

Ordini, reticoli e algebre di Boole

Dispense per gli studenti

Francesco Paoli*

29 settembre 2026

* Ringrazio Copilot Chat Basic per l'aiuto nel preparare questa dispensa.

1 Ordini parziali

Definition 1.1. *Siano A e B insiemi. Una relazione binaria da A a B è un sottoinsieme R di $A \times B$, ovvero un insieme di coppie ordinate il cui primo elemento appartiene ad A e il cui secondo elemento appartiene a B . Se $A = B$, diremo semplicemente che R è una relazione binaria su A .*

Se $a, b \in A$ e $\langle a, b \rangle \in R$, scriveremo per brevità aRb .

Definition 1.2. *Un ordine parziale (per brevità, poset) è una coppia ordinata $\mathbf{P} = \langle P, \leq \rangle$ dove $\leq$ è una relazione binaria su P tale che le seguenti proprietà valgono per ogni $a, b, c \in P$:*

1. *Riflessività:* $a \leq a$;
2. *Antisimmetria:* se $a \leq b$ e $b \leq a$, allora $a = b$;
3. *Transitività:* se $a \leq b$ e $b \leq c$, allora $a \leq c$.

Un ordine parziale $\mathbf{P} = \langle P, \leq \rangle$ si dice un *ordine totale* o anche una *catena* se $\leq$ ha la ulteriore proprietà di Linearità: per ogni a, b in P , o $a \leq b$ o $b \leq a$.

Example 1.3. 1. $\langle \mathbb{N}, \leq \rangle$, ovvero l'insieme dei numeri naturali ordinato mediante la relazione usuale di minore o uguale, è un poset. In particolare, è una catena.

2. Se X è un insieme e $Pw(X)$ è il suo insieme potenza (l'insieme di tutti i sottoinsiemi di X), allora $\langle Pw(X), \subseteq \rangle$ è un poset ma in genere non è una catena.
3. Sia n un numero naturale positivo. $\langle Div(n), | \rangle$, ovvero l'insieme dei divisori di n , ordinato mediante la relazione di divisibilità, è un poset ma in genere non è una catena.

Definition 1.4. *Sia $\mathbf{P} = \langle P, \leq \rangle$ un poset e sia $X \subseteq P$. Scriviamo:*

- $\uparrow X = \{a \in P : \text{esiste almeno un } x \in X \text{ tale che } x \leq a\};$
- $\downarrow X = \{a \in P : \text{esiste almeno un } x \in X \text{ tale che } a \leq x\};$
- $Lb(X) = \{a \in P : \text{per ogni } x \in X, a \leq x\};$
- $Ub(X) = \{a \in P : \text{per ogni } x \in X, x \leq a\}.$

Gli elementi di $Lb(X)$ e $Ub(X)$ si chiamano, rispettivamente, minoranti e maggioranti di X .

Se $a \in P$, scriveremo per brevità $\uparrow a$ e $\downarrow a$ in luogo di $\uparrow \{a\}$ e $\downarrow \{a\}$, rispettivamente.

Definition 1.5. Sia $\mathbf{P} = \langle P, \leq \rangle$ un poset. Un elemento $s \in P$ è detto estremo superiore di $X \subseteq P$ se:

1. $s \in Ub(X);$
2. per ogni $u \in Ub(X)$, si ha $s \leq u$.

Quando esiste, l'estremo superiore di X viene indicato con $\bigvee^{\mathbf{P}} X$.
Un elemento $i \in P$ è detto estremo inferiore di $X \subseteq P$ se:

1. $i \in Lb(X);$
2. per ogni $l \in Lb(X)$, si ha $l \leq i$.

Quando esiste, l'estremo inferiore di X viene indicato con $\bigwedge^{\mathbf{P}} X$.

Definition 1.6. Un poset $\mathbf{P} = \langle P, \leq \rangle$ si dice reticolato se per ogni $a, b \in P$ esistono l'estremo superiore e l'estremo inferiore di $\{a, b\}$.

L'estremo superiore di $\{a, b\}$ si denota con $a \vee^{\mathbf{P}} b$, mentre l'estremo inferiore si denota con $a \wedge^{\mathbf{P}} b$.

Lemma 1.7. Se $\mathbf{P} = \langle P, \leq \rangle$ è un poset reticolato, allora per ogni $a, b \in P$ si ha che:

1. Associatività: $(a \vee^{\mathbf{P}} b) \vee^{\mathbf{P}} c = a \vee^{\mathbf{P}} (b \vee^{\mathbf{P}} c)$, $(a \wedge^{\mathbf{P}} b) \wedge^{\mathbf{P}} c = a \wedge^{\mathbf{P}} (b \wedge^{\mathbf{P}} c);$
2. Commutatività: $a \vee^{\mathbf{P}} b = b \vee^{\mathbf{P}} a$, $a \wedge^{\mathbf{P}} b = b \wedge^{\mathbf{P}} a;$
3. Idempotenza: $a \vee^{\mathbf{P}} a = a$, $a \wedge^{\mathbf{P}} a = a;$
4. Assorbimento: $a \vee^{\mathbf{P}} (a \wedge^{\mathbf{P}} b) = a$, $a \wedge^{\mathbf{P}} (a \vee^{\mathbf{P}} b) = a.$

Dimostrazione. A titolo di esempio, dimostriamo la prima legge di assorbimento. Poiché $a \wedge^{\mathbf{P}} b \leq a$, l'elemento a è un maggiorante di $\{a, a \wedge^{\mathbf{P}} b\}$. Supponiamo che c sia un altro maggiorante. Allora $a \leq c$. Ne segue che a è il minimo fra i maggioranti. Pertanto $a \vee^{\mathbf{P}} (a \wedge^{\mathbf{P}} b) = a$.

