1. Sia X un insieme e sia $\mathcal{P}(X)$ l'insieme delle parti di X. Indichiamo con $\cap$ e $\cup$ le operazioni di intersezione e di unione fra sottoinsiemi di X.
   (a) Dimostrare che $(\mathcal{P}(X), \cap, \cup)$ è un reticolo (verificare che soddisfa gli assiomi);
   (b) Verificare che la relazione di ordine parziale definita a partire dalle operazioni di reticolo

$$A\text{“}\leq\text{”}B \ \text{ se } \ A \cap B = A \qquad (\Leftrightarrow \quad A \cup B = B)$$

   è la relazione di contenenza: $A\text{“}\leq\text{”}B$ se $A \subset B$.

Sol. (a) Dobbiamo verificare i seguenti fatti:

• le operazioni $\cup$ e $\cap$ sono commutative: per ogni $A, B \in \mathcal{P}(X)$ (ossia per ogni A, B sottoinsiemi di X)

$$A \cup B = B \cup A, \qquad A \cap B = B \cap A;$$

• le operazioni $\cup$ e $\cap$ sono associative: per ogni $A, B, C \in \mathcal{P}(X)$ (ossia per ogni A, B, C sottoinsiemi di X)

$$(A \cup B) \cup C = A \cup (B \cup C), \qquad (A \cap B) \cap C = A \cap (B \cap C);$$

• le operazioni $\cup$ e $\cap$ hanno la proprietà dell'assorbimento: $A, B \in \mathcal{P}(X)$

$$A \cap (A \cup B) = A, \qquad A \cup (A \cap B) = A.$$

La verifica di questi fatti è un esercizio di teoria elementare degli insiemi.....(usare le definizioni di unione e intersezione fra insiemi).

(b) Dobbiamo verificare che $\quad A \cap B = A \quad \Leftrightarrow \quad A \subset B$.
Supponiamo che $A \subset B$: per definizione $a \in A \Rightarrow a \in B$. Ne segue che $a \in A \Rightarrow a \in A \cap B$, ossia $A \subseteq A \cap B$. D'altra parte vale sempre l'inclusione $A \cap B \subset A$. In conclusione: $A \subset B \Rightarrow A \cap B = A$.
Viceversa, supponiamo che $A \cap B = A$. In particolare $A \subset A \cap B$ e, per definizione di intersezione, $A \subset B$. In conclusione: $A \cap B = A \Rightarrow A \subset B$.

Analogamente, avremmo ottenuto la stessa relazione d'ordine parziale $A\text{“}\leq\text{”}B$ se $A \subset B$ a partire da

$$A\text{“}\leq\text{”}B \ \text{ se } \ A \cup B = B.$$

2. Sia X un insieme e sia $(\mathcal{P}(X), \subset)$ l'insieme delle parti di X, con la relazione di ordine parziale data dalla relazione di *contenenza*.
   (a) Verificare che per ogni coppia A,B esistono $Z, W \in \mathcal{P}(X)$ tali che

$$\begin{cases} Z \subset A \\ Z \subset B \end{cases}, \qquad \begin{cases} A \subset W \\ B \subset W \end{cases}.$$

   (b) Verificare che le operazioni su $(\mathcal{P}(X), \subset)$ definite da

$$A \wedge B := inf\{A, B\}, \qquad A \vee B := sup\{A, B\}$$

   coincidono rispettivamente con le operazioni di intersezione $\cap$ e di unione $\cup$.

Sol: (a) Dati A e B sottoinsiemi arbitrari di X, si ha che il sottoinsieme $Z = A \cap B$ soddisfa $\begin{cases} Z \subset A \\ Z \subset B \end{cases}$, mentre il sottoinsieme $W = A \cup B$ soddisfa $\begin{cases} A \subset W \\ B \subset W \end{cases}$.

(b) Dobbiamo verificare che, rispetto alla relazione di ordine parziale $U \subset V$, l'intersezione fra sottoinsiemi coincide con l'inf, ossia $A \cap B = inf\{A, B\}$ e l'unione fra sottoinsiemi coincide col sup, ossia $A \cup B = sup\{A, B\}$.

• $A \cap B = inf\{A, B\}$: per definizione $inf\{A, B\}$ è il massimo dei minoranti di $\{A, B\}$. L'insieme dei minoranti di $\{A, B\}$ è formato dai sottoinsiemi di X che sono minori sia di A che di B, rispetto alla relazione di contenenza:

$$min\{A, B\} = \{Z \in \mathcal{P}(X) \mid \begin{cases} Z \subset A \\ Z \subset B \end{cases}\}.$$

Poiché $A \cap B$ è contenuto sia in A che in B, è chiaro che $A \cap B \in min\{A, B\}$. Supponiamo per assurdo che $A \cap B$ non sia il massimo fra i minoranti di $\{A, B\}$. Allora esiste Z tale che

$$\begin{cases} A \cap B \subset Z \subset A \\ A \cap B \subset Z \subset B \end{cases}. \qquad (*)$$

Dalle inclusioni (*) segue che $Z \subset A \cap B$. Contraddizione. Dunque $Z = A \cap B$, come richiesto .

