga propriamente C, cioè non esiste nessun altro elemento $x \in [a,b] \setminus C$ tale che $C \cup \{x\}$ sia ancora una catena.

Le catene massimali sono caratterizzate dal prossimo enunciato:

Teorema 1.2.2. *Sia $(P;\leq)$ un poset, consideriamo una catena massimale finita $C := \{a, x_1, x_2, \ldots, x_h, b\}$ tra due elementi a e b di P, con $a < x_1 < x_2 < \cdots < x_h < b$. Allora si ha necessariamente che $a \prec x_1 \prec x_2 \prec \cdots \prec x_h \prec b$.*

Dimostrazione. Supponiamo che a non sia coperto da x_1; allora esisterà un elemento y diverso da a e da x_1 tale che $a < y < x_1$ e di conseguenza l'insieme $\{a, y, x_1, x_2, \ldots, x_h, b\}$ è una catena tra a e b che contiene propriamente C, e questo è assurdo, perchè C è massimale. Analogamente si prova che ci deve essere copertura tra tutti gli altri elementi consecutivi della catena C. □

Definizione 1.2.9. *Se C è una catena finita, si dice lunghezza di C il numero $|C| - 1$.*

Definizione 1.2.10. *Un poset $(P;\leq)$ si dice con catene finite se, presi comunque due elementi $x, y \in P$, con $x \leq y$, tutte le catene tra x e y sono finite.*

Due esempi importanti di poset con catene finite sono i poset localmente finiti, ovvero quelli in cui tutti gli intervalli sono finiti, e i poset in cui tutte le catene sono finite.
Supponiamo d'ora in avanti di avere a che fare con poset con catene finite. Tale condizione di finitezza in generale non verrà menzionata esplicitamente negli enunciati che seguiranno.
La relazione di inclusione e quella di raffinamento suggeriscono l'introduzione del concetto di rango, che è la generalizzazione del concetto di cardinalità di un insieme e di quella di dimensione per un sottospazio, e di atomicità, che un'astrazione del fatto che un insieme è unione degli elementi che lo compongono o del fatto che uno spazio è unione dei suoi sottospazi unidimensionali.

Definizione 1.2.11. *Si dice che un insieme parzialmente ordinato $(P;\leq)$ verifica la condizione di Jordan Dedekind se , per ogni coppia di elementi $x, y \in P$, con $x \leq y$, tutte le catene massimali da x a y sono finite ed hanno la stessa lunghezza.*

Supponiamo ora che il poset $(P;\leq)$ verifichi la condizione di Jordan-Dedekind e che sia dotato di minimo 0; allora, in particolare, per ogni $x \in P$, tutte le catene da 0 a x hanno la stessa lunghezza finita; tale lunghezza viene chiamata rango dell'elemento x, e indicata con il simbolo $r(x)$.

Esempio 1.2.13. *L'insieme $\mathbb{Z}$ dei numeri interi con l'ordinamento naturale verifica la condizione di Jordan-Dedekind: infatti fissati due qualunque elementi $x, y \in \mathbb{Z}$ con $x \leq y$, esiste un'unica catena tra x e y, la cui lunghezza è pari a $y - x$. Invece l'insieme $\mathbb{Q}$ dei numeri razionali con l'ordinamento usale non verifica la condizione di Jordan-Dedekind, perchè comunque fissati due numeri $x, y \in \mathbb{Q}$ esiste un'unica catena da x a y, che però non è finita.*

Esempio 1.2.14. *Se U è un insieme finito, l'algebra di Boole $\mathcal{B}(U)$ dei sottoinsiemi di U verifica la condizione di Jordan-Dedekind e per ogni $X \subseteq U$ si ha che $r(X) = |X|$.*

Gli insiemi parzialmente ordinati dotati di rango si possono caratterizzare nel modo seguente:

Proposizione 1.2.1. *Sia P un poset dotato di minimo 0. Se P soddisfa la condizione di JD, allora è ben definita la funzione rango $r\colon P \to \mathbb{N}$:*

1. $r(0) = 0$,
2. $a \prec b \implies r(b) = r(a) + 1$.

Viceversa, se P ammette una funzione $r\colon P \to \mathbb{N}$ tale che valgono 1) e 2) allora P soddisfa la condizione di JD e r è la sua funzione rango.

Definizione 1.2.12. *Un atomo di un reticolo L dotato di minimo 0 è un elemento che copre lo 0.*
Un reticolo L , dotato di minimo, si dice atomico se ogni suo elemento diverso dal minimo si può esprimere come estremo superiore di atomi.

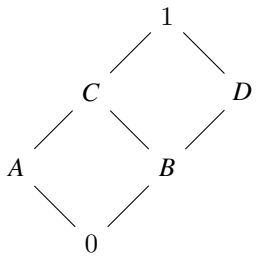
Per enfatizzare la natura geometrica di diversi problemi, gli atomi saranno anche chiamati punti del reticolo. Quindi in un reticolo, dove è ben definita la funzione rango r, i punti p sono elementi del reticolo tali che $r(p) = 1$.

Esempio 1.2.15. *Per ogni insieme $U \neq \emptyset$, gli atomi dell'algebra di Boole $\mathcal{B}(U)$ sono tutti e soli gli insiemi di cardinalità 1. Il reticolo $\mathcal{B}(U)$ è atomico perchè per ogni $S \subseteq U$ si ha che $S = \bigcup_{x \in S}\{x\}$.*

Esempio 1.2.16. *Se V è uno spazio vettoriale di dimensione finita e $S(V)$ è il reticolo dei suoi sottospazi, allora gli atomi di $S(V)$ sono tutti e soli i sottospazi di V avente dimensione 1. $S(V)$ è atomico perchè per ogni U sottospazio di V, se $\{u_1, \ldots, u_m\}$ è una base di U allora risulta che $U = span\{u_1\} \vee \cdots \vee span\{u_m\}$*

Esempio 1.2.17. *Nel reticolo degli interi positivi ordinati per divisibilità gli atomi sono tutti e soli i numeri primi. Tale reticolo non è atomico perchè non tutti i numeri si riescono ad esprimere come prodotto di numeri primi.*

Esempio 1.2.18. *Consideriamo il seguente reticolo:*



Gli atomi sono A e B ma il reticolo non è atomico perchè l'elemento D non si può esprimere come estremo superiore di atomi.

Capitolo 2

Reticoli distributivi

2.1 Rappresentazione come reticolo degli ideali

Definizione 2.1.1. *Un reticolo L si dice distributivo se le seguenti due identità, dette identità distributive, valgono per ogni $x, y, z \in L$:*

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

Dunque in un reticolo distributivo l'operazione di "inf" è distributiva rispetto l'operazione di "sup", e viceversa.
Si noti che:

- *Segue immediatamente dalla definizione che ogni sottoreticolo di un reticolo distributivo L è un reticolo distributivo in quanto le leggi distributive devono valere per ogni terna x, y, z di elementi di L. Analogamente, il prodotto di reticoli distributivi è un reticolo distributivo.*

- *Le due identità sono una duale dell'altra; dunque, se un reticolo è distributivo, anche il suo duale lo è.*

- *Le due identità sono una conseguenza dell'altra infatti,*
  sapendo che vale la prima identità, ricordando le proprietà dell'inf e del sup, ponendo $w = x \vee y$ si ha che :

$$\begin{aligned}(x \vee y) \wedge (x \vee z) = w \wedge (x \vee z) &= (w \wedge x) \vee (w \wedge z) \\ &= ((x \vee y) \wedge x) \vee (x \vee y \wedge z) = x \vee (x \vee y \wedge z) \\ &= x \vee (y \wedge z).\end{aligned}$$

  La dimostrazione è analoga se supponiamo che valga la seconda identità.

- *Le due identità possono essere generalizzate ad un finito numero di variabili:*

$$(\bigvee_{i=1}^{m} x_i) \wedge (\bigvee_{j=1}^{n} y_j) = \bigvee_{i,j=1}^{n,m} (x_i \wedge y_j),$$
$$(\bigwedge_{i=1}^{m} x_i) \vee (\bigwedge_{j=1}^{n} y_j) = \bigwedge_{i,j=1}^{n,m} (x_i \vee y_j).$$

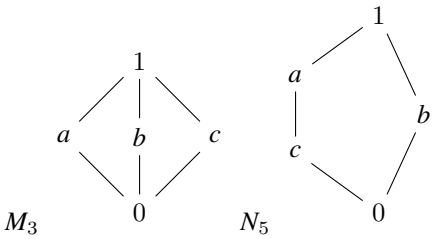
Esempio 2.1.1. *Una catena è sempre un reticolo distributivo. Quindi ogni sottoreticolo di un prodotto di catene è distributivo.*

Esempio 2.1.2. *Sia U un insieme. L'algebra di Boole $\mathcal{B}(U)$ è un reticolo distributivo.*

Esempio 2.1.3. *Un reticolo con al più quattro elementi è distributivo.*
Dei cinque reticoli che contengono 5 elementi, tre sono distributivi, due no:

- *il reticolo M_3 non è distributivo infatti*
  $a \wedge (b \vee c) = a \wedge 1 = a$
  mentre
  $(a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0 \neq a$

- *il reticolo N_5 non è distributivo infatti:*
  $a \wedge (b \vee c) = a \wedge 1 = a$
  mentre
  $a \wedge b) \vee (a \wedge c) = 0 \vee c = c \neq a$



Esaminiamo ora un modo per decomporre gli elementi di un reticolo distributivo come *sup* di particolari elementi detti sup-irriducibili. Tale decomposizione gioca il ruolo della decomposizione dei numeri in prodotto di potenze di primi; infatti se si considera l'insieme dei numeri naturali con l'operazione di minimo comune multiplo e massimo comune divisore la decomposizione che andremo a descrivere coinciderà con la decomposizione di un numero nei suoi fattori primi.

Definizione 2.1.2. *Un elemento a di un reticolo L si dice sup-irriducibile se è diverso dal minimo del reticolo e non si può esprimere come estremo superiore di altri elementi, cioè se,*

$$a = b \vee c \implies b = a \quad \textit{oppure} \quad c = a$$

dualmente, l'elemento a si dice inf-irriducibile se è diverso dal massimo del reticolo e se

$$a = b \wedge c \implies b = a \text{ oppure } c = a.$$

Proposizione 2.1.1. *Sia L un reticolo con catene finite, allora*

1. *a è sup-irriducibile $\iff$ a copre un solo elemento del reticolo.*
2. *gli atomi sono elementi sup-rriducibili del reticolo.*

Dimostrazione. La 2) segue banalmente dalla 1) perchè un atomo è un elemento del reticolo che copre lo 0. Supponiamo che l'elemento a copra un unico elemento che chiamiamo a'. Se a non fosse sup-irriducibile allora esisterebbero $b, c \in L$ tali che $a = b \vee c$ con $a \neq b, c$ e quindi $b, c < a$. Ma siccome l'unico elemento coperto da a è a' segue che $b, c < a'$ e quindi $a \neq b \vee c$. Viceversa, se a è sup-irriducibile, supponiamo per assurdo che esistano $b, c \in L$ tali che $b \prec a$ e $c \prec a$. In tal caso $a = b \vee c$ ma questo è assurdo perchè in ipotesi a è sup-irriducibile. □

In maniera analoga si dimostra che un elemento è inf-irriducibile se e solo se è coperto da un solo elemento.

Esempio 2.1.4. *In una catena tutti gli elementi sono sup-irriducibili.*
Gli elementi sup-irriducibili dell'Algebra di Boole $\mathcal{B}(U)$ sono i sottoinsiemi di U che contengono un solo elemento.
Nel reticolo $(\mathbb{Z}^+; |)$ gli elementi sup-irriducibili sono le potenze dei numeri primi.

Riportiamo alcuni esempi grafici che servono per chiarire il concetto di elemento sup-irriducibile e di elemento inf-irriducibile:

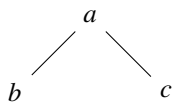


Figura 2.1: a non è sup-irriducibile perchè copre due elementi.

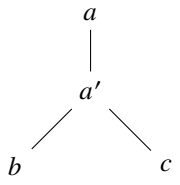


Figura 2.2: a è sup-irriducibile perchè copre solo l'elemento a'

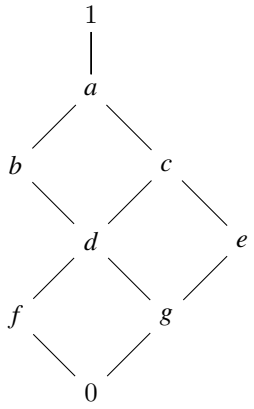


Figura 2.3: Gli elementi sup-irriducibili del reticolo sono: $g, f, e, b, 1$
gli elementi inf-irriducibili del reticolo sono: a, b, c, f, e

Definizione 2.1.3. *Un'espressione $a = p_1 \vee p_2 \vee \cdots \vee p_k$, dove ogni p_i è un sup-irriducibile, è chiamata decomposizione (finita) di a.*
La decomposizione è irridondante se $a \neq p_1 \vee \cdots \vee p_{i-1} \vee p_{i+1} \cdots \vee p_k$ per ogni i.
Ovviamente, in ogni decomposizione irridondante gli elementi sup-irriducibili sono a due a due non confrontabili, e formano un'anticatena.

In un reticolo distributivo con catene finite gli elementi sup-irriducibili consentono di ricostruire ogni altro elemento:

Lemma 2.1.1. *Sia p un elemento sup-irriducibile di un reticolo distributivo L. Si ha:*

$$p \leq a_1 \vee ... \vee a_k \implies p \leq a_i \text{ per qualche } i.$$

Dimostrazione. Dalle leggi distributive abbiamo che $p \leq a_1 \vee \cdots \vee a_k \implies p = p \wedge (\bigvee_{i=1}^{k} a_i) = \bigvee_{i=1}^{k} (p \wedge a_i)$. Dato che p è sup-irriducibile, questo implica che $p = p \wedge a_i$ per qualche i, da cui la tesi. □

Osservazione 2.1.1. *Se $\{p_1, p_2, \dots\}$ è un insieme di atomi di un reticolo distributivo allora $p_1 < p_1 \vee p_2 < p_1 \vee p_2 \vee p_3 < \dots$ forma una catena strettamente crescente (per il lemma).*

Corollario 2.1.1. *Un reticolo distributivo con catene finite è localmente finito.*

Dimostrazione. Applicando l'osservazione agli atomi di un intervallo, possiamo concludere dall'ipotesi di finitezza sulle catene che ogni intervallo di una reticolo distributivo contiene un numero finito di atomi (altrimenti le catene tra due elementi non sarebbero tutte finite). Segue che gli intervalli di un reticolo distributivo con catene finite sono finiti, quindi gli intervalli sono reticoli distributivi finiti, quindi sono dei reticoli completi. □

Lemma 2.1.2. *Se L è un reticolo distributivo dotato di minimo 0 e se $P \subseteq L$ è l'insieme degli elementi sup-irriducibili di L, allora ogni $a \in L$ possiede un'unica decomposizione irridontante $a = p_1 \vee \cdots \vee p_h$*

con $p_1, \ldots, p_h \in P$*;*
in tal caso definiamo $P(a) := \{p_1, ..., p_h\}$ *con* $P(0) := \emptyset$.