L'altra identità si dimostra dualmente.

□

2 Reticoli

2.1 Definizione e proprietà elementari

Definition 2.1. Un reticolo è un'algebra $\mathbf{L} = \langle L, \wedge, \vee \rangle$, di tipo $\langle 2, 2 \rangle$, che soddisfa le seguenti equazioni:

$$\begin{array}{lll} x \vee (y \vee z) \approx (x \vee y) \vee z; & x \wedge (y \wedge z) \approx (x \wedge y) \wedge z; & \text{Associatività} \\ x \vee y \approx y \vee x; & x \wedge y \approx y \wedge x; & \text{Commutatività} \\ x \vee x \approx x; & x \wedge x \approx x; & \text{Idempotenza} \\ x \vee (x \wedge y) \approx x; & x \wedge (x \vee y) \approx x. & \text{Assorbimento} \end{array}$$

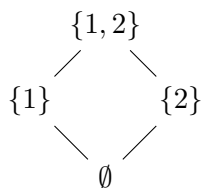
Se $\mathbf{L} = \langle L, \wedge, \vee \rangle$ è un reticolo, l'insieme L si dice *universo* di $\mathbf{L}$.

Example 2.2.

1. Se $\langle P, \leq \rangle$ è una catena, si può sempre costruire un reticolo con universo P . Per esempio, l'insieme $\{0, 1, 2\}$ è l'universo di un reticolo le cui operazioni sono $\min(x, y)$ e $\max(x, y)$, dove, presi due numeri x e y , $\min(x, y)$ e $\max(x, y)$ danno rispettivamente il più piccolo e il più grande tra essi rispetto alla relazione $\leq$:

$$\begin{array}{c} 2 \\ | \\ 1 \\ | \\ 0 \end{array}$$

2. Se X è un insieme, l'insieme $Pw(X)$ è l'universo di un reticolo $\mathbf{Pw}(X)$ le cui operazioni sono $A \cap B$ e $A \cup B$. Per esempio, quando $X = \{1, 2\}$, si ottiene il reticolo



Definition 2.3. Sia $\mathbf{L} = \langle L, \wedge, \vee \rangle$ un reticolo. Definiamo

$$P(\mathbf{L}) := \langle L, \leq^{\mathbf{L}} \rangle,$$

dove per ogni $a, b \in L$, $a \leq^{\mathbf{L}} b$ sse $a \wedge b = a$.

Si osservi che $a \leq^{\mathbf{L}} b$ sse $a \vee b = b$ (esercizio). Nei due reticoli dell'Esempio 2.2, la relazione $\leq^{\mathbf{L}}$ è, rispettivamente, la relazione di minore o uguale tra numeri naturali e la relazione di inclusione insiemistica.

Lemma 2.4. *Se $\mathbf{L} = \langle L, \wedge, \vee \rangle$ è un reticolo, allora $P(\mathbf{L})$ è un poset reticolato.*

Dimostrazione. Dobbiamo far vedere che $\leq^{\mathbf{L}}$ è una relazione di ordine parziale. Si tratta di una relazione riflessiva perché, per la condizione di idempotenza, $a \wedge a = a$. Per l'antisimmetria, supponiamo che $a \wedge b = a$ e $b \wedge a = b$. Per la condizione di commutatività, $a = a \wedge b = b \wedge a = b$. Infine, quanto alla transitività, supponiamo che $a \wedge b = a$ e $b \wedge c = b$. Allora, per associatività,

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

Si ha inoltre

$$(a \wedge b) \wedge a = a \wedge (b \wedge a) = a \wedge (a \wedge b) = (a \wedge a) \wedge b = a \wedge b$$

e

$$(a \wedge b) \wedge b = a \wedge (b \wedge b) = a \wedge b,$$

quindi $a \wedge b$ è un minorante di $\{a, b\}$. Infine, se $c \leq^{\mathbf{L}} a, b$, abbiamo $c \wedge a = c = c \wedge b$ e dunque $c \wedge (a \wedge b) = (c \wedge a) \wedge b = c \wedge b = c$. Ne segue che per ogni $a, b \in L$, $a \wedge^{P(\mathbf{L})} b$, ovvero l'estremo inferiore di $\{a, b\}$ rispetto a $\leq^{\mathbf{L}}$, esiste ed è uguale ad $a \wedge b$. $\square$

Definition 2.5. *Sia $\mathbf{P} = \langle P, \leq \rangle$ un poset reticolato. Definiamo*

$$L(\mathbf{P}) := \langle P, \wedge^{\mathbf{P}}, \vee^{\mathbf{P}} \rangle$$

(vedi Definizione 1.6).

Lemma 2.6. *Se $\mathbf{P} = \langle P, \leq \rangle$ è un poset reticolato, allora $L(\mathbf{P})$ è un reticolo.*

Dimostrazione. Segue dal Lemma 1.7. $\square$

Siano ora $\mathcal{Lat}$ e $\mathcal{PosLat}$ gli insiemi di tutti i reticoli e di tutti i poset reticolati, rispettivamente.

Theorem 2.7. *Le funzioni $P : \mathcal{Lat} \rightarrow \mathcal{PosLat}$ e $L : \mathcal{PosLat} \rightarrow \mathcal{Lat}$ stabiliscono una corrispondenza biunivoca tra reticoli e poset reticolati.*

Dimostrazione. Le due funzioni sono ben definite per i Lemmi 2.4 e 2.6. Inoltre, sono reciprocamente inverse. Infatti, se $\mathbf{L}$ è un reticolo,

$$L(P(\mathbf{L})) = \langle L, \wedge^{P(\mathbf{L})}, \vee^{P(\mathbf{L})} \rangle.$$

Ma nella dimostrazione del Lemma 2.4 abbiamo visto che $a \wedge^{P(\mathbf{L})} b = a \wedge b$ per ogni $a, b \in L$. Analogamente $a \vee^{P(\mathbf{L})} b = a \vee b$. Pertanto $L(P(\mathbf{L})) = \mathbf{L}$.