• $A \cup B = sup\{A, B\}$: per definizione $sup\{A, B\}$ è il minimo dei maggioranti di $\{A, B\}$. L'insieme dei maggioranti di $\{A, B\}$ è formato dai sottoinsiemi di X che sono maggiori sia di A che di B, rispetto alla relazione di contenenza:

$$magg\{A, B\} = \{W \in \mathcal{P}(X) \mid \begin{cases} A \subset W \\ B \subset W \end{cases}\}.$$

Poiché $A \cup B$ è contiene sia A che B, è chiaro che $A \cup B \in magg\{A, B\}$. Supponiamo per assurdo che $A \cup B$ non sia il minimo fra i maggioranti di $\{A, B\}$. Allora esiste W tale che

$$\begin{cases} A \subset W \subset A \cup B \\ B \subset W \subset A \cup B \end{cases}. \qquad (**)$$

Dalle inclusioni (**) segue che $A \cup B \subset W$. Contraddizione. Dunque $W = A \cup B$, come richiesto.

3. Sia $\mathbf{N}$ l'insieme dei numeri naturali. Indichiamo con *mcd* e *mcm* le operazioni di *massimo comun divisore* e *minimo comune multiplo* fra numeri naturali.
   (a) Dimostrare che $(\mathbf{N}, \mathrm{mcd}, \mathrm{mcm})$ è un reticolo (verificare che soddisfa gli assiomi);
   (b) Verificare che la relazione di ordine parziale definita a partire dalle operazioni di reticolo

$$m\text{“} \leq \text{”}n \ \text{ se } \ mcd(m, n) = m \qquad (\Leftrightarrow \quad mcm(m, n) = n)$$

   è la relazione di *divisibilità*: $m\text{“} \leq \text{”}n$ se $m \mid n$.

Sol. (a) Dobbiamo verificare i seguenti fatti:

• le operazioni mcd e mcm sono commutative:

$$\mathrm{mcd}(m, n) = \mathrm{mcd}(n, m), \qquad \mathrm{mcm}(m, n) = \mathrm{mcm}(n, m);$$

la verifica di questi fatti è immediata.

• le operazioni mcd e mcm sono associative:

$$\mathrm{mcd}(m, \mathrm{mcd}(n, l)) = \mathrm{mcd}(\mathrm{mcd}(m, n), l), \qquad \mathrm{mcm}(m, \mathrm{mcm}(n, l)) = \mathrm{mcm}(\mathrm{mcm}(m, n), l);$$

la verifica di questi fatti è immediata (usare le definizioni).

• le operazioni mcd e mcm hanno la proprietà dell'assorbimento:

$$\mathrm{mcd}(m, \mathrm{mcm}(m, l)) = m, \qquad \mathrm{mcm}(m, \mathrm{mcd}(m, l)) = m.$$

Siano

$$m = p_1^{a_1} \dots p_k^{a_k}, \qquad l = p_1^{b_1} \dots p_k^{b_k}$$

le decomposizioni di m ed l in fattori primi, dove gli esponenti a_i e b_j sono interi maggiori o uguali a zero.
Dimostriamo che $\mathrm{mcd}(m, \mathrm{mcm}(m, l)) = m$: abbiamo

$$\mathrm{mcm}(m, l) = p_1^{max(a_1,b_1)} \dots p_k^{max(a_k,b_k)}$$

e

$$\mathrm{mcd}(m, \mathrm{mcm}(m, l)) = \mathrm{mcd}(m, p_1^{max(a_1,b_1)} \dots p_k^{max(a_k,b_k)}) =$$
$$= p_1^{min(a_1,max(a_1,b_1))} \dots p_k^{min(a_k,max(a_k,b_k))} = p_1^{a_1} \dots p_k^{a_k} = m.$$

Dimostriamo che $\mathrm{mcm}(m, \mathrm{mcd}(m, l)) = m$: abbiamo

$$\mathrm{mcd}(m, l) = p_1^{min(a_1,b_1)} \dots p_k^{min(a_k,b_k)}$$

e

$$\mathrm{mcm}(m, \mathrm{mcd}(m, l)) = \mathrm{mcm}(m, p_1^{min(a_1,b_1)} \dots p_k^{min(a_k,b_k)}) =$$
$$= p_1^{max(a_1,min(a_1,b_1))} \dots p_k^{max(a_k,min(a_k,b_k))} = p_1^{a_1} \dots p_k^{a_k} = m.$$

(b) Dobbiamo verificare che $\quad \mathrm{mcd}(m, n) = m \quad \Leftrightarrow \quad m \mid n.$
Per definizione, $\mathrm{mcd}(m, n) = m \Rightarrow m \mid n$.
Viceversa, supponiamo che $m \mid n$. Poiché $m \mid m$, si ha che m è un divisore comune di m ed n, in particolare $m \leq \mathrm{mcd}(m, n)$. D'altra parte $\mathrm{mcd}(m, n) \leq m$, da cui $\mathrm{mcd}(m, n) = m$. In conclusione, vale anche l'implicazione opposta $m \mid n \Rightarrow \mathrm{mcd}(m, n)$, come richiesto.
Analogamente si può dimostrare che $\quad \mathrm{mcm}(m, n) = n \quad \Leftrightarrow \quad m \mid n.$

4. Sia $(\mathbf{N}, \mid)$ l'insieme dei numeri naturali con la relazione di ordine parziale data dalla divisibilità.
   (a) Verficare che per ogni coppia $m, n \in \mathbf{N}$ esistono $z, w \in \mathbf{N}$ tali che

$$\begin{cases} z \mid m \\ z \mid n, \end{cases} \qquad \begin{cases} m \mid w \\ n \mid w. \end{cases}$$

   (b) Verificare che le operazioni su $(\mathbf{N}, \mid)$ definite da

$$A \wedge B := inf\{A, B\}, \qquad A \vee B := sup\{A, B\}$$

   coincidono rispettivamente con le operazioni di intersezione *mcd* e di unione *mcm*.