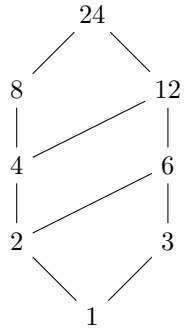
Dimostrazione. Esistenza: sia a è un elemento del reticolo L; se a non è sup-irriducibile, si potrà scrivere come $a = b \vee c$, con $b, c \in L$. Se b e c sono entrambi sup-irriducibili, avremo espresso a nel modo voluto; se invece almeno uno tra b e c non è sup-irriducibile, si potrà scrivere a sua volta come sup di altri due elementi. Proseguendo in questo modo, grazie all'ipotesi di finitezza (F), dopo un numero finito di passi avremo espresso a come sup di elementi sup-irriducibili. Osserviamo poi che, se risulta $a = p_1 \vee \cdots \vee p_k$ e si ha ad esempio $p_1 \leq p_2$, allora $p_1 \vee p_2 = p_2$; dunque, si ha anche $a = p_2 \vee \cdots \vee p_k$; continuando ad eliminare eventuali coppie di elementi confrontabili, si arriva a rappresentare a come sup di elementi tra loro inconfrontabili.
Unicità: supponiamo esistano due decomposizioni irridondanti di a: $P(a) = \{p_1, p_2, \ldots, p_h\} = \{q_1, q_2, \ldots, q_k\}$. Allora si ha $p_1 \vee \cdots \vee p_h = q_1 \vee \cdots \vee q_k$. Per il Lemma precedente, p_1 deve essere minore o uguale di uno dei q_i; supponiamo $p_1 \leq q_1$. D'altronde; $(q_1 \wedge (p_2 \vee \cdots \vee p_h)) = (q_1 \vee p_1) \wedge (p_1 \vee p_2 \vee \cdots \vee p_h) = q_1$ da cui $p_1 = q_1$. Ripetendo il ragionamento si ha la tesi. □

Abbiamo quindi dimostrato che ogni elemento di un reticolo distributivo con catene finite si può esprimere in uno ed un solo modo come estremo superiore di elementi sup-irriducibili tra loro inconfrontabili; ovvero ogni elemento del reticolo corrisponde ad un unico sottoinsieme (che è un'anticatena) $P(a)$ del poset degli elementi sup-irriducibili P.

Esempio 2.1.5. *Facendo riferimento al reticolo in figura, decomponiamo l'elemento* 24*:*

$$24 = 8 \vee 12 = 8 \vee 4 \vee 6 = 8 \vee 4 \vee 2 \vee 3.$$

Abbiamo scritto quindi 24 *come* **sup** *di elementi sup-irriducibili. Togliamo gli elementi ridondanti, ovvero quelli che sono minori di qualche altro elemento nella decomposizione (*4 *e* 2*), allora* $24 = 8 \vee 3$.



Definizione 2.1.4. *Se* P *è un poset, un suo ideale d'ordine (spesso viene chiamato anche solo ideale) è un sottoinsieme* I *di* P *tale che:*

$$\text{se } x \in I,\ y \leq x \implies y \in I.$$

Osserviamo che:

- l'insieme vuoto è un ideale.
- Sia S un sottoinsieme non vuoto dell'insieme parzialmente ordinato P; l'insieme $I(S) := \{x \in P \mid x \leq a \text{ per qualche } a \in S\}$ è un ideale d'ordine, che viene detto ideale generato da S.
  Se poi $S = \{a\}$ l'ideale $I(S)$ viene indicato con $I(a)$ e viene detto ideale principale generato da a.
  Osserviamo che ogni ideale coincide con l'ideale generato dai suoi elementi massimali, quindi un ideale è principale se e solo se esso ammette massimo.
- Il concetto duale di ideale è quello di filtro: precisamente, un filtro di P e un sottoinsieme I di P tale che:

  $$x \in I, x \leq y \implies y \in I.$$

  Ovviamente, i filtri di P sono tutti e soli gli ideali del suo duale P^*, e viceversa.

Esempio 2.1.6. *In un'anticatena tutti i sottoinsiemi sono sia ideali che filtri, inoltre gli ideali e i filtri principali sono i singoletti. In una catena finita tutti gli ideali sono principali.*

Esempio 2.1.7. *Consideriamo il Poset $(\mathbb{Q}; \leq)$ dove $\leq$ è l'ordinamento naturale, l'insieme*

$$A := \{a \in \mathbb{Q} \mid a < 1\}$$

è un ideale ma non è principale perchè per ogni $a \in A$ si ha che $\frac{a+1}{2} \in A$ e $a < \frac{a+1}{2}$.

L'insieme degli ideali di P, ordinati dall'inclusione, fornisce un esempio fondamentale di reticolo distributivo. Infatti:

Teorema 2.1.1 (Primo teorema di Birkhoff)**.** *Sia P un insieme parzialmente ordinato; la famiglia $\mathcal{I}(P)$ degli ideali d'ordine di P, ordinati dall'inclusione, è un reticolo distributivo.*

Dimostrazione. Dal momento che l'unione e l'intersezione di due ideali sono ancora ideali, abbiamo che $\mathcal{I}(P)$ è un sottoreticolo dell'algebra di Boole $\mathcal{B}(P)$. La tesi segue ora dal fatto che ogni sottoreticolo di un reticolo distributivo è distributivo. □

In particolare se P è un'anticatena, gli ideali sono i sono gli insiemi che contengono un singolo elemento di P, quindi il reticolo $\mathcal{I}(P)$ è l'algebra di Boole dei sottoinsiemi di P. Si noti inoltre che gli elementi sup-irriducibili di $\mathcal{I}(P)$ sono gli ideali principali di P.
E' interessante notare come la corrispondenza che associa ad un insieme parzialmente ordinato P il reticolo distributivo $\mathcal{I}(P)$ si "comporti bene" rispetto alla dualità. Infatti:

Teorema 2.1.2. *Sia P^* il duale d'ordine del poset P; allora, il reticolo $\mathcal{I}(P^*)$ è isomorfo al duale di $\mathcal{I}(P)$.*

Dimostrazione. E' sufficiente osservare che il sottoinsieme complementare di un ideale è un filtro, e viceversa, e che la funzione

$$\psi : \mathcal{I}(P) \to \mathcal{I}(P*) \text{ tale che } \psi(I) = P \setminus I$$

è una biezione che inverte l'ordine. □

Osservazione 2.1.2. *Abbiamo quindi dimostrato che il reticolo degli ideali del duale di P è isomorfo al reticolo dei filtri di P, entrambi ordinati dall'inclusione. Indichiamo quest'ultimo $\mathcal{F}(P)$.*

Un altro sottoreticolo è il reticolo $\mathcal{I}_f(P)$ degli ideali di P finiti. Ovviamente, essendo sottoreticolo di un reticolo distributivo, $\mathcal{I}_f(P)$ è distributivo e il seguente teorema mostra come ogni reticolo distributivo con catene finite è di questa forma:

Teorema 2.1.3 (Secondo teorema di Birkhoff)**.** *Sia L un reticolo distributivo con catene finite dotato di minimo 0 e $P \subseteq L$ il poset dei suoi elementi sup-irriducibili, allora $L \cong \mathcal{I}_f(P)$ attraverso l'isomorfismo $\phi : a \mapsto \mathcal{I}(a) = \{p \in P;\ p \leq a\}$ con $a \in L$.*
Viceversa:
ogni reticolo $\mathcal{I}_f(P)$ è distributivo e il poset dei suoi elementi sup-irriducibili è isomorfo a P.

Dimostrazione. ϕ è iniettiva perchè ogni elemento $a \in L$ è determinato univocamente dall'insieme degli elementi irriducibili che compaiono nella sua decomposizione, ovvero dall'insieme $P(a) = \{p_i \in P; p_i \leq a\}$. ϕ è suriettiva perchè dato $I \in \mathcal{I}_f(P)$ con $b = supI$ ho che $I \subseteq I(b)$; ma per ogni $p \in I(b)$, $p \leq supI$, segue che $p \in I$; quindi ogni ideale finito di P è della forma $I(a)$. Abbiamo dimostrato quindi che ϕ è una biezione. Verifichiamo che è un morfismo d'ordine: supponiamo $a \leq b$ in L, chiaramente $I(a) \subseteq I(b)$; viceversa se $I(a) \subseteq I(b)$ si ha che $a = supI(a) \leq supI(b) = b$. Quindi ϕ rispetta gli ordinamenti. Infine nel reticolo distributivo $\mathcal{I}_f(P)$ un elemento (che è un ideale) è irriducibile se e solo se è vuoto oppure della forma $I(a)$ con $a \in P$. □

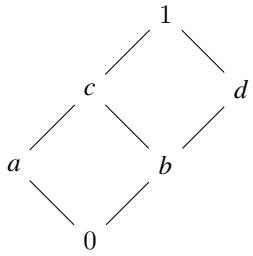
Osservazione 2.1.3. *Nelle notazioni del teorema, L finito $\implies$ $L \cong \mathcal{I}(P)$. Cioè ogni reticolo distributivo finito è isomorfo al reticolo degli ideali dell'insieme parzialmente ordinato dei suoi elementi sup-irriducibili.*

Siccome la relazione d'ordine in $\mathcal{I}_f$ è l'inclusione segue che:

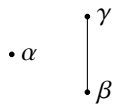
Corollario 2.1.2. *Ogni reticolo distributivo dotato di minimo 0 è isomorfo ad un sottoreticolo dell'algebra di Boole.*

Inoltre, sempre dal secondo teorema di Birkhoff deduciamo che gli elementi sup-irriducibili di un reticolo distributivo permettono di individuare l'intero reticolo, a meno di isomorfismi:

Corollario 2.1.3. *Due reticoli distributivi sono isomorfi se e solo se i rispettivi poset degli elementi sup-irriducibili lo sono.*



Esempio 2.1.8. *Il reticolo*
è isomorfo al reticolo degli ideali d'ordine dell'insieme parzialmente ordinato il cui diagramma di Hasse é:



Un possibile isomorfismo è:

$$0 \mapsto \emptyset \quad a \mapsto \{\alpha\}, \quad b \mapsto \{\beta\},$$
$$c \mapsto \{\alpha, \beta\}, \quad d \mapsto \{\beta, \gamma\}, \quad 1 \mapsto \{\alpha, \beta, \gamma\}$$

Corollario 2.1.4. *In un reticolo distributivo finito, il poset P degli elementi sup-irriducibili e il poset Q degli elementi inf-irriducibili sono isomorfi.*

Dimostrazione. Essendo $P = Q^*$ si ha che $\mathcal{I}(P) \cong \mathcal{F}(Q)$. Dal secondo teorema di Birkhoff $L \cong \mathcal{I}(P)$ e $L^* \cong \mathcal{F}(Q)$, segue che $L \cong L^*$ ed essendo P e Q i rispettivi poset degli elementi sup-irriducibili si ha che $P \cong Q$. □

2.2 Prodotto di catene e codifica

Sia ora L un reticolo distributivo finito. Sappiamo che questo è isomorfo ad un sottoreticolo di un'algebra di Boole $\mathcal{B}(S)$. Posto $n = |S|$, l'applicazione $\phi\colon \mathcal{B}(S) \to \{0,1\}^n$, che manda ogni sottoinsieme di S nel suo vettore caratteristico, è un isomorfismo. Possiamo dunque dire che L è isomorfo ad un sottoreticolo di un prodotto di catene.
Quante catene C_i sono necessarie affinchè L sia immerso nel prodotto $\prod_i C_i$?(Ovvero affinchè $\prod_i C_i$ contenga una copia isomorfa di L).
Senza perdita di generalità supponiamo $C_i = \{0 < 1 < \cdots < c_i\}$ dove $c_i \in \mathbb{N}$ per ogni i.
Un'immersione $\phi\colon L \to \prod_{i=1}^{d} C_i$ è chiamata codifica di L e d la dimensione della codifica.
Ci chiediamo quindi quale sia la minima dimensione tra tutte le possibili dimensioni delle codifiche di L.
Come esempio consideriamo un'Algebra di Boole finita $\mathcal{B}(S)$. Chiaramente $\phi\colon \mathcal{B}(S) \to \{0,1\}^n$ definita come sopra, è una codifica di $\mathcal{B}(S)$ di dimensione n.

Proposizione 2.2.1. *Sia L un reticolo distributivo dotato di minimo 0, P il poset dei suoi elementi sup-irriducibili e $P = \bigcup P_i$ un'arbitraria partizione di P in catene P_i. Ponendo $C_i = P_i \cup \{0\}$ per ogni i esiste un isomorfismo $\phi\colon L \to \prod_i C_i$ di L su un sottoreticolo di $\prod_i C_i$*

Dimostrazione. Definiamo $x_i = sup\{z \in C_i; z \leq x\}$ per ogni $x \in L$ e per ogni i. (La definizione è ben posta perchè gli intervalli sono finiti.) Possiamo allora definire

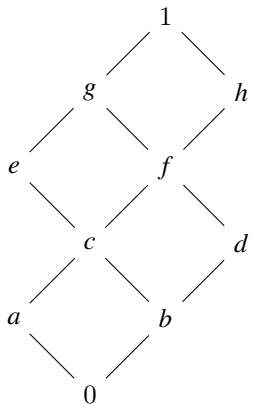
$$\phi\colon L \to \prod_i C_i \ , \ \phi(x) = (\dots, x_i, \dots).$$

Supponiamo $\phi(x) = \phi(y)$ cioè $x_i = y_i$ per ogni i. Allora $I(x) = I(y)$ quindi $x = y$ (per il secondo teorema di Birkhoff l'applicazione che a $x \mapsto I(x)$ è iniettiva). Inoltre

$$(x \vee y)_i = sup\{z \in C_i;\ z \leq x \vee y\} = sup\{z \in C_i;\ z \leq x \text{ o } z \leq y\} = x_i \vee y_i,$$

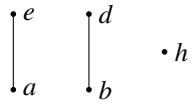
quindi $\phi(x \vee y) = \phi(x) \vee \phi(y)$, e analogamente $\phi(x \wedge y) = \phi(x) \wedge \phi(y)$ □

Esempio 2.2.1. *Gli elementi sup-irriducibili del reticolo in figura sono $P = \{a, b, d, e, h\}$.*



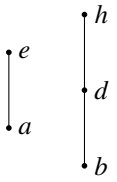
Consideriamo la seguente partizione in catene di P:

$$P_1 = \{a < e\} \quad P_2 = \{b < d\} \quad P_3 = \{h\}.$$



Otteniamo la seguente codifica:

$$\begin{array}{ll} 0 \mapsto (0,0,0) & e \mapsto (2,1,0) \\ a \mapsto (1,0,0) & f \mapsto (1,2,0) \\ b \mapsto (0,1,0) & g \mapsto (2,2,0) \\ c \mapsto (1,1,0) & h \mapsto (1,2,1) \\ d \mapsto (0,2,0) & 1 \mapsto (2,2,1) \end{array}$$



Se invece scegliamo la partizione
otteniamo la codifica:

$$\begin{aligned} 0 &\mapsto (0,0) & e &\mapsto (2,1) \\ a &\mapsto (1,0) & f &\mapsto (1,2) \\ b &\mapsto (0,1) & g &\mapsto (2,2) \\ c &\mapsto (1,1) & h &\mapsto (1,3) \\ d &\mapsto (0,2) & 1 &\mapsto (2,3). \end{aligned}$$

La proposizione ci dice che ogni partizione di P fornisce una codifica del reticolo L. D'altra parte è chiaro che una codifica $\phi\colon L \to \prod_{i=1}^{d} C_i$ induce una partizione di P in catene (scorrendo su ciascuna coordinata).
Qual è dunque il numero minimo di catene disgiunte $d(P)$ nelle quali il poset degli elementi sup-irriducibili P può essere decomposto? Il numero $d(P)$ è chiamato numero di Dilworth di P. Ovviamente, siccome due qualsiasi elementi di un'anticatena devono comparire in catene diverse,

$$d(P) \geq max\{|A|;\ A \text{ anticatena}\}$$

Ritornando all'esempio $\mathcal{B}(S)$ notiamo che siccome $P = S$ (il poset degli atomi coincide con il poset degli elementi sup-irriducibili) è esso stesso un'anticatena, dobbiamo avere che $d(\mathcal{B}(S)) \geq |S| = n$ per ogni codifica; questo significa che n è in effetti la minima dimensione possibile.

