Definizione 1. Sia R un insieme dotato di due leggi di composizione interne $\wedge$ e $\vee$. Si dice che la struttura algebrica $(R, \wedge, \vee)$ è un *reticolo* (algebrico) se $\wedge$ e $\vee$ verificano le proprietà:

(1) $\forall x, y, z \in R, \quad (x \wedge y) \wedge z = x \wedge (y \wedge z); \quad (x \vee y) \vee z = x \vee (y \vee z)$ associativa
(2) $\forall x, y \in R, \quad x \wedge y = y \wedge x; \quad x \vee y = y \vee x$ commutativa
(3) $\forall x, y \in R, \quad x \vee (x \wedge y) = x; \quad x \wedge (x \vee y) = x$ assorbimento.

Osservazione 1. In un reticolo vale il *principio di dualità*, ovvero se si dimostra un teorema, vale lo stesso teorema scambiando tra loro le operazioni $\vee$ e $\wedge$. Questo perchè le proprietà associativa e commutativa valgono per entrambe le leggi di composizione interne e nella proprietà di assorbimento le due leggi sono intercambiabili.

Esempio 1. Un classico esempio di reticolo è fornito dall'insieme delle parti di un assegnato insieme X sul quale si considerino le leggi di composizione interne $\cap$ e $\cup$. Quindi $(\mathscr{P}(X), \cap, \cup)$ è un reticolo, come facilmente si può verificare.

Esempio 2. Si può provare che l'insieme $\mathbb{N}^*$ con le leggi di composizione interne $\wedge = M.C.D.$, $\vee = m.c.m.$ è un reticolo.

Esempio 3. Per ogni $n \in \mathbb{N}$, $n \geq 2$, anche la struttura $(D_n, \wedge, \vee)$, dove D_n è l'insieme dei divisori di n, $\wedge = M.C.D.$, $\vee = m.c.m.$, è un reticolo.

Definizione 2. Sia $(R, \wedge, \vee)$ un reticolo. Un sottoinsieme R' di R si dice sottoreticolo se è chiuso rispetto alle operazioni $\wedge$ e $\vee$, ovvero se

$$\forall x, y \in R' \quad x \wedge y \in R', \quad x \vee y \in R'.$$

Osservazione 2. Se R' è un sottoreticolo di $(R, \wedge, \vee)$, allora diventa a sua volta reticolo con le operazioni indotte.

Osservazione 3. Si può provare che D_n è chiuso rispetto alle due leggi $\wedge$ e $\vee$ del reticolo $(\mathbb{N}^*, \wedge, \vee)$ dell'esempio 2. Quindi $(D_n, \wedge, \vee)$ è un sottoreticolo di $(\mathbb{N}^*, \wedge, \vee)$.

Definizione 3. Un reticolo $(R, \wedge, \vee)$ si dice *distributivo* se

$$\forall x, y, z \in R \quad (x \wedge y) \vee z = (x \vee z) \wedge (y \vee z); \quad (x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z).$$

Notazione 1. Sia $(R, \wedge, \vee)$ un reticolo. Se esiste l'elemento neutro rispetto a $\wedge$, esso si indica con $\widehat{1}$; se esiste l'elemento neutro rispetto a $\vee$, si indica con $\widehat{0}$. Quindi, nel caso esistano $\widehat{0}$ e $\widehat{1}$, si ha:

$$\forall x \in R \quad x \wedge \widehat{1} = x; \quad x \vee \widehat{0} = x.$$

Esempio 4. Nell'esempio 1, si ha: $\widehat{0} = \emptyset$, $\widehat{1} = X$.

Definizione 4. Siano $(R, \wedge, \vee)$ un reticolo dotato di $\widehat{0}$ e $\widehat{1}$, $a \in R$. Si dice che a è *complementato* se esiste un elemento a' tale che:

$$a \vee a' = \widehat{1}, \quad a \wedge a' = \widehat{0};$$

in tal caso si dice che a' è un *complemento* di a.

Esempio 5. Nel caso dell'esempio 1, per ogni $A \in \mathscr{P}(X)$ esiste il complemento di A, $A' = \complement_X A$. Infatti $A \cap \complement_X A = X = \widehat{1}$, $A \cup \complement_X A = \emptyset = \widehat{0}$.