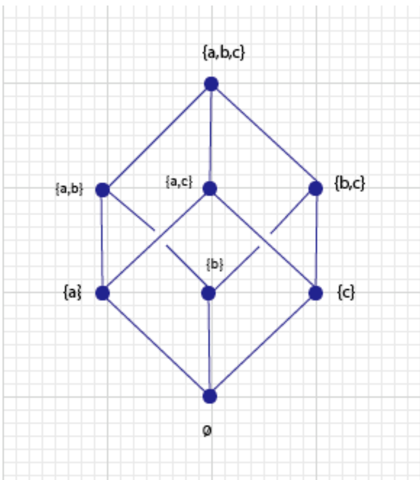
Sol. (a) Dati numeri naturali $m, n \in \mathbf{N}$ si ha che $z = \mathrm{mcd}(m, n)$ soddisfa $\begin{cases} z \mid m \\ z \mid n \end{cases}$, mentre $w = \mathrm{mcm}(m, n)$ soddisfa $\begin{cases} m \mid w \\ n \mid w \end{cases}$.

(b) Dobbiamo verificare che rispetto alla relazione di ordine parziale $x \mid y$, il massimo comun divisore coincide con l'inf, ossia $\text{mcd}(m,n) = inf\{m,n\}$, e il minimo comune multiplo con il sup, ossia $\text{mcm}(m,n) = sup\{m,n\}$.
• $\text{mcd}(m,n) = inf\{m,n\}$: l'insieme dei minoranti di $\{m,n\}$ è costituito dai divisori comuni di m ed n. In particolare $\text{mcd}(m,n)$ appartiene a tale insieme. Supponiamo per assurdo che $\text{mcd}(m,n)$ non sia il massimo dei minoranti di $\{m,n\}$: allora esiste $d \in \mathbf{N}$ tale che $\begin{cases} \text{mcd}(m,n) \mid d \mid m \\ \text{mcd}(m,n) \mid d \mid n \end{cases}$.
Ma ciò contraddice la definizione di massimo comun divisore.
• $\text{mcm}(m,n) = sup\{m,n\}$: l'insieme dei maggioranti di $\{m,n\}$ è costituito dai multipli comuni di m ed n. In particolare $\text{mcm}(m,n)$ appartiene a tale insieme. Supponiamo per assurdo che $\text{mcm}(m,n)$ non sia il minimo dei maggioranti di $\{m,n\}$: allora esiste $M \in \mathbf{N}$ tale che $\begin{cases} m \mid M \mid \text{mcm}(m,n) \\ n \mid M \mid \text{mcm}(m,n \end{cases}$.
Ma ciò contraddice la definizione di minimo comune multiplo.

5. Sia X un insieme e sia $Y \subset X$ un sottoinsieme.
   (a) Verificare che $\mathcal{P}(Y)$ è un sottoreticolo di $(\mathcal{P}(X), \cap, \cup)$, ossia è chiuso rispetto alle operazioni di intersezione e di unione.
   (b) Disegnare il diagramma di Hasse di $\mathcal{P}(\{a,b,c\})$ ed evidenziare il sottoreticolo $\mathcal{P}(\{a,b\})$.

Sol. (a) Siano $A, B \in \mathcal{P}(Y)$, ossia due sottoinsiemi di $Y \subset X$: poiché $A \subset Y$ e $B \subset Y$ abbiamo che $A \cap B \subset Y$ (basta osservare ad esempio che $A \cap B \subset A \subset Y$); inoltre $A \cup B \subset Y$ (basta osservare che $A \cup B \subset Y \cup Y = Y$). Dunque $\mathcal{P}(Y)$ è chiuso rispetto alle operazioni di intersezione e di unione.
(b)

$$\mathcal{P}(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\} \subset \mathcal{P}(\{a,b,c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}.$$



Il reticolo $\mathcal{P}(\{a,b,c\})$.

6. Sia $n \in \mathbf{N}$ un numero naturale fissato e sia D_n l'insieme dei divisori di n

$$D_n = \{a \in \mathbf{N} \mid \ a \mid n\}.$$

   (a) Verificare che D_n è un sottoreticolo di $(\mathbf{N}, mcd, mcm)$, ossia è chiuso rispetto alle operazioni di mcd e di mcm.

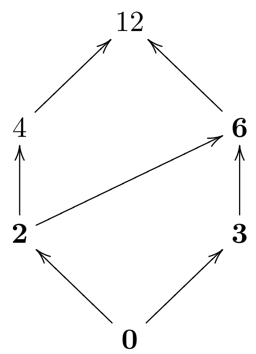
(b) Sia $m < n$ un divisore di n. Verificare che D_m è un sottoreticolo di D_n.
(c) Disegnare il diagramma di Hasse di D_{12} ed evidenziare il sottoreticolo D_6.