Viceversa, sia $\mathbf{P} = \langle P, \leq \rangle$ un poset reticolato. La relazione d'ordine indotta su $L(\mathbf{P})$ è definita da

$$a \leq^{L(\mathbf{P})} b \quad \text{sse} \quad a \wedge^{\mathbf{P}} b = a.$$

Ma questa è precisamente la relazione $\leq$ originaria. Quindi $P(L(\mathbf{P})) = \mathbf{P}$. Ne segue che P e L sono funzioni reciprocamente inverse. $\square$

In virtù del teorema precedente, d'ora in avanti trascureremo (tranne sporadici casi) la distinzione tra reticoli e poset reticolati e considereremo i reticoli, di volta in volta, come algebre o come ordini parziali a seconda della convenienza e degli obiettivi. Il medesimo teorema ci autorizzerà inoltre a non decorare obbligatoriamente con apici le operazioni reticolari e la relazione d'ordine da esse indotta. Lo faremo solo quando i reticoli coinvolti sono più di uno e l'omissione degli indici potrebbe causare confusione.

2.2 Filtri

Definition 2.8. Sia $\mathbf{L} = \langle L, \wedge, \vee \rangle$ un reticolo. Un sottoinsieme non vuoto $F \subseteq L$ si dice un filtro di $\mathbf{L}$ se valgono le seguenti condizioni:

1. se $a, b \in F$, allora $a \wedge b \in F$ (chiusura rispetto ai meet);
2. se $a \in F$ e $a \leq b$, allora $b \in F$ (chiusura verso l'alto).

L'insieme dei filtri di un reticolo $\mathbf{L}$ sarà denotato con $F(\mathbf{L})$. Dato $X \subseteq L$, il più piccolo filtro di $\mathbf{L}$ che contiene X sarà denotato con $F(X)$ e chiamato il filtro *generato* da X . Se $X = \{a\}$, scriveremo $F(a)$ invece di $F(\{a\})$ e chiameremo tale filtro il filtro *principale* generato da a .

Example 2.9. Consideriamo il reticolo $\mathbf{Pw}(\{1, 2\})$ (vedi Esempio 2.2.(2)). I seguenti insiemi sono filtri:

$$\{\{1\}, \{1, 2\}\},$$

$$\{\{2\}, \{1, 2\}\},$$

$$\{\{1, 2\}\}.$$

L'insieme $\{\{1\}, \{2\}\}$ non è invece un filtro, perché non contiene il meet dei suoi elementi: $\{1\} \cap \{2\} = \emptyset$.

Lemma 2.10. Sia $\mathbf{L}$ un reticolo. Per ogni $X \subseteq L$,

$$F(X) = \{a \in L : x_1 \wedge \cdots \wedge x_n \leq a \text{ per qualche } x_1, \dots, x_n \in X\}.$$

Dimostrazione. Sia G il membro di destra dell'uguaglianza precedente. Mostriamo innanzitutto che G è un filtro. Se $a, b \in G$, allora esistono $x_1, \dots, x_n, y_1, \dots, y_m \in X$ tali che $x_1 \wedge \cdots \wedge x_n \leq a$ e $y_1 \wedge \cdots \wedge y_m \leq b$. Allora

$$x_1 \wedge \cdots \wedge x_n \wedge y_1 \wedge \cdots \wedge y_m \leq a \wedge b.$$

Quindi $a \wedge b \in G$. La chiusura verso l'alto è immediata.

Inoltre, $X \subseteq G$, perché se $x \in X$, allora sicuramente esiste un $x_1 \in X$ (ovvero x stesso) tale che $x_1 \leq x$.

Infine, supponiamo che F sia un filtro contenente X e che $a \in G$. Allora esistono $x_1, \dots, x_n \in X$ tali che $x_1 \wedge \dots \wedge x_n \leq a$. Ma poiché $X \subseteq F$ ed F è chiuso rispetto ai meet, $x_1 \wedge \dots \wedge x_n \in F$. Inoltre, F è chiuso verso l'alto, da cui $a \in F$. Ne segue che $G \subseteq F$ e quindi che G è il più piccolo filtro che contiene X . □

Corollary 2.11. *Per ogni $a \in L$, $F(a) = \uparrow a$.*

Definition 2.12. *Un poset $\mathbf{P}$ si dice completo se per ogni sottoinsieme $X \subseteq P$ esistono sia $\bigvee^{\mathbf{P}} X$ sia $\bigwedge^{\mathbf{P}} X$. Un reticolo $\mathbf{L}$ si dice completo se il poset $P(\mathbf{L})$ è completo.*

Theorem 2.13. *Sia $\mathbf{L}$ un reticolo. Allora l'algebra*

$$\mathcal{F}(\mathbf{L}) := \langle F(\mathbf{L}), \cap, \vee^{\mathcal{F}(\mathbf{L})} \rangle$$

dove, per ogni $G, H \in F(\mathbf{L})$, $G \vee^{\mathcal{F}(\mathbf{L})} H = F(G \cup H)$, è un reticolo completo.