Proposizione 1. *Sia $(R, \wedge, \vee)$ un reticolo distributivo dotato di $\widehat{0}$ e $\widehat{1}$, $a \in R$. Allora, se a ammette complemento, esso è unico*

Dimostrazione. Siano a' e a'' complementi di a. Allora si ha:

$$\begin{aligned} a'' &= a'' \vee \widehat{0} = a'' \vee (a' \wedge a) = (a'' \vee a') \wedge (a'' \vee a) = (a'' \vee a') \wedge \widehat{1} \\ &= (a'' \vee a') \wedge (a \vee a') = (a'' \wedge a) \vee a' = \widehat{0} \vee a' = a' \end{aligned}$$

In seguito si vedranno esempi di reticoli che non sono distributivi contenenti elementi che ammettono più di un complemento.

Definizione 5. Si dice che un reticolo $(R, \wedge, \vee)$ è *di Boole* se

B$_1$) è distributivo
B$_2$) ammette $\widehat{0}$ e $\widehat{1}$
B$_3$) ogni elemento è complementato.

Esempio 6. Sia X un insieme. Allora il reticolo $(\mathscr{P}(X), \cap, \cup)$ è di Boole: infatti valgono le proprietà distributive e, come si è già osservato, esistono $\widehat{0} = \emptyset$, $\widehat{1} = X$ e ogni elemento A di $\mathscr{P}(X)$ ha complemento che è $\complement_X A$.

Esempio 7. Il reticolo $(\mathbb{N}^*, \wedge, \vee)$ dell'esempio 2 non è un reticolo di Boole, perchè pur ammettendo $\widehat{0} = 1$, non ammette $\widehat{1}$.

Esempio 8. In generale, il reticolo $(D_n, \wedge, \vee)$ dell'esempio dei divisori di un intero $n \geq 2$ (cf. esempio 3) non è di Boole. Si può dimostrare che lo è se e soltanto se n è prodotto di numeri primi distinti.

Definizione 6. Un insieme ordinato $(R, \leq)$ si dice *reticolo* (ordinato) se ogni coppia di elementi di R ammette estremo superiore ed estremo inferiore. In altri termini

$$\forall x, y \in R \;\; \exists \sup(x, y), \quad \inf(x, y).$$

Esempio 9. L'insieme $(\mathbb{N}^*, |\,)$ è un reticolo ordinato, in quanto, com'è facile osservare, per ogni $a, b \in \mathbb{N}^*$ si ha, rispetto a "$|$"

$$\inf(a, b) = M.C.D.(a, b), \quad \sup(a, b) = m.c.m.(a, b).$$

Esempio 10. Per ogni intero $n \geq 2$, l'insieme dei divisori di n ordinato per divisibilità $(D_n, |\,)$ è un sottoinsieme ordinato di $(\mathbb{N}^*, |\,)$ e, come si è già osservato, $\forall a, b \in D_n$, $M.C.D.(a, b) \in D_n$ e $m.c.m.(a, b) \in D_n$, per cui anche $(D_n, |\,)$ è un reticolo ordinato.

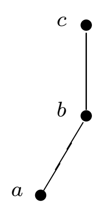
Esempio 11. Sia X un insieme. Allora l'insieme $\mathscr{P}(X)$ delle parti di X, ordinato per inclusione, ovvero $(\mathscr{P}(X), \subseteq)$, è un reticolo ordinato in quanto

$$\forall A, B \in \mathscr{P}(X) \quad \inf(A, B) = A \cap B, \quad \sup(A, B) = A \cup B.$$

Esempio 12. Sia $(G, \cdot)$ un gruppo, H, K ne siano sottogruppi. È noto che $H \cap K$ è un sottogruppo di G, ma $H \cup K$ non lo è, in generale. Si considera allora il più piccolo sottogruppo (per inclusione) $\widehat{H \cup K}$ che contiene $H \cup K$. Si può verificare che la struttura $(\mathcal{H}(G), \subseteq)$, dove $\mathcal{H}(G)$ è l'insieme dei sottogruppi di G è un reticolo ordinato poichè

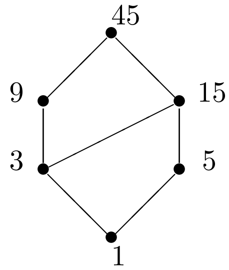
$$\forall H, K \in \mathcal{H}(G) \;\; \inf(H, K) = H \cap K, \quad \sup(H, K) = \widehat{H \cup K}.$$

Osservazione 4. Un insieme $(A, \leq)$ ordinato finito può essere rappresentato mediante un *diagramma di Hasse*. Se $a, b, c \in A$, se $a \leq b$ e se non ci sono elementi intermedi, basta collegare a con b mediante un segmento ascendente. Poichè vale la proprietà transitiva, se $a \leq b$ e $b \leq c$, a sarà collegato con b mediante un segmento ascendente, b sarà collegato con c mediante un altro segmento ascendente, e a sarà collegato con c mediante una spezzata ascendente:

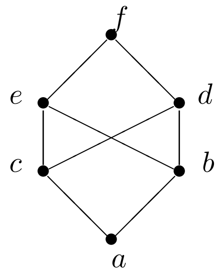


In particolare questo può essere fatto per un reticolo.