Sol. (a) Siano $a, b \in D_n$, ossia interi tali che $a \mid n$ e $b \mid n$. Sia $d = \mathrm{mcd}(a, b)$. Poiché $d \mid a \mid n$ e $d \mid b \mid n$, si ha che $d \mid n$. Dunque $d = \mathrm{mcd}(a, b) \in D_n$, ossia D_n è chiuso rispetto al mcd. Sia $M = \mathrm{mcm}(a, b) = \frac{ab}{\mathrm{mcd}(a,b)}$. Poiché $ab \mid n$ e $\mathrm{mcd}(a, b) \mid ab$, anche $M \mid n$. Dunque $M = \mathrm{mcm}(a, b) \in D_n$ e D_n è chiuso rispetto al mcm.

(b) Se $m < n$ è un divisore di n, si ha innanzitutto che $D_m \subset D_n$: infatti $a \mid m$ e $m \mid n$ implica $a \mid n$. Poiché dati $a, b \in D_m$ si ha che $\mathrm{mcd}(a, b) \mid m$ e $\mathrm{mcm}(a, b) \mid m$ (vedi punto precedente) si ha che $\mathrm{mcd}(a, b)$, $\mathrm{mcm}(a, b) \in D_m$. Dunque D_m è un sottoreticolo di D_n.

(c)

$$D_6 = \{1, 2, 3, 6\} \subset D_{12} = \{1, 2, 3, 4, 6, 12\}.$$



Il reticolo D_{12} e (in grassetto) il sottoreticolo D_6.

7. Stabilire quali dei seguenti sottoinsiemi sono sottoreticoli di $(\mathcal{P}(\{1, 2, 3, 4, 5\}), \cap, \cup)$:
(a) $\{A \in \mathcal{P}(\{1, 2, 3, 4, 5\}) : |A| \text{ dispari } \}$; (c) $\{A \in \mathcal{P}(\{1, 2, 3, 4, 5\}) : A \supseteq \{1, 3\} \}$;
(b) $\{A \in \mathcal{P}(\{1, 2, 3, 4, 5\}) : |A| \geq 2 \}$; (d) $\{A \in \mathcal{P}(\{1, 2, 3, 4, 5\}) : |A| \leq 1 \text{ oppure } |A| = 3\}$

Sol. (a) $X = \{A \in \mathcal{P}(\{1, 2, 3, 4, 5\}) : |A| \text{ dispari } \}$ non è un sottoreticolo di $(\mathcal{P}(\{1, 2, 3, 4, 5\}), \cap, \cup)$. Non è chiuso rispetto all'unione: $A = \{1\}$, $B = \{2\}$ appartengono ad X, ma $A \cup B = \{1, 2\}$ ha cardinalità pari e non appartiene ad X.

(b) $Y = \{A \in \mathcal{P}(\{1, 2, 3, 4, 5\}) : |A| \geq 2 \}$ non è un sottoreticolo di $(\mathcal{P}(\{1, 2, 3, 4, 5\}), \cap, \cup)$. Non è chiuso rispetto all'intersezione: $A = \{1, 2\}$, $B = \{2, 3\} \in Y$, ma $A \cap B = \{2\} \notin Y$.

(c) $Z = \{A \in \mathcal{P}(\{1, 2, 3, 4, 5\}) : A \supseteq \{1, 3\} \}$ è un sottoreticolo di $(\mathcal{P}(\{1, 2, 3, 4, 5\}), \cap, \cup)$. Infatti se $\{1, 3\} \subset A$ e $\{1, 3\} \subset B$, allora $\{1, 3\} \subset A \cap B$ e $\{1, 3\} \subset A \cup B$. In altre parole $A \cap B$, $A \cup B \in Z$, ossia Z è chiuso rispetto alle operazioni $\cap$, $\cup$.

(d) $W = \{A \in \mathcal{P}(\{1, 2, 3, 4, 5\}) : |A| \leq 1 \text{ oppure } |A| = 3\}$ non è un sottoreticolo di $(\mathcal{P}(\{1, 2, 3, 4, 5\}), \cap, \cup)$. Non è chiuso rispetto all'unione: $A = \{1\}$, $B = \{2\}$ appartengono ad W, ma $A \cup B = \{1, 2\}$ ha cardinalità 2 e non appartiene a W.

8. Siano $(L, \vee, \wedge)$ e $(L', \vee', \wedge')$ due reticoli. Un *isomorfismo di reticoli* è una funzione biettiva $f : L \to L'$ tale che per ogni $x, y \in L$ valgono

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

In tal caso i due reticoli si dicono *isomorfi*.