2.3 Sottoreticoli

Definition 2.14. *Sia $\mathbf{L} = \langle L, \wedge^{\mathbf{L}}, \vee^{\mathbf{L}} \rangle$ un reticolo. Un sottoinsieme $S \subseteq L$ si dice un sottoreticolo di $\mathbf{L}$ se, per ogni $a, b \in L$, $a, b \in S$ implica $a \vee b \in S$ e $a \wedge b \in S$.*

In base alla Definizione 2.14, un sottoreticolo è un *insieme*, non un'algebra. Tuttavia, esso determina univocamente un'algebra $\mathbf{S} = \langle S, \wedge^{\mathbf{S}}, \vee^{\mathbf{S}} \rangle$, dove $\wedge^{\mathbf{S}}$ e $\vee^{\mathbf{S}}$ sono le rispettive restrizioni di $\wedge^{\mathbf{L}}$ e $\vee^{\mathbf{L}}$ ad elementi di S . La Definizione 2.14 implica che tali operazioni sono totali e quindi l'algebra $\mathbf{S}$ è ben definita. Risulta immediato controllare che essa è un reticolo.

D'ora in avanti, quando parleremo di un sottoreticolo, saranno il contesto e la notazione usata a determinare senza ambiguità se lo considereremo come insieme o come algebra.

Example 2.15. Se $\mathbf{L} = \mathbf{Pw}(X)$ (vedi Esempio 2.2.(2)) e $Y \subseteq X$, allora $\mathbf{Pw}(Y)$ è un sottoreticolo di $\mathbf{Pw}(X)$. Infatti l'unione e l'intersezione di sottoinsiemi di Y sono ancora sottoinsiemi di Y .

2.4 Omomorfismi e congruenze

Definition 2.16. *Siano $\mathbf{L}$ e $\mathbf{M}$ reticoli. Una funzione $h : L \rightarrow M$ è un omomorfismo di reticoli se per ogni $a, b \in L$ si ha che $h(a \vee^{\mathbf{L}} b) = h(a) \vee^{\mathbf{M}} h(b)$ e $h(a \wedge^{\mathbf{L}} b) = h(a) \wedge^{\mathbf{M}} h(b)$.*

Se un omomorfismo di reticoli è biiettivo come funzione, si dice un *isomorfismo*, e due reticoli $\mathbf{L}$ e $\mathbf{M}$ si dicono *isomorfi* se esiste un isomorfismo da $\mathbf{L}$ a $\mathbf{M}$ (equivalentemente, da $\mathbf{M}$ a $\mathbf{L}$).

Example 2.17.

1. Consideriamo il reticolo $\mathbf{D}_2 = \langle \{0, 1\}, \wedge^{\mathbf{D}_2}, \vee^{\mathbf{D}_2} \rangle$ e il reticolo $\mathbf{D}_3 = \langle \{0, a, 1\}, \wedge^{\mathbf{D}_3}, \vee^{\mathbf{D}_3} \rangle$ tale che $0 <^{\mathbf{D}_3} a <^{\mathbf{D}_3} 1$. La funzione $h : \{0, a, 1\} \rightarrow \{0, 1\}$ definita da

$$h(0) = 0, \quad h(a) = 1, \quad h(1) = 1$$

è un omomorfismo da $\mathbf{D}_3$ a $\mathbf{D}_2$. Infatti, poiché i reticoli coinvolti sono catene, i join coincidono con i massimi e i meet coincidono con i minimi. È quindi sufficiente verificare direttamente che h preserva massimo e minimo di ogni coppia di elementi.

2. Consideriamo di nuovo il reticolo $\mathbf{Pw}(\{1, 2\})$ dell'Esempio 2.2.(2). La funzione $f : Pw(\{1, 2\}) \rightarrow \{0, 1\}$ definita da

$$f(A) = \begin{cases} 0 & \text{se } A = \emptyset, \\ 1 & \text{altrimenti} \end{cases}$$

è un omomorfismo da $\mathbf{Pw}(\{1, 2\})$ a $\mathbf{D}_2$. Infatti $f(A \cup B) = f(A) \vee^{\mathbf{D}_2} f(B)$ e $f(A \cap B) = f(A) \wedge^{\mathbf{D}_2} f(B)$ per ogni $A, B \subseteq \{1, 2\}$.

3. Mantenendo gli stessi reticoli dell'esempio precedente, la funzione $g : Pw(\{1, 2\}) \rightarrow \{0, 1\}$ definita da

$$g(\emptyset) = 0, \quad g(\{1\}) = 1, \quad g(\{2\}) = 1, \quad g(\{1, 2\}) = 0$$

non è un omomorfismo. Infatti $g(\{1\} \cup \{2\}) = g(\{1, 2\}) = 0$, mentre $g(\{1\}) \vee g(\{2\}) = 1 \vee 1 = 1$. Pertanto g non preserva il join.

Lemma 2.18. *Ogni omomorfismo di reticoli preserva l'ordine.*

Dimostrazione. Supponiamo che h sia un omomorfismo di reticoli da $\mathbf{L}$ a $\mathbf{M}$. Siano $a, b \in L$ tali che $a \leq^{\mathbf{L}} b$. Poiché $a = a \wedge^{\mathbf{L}} b$, abbiamo $h(a) = h(a \wedge^{\mathbf{L}} b) = h(a) \wedge^{\mathbf{M}} h(b)$. Pertanto $h(a) \leq^{\mathbf{M}} h(b)$. $\square$

Theorem 2.19. *Se h è un omomorfismo di reticoli da $\mathbf{L}$ a $\mathbf{M}$, l'insieme $Im(h) := \{h(a) : a \in L\}$ è un sottoreticolo di $\mathbf{M}$.*

Dimostrazione. Prendiamo $h(a), h(b) \in Im(h)$. Allora $h(a) \vee^{\mathbf{M}} h(b) = h(a \vee^{\mathbf{L}} b)$. Poiché $a \vee^{\mathbf{L}} b \in L$, si ha che $h(a) \vee^{\mathbf{M}} h(b) \in Im(h)$. Analogamente per il meet. $\square$

Definition 2.20. *Sia A un insieme. Una relazione binaria θ su A si dice una relazione di equivalenza se le seguenti proprietà valgono per ogni $a, b, c \in A$:*

1. *Riflessività:* $a\theta a$;
2. *Simmetria:* se $a\theta b$, allora $b\theta a$;
3. *Transitività:* se $a\theta b$ e $b\theta c$, allora $a\theta c$.