2.3 La funzione rango

La terza caratterizzazione dei reticoli distributivi coinvolge la funzione rango. Dobbiamo innanzitutto provare l'esistenza di tale funzione in ogni reticolo distributivo dotato di minimo 0 usando il secondo teorema di Birkhoff e successivamente caratterizzare la distributività dando certe condizioni di regolarità sul rango. Usiamo le notazioni $P(a)$, $I(a)$ e $\mathcal{F}_f(P)$ come nella prima sezione.

Proposizione 2.3.1. *Sia L un reticolo distributivo dotato di minimo 0 e $x \mapsto I(x), x \in L$ l'isomorfismo del secondo teorema di Birkhoff; allora*

$$x \prec y \iff I(y) = I(x) \cup \{p\} \text{ per un qualche } p \in P(y) \setminus P(x).$$

Segue che y copre precisamente $|P(y)|$ elementi in L, per ogni $y \in L$.
Inoltre, L possiede una funzione rango r, e si ha

$$r(x) = |I(x)| \text{ per ogni } x \in L$$

Dimostrazione. Se si elimina da $I(y)$ un qualsiasi elemento massimale $p \in P(y)$, allora $I(y) - \{p\}$ è ancora in $I_f(P)$. Il reticolo degli ideali è un sottoordine dell'algebra di Boole. Siccome nell'algebra di Boole si ha che $I(x) \prec I(y)$, a maggior ragione questo continua a valere anche nel reticolo. Per il secondo teorema di Birkhoff si ha che $L \cong I_{\mathrm{f}}$ quindi $x \prec y$. Supponiamo viceversa che $x \prec y$.Per il secondo teorema di Birkhoff questo implica che $I(x) \prec I(y)$ e l'elemento per cui differiscono i due ideali e necessariamente unico. Per verificare l'ultima affermazione notiamo per prima cosa che $r(0) = 0 = |\emptyset|$. Adesso, per un elemento qualsiasi $x \neq 0$ abbiamo appena mostrato che ogni catena massimale

$$0 \prec x_1 \prec x_2 \prec \cdots \prec x$$

corrisponde ad una catena finita di ideali

$$\emptyset \prec I(x_1) \prec I(x_2) \prec \ldots I(x)$$

dove la cardinalità di $I(x_i)$ cresce di uno ad ogni passo. □

Corollario 2.3.1. *Per ogni reticolo distributivo finito L abbiamo che $r(L) = |P|$, dove P è il poset degli elementi sup-irriducibili di L. Inoltre L è isomorfo ad un sottoreticolo di $\mathcal{B}(n)$ dove $n = |P|$.*

La formula per il rango della proposizione, suggerisce l'utilizzo della funzione cardinalità per dedurre ulteriori proprietà sul rango.

Proposizione 2.3.2. *Siano $A_1, \ldots, A_t$ una famiglia finita di sottoinsiemi finiti di un insieme S. Allora*

$$|\textstyle\bigcup_{i=1}^{t} A_i| = \sum_{i=1}^{t} |A_i| - \sum_{i<j}^{t} |A_i \cap A_j| + \sum_{i<j<k}^{k} |A_i \cap A_j \cap A_k| \mp \cdots + (-1)^{\mathrm{t}-1} |A_1 \ldots A_t|.$$

Dimostrazione. Si procede per induzione su t. □

Quest'ultima formula consente di classificare i reticoli distributivi attraverso la funzione rango.

Definizione 2.3.1. *Sia L un reticolo con una funzione rango r. Si dice che r possiede una proprietà di regolarità (R_t), $t \geq 2$, se per ogni $x_1, \ldots, x_t \in L$:*

$$r(x_1 \ldots x_t) = \sum_{i=1}^{t} r(x_i) - \sum_{i<j}^{t} r(x_1 \wedge x_j) \mp \cdots + (-1)^{\mathrm{t}-1} r(x_1 \wedge \cdots \wedge x_t)$$

Si osservi che ponendo $x_t = x_{t-1}$ e cancellando gli addendi superflui nella sommatoria si dimostra che (R_t) implica (R_{t-1}) e quindi (R_i) per ogni $i \leq t$.Il prossimo teorema mostra viceversa che (R_3) implica (R_t) per ogni $t \geq 3$. Ci rimangono quindi da analizzare le condizioni (R_3) e (R_2) che mostreremo caratterizzare rispettivamente i reticoli distributivi e modulari.

Teorema 2.3.1. *Sia L un reticolo con catene finite dotato di minimo 0. L è distributivo se e solo se possiede una funzione rango che soddisfa (R_3). In particolare (R_3) implica (R_t) per ogni t.*

Dimostrazione. Supponiamo che il reticolo L sia distributivo; allora siccome $L \cong I_f(P)$ si ha che r soddisfa (R_t) per ogni t. Viceversa supponiamo che L dotato di una funzione rango tale che per ogni $a, b, c \in L$ si ha $r(a \vee b \vee c) = r(a) + r(b) + r(c) - r(a \wedge b) - r(a \wedge c) - r(b \wedge c)$. Dalla disuguaglianza

$$a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$$

che vale per ogni reticolo, per dimostrare che L è distributivo è sufficiente mostrare che

$$r(a \wedge (b \vee c)) = r((a \wedge b) \vee (a \wedge c)).$$

Adesso siccome (R_3) implica (R_2), vale che

$$r(a \wedge (b \vee c)) = r(a) + r(b \vee c) - r(a \vee b \vee c) = r(a) + r(b) + r(c) - r(b \wedge c) - r(a \vee b \vee c).$$

Sfruttando (R_3),

$$r(a \wedge (b \vee c)) = r(a \wedge b) + r(a \wedge c) - r(a \wedge b \wedge c),$$

sfruttando ancora (R_2)

$$r(a \wedge (b \vee c)) = r((a \wedge b) \vee (a \wedge c)).$$

□

Capitolo 3

Reticoli Modulari e Semimodulari

3.1 Reticoli modulari

Definizione 3.1.1. *Un reticolo L si dice modulare se per ogni $a, b, c \in L$ si ha che*

$$c \leq a \implies a \wedge (b \vee c) = (a \wedge b) \vee c.$$

Osserviamo che:

- La legge modulare è una forma debole della legge distributiva; infatti se L è un reticolo distributivo presi $a, b, c \in L$ tali che $c \leq a$ applicando la prima legge distributiva si ha che $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) = (a \wedge b) \vee c$. Quindi un reticolo distributivo è sempre modulare.
- La legge modulare è autoduale; quindi se un reticolo è modulare anche il suo duale lo è.
- Siccome la legge modulare deve valere per ogni terna del reticolo:
  - ogni sottoreticolo di un reticolo modulare è modulare, in particolare ogni intervallo di un reticolo modulare è modulare;
  - il prodotto cartesiano di reticoli modulari è modulare.

Esempio 3.1.1. *Una catena è sempre un reticolo modulare.*

Esempio 3.1.2. *Sia $(G; \cdot)$ un gruppo. L'insieme dei sottogruppi di G, ordinati dall'inclusione, è un reticolo che indichiamo con $\mathcal{L}(G)$. L'operazione di inf è l'intersezione insiemistica mentre il sup di due sottogruppi H e K è il sottogruppo generato dal sottoinsieme $K \cup H$ cioè:*

$$H \vee K = \{h_1 \cdot k_1 \cdot h_2 \cdot k_2 \ldots h_n \cdot k_n; h_i \in H, k_i \in K, n \in \mathbb{Z}^+\}.$$

Dimostriamo che il sottoinsieme di $\mathcal{L}(G)$ costituito dai sottogruppi normali di G è un sottoreticolo di $\mathcal{L}(G)$, inoltre esso è modulare.

Dimostrazione. Ricordiamo che un sottogruppo H di G si dice normale se, per ogni $g \in G$, risulta $gH = Hg$, dove

$$gH = \{g \cdot x; x \in H\} \qquad Hg = \{x \cdot g; x \in H\}.$$

Siano ora H e K due sottogruppi normali di G. Dobbiamo provare che anche il sottogruppo $H \cap K$ è normale. Per ogni $g \in G$ sia $x \in g(H \cap K)$, allora esiste un elemento $h \in H \cap K$ tale che $x = g \cdot h$. Questo implica che $x \in gH \cap gK$. Siccome H e K sono normali si ha che $gH = Hg$ e $gK = Kg$, questo implica che esistono $h \in H$ e $k \in K$ tali che $h \cdot g = x = k \cdot g$, da cui $h = k$. Dunque $x \in (H \cap K)g$ cioè $g(H \cap K) \subseteq (H \cap K)g$. Per provare l'inclusione inversa si procede allo stesso modo. Inoltre siccome H e K sono normali si ha che

$$H \vee K = H \cdot K = \{h \cdot k; h \in H, k \in K\} = \{k \cdot h; k \in K, h \in H\} = K \cdot H.$$

Infatti $H \cdot K \subseteq K \cdot H$ perchè se $h \in H$, $k \in K$ abbiamo

$$h \cdot k \in Hk = kH \subseteq K \cdot H$$

da cui segue che $H \cdot K \subseteq K \cdot H$. Per provare l'inclusione inversa si procede allo stesso modo. Sia $x = h_1 \cdot k_1 \cdot h_2 \cdot k_2 \cdot \cdots \cdot h_s \cdot k_s \in H \vee K$. Siccome H è normale abbiamo $h_1 \cdot k_1 \in Hk_1 = k_1H$. Esiste dunque $h_1' \in H$ tale che $h_1 \cdot k_1 = k_1 \cdot h_1'$. Ora $h = h_1 \cdot h_1'$ è un elemento di H; allora

$$x = k_1 \cdot h \cdot k_2 \cdot \cdots \cdot h_s \cdot k_s.$$

In modo analogo esiste $h' \in H$ tale che $h \cdot k_2 = k_2 \cdot h'$. Procedendo in questo modo otteniamo

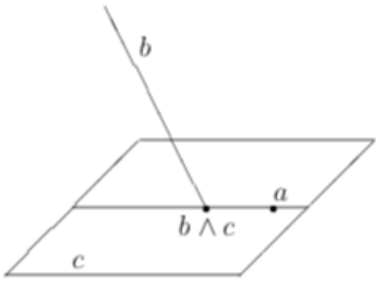
$$x = k_1 \cdot k_2 \cdot \cdots \cdot k_s \cdot h = k \cdot h$$

dove $k = k_1 \cdot k_2 \cdot \cdots \cdot k_s$. Si verifica ora banalmente che $H \vee K$ è un sottogruppo normale.
Modularità: Sia $(G; \cdot)$ un gruppo e $\mathcal{N}(G)$ il reticolo dei sottogruppi normali di G. Siano $H, K, T \triangleleft G$ con $T \subseteq H$, dobbiamo provare che $H \cap (K \cdot T) = (H \cap K) \cdot T$. In generale vale sempre che se ho un reticolo $(L, \wedge, \vee)$, $x, y, z \in L$, $z \leq x \implies x \wedge (y \vee z) \geq (x \wedge y) \vee z$. Quindi la prima "metà" della legge modulare vale sempre. Dobbiamo quindi dimostrare che $H \cap (K \cdot T) \subseteq (H \cap K) \cdot T$. Sia $h \in H \cap (K \cdot T)$ allora esiste un $k \in K$ e un $t \in T$ tali che $h = k \cdot t$ equivalentemente $k = h \cdot t^{-1}$. Siccome $h \in H$ e $t^{-1} \in T \subseteq H$ allora $k \in H$, quindi $k \in K \cap H$. Si ha dunque che $h = k \cdot t \in (H \cap K) \cdot T$. □

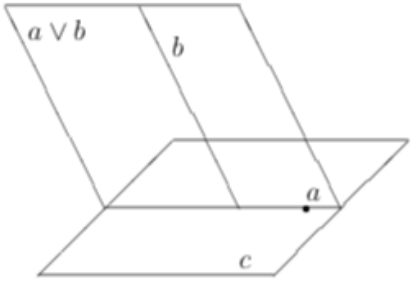
Esempio 3.1.3. *Sia V uno spazio vettoriale di dimensione finita e sia $\mathcal{S}(V)$ l'insieme dei sottospazi di V ordinati per l'inclusione. Si dimostra che $\mathcal{S}(V)$ è un reticolo dove l'operazione di inf è l'intersezione insiemistica, mentre il sup è la somma di sottospazi, ovvero se U e W sono due sottospazi di V, $U \vee W$ è il sottospazio generato dall'insieme $U \cup W$ cioè $span(U \cup W)$. Si dimostra che tale reticolo è modulare procedendo come nell'esempio precedente.*

Esempio 3.1.4. *Si consideri il reticolo dei sottospazi di $\mathbb{R}^4$: esso rappresenta la costruzione classica della geometria proiettiva reale a tre dimensioni, in cui si denotano i "punti" come spazi unidimensionali,*

le "rette" come spazi bidimensionali, i "piani" come spazi tridimensionali. A grandi linee la geometria proiettiva è quella che non ammette rette parallele, quindi se due rette sono complanari necessariamente sono incidenti. Tale ambiente offre un'utile visualizzazione delle legge modulare.Nella figura: a è un punto nel piano c, b è una retta che non passa per a e che non è contenuta nel piano c.

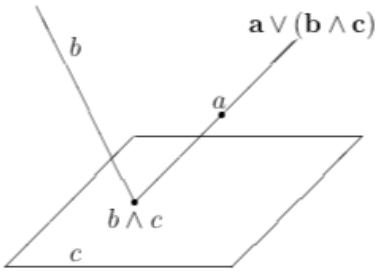


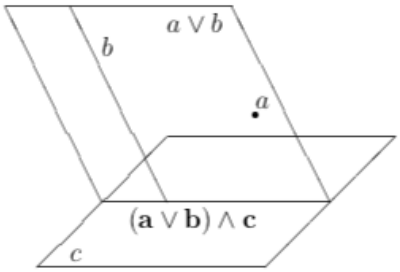
$\mathbf{a \vee (b \wedge c)}$



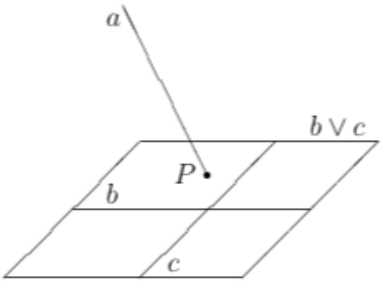
$\mathbf{(a \vee b) \wedge c}$

Si noti che la condizione $a \leq c$ è fondamentale affinchè l'identità modulare valga. La seguente figura mostra l'esempio precedente dove si è preso a non appartenente al piano c.