(a) Dimostrare che se $f : L \to L'$ è un isomorfismo di reticoli allora anche $f^{-1} : L' \to L$ lo è;

(b) Siano " $\leq$ " e " $\leq'$ " le relazioni di ordine parziale su L e su L' definite a partire dalle rispettive operazioni. Verificare che se $f\colon L \to L'$ è un isomorfismo di reticoli allora

$$a\text{``}\leq\text{''}b \quad \Rightarrow \quad f(a)\text{``}\leq'\text{''}f(b).$$

Sol. (a) Dobbiamo verificare che $f^{-1} : L' \to L$ soddisfa le relazioni

$$f^{-1}(u \wedge' v) = f^{-1}(u) \wedge f^{-1}(v), \qquad f^{-1}(u \vee' v) = f^{-1}(u) \vee f^{-1}(v),$$

per ogni $u, v \in L'$. Poiché f è un isomorfismo di reticoli ed in particolare è biiettiva, esistono unici $x, y \in L$ tali che $u = f(x)$ e $v = f(y)$. Inoltre $u \wedge' v = f(x \wedge y)$ e $u \vee' v = f(x \vee y)$. Ne segue che

$$f^{-1}(u\wedge' v) = f^{-1}(f(x)\wedge' f(y)) = f^{-1}(f(x\wedge y)) = x\wedge y = f^{-1}(f(x))\wedge f^{-1}(f(y)) = f^{-1}(u)\wedge f^{-1}(v)$$

e

$$f^{-1}(u\vee' v) = f^{-1}(f(x)\vee' f(y)) = f^{-1}(f(x\vee y)) = x\vee y = f^{-1}(f(x))\vee f^{-1}(f(y)) = f^{-1}(u)\vee f^{-1}(v).$$

(b) Supponiamo che valga $a\text{``}\leq\text{''}b$ . Per definizione $a\text{``}\leq\text{''}b$ se $a \wedge b = a$. Poiché $f(a \wedge b) = f(a) \wedge' f(b) = f(a)$, segue che $f(a)\text{``}\leq'\text{''}f(b)$.

9. Verificare che i reticoli (D_6, mcd, mcm) e (D_{15}, mcd, mcm) sono isomorfi (esibire un isomorfismo di reticoli);

Sol. $D_6 = \{1, 2, 3, 6\}$ e $D_{15} = \{1, 3, 5, 15\}$. Consideriamo l'applicazione biiettiva

$$f\colon D_6 \to D_{15}, \qquad f(1) = 1,\ f(2) = 3,\ f(3) = 5,\ f(6) = 15$$

e verifichiamo che si tratta di un isomorfismo, ossia che rispetta le operazioni di reticolo:

• $f(\mathrm{mcd}(a, b)) = \mathrm{mcd}(f(a), f(b)), \quad \forall a, b \in D_6$.

$$f(\mathrm{mcd}(1, 1)) = f(1) = 1 = \mathrm{mcd}(f(1), f(1)) = f(1) = 1;$$

$$f(\mathrm{mcd}(1, 2)) = f(\mathrm{mcd}(1, 3)) = f(\mathrm{mcd}(1, 6)) = f(1) = 1 =$$

$$= \mathrm{mcd}(f(1), f(2)) = \mathrm{mcd}(1, 3) = \mathrm{mcd}(f(1), f(3)) = \mathrm{mcd}(1, 5) = \mathrm{mcd}(f(1), f(6)) = \mathrm{mcd}(1, 15) = 1;$$

$$f(\mathrm{mcd}(2, 3)) = f(1) = 1 = \mathrm{mcd}(f(2), f(3)) = \mathrm{mcd}(3, 5) = 1, \quad f(\mathrm{mcd}(2, 6)) = f(2) = 3 = \mathrm{mcd}(3, 15) = 3;$$

$$f(\mathrm{mcd}(3, 6)) = f(3) = 5 = \mathrm{mcd}(f(3), f(6)) = \mathrm{mcd}(5, 15) = 5;$$

$$f(\mathrm{mcd}(6, 6)) = f(6) = 15 = \mathrm{mcd}(f(6), f(6)) = f(6) = 15.$$

• $f(\mathrm{mcm}(a, b)) = \mathrm{mcm}(f(a), f(b)), \quad \forall a, b \in D_6$.

$$f(\mathrm{mcm}(1, 1)) = f(1) = 1 = \mathrm{mcm}(f(1), f(1)) = f(1) = 1;$$

$$f(\mathrm{mcm}(1, 2)) = f(2) = 3 = \mathrm{mcm}(f(1), f(2)) = \mathrm{mcm}(1, 3) = 3;$$

$$f(\mathrm{mcm}(1, 3)) = f(3) = 5 = \mathrm{mcm}(f(1), f(3)) = \mathrm{mcm}(1, 5) = 5;$$

$$f(\mathrm{mcm}(1,6)) = f(6) = 15 = \mathrm{mcm}(f(1), f(6)) = \mathrm{mcm}(1,15) = 15;$$
$$f(\mathrm{mcm}(2,3)) = f(6) = 15 = \mathrm{mcm}(f(2), f(3)) = \mathrm{mcm}(3,5) = 15;$$
$$f(\mathrm{mcm}(2,6)) = f(6) = 15 = \mathrm{mcm}(f(2), f(6)) = \mathrm{mcm}(3,15) = 15;$$
$$f(\mathrm{mcm}(3,6)) = f(6) = 15 = \mathrm{mcm}(f(3), f(6)) = \mathrm{mcm}(5,15) = 15;$$
$$f(\mathrm{mcm}(6,6)) = f(6) = 15 = \mathrm{mcm}(f(6), f(6)) = f(6) = 15.$$

Osservazione. Per l'Esercizio 8(b), un isomorfismo fra D_6 e D_{15} deve "rispettare" gli ordinamenti dei due reticoli. Quindi necessariamente manda $1 \mapsto 1$ e $6 \mapsto 15$. L'altro isomorfismo fra D_6 e D_{15} è dato da
$$g\colon D_6 \to D_{15}, \qquad g(1) = 1,\ g(2) = 5,\ g(3) = 3,\ g(6) = 15.$$
Non ce ne sono altri.