Se θ è una relazione di equivalenza sull'insieme A e $a \in A$, la classe di equivalenza di a modulo θ è l'insieme $\{b \in A : a\theta b\}$ e verrà indicata con $[a]_\theta$.

Definition 2.21. Sia $\mathbf{L}$ un reticolo. Una congruenza su $\mathbf{L}$ è una relazione di equivalenza θ su L tale che, per ogni $a, b, c, d \in L$, se $a\theta b$ e $c\theta d$, allora $(a \vee c)\theta(b \vee d)$ e $(a \wedge c)\theta(b \wedge d)$.

L'insieme di tutte le congruenze su un reticolo $\mathbf{L}$ verrà indicato con $Con(\mathbf{L})$. Se $X \subseteq L^2$, $Cg^{\mathbf{L}}(X)$ denoterà l'intersezione di tutte le congruenze su $\mathbf{L}$ contenenti X . Tale relazione è anch'essa una congruenza su $\mathbf{L}$ (esercizio).

Example 2.22. In ogni reticolo $\mathbf{L}$, la relazione identità $\Delta_L = \{\langle a, a \rangle : a \in L\}$ e la relazione universale $\nabla_L = L^2$ sono sempre congruenze.

Definition 2.23. Sia $\mathbf{L}$ un reticolo e sia θ una congruenza su $\mathbf{L}$. Definiamo

$$\mathbf{L}/\theta := \langle L/\theta, \wedge^{\mathbf{L}/\theta}, \vee^{\mathbf{L}/\theta} \rangle,$$

dove:

- $L/\theta := \{[a]_\theta : a \in L\};$
- $[a]_\theta \wedge^{\mathbf{L}/\theta} [b]_\theta := [a \wedge^{\mathbf{L}} b]_\theta;$
- $[a]_\theta \vee^{\mathbf{L}/\theta} [b]_\theta := [a \vee^{\mathbf{L}} b]_\theta.$

Questa struttura viene detta il quoziente di $\mathbf{L}$ modulo θ .

Lemma 2.24. Se $\mathbf{L}$ è un reticolo, anche $\mathbf{L}/\theta$ è un reticolo.

Dimostrazione. Mostriamo per prima cosa che le operazioni in $\mathbf{L}/\theta$ sono ben definite. Supponiamo che $a\theta a'$ e $b\theta b'$. Poiché θ è una congruenza, $(a \vee b)\theta(a' \vee b')$. Quindi $[a]_\theta \vee^{\mathbf{L}/\theta} [b]_\theta = [a \vee b]_\theta = [a' \vee b']_\theta = [a']_\theta \vee^{\mathbf{L}/\theta} [b']_\theta$. Lo stesso vale per il meet.

Per far vedere che gli assiomi di reticolo sono soddisfatti, esemplifichiamo con l'idempotenza del join. Abbiamo che $[a]_\theta \vee^{\mathbf{L}/\theta} [a]_\theta = [a \vee^{\mathbf{L}} a]_\theta = [a]_\theta$. In modo simile si controllano le altre identità.

□

Definition 2.25. Se h è un omomorfismo di reticoli da $\mathbf{L}$ a $\mathbf{M}$, definiamo

$$Ker(h) := \{\langle a, b \rangle \in L^2 : h(a) = h(b)\}.$$

$Ker(h)$ viene detto il nucleo di h .

Lemma 2.26. Se h è un omomorfismo di reticoli da $\mathbf{L}$ a $\mathbf{M}$, $Ker(h)$ è una congruenza su $\mathbf{L}$.

Dimostrazione. Innanzitutto, $Ker(h)$ è una relazione di equivalenza (esercizio).

Supponiamo adesso $[a]_{Ker(h)} = [b]_{Ker(h)}$ e $[c]_{Ker(h)} = [d]_{Ker(h)}$. Ciò significa che $h(a) = h(b)$ e $h(c) = h(d)$. Ne segue:

$$h(a \vee^{\mathbf{L}} c) = h(a) \vee^{\mathbf{M}} h(c) = h(b) \vee^{\mathbf{M}} h(d) = h(b \vee^{\mathbf{L}} d),$$

da cui $[a \vee^{\mathbf{L}} c]_{Ker(h)} = [b \vee^{\mathbf{L}} d]_{Ker(h)}$.

Analogamente si ragiona per il meet.

□

Theorem 2.27. *Sia $\mathbf{L}$ un reticolo. Allora l'algebra*

$$\mathbf{Con}(\mathbf{L}) := \langle \text{Con}(\mathbf{L}), \cap, \vee^{\mathbf{Con}(\mathbf{L})} \rangle$$

dove, per ogni $\theta, \psi \in \text{Con}(\mathbf{L})$, $\theta \vee^{\mathbf{Con}(\mathbf{L})} \psi = Cg^{\mathbf{L}}(\theta \cup \psi)$, è un reticolo completo.

2.5 Reticoli distributivi

Definition 2.28. *Un reticolo si dice distributivo se soddisfa l'identità*

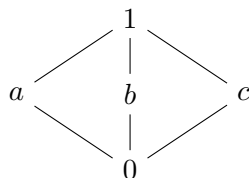
$$x \wedge (y \vee z) \approx (x \wedge y) \vee (x \wedge z)$$

o, equivalentemente,

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

Example 2.29.