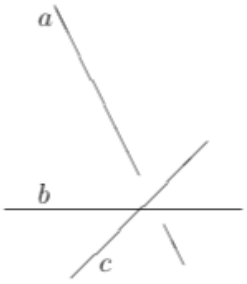




Tale reticolo non è distributivo, infatti se a, bc, sono rette tali che a e c siano complanari e a sia sghemba rispetto alle altre due si ha



$\mathbf{a \wedge (b \vee c) = P}$



$\mathbf{(a \wedge b) \vee (a \wedge c) = \emptyset}$

I reticoli modulari possiedono altre caratterizzazioni: se scegliamo $c \in [a \wedge b, a]$ otteniamo $(c \vee b) \wedge a = c$. Il prossimo lemma mostra che possiamo dare condizioni necessarie e sufficienti sulla terna di elementi $\{a, b, c\}$ affinchè il reticolo sia modulare.

Lemma 3.1.1. *Un reticolo L con catene finite è modulare se e solo se per ogni $a, b \in L$ e per ogni $z \in [a \wedge b, a]$ abbiamo $(z \vee b) \wedge a = z$, equivalentemente, $(w \wedge a) \vee b = w$ per ogni $w \in [b, a \vee b]$.*

Dimostrazione. Se L è un reticolo modulare allora per ogni $z \in [a \wedge b, a]$ abbiamo $(z \vee b) \wedge a = z \vee (b \wedge a) = z$. Viceversa, siccome $z \leq a \implies z \vee (a \wedge b) \leq (z \vee b) \wedge a$ vale in ogni reticolo L, per avere la modularità è necessario e sufficiente provare che $z \vee (a \wedge b) \geq (z \vee b) \wedge a$ per ogni $a, b, z \in L$ con $z \leq a$. Supponiamo $a \wedge b \not\leq z$, $z \leq a$ (se $a \wedge b \leq z$ la tesi segue banalmente). Allora $z \vee (a \wedge b) \in [a \wedge b, a]$. Quindi applicando l'ipotesi all'elemento $z \vee (a \wedge b)$ si ha che:

$$z \vee (a \wedge b) = [(z \vee (a \wedge b) \vee b] \wedge a \geq (z \vee b) \wedge a.$$

□

Introduciamo adesso due morfismi d'ordine ϕ_{b} ψ_{a} definite su L:

$$\phi_{\mathrm{b}}(z) = z \vee b, \qquad \psi_{\mathrm{a}}(w) = w \wedge a. \tag{3.1}$$

Notiamo che per ogni reticolo modulare L e per ogni $a, b \in L$:

- $\phi_{\mathrm{b}}\psi_{\mathrm{a}}\phi_{\mathrm{b}} = \phi_{\mathrm{b}}$ su $[a \wedge b, a]$, infatti:
  $\phi_{\mathrm{b}}\psi_{\mathrm{a}}\phi_{\mathrm{b}}(z) = \phi_{\mathrm{b}}\psi_{\mathrm{a}}(z \vee b) = \phi_{\mathrm{b}}((z \vee b) \wedge a) = [(z \vee b) \wedge a] \vee b = z \vee b.$
- $\psi_{\mathrm{a}}\phi_{\mathrm{b}}\psi_{\mathrm{a}} = \psi_{\mathrm{a}}$ su $[b, a \vee b]$, infatti:
  $\psi_{\mathrm{a}}\phi_{\mathrm{b}}\psi_{\mathrm{a}}(w) = \psi_{\mathrm{a}}\phi_{\mathrm{b}}(w \wedge a) = \psi_{\mathrm{a}}((w \wedge a) \vee b) = [(w \wedge a) \vee b] \wedge a] = w \wedge a.$

Quindi:

- $\phi_{\mathrm{b}}\colon [a \wedge b, a] \to [b, a \vee b]$ è una mappa iniettiva $\iff$ $(z \vee b) \wedge a = z$ per ogni $z \in [a \wedge b, a]$.
- $\psi_{\mathrm{a}}\colon [b, a \vee b] \to [a \wedge b, a]$ è una mappa iniettiva $\iff$ $(w \wedge a) \vee b = w$ per ogni $w \in [b, a \vee b]$

Teorema 3.1.1 (di isomorfismo canonico)**.** *Un reticolo L è modulare se e solo se le applicazioni ϕ_{b} e ψ_{a} ristrette rispettivamente agli intervalli $[a \wedge b, a]$ e $[b, a \vee b]$ sono due isomorfismi di reticoli uno inverso dell'altro.*

Dimostrazione. ϕ_{b} e ψ_{a} sono morfismi d'ordine perchè le operazioni di sup e di inf sono isotone, ovvero

$$\text{per ogni } x, y, z \in L \text{ se } x \leq y \text{ si ha che } (x \vee z) \leq (y \vee z) \text{ e } (x \wedge z) \leq (y \wedge z);$$

infatti se $x \leq y$ allora $x \vee y = y$ quindi $(x \vee z) \vee (y \vee z) = (x \vee y) \vee (z \vee z) = y \vee z$, quindi $x \vee z \leq y \vee z$ (analogamente si dimostra la seconda disuguaglianza). Inoltre dalla legge modulare,

per ogni $x \in [a \wedge b, a]$ si ha $\psi_a \circ \phi_b(x) = \psi_a(b \vee x) = a \wedge (b \vee x) = (a \wedge b) \vee x = x$,
per ogni $y \in [b, a \vee b]$ si ha $\phi_b \circ \psi_a(y) = \phi_b(a \wedge y) = b \vee (a \wedge y) = (a \vee b) \wedge y = y$.

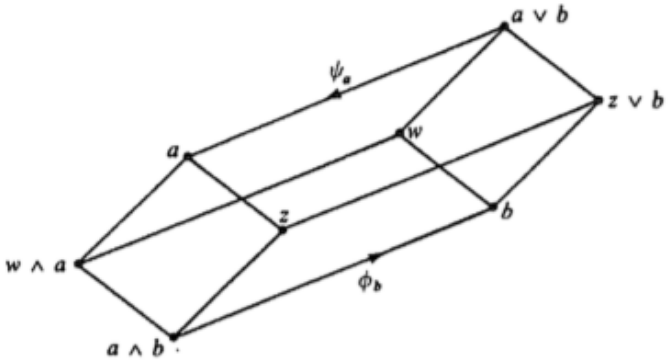
Banalmente ψ_a e ϕ_b si "comportano bene" rispettivamente con le operazioni di *inf* e di *sup* per come sono state definite le due mappe. Mostriamo che ψ_a si "comporta bene" anche rispetto l'operazione di *sup*, ovvero per ogni z, z' vale che:

$$\psi_a(z \vee z') = \psi_a(z) \vee \psi_a(z').$$

Abbiamo mostrato che ψ_a e ϕ_b, ristrette ai rispettivi intervalli, sono una l'inversa dell'altra; allora esistono w, w' tali che $z = \phi_b(w)$ e $z' = \phi_b(w')$. ϕ_b si comporta bene rispetto al *sup*, quindi

$$\phi_b(\psi_a(w) \vee \psi_a(w')) = \phi_b(\psi_a(w \vee w')) = w \vee w' = \phi_b(z) \vee \phi_b(z').$$

In modo analogo si dimostra che ϕ_b si "comporta bene" anche rispetto l'operazione di *inf*. □



Proposizione 3.1.1. *Un reticolo L con catene finite è modulare se e solo se per ogni $a, b \in L$ risulta:*

$$a \wedge b \prec a \iff b \prec a \vee b. \tag{3.2}$$

Equivalentemente:

$$a \wedge b \prec a, b \iff a, b \prec a \vee b. \tag{3.3}$$

Dimostrazione. La dimostrazione segue direttamente dal fatto che un reticolo è modulare se e solo se per ogni a, b gli intervalli $[a \wedge b, a]$ e $[b, a \vee b]$ sono isomorfi. □

Osservazione 3.1.1. *Abbiamo detto che ogni reticolo distributivo è anche modulare. Tuttavia non tutti i reticoli modulari sono distributivi infatti il reticolo M_3 è modulare ma non distributivo. Inoltre si noti che il reticolo N_5 non è modulare, infatti si ha $a \leq b$ ma $b \wedge (c \vee a) = b \wedge 1 = b$ mentre $(b \wedge c) \vee a = 0 \vee a = a \neq b$.*

I reticoli modulari e distributivi possono essere caratterizzati mediante una "configurazione proibita", più precisamente abbiamo:

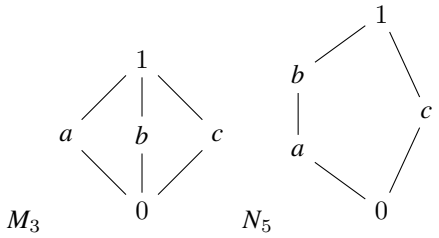
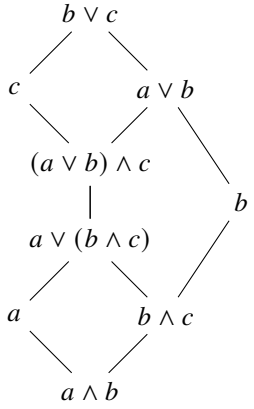


Figura 3.1:

Teorema 3.1.2. *Un reticolo è modulare se e solo se non contiene nessun sottoreticolo isomorfo a* N_5.

Dimostrazione. Se L è un reticolo modulare ogni suo sottoreticolo, essendo modulare, non può essere isomorfo a N_5. Viceversa, se L non è modulare esisteranno in esso tre elementi a due a due distinti a, b, c tali che $a < c$ e $a \vee (b \wedge c) < (a \vee b) \wedge c$. Queste due condizioni garantiscono che l'elemento b non è confrontabile nè con a nè con c. Come si può controllare facilmente, gli elementi $b \wedge c, a \vee (b \wedge c), (a \vee b) \wedge c, a \vee b, b$ sono tutti distinti e costituiscono un sottoreticolo di L isomorfo a N_5.



□

Teorema 3.1.3. *Un reticolo* L *è distributivo se e solo se non contiene nessun sottoreticolo isomorfo a* N_5 *o a* M_3.

Dimostrazione. Supponiamo che L sia distributivo, allora L è anche modulare. Segue dalla proposizione precedente che L non può avere un sottoreticolo isomorfo a N_5. Inoltre siccome ogni sottoreticolo di un reticolo distributivo è a sua volta distributivo, L non può avere un sottoreticolo isomorfo a M_3 (che è un reticolo modulare ma non distributivo). Viceversa supponiamo che L non sia un reticolo distributivo. Se L non è neppure modulare, abbiamo già dimostrato che non contiene un sottoreticolo isomorfo a N_5. Supponiamo dunque che L sia un reticolo modulare ma non distributivo e mostriamo che contiene un sottoreticolo isomorfo a M_3. Scegliamo x, y, z in modo tale che

$$x \wedge (y \vee z) > (x \wedge y) \vee (z \wedge x).$$

Allora risulta anche:

$$y \wedge (z \vee x) > (y \wedge z) \vee (x \wedge y)$$
$$z \wedge (x \vee y) > (z \wedge x) \wedge (y \wedge z).$$

Poniamo ora:

$a := (x \wedge (y \vee z)) \vee (y \wedge z)$, $\quad b := (y \wedge (z \vee x)) \vee (z \wedge x)$,

$c := (z \wedge (x \vee y)) \vee (x \wedge y)$, $\quad d := (x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$,

$e := (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$.

Applicando le mappe $\phi_{\mathrm{y}\wedge\mathrm{z}}$, $\phi_{\mathrm{z}\wedge\mathrm{x}}$ e $\phi_{\mathrm{x}\wedge\mathrm{y}}$ otteniamo che

$$d < a < e, \qquad d < b < e, \qquad d < c < e$$

Usando le leggi modulari è facile vedere che $\{a, b, c, d, e\}$ genera un sottoreticolo isomorfo a M_3. □

Grazie a questi due ultimi risultati possiamo dare una nuova caratterizzazione ai reticoli modulari e distributivi.

Corollario 3.1.1. *1. Un reticolo è distributivo se e solo se per ogni a, b, c:*

$$a \wedge c = b \wedge c, \quad a \vee c = b \vee c \implies a = b.$$

2. Un reticolo è modulare se e solo se per ogni a, b, c:

$$b \leq a, \quad a \wedge c = b \wedge c, \quad a \vee c = b \vee c \implies a = b.$$

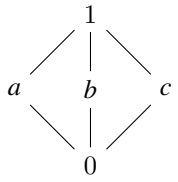
Sia L un reticolo modulare dotato di minimo 0 e sia P il poset dei suoi elementi sup-irriducibili. Se L ha catene finite allora per ogni elemento $a \in L$ esiste una decomposizione finita $a = p_1 \vee \cdots \vee p_t$ e il secondo teorema di Birkhoff garantisce l'unicità di tale decomposizione (a patto che sia irridondante) se L è un reticolo distributivo. Per un reticolo modulare l'unicità non è più garantita; ma si può provare che il numero di elementi usati in ogni decomposizione irridondante è sempre uguale.

Proposizione 3.1.2 (Proprietà di scambio)**.** *Sia L un reticolo modulare dotato di minimo 0 e sia $P \subseteq L$ il poset dei suoi elementi sup-irriducibili. Se $a \in L$ ammette due decomposizioni $a = p_1 \vee \cdots \vee p_s = q_1 \vee \cdots \vee q_t$ allora si ha che*

$$\forall p_i \text{ esiste un certo } q_j \text{ tale che } a = p_1 \vee \cdots \vee p_{i-1} \vee q_j \vee p_{i+1} \vee \cdots \vee p_s.$$

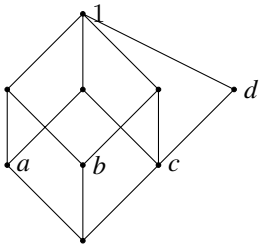
In particolare, ogni decomposizione irridondante di a contiene lo stesso numero di elementi.