Esempio 13. Il diagramma di Hasse del reticolo $(D_{45}, \mid)$ dei divisori di 45 ordinato per divisibilità è:

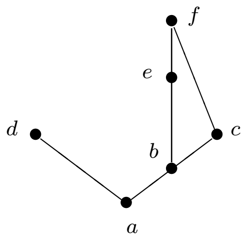


Esempio 14. L'insieme ordinato rappresentato dal seguente diagramma di Hasse



non è un reticolo, poichè la coppia $\{e, d\}$ ha come insieme dei minoranti $X = \{a, b, c\}$ che non presenta massimo.

Esercizio 1. Stabilire perchè l'insieme ordinato rappresentato dal seguente diagramma:



non è un reticolo.

Lemma 1. Sia $(R, \wedge, \vee)$ un reticolo. Allora si ha

$$\forall x, y \in R, \quad (x \wedge y = x) \ \Leftrightarrow \ (x \vee y = y).$$

Dimostrazione. Siano $x, y \in R$, tali che $x \wedge y = x$, allora, per l'assorbimento,

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

Viceversa, se $x \vee y = y$, allora, in modo analogo

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

Teorema 1. *Sia $(R, \wedge, \vee)$ un reticolo (algebrico). Se $\forall x, y \in R$ si pone*

$$x \leq y \Longleftrightarrow x \wedge y = x \overset{Lemma1}{\Longleftrightarrow} x \vee y = y,$$

allora " $\leq$ " è una relazione di ordine rispetto alla quale R risulta essere un reticolo (ordinato).

Vale anche il teorema inverso

Teorema 2. *Sia* $(R, \leq)$ *un reticolo (ordinato). Se* $\forall x, y \in R$ *si pone*

$$x \wedge y = \inf(x, y), \quad x \vee y = \sup(x, y)$$

allora $(R, \wedge, \vee)$ *è un reticolo (algebrico).*

In virtù del Teorema 2, si hanno i seguenti esempi:

Esempio 15. I reticoli (ordinati) $(\mathbb{N}^*, |\,)$ e $(D_n, |\,)$ diventano reticoli (algebrici) ponendo

$$\forall a, b \;\; a \wedge b = M.C.D.(a, b) \quad a \vee b = m.c.m.(a, b).$$

Esempio 16. Sia X un insieme. Allora il reticolo (ordinato) $\mathscr{P}(X)$ diventa reticolo (algebrico) ponendo

$$\forall A, B \in \mathscr{P}(X) \quad A \wedge B = A \cap B \quad A \vee B = A \cup B.$$

Esempio 17. Sia $(G, \cdot)$ un gruppo. Allora il reticolo (ordinato) $(\mathcal{H}(G), \subseteq)$ dei sottogruppi di $(G, \cdot)$ ordinato per inclusione diventa reticolo (algebrico) ponendo

$$\forall H, K \in \mathcal{H}(G) \;\; H \wedge K = H \cap K, \quad H \vee K = \widehat{H \cup K}.$$

Esercizio 2. Usando il Teorema 1, fare il procedimento inverso nei tre esempi precedenti.

Osservazione 5. Sia $(R, \leq)$ un reticolo ordinato. Se il reticolo algebrico associato ammette $\widehat{0}$, questo è il più piccolo elemento di R rispetto a $\leq$. Infatti, per il Teorema 9,

$$\forall x \in R \;\; x = x \vee \widehat{0} \;\Leftrightarrow\; \widehat{0} \leq x.$$

Analogamente, Se il reticolo algebrico associato ammette $\widehat{1}$, questo è il più grande elemento di R rispetto a $\leq$.

Osservazione 6. Sia $(R, \leq)$ un reticolo ordinato. Se il reticolo algebrico associato ammette $\widehat{0}$, allora si ha:

$$\forall x \in R, \quad x \vee \widehat{0} = x \overset{Lemma 1}{\Longleftrightarrow} x \wedge \widehat{0} = \widehat{0}.$$

Se il reticolo algebrico associato ammette $\widehat{1}$, allora

$$\forall x \in R, \quad x \wedge \widehat{1} = x \overset{Lemma 1}{\Longleftrightarrow} x \vee \widehat{1} = \widehat{1}.$$

Osservazione 7. Si dimostra che ogni reticolo finito ha necessariamente $\widehat{0}$ e $\widehat{1}$.