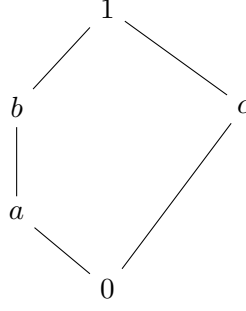
1. Ogni catena è distributiva. Infatti, se a, b sono elementi di una catena, uno dei due è il massimo di $\{a, b\}$ e uno è il minimo. Le operazioni di meet e join coincidono quindi con minimo e massimo, e le identità distributive risultano automaticamente soddisfatte.
2. Per ogni insieme X , il reticolo $\mathbf{Pw}(X)$ è distributivo. Infatti, si verifica agevolmente che $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ e $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ per tutti i sottoinsiemi A, B, C di X .
3. Sia $\mathbf{M}_3$ il reticolo specificato dal seguente diagramma di Hasse.



Tutti gli elementi a, b, c sono incomparabili tra loro. Per ogni coppia distinta di tali elementi si ha $a \vee b = a \vee c = b \vee c = 1$ e $a \wedge b = a \wedge c = b \wedge c = 0$.

$\mathbf{M}_3$ non è distributivo. Infatti $a \wedge (b \vee c) = a \wedge 1 = a$, mentre $(a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0$. Pertanto $a \wedge (b \vee c) \neq (a \wedge b) \vee (a \wedge c)$.

4. Sia $\mathbf{N}_5$ il reticolo specificato dal seguente diagramma di Hasse:



Si ha $0 < a < b < 1$ e $0 < c < 1$, mentre c è incomparabile con a e b .

Anche $\mathbf{N}_5$ non è distributivo. Infatti $b \wedge (a \vee c) = b \wedge 1 = b$, mentre $(b \wedge a) \vee (b \wedge c) = a \vee 0 = a$. Quindi $b \wedge (a \vee c) \neq (b \wedge a) \vee (b \wedge c)$.

I due esempi precedenti sono importanti in virtù del seguente teorema, che non dimostreremo:

Theorem 2.30. *Un reticolo è distributivo se e solo se non contiene sottoreticoli isomorfi a $\mathbf{M}_3$ oppure $\mathbf{N}_5$.*

3 Algebre di Boole

3.1 Definizione e proprietà elementari

Definition 3.1. *Un'algebra di Boole è un'algebra*

$$\mathbf{B} = \langle B, \wedge, \vee, \neg, 0, 1 \rangle$$

di tipo $\langle 2, 2, 1, 0, 0 \rangle$ tale che:

1. $\langle B, \wedge, \vee \rangle$ è un reticolo distributivo;
2. per ogni $a \in B$, $a \wedge 0 = 0$ e $a \wedge 1 = a$ (ossia, 0 e 1 sono rispettivamente il minimo e il massimo rispetto all'ordine $\leq^{\mathbf{B}}$ indotto da $\langle B, \wedge, \vee \rangle$);
3. per ogni $a \in B$, $a \vee \neg a = 1$ e $a \wedge \neg a = 0$.

Example 3.2. L'algebra delle “tavole di verità”

$$\mathbf{B}_2 = \langle \{0, 1\}, \wedge, \vee, \neg, 0, 1 \rangle$$

con le usuali operazioni, è un'algebra di Boole.

Example 3.3. Per ogni insieme X , l'algebra

$$\mathbf{Pw}(X) = \langle Pw(X), \cap, \cup, -, \emptyset, X \rangle$$

dove, per ogni $Y \subseteq X$, $-Y := \{a \in X : a \notin Y\}$, è un'algebra di Boole.

Lemma 3.4. *Sia $\mathbf{B}$ un'algebra di Boole. Per ogni $a, b \in B$ valgono le seguenti proprietà:*

1. *se $a \wedge b = 0$ e $a \vee b = 1$, allora $b = \neg a$;*
2. *$\neg(a \vee b) = \neg a \wedge \neg b$ e $\neg(a \wedge b) = \neg a \vee \neg b$;*
3. *$\neg\neg a = a$.*

Dimostrazione. (1) Supponiamo che $a \wedge b = 0$ e $a \vee b = 1$. Sappiamo anche che $b = b \wedge 1$ e quindi $b = b \wedge (a \vee \neg a)$. Distribuendo, $b = (b \wedge a) \vee (b \wedge \neg a)$. Ma poiché $b \wedge a = a \wedge b = 0$, segue $b = 0 \vee (b \wedge \neg a) = b \wedge \neg a$, ovvero $b \leq^{\mathbf{B}} \neg a$. Similmente, $\neg a \leq^{\mathbf{B}} b$. Quindi $\neg a = b$.

(2) Mostriamo la prima identità. Per (1), basta far vedere che $(a \vee b) \wedge (\neg a \wedge \neg b) = 0$ e $(a \vee b) \vee (\neg a \wedge \neg b) = 1$. Ma

$$\begin{aligned} (a \vee b) \wedge \neg a \wedge \neg b &= ((a \wedge \neg a) \vee (b \wedge \neg a)) \wedge \neg b \\ &= b \wedge \neg a \wedge \neg b \\ &= 0. \end{aligned}$$

Inoltre

$$\begin{aligned} a \vee b \vee (\neg a \wedge \neg b) &= a \vee ((b \vee \neg a) \wedge (b \vee \neg b)) \\ &= a \vee b \vee \neg a \\ &= 1. \end{aligned}$$

(3) Per (1) è sufficiente far vedere che $\neg a \wedge a = 0$ e $\neg a \vee a = 1$. Ma questa è una conseguenza della Definizione 3.1. $\square$

Theorem 3.5. *Sia $\mathbf{B}$ un'algebra di Boole. Per ogni $a, b \in B$, si ha che $a \leq^{\mathbf{B}} b$ sse $\neg a \vee b = 1$.*

Dimostrazione. Se $a \wedge b = a$, usando il Lemma 3.4.(2) e la Definizione 3.1 abbiamo che $\neg a \vee b = \neg(a \wedge b) \vee b = \neg a \vee \neg b \vee b = \neg a \vee 1 = 1$.