Dimostrazione. Sia $\bar{p}_i = p_1 \vee \cdots \vee p_{i-1} \vee p_{i+1} \vee \cdots \vee p_s$ e $r_j = \bar{p}_i \vee q_j$ per $j = 1, \ldots, t$. Siccome $[p_i \wedge \bar{p}_i, p_i] \cong [\bar{p}_i, p_i \vee \bar{p}_i = a]$ e p_i è irriducibile in $[p_i \wedge \bar{p}_i, p_i]$ possiamo concludere che a è irriducibile in $[\bar{p}_i, a]$. Inoltre $\bar{p}_i \leq r_j \leq a$, $q_j \leq r_j$, quindi $a = q_1 \vee \cdots \vee q_t \leq r_1 \vee \cdots \vee r_t \leq a$, allora $a = r_1 \vee \cdots \vee r_t$. Ma $r_1, \ldots, r_t \in [\bar{p}_i, a]$, allora necessariamente esiste un certo j tale che $a = r_j = \bar{p}_i \vee q_j = p_1 \vee \cdots \vee p_{i-1} \vee q_j \vee p_{i+1} \vee \cdots \vee p_s$. □



Esempio 3.1.5. *Nel reticolo M_3, gli elementi irriducibili sono i tre atomi $P = \{a, b, c\}$ e $1 = a \vee b = a \vee c = b \vee c$ sono tre decomposizioni irridondanti di 1.*

Esempio 3.1.6. *Nella figura il poset degli elementi irriducibili è $P = \{a, b, c, d\}$ e $1 = a \vee b \vee c = a \vee d$ sono due decomposizioni irridondanti di 1 che hanno numero diversi di elementi, quindi il reticolo non è modulare.*



3.2 Reticoli semimodulari

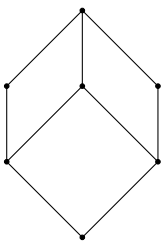
Definizione 3.2.1. *Un reticolo L si dice semimodulare se per ogni $a, b \in L$ risulta:*

$$a \wedge b \prec a \implies b \prec a \vee b. \tag{3.4}$$

Un reticolo L è semimodulare inferiormente se per ogni $a, b \in L$ risulta:

$$b \prec a \vee b \implies a \wedge b \prec a. \tag{3.5}$$

Esempio 3.2.1. *Il più piccolo reticolo semimodulare (si verifica banalmente) che non è modulare (contiene un sottoreticolo isomorfo a N_5) è quello il cui diagramma di Hasse è:*



Esempio 3.2.2. *Definiamo il reticolo delle partizioni di un insieme finito.*
Sia A un insieme finito non vuoto e $\mathcal{P}(A)$ l'insieme delle partizioni di A. Definiamo su $\mathcal{P}(A)$ una relazione d'ordine $\leq$, detta raffinamento, nel modo seguente:

$$\text{per ogni } \pi, \sigma \in \mathcal{P}(A), \pi \leq \sigma \iff \text{per ogni blocco } X \text{ di } \pi \text{ esiste un blocco } Y \text{ di } \sigma \text{ tale che } X \subseteq Y$$

in tal caso si dice che π è più fine di σ, o che σ è meno fine di π.
Così $\mathcal{P}(A)$ diviene un insieme parzialmente ordinato, il cui minimo è la partizione discreta $0 := \{\{x\}; x \in A\}$ mentre il massimo è la partizione banale $1 := \{A\}$. Di più, $\mathcal{P}(A)$ risulta essere un reticolo. Si può verificare che la relazione di copertura associata al raffinamento risulta essere:

$$\text{per ogni } \pi, \sigma \in \mathcal{P}(A), \pi \prec \sigma \iff \text{esistono due blocchi distinti } A \text{ e } B \text{ di } \pi \text{ tali che } A \cup B \text{ sia un blocco di } \sigma \text{ mentre tutti i blocchi di } \sigma \text{ diversi da } A \cup B \text{ sono anche blocchi di } \pi.$$

A partire da questo fatto si dimostra che $\mathcal{P}(A)$ è dotato di rango e che per ogni partizione π risulta che $r(\pi) = |A| -$numero di blocchi di π. Quindi dato che la struttura di $\mathcal{P}(A)$ dipende solo dalla cardinalità di A, indichiamo il reticolo con $\mathcal{P}(n)$ dove $n = |A|$.
Per ogni intero n, il reticolo delle partizioni $\mathcal{P}(n)$ è semimodulare, ma per $n > 3$ non modulare.

Dimostrazione. Siano π, σ due partizioni tali che $\pi \wedge \sigma \prec \pi$ e $\pi \wedge \sigma \prec \sigma$. Siano $A_1, \ldots, A_k$ i blocchi di $\pi \wedge \sigma$. Allora, per esempio, avremo che i blocchi di π sono $A_1 \cup A_2, A_3, \ldots, A_k$ e quindi quelli di σ possono essere $A_1, A_2, A_3 \cup A_4, \ldots, A_k$ oppure $A_1, A_2 \cup A_3, \ldots, A_k$. Nel primo caso abbiamo

$$\pi \vee \sigma = \{A_1 \cup A_2, A_3 \cup A_4, \ldots, A_k\}$$

e nel secondo caso

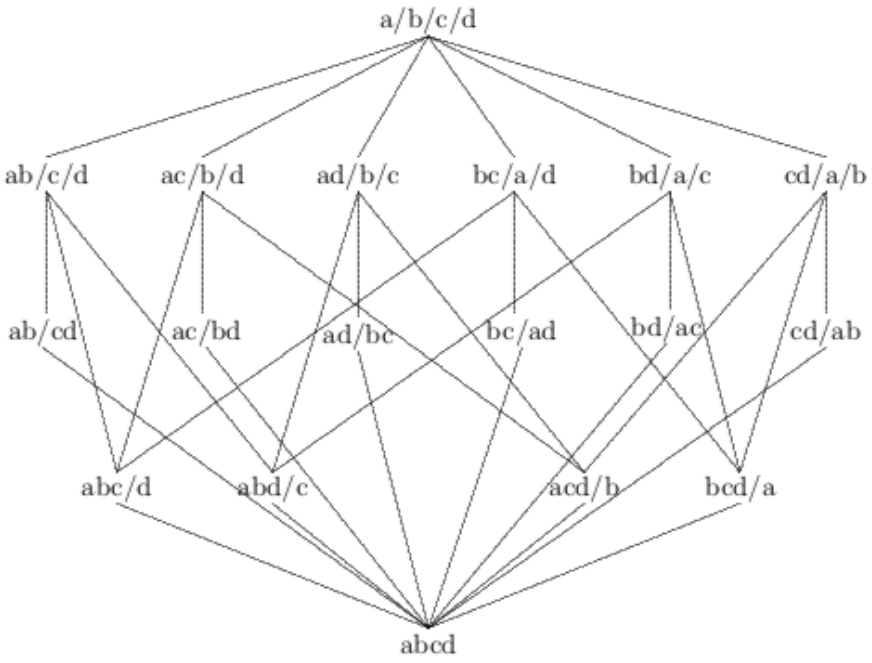
$$\pi \vee \sigma = \{A_1 \cup A_2 \cup A_3, \ldots, A_k\}.$$

In entrambi i casi risulta $\pi \prec \pi \vee \sigma$ e $\sigma \prec \pi \vee \sigma$, dunque il reticolo è semimodulare.
Se $n > 3$ consideriamo le due partizioni

$$\pi = \{\{a, b\}, S - \{a, b\}\} \text{ e } \sigma = \{\{a, c\}, S - \{a, c\}\} \text{ con } a, b, c \text{ elementi distinti.}$$

Si ha che $\pi \vee \sigma = 1$, mentre $\pi \wedge \sigma$ ha come blocchi $\{a\}, \{b\}, \{c\}, S - \{a, b, c\}$.
Allora $\pi, \sigma \prec \pi \vee \sigma$ ma $\pi \wedge \sigma \not\prec \pi, \sigma$; quindi $\mathcal{P}(n)$ non è modulare. □

In figura è rappresentato il diagramma di Hasse del reticolo delle partizioni dell'insieme $\{a, b, c, d\}$:



Si noti che un reticolo è modulare se e solo se è semimodulare e inferiormente semimodulare. Infatti, equivalentemente a quanto detto per i reticoli modulari, si ha:

Proposizione 3.2.1. *Un reticolo è semimodulare se e solo se per ogni a, b si ha che:*

$$a \wedge b \prec a, b \implies a, b \prec a \vee b. \tag{3.6}$$

La proposizione duale definisce i reticoli semimodulari inferiormente.

Corollario 3.2.1. *Sia L un reticolo semimodulare. Allora*

$$x \prec y \implies x \vee z = y \vee z \quad \text{oppure} \quad x \vee z \prec y \vee z \qquad \text{per ogni } x, y, z \in L.$$

In particolare, per ogni atomo p e per ogni $a \in L$ con $p \not\leq a$, si ha $a \prec a \vee p$.

Lemma 3.2.1. *Un reticolo semimodulare con catene finite soddisfa la condizione di Jordan-Dedekind.*

Dimostrazione. Proviamo per induzione che, se L è un reticolo semimodulare, la seguente affermazione è vera per ogni $m \geq 1$:

$P(m)$: Per ogni coppia (a, b) di elementi di L, con $a < b$, se esiste una catena massimale tra a e b di lunghezza m, allora tutte le catene massimali tra a e b hanno lunghezza m.

- P(1) è ovviamente vera.

- Supponiamo vera P(m) per un dato $m > 1$, e consideriamo $a, b \in L$ con $a < b$, tali che esista una catena massimale di lunghezza $m+1$, $a = c_0 \prec c_1 \prec \cdots \prec c_m = b$. Consideriamo un'altra catena massimale tra a e b $a = d_0 \prec d_1 \prec \cdots \prec d_n = b$.
  - Se $c_1 = d_1$ allora applicando l'ipotesi induttiva sulla catena tra c_1 e b si ha che $m = n$.
  - Se invece $c_1 \neq d_1$ si ha $c_1 \wedge d_1 = a \prec x_1, d_1$ e per (3.6) questo implica $c_1, d_1 \prec c_1 \vee d_1$. Ora se C è una catena massimale tra $c_1 \vee d_1$ e b, allora $C \cup \{c_1\}$ e $C \cup \{d_1\}$ sono rispettivamente una catena massimale tra c_1 e b e d_1 e b che hanno entrambe lunghezza $|C| + 1$. D'altra parte, per l'ipotesi di induzione, la prima catena ha la stessa lunghezza di $d_1 \prec d_2 \prec \cdots \prec d_n = b$, cioè n; dunque $m = n$.

□

Si noti che anche i reticoli modulari soddisfano la (3.6) e quindi soddisfano la condizione di Jordan-Dedekind.
I reticoli che soddisfano la condizione di JD, se ammettono minimo, sono dotati di rango. Diamo ora una caratterizzazione dei reticoli modulari e semimodulari per mezzo di un'identità soddisfatta dalla loro funzione rango.

Teorema 3.2.1. *Sia L è un reticolo dotato di minimo* 0.

- *L è semimodulare se e solo se possiede una funzione rango r tale che per ogni $a, b \in L$ risulta:*

$$r(a \wedge b) + r(a \vee b) \leq r(a) + r(b). \tag{3.7}$$

- *L è modulare se e solo se possiede una funzione rango r tale che per ogni $a, b \in L$ risulta:*

$$r(a \wedge b) + r(a \vee b) = r(a) + r(b). \tag{3.8}$$

Dimostrazione. Un reticolo semimodulare dotato di minimo 0 possiede una funzione rango per 3.2.1. Per provare la tesi procediamo per induzione completa su $k := r(a) - r(a \wedge b)$.

- se $k = 1$, si ha $a \wedge b \prec a$, per (3.6) abbiamo che $b \prec a \vee b$, da cui $r(a \vee b) = r(b) + 1$. Quindi $r(a \wedge b) + r(a \vee b) = r(a) - 1 + r(b) + 1$ e quindi (3.7) è soddisfatta.

- Supponiamo ora la (3.7) ver per ogni $h \leq k$. Consideriamo due elementi $a, b \in L$ per cui $r(a) - r(a \wedge b) = k+1$. Allora dato che l'elemento $a \wedge b$ non può essere coperto da a, esisterà un elemento $x \in L$ tae che $a \wedge b < x < a$. Questo implica $a \wedge b \leq x \wedge b \leq a \wedge b$, da cui $x \wedge b = a \wedge b$. Di conseguenza $r(x) - r(x \wedge b) = r(x) - r(a \wedge b) \leq k$. Per ipotesi induttiva,

$$r(a \wedge b) + r(x \vee b) = r(x \wedge b) + r(x \vee b) \leq r(x) + r(b)$$

ovvero,

$$r(x \vee b) - r(x) \leq r(b) - r(a \wedge b). \tag{3.9}$$

Consideriamo ora i due elementi a e $x \vee b$. Per l'identità semimodulare risulta $a \wedge (x \vee b) = (a \wedge b) \vee x = x$, dunque $r(a \wedge (x \vee b)) - r(a) = r(x) - r(a) \leq k$ (perchè $a \wedge b < x < a$e $r(a) - r(a \wedge b) = k + 1$). Allora sempre per ipotesi induttiva,

$$r(a) + r(x \vee b) \leq r(a \wedge (x \vee b)) + r(a \vee x \vee b) = r(x) + r(a \vee b)$$

ovvero,

$$r(x \vee b) - r(x) \leq r(a \vee b) - r(a). \tag{3.10}$$

La tesi si ottiene confrontando (3.9) e (3.10).

Viceversa, supponiamo che il reticolo L possieda una funzione rango r tale che per ogni $a, b \in L$ valga (3.7). Supponiamo che gli elementi $a, b \in L$ siano tali che $a \wedge b \prec a$, allora $r(a) = r(a \wedge b) + 1$. Per la (3.7) ho che $r(a \vee b) \leq r(b) + 1$ quindi $r(b) \geq r(a \vee b) - 1$. Siccome $a \vee b \geq b$ e quindi $r(a \vee b) \geq r(b)$, necessariamente $r(b) = r(a \vee b) - 1$ che implica $b \prec a \vee b$.
Per dimostrare la (3.8) si procede in modo analogo. □

Esempio 3.2.3. *Abbiamo visto che il reticolo dei sottospazi vettoriali di uno spazio vettoriale V è modulare. In particolare tale reticolo è dotato di una funzione rango r tale che per ogni sottospazio U di V si ha $r(U) = dim(U)$. Dunque la* (3.8) *è l'identità di Grassmann.*

Un classico esempio di reticoli semimodulari sono quelli definiti da un insieme e da un operatore di chiusura che soddisfa l'assioma di scambio di Steinitz. Ricordiamo che una mappa $A \mapsto \overline{A}$ è chiamata operatore di chiusura se per ogni $A, B \subseteq S$:

1. $A \subseteq \overline{A}$,
2. $A \subseteq B \implies \bar{A} \subseteq \overline{B}$,
3. $\overline{\overline{A}} = \overline{A}$.

Un insieme $A \subseteq S$ tale che $A = \overline{A}$ si dice che è chiuso. Una famiglia costituita da insiemi chiusi è un reticolo completo ordinato dall'inclusione con le operazioni di sup e di inf definite da

$$A \wedge B = A \cap B \quad \text{e} \quad A \vee B = \overline{A \cup B}.$$

Quindi l'intersezione di insiemi chiusi è ancora un insieme chiuso e $\overline{A \cup B}$ è il più piccolo insieme chiuso che contiene sia A che B.
Se inoltre la mappa $A \mapsto \overline{A}$ soddisfa l'assioma di Steinitz,ovvero
per ogni $A \subseteq S, p, q \in S$:

$$p \notin \overline{A}, p \in \overline{A \cup q} \implies q \in \overline{A \cup p}$$

allora il reticolo completo costituito dai sottoinsiemi chiusi di S è semimodulare.