10. Verificare che i reticoli (D_6, mcd, mcm) e $(\mathcal{P}(\{1,2\}), \cap, \cup)$ sono isomorfi (esibire un isomorfismo di reticoli);

Sol. $D_6 = \{1,2,3,6\}$ e $\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$. Consideriamo l'applicazione biiettiva
$$f\colon D_6 \to \mathcal{P}(\{1,2\}), \qquad f(1) = \emptyset,\ f(2) = \{1\},\ f(3) = \{2\},\ f(6) = \{1,2\}$$
e verifichiamo che si tratta di un isomorfismo, ossia che rispetta le operazioni di reticolo:

- $f(\mathrm{mcd}(a,b)) = f(a) \cap f(b), \quad \forall a,b \in D_6.$

$$f(\mathrm{mcd}(1,1)) = f(1) = \emptyset = f(1) \cap f(1) = \emptyset \cap \emptyset = \emptyset;$$
$$f(\mathrm{mcd}(1,2)) = f(1) = \emptyset = f(1) \cap f(2) = \emptyset \cap \{1\} = \emptyset;$$
$$\dots \quad \dots \quad \dots$$
$$f(\mathrm{mcd}(3,6)) = f(3) = \{2\} = f(3) \cap f(6) = \{2\} \cap \{1,2\} = \{2\};$$
$$\dots \quad \dots \quad \dots$$

- $f(\mathrm{mcm}(a,b)) = f(a) \cup f(b), \quad \forall a,b \in D_6.$

$$f(\mathrm{mcm}(1,1)) = f(1) = \emptyset = f(1) \cup f(1) = \emptyset \cup \emptyset = \emptyset;$$
$$f(\mathrm{mcm}(1,2)) = f(2) = \{1\} = f(1) \cup f(2) = \emptyset \cup \{2\} = \{2\};$$
$$\dots \quad \dots \quad \dots$$
$$f(\mathrm{mcm}(3,6)) = f(6) = \{1,2\} = f(3) \cup f(6) = \{2\} \cup \{1,2\} = \{1,2\};$$
$$\dots \quad \dots \quad \dots$$

L'altro isomorfismo fra reticoli è quello che manda $1 \mapsto \emptyset$, $2 \mapsto \{2\}$, $3 \mapsto \{1\}$, $6 \mapsto \{1,2\}$ (vedi Osservazione sopra).

11. Verificare che i reticoli (D_6, mcd, mcm) e (D_8, mcd, mcm) non sono isomorfi.

Sol. $D_6 = \{1,2,3,6\}$ e $D_8 = \{1,2,4,8\}$. Un eventuale isomorfismo di reticoli necessariamente manda $1 \mapsto 1$ e $6 \mapsto 8$ (vedi Osservazione sopra). Le alternative adesso sono due:

• $f(1) = 1,\ f(2) = 4,\ f(3) = 2,\ f(6) = 8.$
Poiché $f(\mathrm{mcd}(2,3)) = f(1) = 1 \neq \mathrm{mcd}(f(2), f(3)) = \mathrm{mcd}(4,2) = 2$, non si tratta di un isomorfismo.

• $f(1) = 1,\ f(2) = 2,\ f(3) = 4,\ f(6) = 8.$
Poiché $f(\mathrm{mcd}(2,3)) = f(1) = 1 \neq \mathrm{mcd}(f(2), f(3)) = \mathrm{mcd}(2,4) = 2$, non si tratta di un isomorfismo.

12. Un isomorfismo $f\colon (L, \wedge, \vee) \to (L, \wedge, \vee)$ di un reticolo in sè si dice un *automorfismo* del reticolo. Determinare quanti sono gli automorphismi del reticolo (D_6, mcd, mcm).

Sol. $D_6 = \{1, 2, 3, 6\}$ e le stesse considerazione dell'esercizio precedente ci dicono che per un automorfismo di D_6 ci sono due possibilità:

l'identità $f(1) = 1,\ f(2) = 2,\ f(3) = 3,\ f(6) = 6$

oppure $f(1) = 1,\ f(2) = 3,\ f(3) = 2,\ f(6) = 6.$

Si verifica facilmente che quest'ultimo è effettivamente un automorfismo di D_6...

13. Stabilire se $\mathbf{D}_{30}$ e $\mathcal{P}(\{1, 2, 3\})$ sono reticoli isomorfi; in caso affermativo, stabilire quanti sono gli isomorfismi di reticolo $f : \mathbf{D}_{30} \to \mathcal{P}(\{1, 2, 3\})$.