Viceversa, supponiamo $\neg a \vee b = 1$. Allora $a \wedge \neg b = \neg(\neg a \vee b) = 0$. Quindi $b = 0 \vee b = (a \wedge \neg b) \vee b = (a \vee b) \wedge (\neg b \vee b) = (a \vee b) \wedge 1 = a \vee b$. $\square$

Le nozioni di sottomalgebra, omomorfismo, congruenza e quoziente definite per i reticoli si lasciano adattare senza particolari difficoltà per le algebre di Boole (come per le altre algebre: si veda la dispensa dedicata all'algebra universale). Ad esempio, un omomorfismo di algebre di Boole sarà un omomorfismo dei rispettivi ridotti reticolari che preserva, oltre al meet e al join, anche la negazione (e anch'esso si dirà un isomorfismo se è biiettivo come funzione); una congruenza su un'algebra di Boole sarà una congruenza sul suo ridotto reticolare che è compatibile, oltre che col meet e col join, anche con la negazione, e così via.

3.2 Filtri e ultrafiltri

Definition 3.6. Sia $\mathbf{B}$ un'algebra di Boole. Un filtro di $\mathbf{B}$ è un filtro del suo ridotto reticolare. Un filtro si dice:

- proprio se $F \neq B$;
- massimale se è proprio e per ogni filtro G , $F \subset G$ implica $G = B$.

Lemma 3.7. Sia $\mathbf{B}$ un'algebra di Boole e sia F un filtro di $\mathbf{B}$.

1. F è proprio sse $0 \notin F$;
2. F è massimale sse F è un ultrafiltro, ovvero un filtro proprio tale che per ogni $a \in B$, o $a \in F$ oppure $\neg a \in F$.

Dimostrazione. (1) Dimostriamo entrambe le direzioni per contrapposizione. Se $0 \in F$, per chiusura verso l'alto segue che ogni elemento appartiene a F . Dunque $F = B$. Viceversa, se $F = B$, allora certamente $0 \in F$.

(2) Supponiamo che F sia massimale e che $a \notin F$. Consideriamo il filtro generato da $F \cup \{a\}$. Per la massimalità di F , esso coincide con tutto B e dunque contiene 0 . Per il Lemma 2.10 esiste $b \in F$ tale che $b \wedge a \leq 0$. Ma poiché 0 è il minimo di $\mathbf{B}$, anche $0 \leq b \wedge a$. Di conseguenza $b \wedge a = 0$ e quindi, per la dimostrazione del Lemma 3.4.(1), $b \leq \neg a$. Essendo F chiuso verso l'alto, $\neg a \in F$. Ossia, F è un ultrafiltro.

Viceversa, supponiamo che F sia un ultrafiltro. Quindi è proprio ed esiste $a \notin F$. Se consideriamo $F \cup \{a\}$ abbiamo che $a, \neg a \in F \cup \{a\}$ e quindi, poiché F è un filtro, $0 = a \wedge \neg a \in F \cup \{a\}$. Per (1), dunque, $F \cup \{a\} = B$ e F è massimale. □

L'insieme dei filtri massimali (o degli ultrafiltri, per il Lemma 3.7) di un'algebra di Boole $\mathbf{B}$ verrà denotato con $Ult(\mathbf{B})$.

Lemma 3.8. Sia $\mathbf{B}$ un'algebra di Boole e sia θ una congruenza su $\mathbf{B}$. La classe di congruenza $[1]_\theta$ è un filtro di $\mathbf{B}$.

Dimostrazione. Poiché $1 \in [1]_\theta$, tale classe è non vuota. Dobbiamo far vedere la chiusura verso l'alto. Supponiamo dunque $a \in [1]_\theta$ e $a \leq^{\mathbf{B}} b$. Allora $1\theta a = a \wedge b\theta 1 \wedge b = b$, da cui $b \in [1]_\theta$. Riguardo alla chiusura rispetto ai meet, se $a, b \in [1]_\theta$, allora $a\theta 1$ e $b\theta 1$, da cui $a \wedge b\theta 1 \wedge 1 = 1$. Di conseguenza $a \wedge b \in [1]_\theta$. □

Definition 3.9. Sia F un filtro di un'algebra di Boole $\mathbf{B}$. Definiamo

$$\theta_F := \{\langle a, b \rangle \in B^2 : (\neg a \vee b) \wedge (\neg b \vee a) \in F\}.$$

Lemma 3.10. θ_F è una congruenza di $\mathbf{B}$.

Dimostrazione. θ_F è riflessiva per la Definizione 3.1.(2)-(3) e simmetrica per definizione. Per quanto riguarda la transitività, se $\langle a, b \rangle, \langle b, c \rangle \in \theta_F$, per la chiusura rispetto ai meet si ha che

$$s := (\neg a \vee b) \wedge (\neg b \vee a) \wedge (\neg b \vee c) \wedge (\neg c \vee b) \in F.$$

Tuttavia, si può controllare che $(\neg a \vee b) \wedge (\neg b \vee c) \leq \neg a \vee c$ (esercizio). Similmente, $(\neg b \vee a) \wedge (\neg c \vee b) \leq \neg c \vee a$. Quindi $s \leq (\neg a \vee c) \wedge (\neg c \vee a)$ e, per la chiusura verso l'alto, quest'ultimo elemento appartiene a F . Ne segue che $\langle a, c \rangle \in \theta_F$.