Proposizione 2. *Sia* $(R, \wedge, \vee)$ *un reticolo di Boole. Allora* $\forall a, b \in R$ *risulta*

$$(a \vee b)' = a' \wedge b'; \quad (a \wedge b)' = a' \vee b' \quad \text{Leggi di De Morgan.}$$

Dimostrazione. Bisogna provare che $\forall a, b \in R$

$$(a \vee b) \wedge (a' \wedge b') = \widehat{0}; \quad (a \vee b) \vee (a' \wedge b') = \widehat{1}$$

$$(a \wedge b) \wedge (a' \vee b') = \widehat{0}; \quad (a \wedge b) \vee (a' \vee b') = \widehat{1}.$$

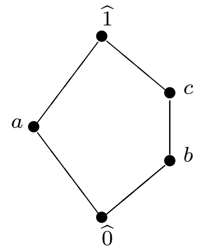
Si prova solamente la prima delle quattro: la seconda si verifica in maniera analoga, le altre due seguono per il principio di dualità.

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

Osservazione 8. Dato un reticolo algebrico, si può considerare il reticolo ordinato ad esso canonicamente associato e viceversa. Pertanto da ora in avanti si parlerà indifferentemente di struttura algebrica o ordinata di un assegnato reticolo.

Definizione 7. Si dice *pentagonale*, e si indica con N_5, un reticolo ordinato $R = \{\widehat{0}, a, b, c, \widehat{1}\}$ con la condizione che $b \leq c$.

Il diagramma di Hasse di N_5 è:



Si osserva che a ha due complementi che sono b e c. Pertanto non è detto che il reticolo sia distributivo (cf. Proposizione 4). Poiché risulta

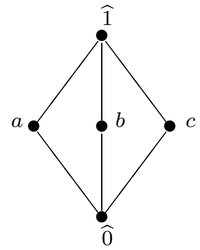
$$b \vee (a \wedge c) = b \vee \widehat{1} = \widehat{1}$$

$$(b \vee a) \wedge (b \vee c) = \widehat{1} \wedge c = c$$

il reticolo non è distributivo.

Definizione 8. Si dice *trirettangolo*, e si indica con M_3, un reticolo ordinato isomorfo al seguente: $R = \{\widehat{0}, a, b, c, \widehat{1}\}$, senza ulteriori condizioni.

Il diagramma di Hasse del reticolo trirettangolo è il seguente:



Si osservi che a ha due complementi, ovvero b e c; b ha due complementi, ovvero a e c; c ha due complementi, ovvero a e d. Quindi, come nel caso di N_5 non è detto si tratti di un reticolo distributivo: e infatti si ha:

$$a \wedge (b \vee c) = a \wedge \widehat{1} = a$$

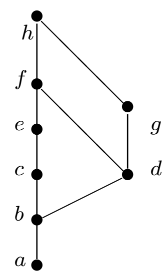
$$(a \wedge b) \vee (a \wedge c) = \widehat{0} \vee \widehat{0} = \widehat{0}.$$

Se si deve provare che un reticolo finito è distributivo e non lo si può fare con tre generici suoi elementi, non è consigliabile verificare tutti i possibili casi. Infatti si ricorre al seguente criterio.

Teorema 3. *Un reticolo finito $(R, \wedge, \vee)$ è distributivo se e soltanto se non ammette sottoreticoli isomorfi a N_5 o a M_3.*

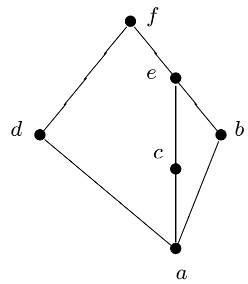
Osservazione 9. Per vedere se un tale sottoreticolo esiste, si utilizzano i diagrammi di Hasse, come nei seguenti esempi.

Esempio 18. Il reticolo rappresentato dal seguente diagramma di Hasse, non è distributivo:



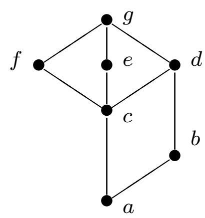
Infatti $\{b, d, c, e, f\}$ formano un sottoreticolo isomorfo a N_5.