Esempio 3.2.4. $\mathbb{R}^2 = \{(a, b); a, b \in \mathbb{R}\}$ *può essere visto sia come spazio vettoriale di dimensione* 2*, ovvero* $\mathbb{R}^2 = span((0, 1), (1, 0))$*, sia come piano affine. In entrambi i casi il concetto di chiuso coincide con il concetto di sosttospazio.*

- *Nel primo caso abbiamo che i sottospazi di* $\mathbb{R}^2$ *sono*
  - *il vettore nullo,*
  - *le rette che passano per l'origine,*
  - *l'intero piano.*

  La chiusura di un insieme costituito da due punti diversi dall'origine è la retta per i due punti se questi sono allineati con l'origine, tutto il piano in caso contrario. Quindi la chiusura di $\{(1, 0), (0, 1)\}$ *coincide con tutto il piano. In questo caso il reticolo dei chiusi è modulare.*

- *Nel secondo caso i sottospazi di* $\mathbb{R}^2$ *sono*
  - *i punti,*
  - *le rette,*
  - *l'intero piano.*

  In questo caso, la chiusura dell'insieme costituito da due punti distinti è l'insieme costituito da tutte le combinazioni lineari dei due punti con coefficienti la cui cui somma è 1*. Quindi in ogni caso è la retta passante per i due punti. In questo caso il reticolo dei chiusi è semimodulare.*

Si hanno quindi due operatori di chiusura diversi che operano sullo stesso insieme.

Capitolo 4

Reticoli geometrici

4.1 Reticoli geometrici e matroidi

Definizione 4.1.1. *Un reticolo è geometrico se è*

1. *atomico*
2. *semimodulare*
3. *con catene finite*

Per comprendere meglio la definizione diamo la rappresentazione di alcuni reticoli attraverso il loro diagramma di Hasse.

Figura 4.1: Reticolo atomico che non è semimodulare: $x \wedge y \prec x, y$ ma $x, y \prec x \vee y$

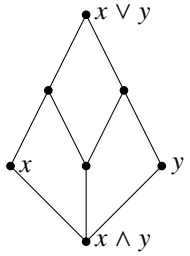
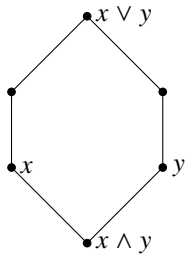


Figura 4.2: Reticolo semimodulare che non è atomico

Figura 4.3: Reticolo che non è nè atomico nè semimodulare



Esempio 4.1.1. *Le algebre di Boole finite e i reticoli di sottospazi di uno spazio vettoriale di dimensione finita sono reticoli geometrici.*
Consideriamo adesso il reticolo delle partizioni di un qualunque insieme finito $\mathcal{P}(n)$ e dimostriamo che tale reticolo è geometrico. Abbiamo già dimostrato in 3.2.2 che $\mathcal{P}(n)$ è semimodulare, quindi rimane da mostrare che $\mathcal{P}(n)$ è atomico. Gli atomi di $\mathcal{P}(S)$, con $|S| = n$, sono tutte le partizioni aventi un solo blocco di cardinalità due e tutti gli altri di cardinalità uno, ovvero $\pi_{\mathrm{a,b}} = \{\{a, b\}, \{c\}, \{d\}, \dots\}$. Quindi se π è una partizione arbitraria di S si può scrivere come estremo superiore degli atomi il cui unico blocco di due elementi è contenuto in un blocco di π, ovvero $\pi = \bigvee_{\mathrm{a,b}} \pi_{\mathrm{a,b}}$.

Vediamo una prima caratterizzazione dei reticoli geometrici:

Proposizione 4.1.1. *Un reticolo L dotato di minimo 0 con catene finite è geometrico se e solo se per ogni $a, b \in L$ risulta:*

$$a \prec b \iff \textit{esiste un atomo } p \textit{ con } p \not\leq a \textit{ e } b = a \vee p.$$

Dimostrazione. Sia L un reticolo geometrico, in particolare L è atomico. Dunque presi $a, b \in L$ si ha che esistono $p_1, \dots, p_{\mathrm{k}}, q_1, \dots, q_{\mathrm{s}}$ atomi di L tali che

$$a = p_1 \vee \cdots \vee p_{\mathrm{k}} \qquad b = q_1 \vee \cdots \vee q_{\mathrm{s}}.$$

- Se $a \prec b$ allora esiste un atomo q_{t} tale che $q_{\mathrm{t}} \not\leq a$ ma $q_{\mathrm{t}} \leq b$. Siccome L è semimdulare

$$a \prec a \vee q_{\mathrm{t}}.$$

Siccome $a \leq b$, $q_{\mathrm{t}} \leq b$ si ha

$$a \prec a \vee q_{\mathrm{t}} \leq b.$$

Ma $a \prec b$ quindi necessariamente $b = a \vee q_{\mathrm{t}}$.

- Se invece $b = a \vee p$, con p atomo tale che $p \not\leq a$ per la semimodularità del reticolo segue che $a \prec b$.

Viceversa supponiamo che valga: $a \prec b \iff$ esiste un atomo p con $p \not\leq a$ e $b = a \vee p$, allora

- L è atomico:
  preso $a \in L$ vogliamo mostrare che a è *sup* di atomi del reticolo. Ragioniamo per induzione sulla lunghezza della catena massimale da 0 ad a. Se a è un atomo, allora a è sup di se stesso. Se a non è un atomo esiste un elemento a' nella catena coperto da a. Applicando l'ipotesi induttiva sulla catena massimale di estremi 0 e a' abbiamo che a' si scrive come *sup* di atomi, quindi $a' = q_1 \vee \dots q_{\mathrm{n}}$ con q_{i} atomi. Siccome $a' \prec a$ grazie all'ipotesi del teorema si ha che esiste un atomo $p \not\leq a'$ tale che $a = a' \vee p = q_1 \vee \dots q_{\mathrm{n}} \vee p$.

- L è semimodulare:
  siano $a, b \in L$ tali che $a \wedge b \prec a$ allora esiste un atomo $p \not\leq a \wedge b$ tale che $a = (a \wedge b) \vee p$. Allora $a \vee b = (a \wedge b) \vee p \vee b = b \vee p$. Quindi, grazie all'ipotesi del teorema, $b \prec a \vee b$.

□

In altre parole, in un reticolo geometrico, presi comunque due elementi a, b con $a \leq b$, si ha una corrispondenza biunivoca tra ogni catena massimale $a = x_0 \prec x_1 \prec \cdots \prec x_k = b$ e una successione finita di atomi $p_1, p_2, \dots$ tale che

$$p_i \not\leq x_{i-1} \quad \forall i \quad \text{e} \quad x_1 = a \vee p_1, \quad x_2 = x_1 \vee p_2, \dots.$$

In particolare il rango di un elemento a del reticolo si può scrivere come

$$r(a) = min\{k; a = p_1 \vee \cdots \vee p_k; p_1, \dots p_k \text{ atomi}\}.$$

Definizione 4.1.2. *Sia S è un insieme arbitrario, e I una collezione di sottoinsiemi di S tali che :*

1. $I \neq \emptyset$,
2. $\forall A \in I$, $B \subseteq A \implies B \in I$ *(ovvero I è una collezione chiusa rispetto l'inclusione),*
3. $\forall A, B \in I$ *tali che* $|A| > |B|$ *esiste* $x \in A \setminus B$ *tale che* $B \cup \{x\} \in I$ *(proprietà di scambio),*

allora la coppia (S, I) si dice matroide degli indipendenti di S.
S viene chiamato insieme ambiente della matroide ed I insieme degli indipendenti della matroide.

Si osservi che:

- l'insieme vuoto è un indipendente,

- ogni sottoinsieme di un indipendente è a sua volta un indipendente,
- se A e B sono due insiemi indipendenti e A possiede più elementi di B, allora esiste un elemento in A ma non in B tale che aggiunto a B porta a un altro insieme indipendente.

Un sottoinsieme indipendente massimale viene chiamato base della matroide $\mathcal{M}$,
un sottoinsieme di S che non è indipendente viene detto dipendente, inoltre se il sottoinsieme dipendente è minimale viene detto circuito.
Si può inoltre definire un operatore di chiusura ϕ sull'insieme degli indipendenti: se $A \subseteq S$ allora ϕ amplia A aggiungendo ad A tutti gli elementi $x \in S \setminus A$ in modo tale che esista un circuito C di $\mathcal{M}$ che contiene x e che è contenuto nell'unione di $A \cup \{x\}$.

Esempio 4.1.2. *Sia E un insieme, $k \in \mathbb{N}$. I sottoinsiemi di E con al più k elementi costituiscono gli insiemi indipendenti di una matroide definita su E ,infatti:*

- *per ogni $k \in \mathbb{N}$, $\emptyset$ non ha più di k elementi,*
- *ogni sottoinsieme di un insieme che ha al più k elementi, ha al più k elementi,*
- *Se $|A| > |B|$ allora A deve contenere qualche elemento $x \notin B$. Dato che B ha cardinalità al più $k-1$ allora aggiungendo x a B si mantiene l'indipendenza.*

Definizione 4.1.3. *Sia S un insieme e $\phi\colon A \mapsto \overline{A}$ un operatore di chiusura definito su $\mathcal{B}(S)$ tali che:*

1. *$a \notin \overline{A}, a \in \overline{A \cup b} \implies b \in \overline{A \cup a}$ (proprietà di scambio di Steinitz);*
2. *per ogni $A \subseteq S$ esiste $B \subseteq A$, B finito, tale che $\overline{B} = \overline{A}$ (proprietà della base finita);*

allora la coppia (S, ϕ) si chiama matroide della chiusura sull'insieme S e si indica con $\mathcal{M}(S)$.
Inoltre $\mathcal{M}(S)$ è detta semplice se:

$$\overline{\emptyset} = \emptyset \quad e \quad \overline{p} = p \text{ per ogni } p \in S \text{ (proprietà di semplicità).}$$

Si dimostra che la matroide della chiusura è equivalente ad una matroide di indipendenti il cui operatore di chiusura definito sugli insiemi indipendenti coincide con l'opertore di chiusura appena introdotto. Abitualmente si usa denotare con $\mathcal{M}$ la matroide $\mathcal{M}(S)$ se è chiaro l'insieme sul quale è definita la matroide. Quando si deve trattare con una matroide si può scegliere se definirla mediante il suo operatore di chiusura oppure mediante i suoi insiemi indipendenti.

Esempio 4.1.3. *Uno spazio vettoriale di dimensione finita V, con l'usuale chiusura lineare (ovvero per ogni $U \subseteq V$ si ha che $\overline{U}$ è il sottospazio generato da U) è una matroide semplice. Lo stesso vale per uno spazio affine con dimensione finita, con la chiusura affine.*

Teorema 4.1.1 (Birkhoff-Whitney)**.** *Il reticolo dei chiusi della matroide $\mathcal{M}(U)$ sull'insieme U , che indicheremo con $\mathcal{L}(U)$, è geometrico. Viceversa, se L è un reticolo geometrico, l'insieme U dei suoi atomi con l'operatore di chiusura $\phi\colon A \mapsto \overline{A} := \{p \in U; p \leq \vee A\}$ è una matroide semplice; inoltre, il reticolo dei chiusi di questa matroide è isomorfo a L attraverso l'isomorfismo $\psi : L \to \mathcal{L}(U); \psi(x) = \{p \in U; p \leq x\}$.*

Dimostrazione. Vogliamo dimostrare che il reticolo dei chiusi della matroide è un reticolo geometrico:

- $\mathcal{L}(U)$ è atomico perchè per ogni chiuso A risulta che $A = \vee\{\overline{p}; p \in A\}$.
- Verifichiamo che il reticolo è semimodulare: siano $A, B \in \mathcal{L}(U)$ con $A \cap B \prec A$, allora esiste un elemento $p \in A \setminus B$ tale che $A = \overline{(A \cap B) \cup p}$; questo implica che $\overline{A \cup B} = \overline{B \cup p} \succ B$.
- Supponiamo ora che $\mathcal{L}(U)$ possieda catene infinite; allora, in esso esisterà una catena ascendente oppure discendente numerabile.
  - Nel primo caso: sia $A_1 < A_2 < \dots$ una catena ascendente in $\mathcal{L}(U)$. Per la proprietà della base finita sappiamo che esiste un insieme finito $B \subseteq \bigcup A_i$ tale che $\overline{B} = \overline{\bigcup A_i}$. Ma il fatto che $B \subseteq \bigcup A_i$ implica che $B \subseteq A_m$ per un certo m. Siccome gli A_i sono dei chiusi risulta che $A_j \subseteq \overline{\bigcup A_i} = \overline{B} \subseteq A_m$, ovvero la catena è stazionaria dopo A_m.
  - Nel secondo caso: sia $A_1 > A_2 \dots$ una catena discendente in $\mathcal{L}(U)$. Per ogni i scegliamo un elemento $a_i \in A_i \setminus A_{i+1}$ e poniamo $A = \{a_1, a_2, \dots\}$ e $S_i = \{a_i, a_{i+1}, \dots\}$. Evidentemente $S_i \subseteq A_i$, allora siccome per ogni i gli A_i sono dei chiusi avremo che $\overline{S_{i+1}} \subseteq A_{i+1}$. Di conseguenza l'elemento $a_i \notin \overline{S_{i+1}}$. Poniamo ora $B_i = A \setminus a_i$ e supponiamo che $a_i \in \overline{B_i}$. Scegliendo il massimo indice j per cui $a_i \in \overline{S_j \setminus a_i}$ ($j \leq i-1$ perchè $a_i \notin S_{i+1}$) possiamo concludere che $a_i \notin \overline{S_{j+1} \setminus a_i} = \overline{(S_j \setminus a_j) \setminus a_i} = \overline{(S_j \setminus a_i) \setminus a_j}$. Per la proprietà di scambio $a_j \in \overline{S_{j+1}}$, e questo è assurdo per come abbiamo definito gli S_i.

Viceversa supponiamo che L sia un reticolo geometrico, e chiamiamo U l'insieme dei suoi atomi. Si verifica facilmente, sfruttando la definizione 4.1.1, che U con l'operatore di chiusura $A \mapsto \overline{A} = \{p \in U; p \leq supA\}$ è una matroide semplice. Infine la funzione $\psi(x) = \{p \in U; p \leq x\}$ per ogni x è un isomorfismo d'ordine, e quindi di reticoli; questo perchè i chiusi della matroide che abbiamo definito sono tutti e soli i sottoinsiemi del tipo $U \cap [0, x]$, dove x è un elemento del reticolo diverso dal minimo. □

Esempio 4.1.4. *Per ogni intero n il reticolo delle partizioni $\mathcal{P}(n)$ è geometrico. Vediamo qual'è la matroide corrispondente. Indichiamo con S l'insieme di cardinalità n di cui stiamo prendendo le partizioni. Abbiamo visto che gli atomi di $\mathcal{P}(n)$ sono in corrispondenza biunivoca con i sottoinsiemi di cardinalità due di S. Dunque, il sostegno della matroide è l'insieme di tutte le coppie non ordinate di elementi di S, cioè l'insieme dei lati del grafo completo $K(S)$ con insieme dei vertici in S. Inoltre dato un insieme A di lati, la sua chiusura nella matroide è costruita nel modo seguente: siano $C_1, C_2, \dots, C_k$ le componenti connesse del grafo avente come insieme dei lati A; allora $\overline{A} = \overline{C_1} \cup \dots \cup \overline{C_k}$ dove $\overline{C_i}$ è ottenuto da C_i aggiungendo tutti i lati di $K(S)$ i cui vertici appartengono entrambi alla componente connessa C_i.*

4.2 Complementazione

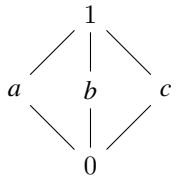
Definizione 4.2.1. *Sia L un reticolo dotato di minimo 0 e massimo 1, e sia x un elemento del reticolo. Diciamo che x ammette complemento in L se esiste un elemento $y \in L$ tale che*

$$x \vee y = 1 \qquad x \wedge y = 0.$$

Un reticolo nel quale ogni elemento ammette complemento si dice complementato.