Sol. $\mathbf{D}_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ e $\mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$: i due reticoli hanno almeno lo stesso numero di elementi... Poiché un isomorfismo $f\colon \mathbf{D}_{30} \to \mathcal{P}(\{1, 2, 3\})$ deve rispettare le relazioni di ordine parziale dei due reticoli (divisibilità in $\mathbf{D}_{30}$ e contenenza in $\mathcal{P}(\{1, 2, 3\})$), necessariamente $f(1) = \emptyset$ e $f(30) = \{1, 2, 3\}$. Inoltre la terna $\{2, 3, 5\}$ deve essere mandata nella terna $\{\{1\}, \{2\}, \{3\}\}$. Questo può essere fatto in 3! modi diversi. Ma una volta fissati $f(2)$, $f(3)$ ed $f(5)$, anche $f(6)$, $f(10)$ ed $f(15)$ risultano univocamente determinati (sempre per dover rispettare gli ordinamenti).
Ad esempio, se $f(2) = \{3\}$, $f(3) = \{1\}$, $f(5) = \{2\}$, allora necessariamente $f(6) = \{1, 3\}$, $f(10) = \{2, 3\}$ ed $f(15) = \{1, 2\}$.

In conclusione, ci sono 3! isomorfismi di reticolo $f : \mathbf{D}_{30} \to \mathcal{P}(\{1, 2, 3\})$.

14. Stabilire se i reticoli $\mathbf{D}_{30}$ e $\mathbf{D}_{105}$ sono isomorfi. In caso affermativo, determinare tutti gli isomorfismi di reticolo $f : \mathbf{D}_{30} \to \mathbf{D}_{105}$.

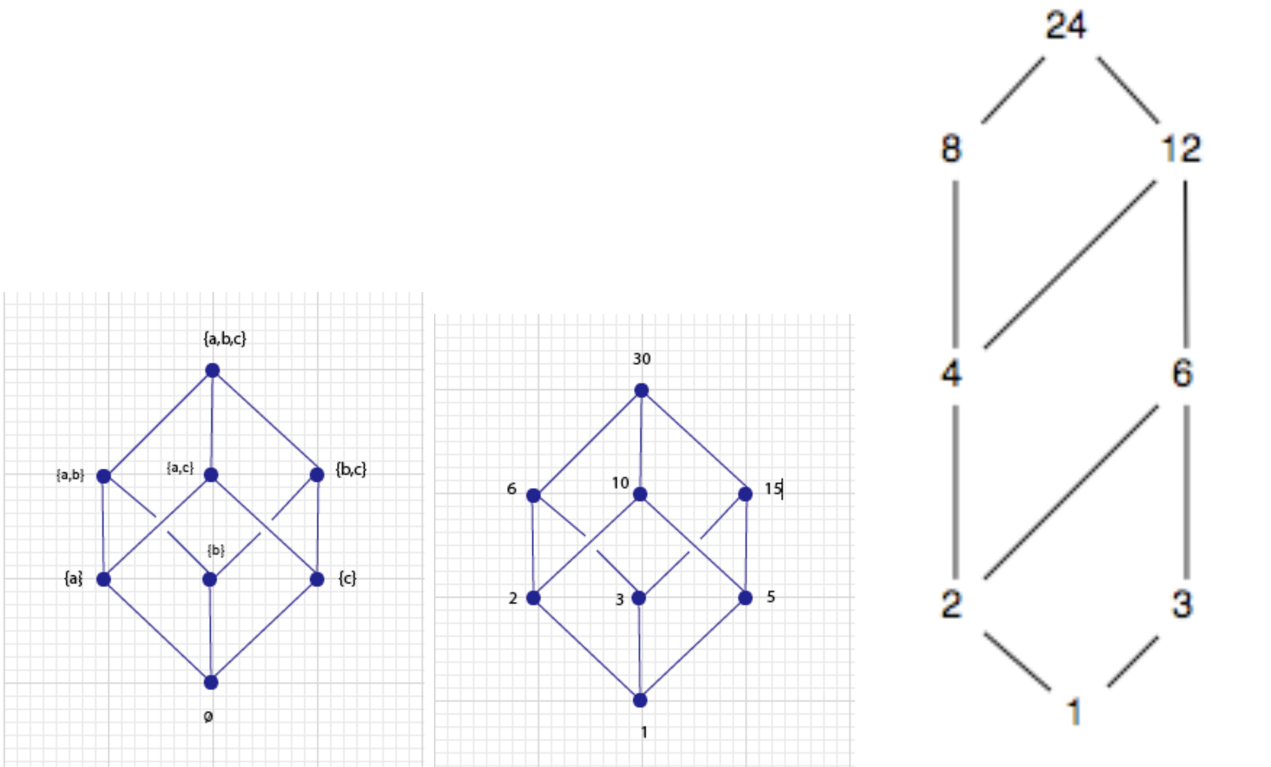
Sol. $\mathbf{D}_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ e $\mathbf{D}_{105} = \{1, 3, 5, 7, 15, 21, 35, 105\}$. Ci sono 3! isomorfismi di reticolo $f : \mathbf{D}_{30} \to \mathbf{D}_{105}$.
Vedi esercizio precedente....

15. Stabilire se i reticoli $\mathcal{P}(\{1, 2, 3\})$ e $\mathbf{D}_{24}$ sono isomorfi. Stabilire se uno dei due reticoli è isomorfo a $\mathbf{D}_{30}$.