Esempio 19. Analogo discorso vale per il reticolo individuato dal diagramma di Hasse:



poichè $\{a, c, d, e, f\}$ formano un sottoreticolo isomorfo a N_5.

Esempio 20. Il reticolo il cui diagramma di Hasse è:



non è distributivo, in quanto $\{c, d, e, f, g\}$ è un sottoreticolo isomorfo a M_3.

Esercizio 3. Nell'esempio precedente $\{a, b, c, f, g\}$ non forma un sottoreticolo: perchè?

Definizione 9. Si dice che un anello $(A, +, \cdot)$ è *di Boole* se

$$\forall a \in A \quad a^2 = a$$

Proposizione 3. *Sia* $(A, +, \cdot)$ *un anello di Boole. Allora*

$$\forall a \in A \quad a + a = 0$$

Dimostrazione Sia $a \in A$, allora

$$a + a = (a + a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a.$$

Per le leggi di cancellazione $a + a = 0$.

Esempio 21. $(\mathbb{Z}_2, +, \cdot)$ è anello di Boole.

Osservazione 10. Siano $(A_1, +, \cdot), \ldots, (A_n, +, \cdot)$ anelli e sia

$$A = A_1 \times \cdots \times A_n.$$

Si può munire A della struttura di anello ponendo

$$\forall (a_1, \ldots, a_n), (b_1, \ldots, b_n) \in A$$

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$$
$$(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (a_1 \cdot b_1, \dots, a_n \cdot b_n).$$

In particolare, se $(B, +, \cdot)$ è un anello, si può considerare l'anello $(B^n, +, \cdot)$, dove $B^n = B \times \dots \times B$. È facile osservare che se $(B, +, \cdot)$ è un anello di Boole, allora anche $(B^n, +, \cdot)$ è di Boole. Quindi per ogni $n \in \mathbb{N}^*$, $(\mathbb{Z}_2^n, +, \cdot)$ è un anello di Boole.

Teorema 4. *Sia $(A, +, \cdot)$ un anello di Boole. Posto*

$$\forall a, b \in A \quad a \wedge b = a \cdot b, \quad a \vee b = a + b + a \cdot b,$$

si ha che $(A, \wedge, \vee)$ è un reticolo di Boole. Viceversa se $(R, \wedge, \vee)$ è un reticolo di Boole, allora le due leggi di composizione "+" e "·" così definite

$$\forall x, y \in R \quad x + y = (x \wedge y') \vee (x' \wedge y) \quad x \cdot y = x \wedge y$$

conferiscono a R la struttura di anello di Boole.

Esempio 22. Dato X insieme, $(\mathscr{P}(X), \cap, \cup)$ è un reticolo di Boole. Allora si pone per ogni $A, B \in \mathscr{P}(X)$

$$A + B = (A \cap \complement_X(B)) \cup (\complement_X(A) \cap B) = (A \setminus B) \cup (B \setminus A) = A \Delta B$$

che si chiama anche *differenza simmetrica* di A e B,

$$A \cdot B = A \cap B.$$

Quindi $(\mathscr{P}(X), \Delta, \cdot)$ è un anello di Boole.

Definizione 10. Si dice che due anelli $(A_1, +, \cdot)$ e $(B, +. \cdot)$ sono *isomorfi* se esiste un'applicazione bigettiva $f : A \to B$ tale che:

- $\forall a, a' \in A \quad f(a + a') = f(a) + f(a')$
- $\forall a, a' \in A \quad f(a \cdot a') = f(a) \cdot f(a')$
- $f(1_A) = 1_B$.

In tal caso f si dice *isomorfismo di anelli.*

Osservazione 11. Si può provare che per un isomorfismo di anelli $f(0_A) = 0_B$.

Teorema 5. *Sia $(A, +, \cdot)$ anello di Boole finito. Allora esiste $n \in \mathbb{N}^*$ tale che $(A, +, \cdot)$ sia isomorfo all'anello di Boole $(\mathbb{Z}_2^n, +, \cdot)$.*

Osservazione 12. Ogni anello di Boole finito ha cardinalità che è una potenza di 2. Quindi se un anello ha cardinalità diversa da una potenza di 2, sicuramente non è di Boole. Inoltre, dal Teorema 4 si sa che ogni reticolo di Boole si può riguardare come un anello di Boole e dunque un reticolo di Boole finito ha cardinalità una potenza di 2. Pertanto se un reticolo non ha come cardinalità una potenza di 2 non è di Boole, ma non è vero che se un reticolo ha cardinalità una potenza di 2 allora è un reticolo di Boole!