Per quanto riguarda la compatibilità rispetto alle operazioni, limitiamoci a dimostrare che $a\theta_F b$ implica $\neg a\theta_F \neg b$. Per la Definizione 3.1.(1) e il Lemma 3.4.(3), se $(\neg a \vee b) \wedge (\neg b \vee a) \in F$, allora $(\neg \neg a \vee \neg b) \wedge (\neg \neg b \vee \neg a) \in F$, da cui la conclusione. $\square$

Theorem 3.11. *Sia $\mathbf{B}$ un'algebra di Boole. Le funzioni $f : \text{Con}(\mathbf{B}) \rightarrow F(\mathbf{B})$ e $g : F(\mathbf{B}) \rightarrow \text{Con}(\mathbf{B})$ definite da:*

$$f(\theta) = [1]_\theta; \quad g(F) = \theta_F$$

stabiliscono un isomorfismo di reticoli tra $\mathcal{F}(\mathbf{B})$ e $\mathbf{Con}(\mathbf{B})$.

Dimostrazione. Per i Lemmi 3.8 e 3.10, f e g sono ben definite. Rimane da verificare che $f(g(F)) = F$ e $g(f(\theta)) = \theta$ per ogni $F \in F(\mathbf{B})$ e per ogni $\theta \in \text{Con}(\mathbf{B})$. Tuttavia,

$$\begin{aligned} f(g(F)) &= [1]_{\theta_F} \\ &= \{a \in B : \langle a, 1 \rangle \in \theta_F\} \\ &= \{a \in B : (\neg a \vee 1) \wedge (\neg 1 \vee a) \in F\} \\ &= \{a \in B : a \in F\} \\ &= F. \end{aligned}$$

e

$$\begin{aligned} g(f(\theta)) &= \theta_{[1]_\theta} \\ &= \{\langle a, b \rangle \in B^2 : (\neg a \vee b) \wedge (\neg b \vee a) \in [1]_\theta\} \\ &= \{\langle a, b \rangle \in B^2 : \langle (\neg a \vee b) \wedge (\neg b \vee a), 1 \rangle \in \theta\} \\ &= \theta. \end{aligned}$$

L'ultima uguaglianza si giustifica come segue. Se $a\theta b$, allora applicando ripetutamente la compatibilità di θ con le operazioni,

$$(\neg a \vee b) \wedge (\neg b \vee a)\theta(\neg a \vee a) \wedge (\neg a \vee a) = 1.$$

Se viceversa

$$(\neg a \vee b) \wedge (\neg b \vee a)\theta 1,$$

allora per compatibilità

$$a \wedge b = a \wedge (\neg a \vee b) \wedge (\neg b \vee a)\theta a \wedge 1 = a$$

e similmente $a \wedge b\theta b$, da cui $a\theta b$. $\square$

3.3 Il teorema di rappresentazione di Stone

Uno dei risultati più profondi della teoria delle algebre di Boole è il teorema di Stone, che mostra come ogni algebra di Boole possa essere rappresentata come un'algebra di insiemi.

Sia $\mathbf{B}$ un'algebra di Boole. Consideriamo l'algebra $\mathbf{Pw}(Ult(\mathbf{B}))$. Per l'Esempio 3.3, si tratta di un'algebra di Boole. Definiamo adesso la seguente funzione da B a $Pw(Ult(\mathbf{B}))$:

$$\widehat{a} := \{U \in Ult(\mathbf{B}) : a \in U\}.$$

Lemma 3.12. *Per ogni $a, b \in B$ valgono:*

$$\widehat{a \vee b} = \widehat{a} \cup \widehat{b},$$

$$\widehat{a \wedge b} = \widehat{a} \cap \widehat{b},$$

$$\widehat{\neg a} = Ult(\mathbf{B}) - \widehat{a}.$$

Dimostrazione. Dimostriamo la terza identità. Sia U un ultrafiltro. Allora $U \in \widehat{\neg a}$ sse $\neg a \in U$. Poiché U è un ultrafiltro, questo equivale a $a \notin U$, ovvero a $U \in Ult(\mathbf{B}) - \widehat{a}$. Le altre identità si dimostrano analogamente. □

Theorem 3.13 (Stone). *Sia $\mathbf{B}$ un'algebra di Boole. $\mathbf{B}$ è isomorfa a una sottalgebra booleana di $\mathbf{Pw}(Ult(\mathbf{B}))$.*

Dimostrazione. (Abbozzo.) Si consideri l'insieme M degli ultrafiltri di $\mathbf{B}$ che hanno la forma $\widehat{a}$, per qualche $a \in A$. Per il Lemma 3.12, M è l'universo di una sottalgebra $\mathbf{M}$ di $\mathbf{Pw}(Ult(\mathbf{B}))$ che è a sua volta un'algebra di Boole. Inoltre, la funzione $s : B \rightarrow M$ definita da

$$s(a) = \widehat{a}$$

preserva tutte le operazioni in virtù del Lemma 3.12 ed è chiaramente suriettiva. Se $a \neq b$, assumiamo senza perdita di generalità che $a \not\leq b$. Allora $b \notin F(a)$. Per il Teorema dell'ultrafiltro (che qui non dimostreremo) esiste un ultrafiltro U di $\mathbf{B}$ che contiene $F(a)$ e tale che $b \notin U$. Quindi $s(a) \neq s(b)$ e dunque la funzione s è anche iniettiva. □