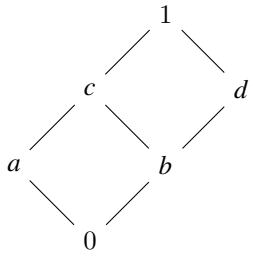
Esempio 4.2.1. *In un reticolo L dotato di minimo 0 e massimo 1, si ha che 0 e 1 sono uno il complemento dell'altro, infatti $0 \wedge 1 = 0$ e $0 \vee 1 = 1$.*

Esempio 4.2.2. *Il reticolo M_3 è complementato perchè ciascuno degli elementi a, b, c è complemento degli altri due. M_3 fornisce un esempio di un reticolo complementato in cui però esistono elementi che*



hanno più di un complemento.

Esempio 4.2.3. *Nel reticolo in figura gli elementi a e d sono uno complemento dell'altro, mentre gli*



elementi b e c non possiedono complemento.
Questo reticolo non è complementato, ma se un elemento possiede complemento, questo è unico.

Esempio 4.2.4. *Sia U un insieme; nell'algebra di Boole $\mathcal{B}(U)$ il complemento di un sottoinsieme A di U è il sottoinsieme complementare di A. $\mathcal{B}(U)$ fornisce un esempio di reticolo complementato in cui ogni elemento ha un unico complemento.*

Esempio 4.2.5. *In una catena dotata di minimo e di massimo gli unici elementi dotati di complemento sono questi ultimi.*

Si noti che l'unico reticolo non distributivo, tra gli esempi citati, è M_3; infatti:

Proposizione 4.2.1. *In un reticolo distributivo il complemento di un elemento, se esiste, è unico.*

Dimostrazione. Se L è distributivo e b e c sono due complementi di $a \in L$, per la distributività di L abbiamo:

$$b = b \vee 0 = b \vee (a \wedge c) = (b \vee a) \wedge (b \vee c) = 1 \wedge (b \vee c) = b \vee c$$

questo implica che $c \leq b$; scambiando i ruoli di b e c ottieniamo che $b \leq c$, da cui $b = c$. □

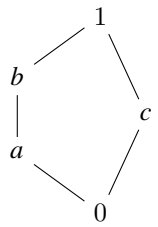
Definizione 4.2.2. *Sia L un reticolo dotato di minimo e massimo. Se per ogni $a, b \in L$ tali che $a \leq b$, l'intervallo $[a, b]$ è un reticolo complementato, allora L si dice relativamente complementato.*

Osservazione 4.2.1. *Sia L un reticolo dotato di minimo e massimo. Siano $x, y \in L$ con $x \leq y$. Se y è complemento di x allora $x = 0$ e $y = 1$.*

Dimostrazione. Se $x \leq y$ allora si ha che $0 = x \wedge y = x$ e $1 = x \vee y = y$. □

Si noti che se un reticolo è relativamente complementato ovviamente è anche complementato. L'implicazione inversa è falsa.

Esempio 4.2.6. *Il reticolo N_5 è complementato ma non è relativamente complementato perchè l'intervallo $[a, 1]$ non è completo.*



Proposizione 4.2.2. *Un reticolo semimodulare con catene finite è geometrico se e solo se è relativamente complementato.*

Dimostrazione. Supponiamo che L sia un reticolo geometrico. Sia $[a, b]$ un intervallo di L e siano $x, x' \in [a, b]$ con $x \wedge x' = a$. Se $x \vee x' = b$ abbiamo finito. Supponiamo allora che $x \vee x' < b$. Siccome L è atomico, ogni elemento del reticolo si scrive come *sup* di atomi. Quindi esiste sicuramente un atomo q che compare nella scomposizione di b ma non in quella di $x \vee x'$, ovvero:

$$q \leq b, \qquad q \not\leq x \vee x'.$$

Poniamo $x'' = x' \vee q$. Chiaramente $x'' \in [a, b]$e si ha che

$$x \vee x'' > x \vee x'.$$

Quest'ultima disuguaglianza si ha perchè per come abbiamo definito x'' si ha che $x'' = q \vee x' \geq x'$; non può valere l'uguaglianza perchè se per assurdo $x \vee x'' = x \vee (q \vee x') = x \vee x'$ allora si avrebbe $x' \vee q = x'$ che implica $q \leq x'$, d'altra parte $x \vee (q \vee x') = (x \vee q) \vee x' = x \vee x'$ allora si avrebbe $x \vee q = x$ che implica $q \leq x$; allora avremmo $q \leq x$ e $q \leq x'$ che implica $q \leq x \vee x'$ e questo è assurdo per come abbiamo scelto q.
Risulta che $x \wedge x'' = a$. Infatti se così non fosse avremmo $a = x \wedge x' < x \wedge x'' = x \wedge (x' \vee q)$, quindi esisterebbe un elemento p tale che $x \wedge x' < (x \wedge x') \vee p \leq x \wedge (x' \vee q)$.

Da qui segue che $p \not\leq x'$ e $p \leq x' \vee q$. Grazie alla legge di scambio si ha che $x' \vee p = x' \vee q$ quindi $x \vee x' \vee q = (x \vee x') \vee p = x \vee x'$ assurdo. Ripetendo questo procedimento iterativamente si arriva a trovare il complemento di x in $[a, b]$.
Viceversa supponiamo che L sia relativamente complementato. Sia $a \in L$, poniamo $b := sup\{p \in L; 0 \prec p \leq a\}$ e supponiamo che $b < a$. Scegliamo un complemento b' di b in $[0, a]$. Siccome $b' > 0$ si ha che esiste un atomo q con $q \leq b' \leq a$ e $q \not\leq b$ Allora q appartiene all'insieme di cui b è sup ma $q \not\leq b$, contraddizione. Si ha dunque che $b = a$, ovvero ogni elemento $a \in L$ è sup degli elementi del reticolo che lo precedono. Segue che il reticolo L è atomico. □

Si noti che un reticolo atomico con catene finite non deve necessariamente essere complementato e a maggior ragione relativamente complementato. Il reticolo in figura 4.4 è atomico e semimodulare inferiormente ma l'elemento a non possiede complemento.

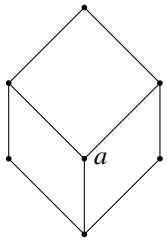


Figura 4.4:

Viceversa un reticolo semimodulare e complementato non deve essere necessariamente atomico 4.5. Ma si ha che:

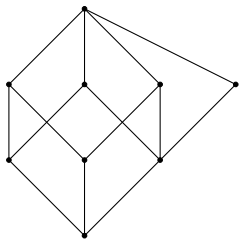


Figura 4.5:

Proposizione 4.2.3. *Un reticolo modulare e complementato è relativamente complementato.*

Dimostrazione. Prendiamo $x \in [a, b]$ e supponiamo che y sia un complemento di x. Verifichiamo che l'elemento $b \wedge (y \vee a) = (b \wedge y) \vee a$ è il complemento di x in $[a, b]$:

- $y \vee a \geq y \vee x = 1$ quindi $b \wedge (y \vee a) \geq b \wedge 1 = b$ che implica $b \wedge (y \vee a) = b$,
- $y \wedge b \leq y \wedge x = 0$ quindi $(b \wedge y) \vee a \leq 0 \vee a = a$ che implica $(b \wedge y) \vee a = a$.

Quindi si ha che

$$x \wedge (b \wedge (y \vee a)) = x \wedge b = b, \qquad x \vee ((b \wedge y) \vee a)) = a.$$

□

Si noti che in 4.2.2 in realtà abbiamo dimostrato un risultato più forte che infatti vale in ogni reticolo relativamente complementato con catene finite:

Proposizione 4.2.4. *Sia L un reticolo relativamente complementato con catene finite. Siano $a, b \in L$ e $x, y \in [a, b]$ con $x \wedge y = a$. Allora riusciamo a trovare un elemento $x' \in [a, b]$ che è un complemento di x in $[a, b]$ e tale che $x' \geq y$.*

Dimostrazione. Supponiamo che $x \vee y < b$ e supponiamo che x' sia un complemento di $x \vee y$ in $[y, b]$ quindi

$$x' \wedge (x \vee y) = y, \qquad x' \vee (x \vee y) = b.$$

Verifichiamo che x' è un complemento di x in $[a, b]$ supponendo $x' \geq y$:

- $x \wedge x' = (x \wedge (x \vee y)) \wedge x' = x \wedge ((x \vee y) \wedge x') = x \wedge y = a$,
- $x \vee x' = x \vee (y \vee x') = (x \vee y) \vee x' = b$.

□

La relativa complementazione è un proprietà che viene ereditata dal prodotto diretto e dagli intervalli. Inoltre, siccome la relativa complementazione è una proprietà autoduale, segue che possiamo ottenere una proposizione duale per ogni proposizione dimostrata. Per esempio si ha:

Proposizione 4.2.5. *Un intervallo di un reticolo geometrico, così come un prodotto diretto di reticoli geometrici, è a sua volta geometrico.*

Corollario 4.2.1. *Sia L un reticolo geometrico.*

1. *Ogni elemento si può scrivere come $\mathbf{sup}$ di atomi. Dualmente ogni elemento si può scrivere come inf di iperpiani.*
2. *Sia $[a, b] \subseteq L$, $x, y \in [a, b]$ con $x \wedge y = a$; allora esiste un complemento x' di x in $[a, b]$ con $x' \geq y$. Dualmente, supponiamo $x, y \in [a, b]$ con $x' \geq y$; allora esiste un complemento x' di x in $[a, b]$ con $x' \leq y$.*
3. *Sia $a \in L$. Se un atomo $p \nleq a$ allora $p \leq a'$ dove a' è un complemento di a. Dualmente se un iperipiano $h \ngeq a$ allora $h \geq a'$ dove a' è un complemento di a.*

Grazie alla complementazione riusciamo a dare un'utile descrizione dei reticoli distributivi e modulari.

Definizione 4.2.3. *Sia L un reticolo geometrico.*

- *La coppia $a, b \in L$ è chiamata coppia modulare, ed è denotato con$(a, b)M$, se $r(a \wedge b) + r(a \vee b) = r(a) + r(b)$.*
- *L'elemento a si dice modulare, ed è denotato con aM, se per ogni $x \in L$ si ha $(a, x)M$.*
- *Tre elementi $a, b, c \in L$ formano una tripletta distributiva, che viene denotata con $(a, b, c)D$ se (R_3) vale per $\{a, b, c\}$.*
- *L'elemento a si dice distributivo, ed è denotato con aD, se per ogni $x, y \in L$ si ha $(a, x, y)D$.*

Equivalentemente possiamo chiamare a elemento distributivo se le identità

$$a \wedge (x \vee y) = (a \wedge x) \vee (a \wedge y), \qquad x \wedge (a \vee y) = (x \wedge a) \vee (x \wedge y)$$

e le loro duali sono verificate per ogni x, y. Ovviamente L è modulare, rispettivamente distributivo, se ogni elemento di L è modulare, rispettivamente distributivo.

Proposizione 4.2.6. *In un reticolo geometrico le seguenti affermazioni sono equivalenti:*

1. *$(a, b)M$.*
2. *b è il minimo complemento di a nell'intervallo $[a \wedge b, a \vee b]$ (equivalentemente a è il minimo complemento di b nell'intervallo $[a \wedge b, a \vee b]$).*
3. *ϕ_{b} definita in (3.1) è una mappa iniettiva che manda $[a \wedge b, a]$ in $[b, a \vee b]$ (equivalentemente ϕ_{a} è una mappa iniettiva che manda $[a \wedge b, b]$ in $[a, a \vee b]$).*

Dimostrazione. $1 \implies 2$. Se per assurdo esiste t complemento di a in $[a \wedge b, a \vee b]$ tale che $t < b$, allora per la semimodularità si ha che $r(b) > r(t) \geq r(t \vee a) + r(t \wedge a) - r(a) = r(a \vee b) + r(a \wedge b) - r(a) = r(b)$ assurdo.
$2 \implies 3$. Se per assurdo ϕ_{b} non fosse iniettiva sull'intervallo $[a \wedge b, a]$, allora esisterebbe $z \in [a \wedge b, a]$ con $(z \vee b) \wedge a > z$ da 3.1. Supponiamo che t sia un complemento di $(z \vee b) \wedge a$ nell'intervallo $[z, a]$. Allora si ha che

$$(a \wedge b) \wedge b \leq z \wedge b \leq t \wedge b \leq a \wedge b \text{ che implica } t \wedge b = a \wedge b,$$
$$t \vee b = t \vee (z \vee b) = t \vee ((z \vee b) \wedge a) \vee b = a \vee b.$$

Quindi abbiamo che t è un complemento di b nell'intervallo $[a \wedge b, a \vee b]$, ma $t < a$ e per ipotesi è il più piccolo complemento nello stesso intervallo, quindi la conclusione è assurda.
$3 \implies 1$. Segue direttamente da 3.2.1. □

Proposizione 4.2.7. *In un reticolo geometrico le seguenti affermazioni sono equivalenti:*

1. *aM.*
2. *I complementi di a formano un'anticatena.*

3. ϕ_b, ψ_a *sono due isomorfismi, uno inverso dell'altro, tra* $[a \wedge b, a]$ *e* $[b, a \vee b]$ *per ogni* b*, cioè:*

$$(z \vee b) \wedge a = z \text{ per ogni } z \in [a \wedge b, a] \quad e \quad (w \wedge a) \vee b = w \text{ per ogni } w \in [b, a \vee b].$$

Osservazione 4.2.2. *Se* a *è un elemento modulare del reticolo allora si ha* $[a \wedge b, a] \cong [b, a \vee b]$ *per ogni* b*. Ma in generale non vale che* $[a \wedge b, b] \cong [a, a \vee b]$*.*

Un corollario interessante di 4.2.6 è la seguente caratterizzazione dei reticoli geometrici che sono anche modulari.

Corollario 4.2.2. *Un reticolo geometrico è modulare se e solo se* $h \wedge l > 0$ *per ogni iperpiano* h *e ogni retta* l*.*

Dimostrazione. Se L è modulare la tesi segue da 3.8. Viceversa supponiamo che L non sia modulare. Allora la (3.2) non è verfiicata. Esistono quindi due elementi a, b con $b \prec a \vee b, a \wedge b \prec a$ ma $a \wedge b \not\prec a$. Possiamo scegliere a in modo tale che $r(a) = r(a \wedge b) + 2$. Sia poi h il minimo dei complementi di $a \vee b$ in $[b, 1]$ e l il minimo dei complementi di $a \wedge b$ in $[0, a]$. Da 4.2.6 ho che la coppia $(h, a \vee b)$ è modulare, quindi si ha che

$$\begin{aligned} &r(h \vee (a \vee b)) + r(h \wedge (a \vee b)) = r(h) + r(a \vee b) \iff \\ &r(1) + r(b) = r(h) + r(a \vee b) \iff \\ &r(h) = r(1) + r(b) - r(a \vee b) = r(1) - 1 \end{aligned}$$

Analogamente la coppia $(l, a \wedge b)$ è modulare, quindi si ha che

$$\begin{aligned} &r(l \vee (a \wedge b)) + r(l \wedge (a \wedge b)) = r(l) + r(a \wedge b) \iff \\ &r(a) + r(0) = r(l) + r(a \wedge b) \iff \\ &r(l) = r(a) - r(a \wedge b) = r(a \wedge b) + 2 - r(a \wedge b) = 2. \end{aligned}$$

Si ha dunque che h è un iperpiano ed l è una retta. Inoltre $h \wedge l = h \wedge a \wedge l = (h \wedge (a \vee b)) \wedge a \wedge l = (b \wedge a) \wedge l = 0$. □

Un'altra conseguenza di 4.2.6 è che un reticolo geometrico può in qualche misura essere già determinato dalla struttura dei suoi intervalli superiori.

Proposizione 4.2.8. *Ogni intervallo di un reticolo geometrico è isomorfo ad un intervallo superiore.*

Dimostrazione. Consideriamo l'intervallo $[a, b]$. Sia c il minimo complemento di b in $[a, 1]$. Sia poi $\phi_c \colon [a, b] \longrightarrow [c, 1]$ tale che $\phi_c(x) = x \vee c$. Segue che $\phi_c(a) = a \vee c = c, \phi_c(b) = b \vee c = 1$ da cui la tesi. □

Capitolo 5

Esempi fondamentali

Tutti i reticoli di cui abbiamo parlato sono dotati di una funzione rango. Ha senso dunque classificare gli elementi di un reticolo in base al loro rango. Per un insieme parzialmente ordinato P dotato di rango l'insieme $P^{\mathrm{k}} = \{a \in P; r(a) = k\}$ è chiamato livello k di P. Per esempio P^0 è l'insieme degli elementi minimali di P e P^1 è l'insieme dei suoi atomi. Se P è finito, la cardinalità dell'insieme di livello k, $\left|P^{\mathrm{k}}\right|$, assume un significato combinatorio.

5.1 Catene

Indichiamo con $C(n)$ una catena di lunghezza $n \in \mathbb{N}$; per semplicità identificheremo $C(n)$ con $\{0, 1, \ldots, n\}$. Abbiamo già visto che $C(n)$ è un reticolo distributivo.

Si noti che $|C(n)| = n + 1$ e $C(n) \cong C(n)^*$. Si ha che $r(i) = i$ per ogni $i \in \mathbb{N}_0$, quindi $r(C(n)) = n$. Inoltre $\left|C(n)^{\mathrm{k}}\right| = 1$ per ogni k e n.

$[i, j] \cong C(j - i) = C(r[i, j])$ per ogni $i, j \in \mathbb{N}_0$ con $i \leq j$. Quindi due intervalli $[i, j]$ e $[k, l]$ sono isomorfi se e solo se hanno lo stesso rango. Partizionando l'insieme degli intervalli della catena, $Int(C(n))$, nelle sue classi di isomorfismo, possiamo vedere che ogni classe di isomorfismo è univocamente determinata dal rango dei suoi membri. Quindi ad ogni classe di isomorfismo possiamo associare il simbolo (n) con

$$[i, j] \in (n) \iff j - i = n \qquad (n \in \mathbb{N}_0)$$

(n) si dice essere il *tipo* dell'intervallo.

5.2 Il reticolo dei divisori

Abbiamo già mostrato che il reticolo degli interi positivi ordinati dalla relazione di divisibilità $(\mathbb{Z}^+, |)$ è distributivo. Se $n = p_1^{k_1} \dots p_t^{k_t} \in \mathbb{Z}^+$ allora $r(n) = \sum_{i=1}^{t} k_i$. Ogni livello $(\mathbb{Z}^+, |)^k$, eccetto per $k = 0$, contiene tutti i numeri naturali la cui fattorizzazione contiene k numeri numeri primi, non necessariamente distinti.

$[l, m] \cong [1, m/l]$ per ogni $[l, m] \in int((\mathbb{Z}^+, |))$ attraverso $\phi\colon i \mapsto i/l$. Se $n = p_1^{k_1} \dots p_t^{k_t}$ allora $[l, n] \cong \prod_{i=1}^{t} C(k_i)$ attraverso l'isomorfismo $\phi\colon p_1^{i_1} \dots p_t^{i_t} \mapsto (i_1, \dots, i_t)$. Quindi, in particolare $[l, m]^* \cong [l, m]$ e $|[l, m]| = |[1, m/l]| = \sum_{i=1}^{t}(k_i + 1)$ se $m/l = p_1^{k_1} \dots p_t^{k_t}$. Il *tipo* (n) dell'intervallo $[l, m]$ è definito da

$$[l, m] \in (n) \iff m/l = n \qquad (n \in \mathbb{N})$$

Intervalli che non sono isomorfi sono di *tipi* differenti, ma non vale il viceversa. Per gli interi $m = p_1^{k_1} \dots p_t^{k_t}$ e $n = q_1^{k_1} \dots q_t^{k_t}$ che hanno lo stesso numero di primi nella loro fattorizzazione e gli stessi esponenti (a meno dell'ordine) abbiamo che $[1, m] \cong [1, n] \cong \prod_{i=1}^{t} C(k_i)$ ma in generale $(m) \neq (n)$. Per esempio $12 = 2^2 3, 45 = 3^2 5$, quindi $[1, 12] \cong [1, 45] \cong C(2) \times C(1)$ ma $(12) \neq (45)$. In altre parole, i *tipi* forniscono una partizione più fine di $Int((\mathbb{Z}^+, |))$ rispetto agli isomorfismi di intervalli.

5.3 Algebre di Boole

$\mathcal{B}(n)$ indica il reticolo dei sottoinsiemi di un insieme finito, che contiene esattamente $n < \infty$ elementi, ordinati con l'inclusione. Useremo le lettere $A, B, C, \dots$ per indicare i sottoinsiemi e la lettera S per indicare l'insieme ambiente. $\mathcal{B}(n)$ è un reticolo distributivo e complementato.

Se $n < \infty$, abbiamo che $\mathcal{B}(n) \cong \mathcal{B}(n)^*$ attraverso l'isomorfismo che manda ogni sottoinsieme nel suo complementare. Inoltre, $\mathcal{B}(n) \cong [C(1)]^n$, quindi $|\mathcal{B}(n)| = 2^n$. Per ogni $A \subseteq S, r(A) = |A|$, segue che $r(\mathcal{B}(n)) = n$. Per come abbiamo definito la funzione rango su questo reticolo si ha che $\mathcal{B}(n)^k$ consiste in tutti i sottoinsiemi di S con cardinalità k. Indichiamo la cardinalità dell'insieme $\mathcal{B}(n)^k$ con $\binom{n}{k}$, cioè $\left|\mathcal{B}(n)^k\right| := \binom{n}{k}$. Gli interi $\binom{n}{k}$ vengono chiamati "coefficienti binomiali". Dalla definizione segue che

$$\binom{n}{k} = \binom{n}{n-k} \quad \text{e} \quad 2^n = \sum_{k=0}^{n} \binom{n}{k} \qquad \text{per ogni } n, k \in \mathbb{N}_0$$

$[A, B] \cong \mathcal{B}(|B \setminus A|) = \mathcal{B}(r[A, B])$ per ogni $A \subseteq B \subseteq S$. Le classi di isomorfismo sono univocamente determinate dal loro *tipo* (n) dove

$$[A, B] \in (n) \iff |B \setminus A| = n \qquad (n \in \mathbb{N}_0).$$

5.4 Reticoli di sottospazi vettoriali

$\mathcal{L}(n, K)$ denota il reticolo dei sottospazi di uno spazio vettoriale di dimensione $n < \infty$ costruito su campo K. Usiamo le lettere $U, W, Z, \dots$ per indicare i sottospazi e la lettera V per indicare lo spazio

vettoriale su cui lavoriamo. La dimensione algebrica e il rango di uno spazio sono sinonimi e useremo denotarli rispettivamente con $dim(V)$ e $r(V)$. Si è precedentemente dimostrato che $\mathcal{L}(n,K)$ è un reticolo modulare e complementato.

$\mathcal{L}(n,K)^{\mathrm{k}}$ consiste in tutti i sottospazi di dimensione k di uno spazio vettoriale di dimensione n, e si ha che $r(\mathcal{L}(n,K)=n$. Supponiamo che il campo K abbia ordine $q<\infty$ indichiamo con $\binom{n}{k}_{\mathrm{q}}$ il numero $\left|\left|\mathcal{L}(n,q)^{\mathrm{k}}\right|\right.$. Gli interi $\binom{n}{k}_{\mathrm{q}}$ vengono chiamati "coefficienti Gaussiani". Si verifica che

$$\binom{n}{k}_{\mathrm{q}}=\binom{n}{n-k}_{\mathrm{q}} \text{ per ogni } n,k\in\mathbb{N}_0.$$

$[U,W]\cong\mathcal{L}(k,K)$ con $k=r(W)-r(U)$ per ogni $U\subseteq W\subseteq V$. Quindi le classi di isomorfismo di $Int(\mathcal{L}(n,K))$ sono univocamente determinate dal *tipo* (n), dove

$$[U,W]\in(n)\iff r(W)-r(U)=n \qquad (n\in\mathbb{N}_0).$$

5.5 Reticolo delle partizioni

$\mathcal{P}(n)$ denota il reticolo delle partizioni di un insieme di $n<\infty$ elementi. Useremo le lettere $\pi,\sigma,\rho,\tau,\ldots$ per indicare le partizioni dell'insieme con n elementi S, $b(\pi)$ indica i blocchi della partizione π. Abbiamo dimostrato che $\mathcal{P}(n)$ è un reticolo geometrico.

Si ha che $r(\pi)=n-b(\pi)$ per ogni $\pi\in\mathcal{P}(n)$. Quindi il livello $(n-k)$ di $\mathcal{P}(n)$ comprende tutte e sole le partizioni che hanno esattamente k blocchi. I numeri $\left|\mathcal{P}(n)^{(\mathrm{n-k})}\right|=:S_{\mathrm{n,k}}$ sono chiamati "numeri di Stirling di seconda specie" e i numeri $|\mathcal{P}(n)|=:B_{\mathrm{n}}$ sono chiamati "numeri di Bell". Dunque si ha

$$B_{\mathrm{n}}=\textstyle\sum_{k=1}^{n}S_{\mathrm{n,k}} \text{ per ogni } n,k\in\mathbb{N}$$

Sia $\pi=\{A_1,\ldots,A_{\mathrm{b}(\pi)}\}\in\mathcal{P}(n)$ con $|A_{\mathrm{i}}|=n_{\mathrm{i}}$, quindi $\sum_{i=1}^{b(\pi)}n_{\mathrm{i}}=n$. Siccome ogni partizione $\sigma\in[\pi,1]$ si ottiene combinando due o più blocchi di π si ha che $[\pi,1]\cong\mathcal{P}(b(\pi))$. D'altra parte, ogni partizione $\tau\in[0,\pi]$ si ottiene partizionando i blocchi A_{i} in blocchi più piccoli, quindi si ha che $[0,\pi]\cong\prod_{i=1}^{b(\pi)}\mathcal{P}(n_{\mathrm{i}})$. Riassumendo:

$$[\pi,1]\cong\mathcal{P}(b(\pi)) \qquad [0,\pi]\cong\textstyle\prod_{i=1}^{b(\pi)}\mathcal{P}(n_{\mathrm{i}}).$$

$$[\pi,\sigma]\cong\textstyle\prod_{i=1}^{b(\sigma)}\mathcal{P}(m_{\mathrm{i}}) \quad \text{per qualche } m_{\mathrm{i}} \text{ tale che } \sum_{i=1}^{n}m_{\mathrm{i}}=b(\pi)$$

Definiamo il *tipo* dell'intervallo $[\pi,\sigma]$ attraverso la seguente espressione formale:

$$tipo\,[\pi,\sigma]:=1^{\mathrm{b_1}}2^{\mathrm{b_2}}\ldots n^{\mathrm{b_n}} \quad \text{ se } [\pi,\sigma]\cong\textstyle\prod_{i=1}^{n}[\mathcal{P}(i)]^{\mathrm{b_i}}$$

Da qui si vede che le classi di isomorfismo di $Int(\mathcal{P}(n))$ sono univocamente determinate dal tipo a cui sono associate.
In modo analogo definiamo il *tipo* di una singola partizione π attraverso l'espressione

$$tipo(\pi) := 1^{b_1} 2^{b_2} \dots n^{b_n} \text{ se } [0,\pi] \cong \prod_{i=1}^{n} [\mathcal{P}(i)]^{b_i}$$

cioè, se π contiene esattamente b_i blocchi di cardinalità i ($i = 1, \dots, n$). Si noti che il tipo della partizione π è in corrispondenza biunivoca con il numero di tutte le possibili partizioni di n:

$$1^{b_1} 2^{b_2} \dots n^{b_n} \longleftrightarrow \underbrace{1 + \dots + 1}_{b_1} + \underbrace{2 + \dots + 2}_{b_2} + \dots + \underbrace{n + \dots + n}_{b_n}.$$

Bibliografia

[1] M. Aigner, *Combinatorial Theory*, Springer-Verlag, New York, 1979 .

[2] M. Barnabei e F. Bonetti, *Matematica Discreta Elementare*, Pitagora, Bologna, 1995.

[3] M. Barnabei, A. Brini e G.-C. Rota, *Un'introduzione alla teoria delle funzioni di Mobius*, in: Matroid Theory and its Applications, CIME 1980, Liguori Ed., 7–109.

[4] H. Crapo e G.-C. Rota, *On the foundations of combinatorial theory II: Combinatorial geometries*, Stud. Appl. Math. 49 (1970), 109–133.

[5] R. Stanley, *Enumerative Combinatorics*, Volume I, Cambridge University Press, 1997

Ringraziamenti

Ringrazio la Prof.ssa Marilena Barnabei per la disponibilità ed i preziosi consigli,
Ringrazio i miei compagni d'università con i quali ho condiviso questo persorso,
Ringrazio le amiche di una vita che mi hanno sempre supportata,
Grazie ai miei genitori, Mirna e Andrea, senza i quali questo non sarebbe stato possibile,
Grazie a mia sorella Lara, che è la mia certezza, a lei dedico questo mio traguardo.