Sol. $\mathbf{D}_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$. Ha lo stesso numero di elementi di $\mathcal{P}(\{1, 2, 3\})$, ma non è isomorfo a $\mathcal{P}(\{1, 2, 3\})$:
un isomorfismo $f\colon \mathbf{D}_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\} \to \mathcal{P}(\{1, 2, 3\})$, dovendo rispettare gli ordinamenti dei due reticoli, deve mandare $1 \mapsto \emptyset$ e $24 \mapsto \{1, 2, 3\}$. Per la stessa ragione $f(2)$ ed $f(3)$ devono essere scelti fra $\{1\}$, $\{2\}$, $\{3\}$.
Supponiamo ad esempio che $f(2) = \{1\}$ e $f(3) = \{2\}$.
$f(6)$ deve essere "$\geq$" di $f(2)$ ed $f(3)$ in $\mathcal{P}(\{1, 2, 3\})$: dunque $f(6) = \{1, 2\}$.
$f(4)$ deve essere "$\geq$" di $f(2)$: dunque $f(4) = \{2, 3\}$.

A questo punto, $f(8)$ chi può essere?? non ci sono scelte che rispettino gli ordinamenti dei due reticoli... Ripetendo gli stessi ragionamenti per le altre scelte di $f(2)$ e $f(3)$, arriviamo alla conclusione che i reticoli non sono isomorfi.

Il reticolo $\mathcal{P}(\{1,2,3\})$ è isomorfo a $\mathbf{D}_{30}$ (vedi Esercizio 13), $\mathbf{D}_{24}$ no.



I reticoli isomorfi $\mathcal{P}(\{a,b,c\})$ e D_{30} e il reticolo D_{24} che non è isomorfo ai primi due.

Un altro modo per vedere che $\mathcal{P}(\{1,2,3\})$ e $\mathbf{D}_{24}$ non sono isomorfi:
$\mathcal{P}(\{1,2,3\})$ è un'algebra do Boole, mentre $\mathbf{D}_{24}$ non lo è.
In $\mathcal{P}(\{1,2,3\})$ ogni elemento ha un unico complemento: per ogni sottoinsieme $A \in \mathcal{P}(\{1,2,3\})$ esiste un unico sottoinsieme $\bar{A}$, precisamente il complementare di A in $\{1,2,3\}$, con la proprietà che $A \cap \bar{A} = \emptyset$ e $A \cup \bar{A} = \{1,2,3\}$.
In $\mathbf{D}_{24}$ ci sono elementi che non hanno complemento: ad esempio 6. Infatti non esiste nessun elemento $a \in \mathbf{D}_{24}$ tale che $mcd(a,6) = 1$ e $mcm(a,6) = 24$.

16. Stabilire se i reticoli $\mathbf{D}_{12}$ e $\mathbf{D}_{18}$ sono isomorfi. In caso affermativo, determinare tutti gli isomorfismi di reticolo $f : \mathbf{D}_{12} \to \mathbf{D}_{18}$.

Sol. $\mathbf{D}_{12} = \{1,2,3,4,6,12\}$ e $\mathbf{D}_{18} = \{1,2,3,6,9,18\}$. Hanno lo stesso numero di elementi. Si può verificare facilmente che l'applicazione $f\colon \mathbf{D}_{12} \to \mathbf{D}_{18}$ definita da

$$f(1) = 1, \quad f(2) = 3, \quad f(3) = 2, \quad f(6) = 6, \quad f(4) = 9, \quad f(12) = 18$$

è un isomorfismo di reticoli (è quella che sovrappone il diagramma di Hasse di $\mathbf{D}_{12}$ su quello di $\mathbf{D}_{18}$).
Non ce ne sono altri: basta verificare che l'altra possibile scelta

$$f(1) = 1, \quad f(3) = 3, \quad f(2) = 2, \ldots\ldots$$

non rispetterebbe gli ordinamenti.

17. Verificare che il reticolo $(\mathbf{N}, mcd, mcm)$ ha limite inferiore, ma non ha limite superiore.

Sol. $\mathbf{N} = \{1, 2, 3, \ldots\}$ ed in $\mathbf{N}$ si ha m "$\leq$"n se m divide n. Poiché $1 \in \mathbf{N}$ divide ogni numero naturale, 1 è limite inferiore e minimo di $\mathbf{N}$. Invece $\mathbf{N}$ non ha limite superiore: non c'è nessun numero naturale che è diviso da tutti gli altri...

18. Sia X un insieme arbitrario (possibilmente infinito).Verificare che il reticolo $(\mathcal{P}(X), \cap, \cup)$ ha limite inferiore e limite superiore. Chi sono?

Sol. $(\mathcal{P}(X)$ è l'insieme dei sottoinsiemi di X e in $(\mathcal{P}(X)$ si ha A "$\leq$"B se A è contenuto in B. Poiché $\emptyset \in \mathcal{P}(X)$ è contenuto in ogni altro sottoinsieme di X, si ha che $\emptyset$ è limite inferiore e minimo di $\mathcal{P}(X)$. Poiché ogni sottoinsieme $A \in \mathcal{P}(X)$ è contenuto in X (per definizione...) si ha che X è limite superiore e massimo di $\mathcal{P}(X)$.

N.B.: Il reticolo $(\mathcal{P}(X)$ è limitato anche quando X è un insieme infinito.

19. Sia $n \in \mathbf{N}$ un numero naturale fissato.
    (a) Determinare il limite inferiore e il limite superiore del reticolo (D_n, mcd, mcm);
    (b) Dimostrare che D_n è complementato se e solo se n è prodotto di primi distinti.

Sol. (a) Ricordiamo che in D_n si ha a"$\leq$"b se a divide b.
Il limite inferiore e minimo del reticolo (D_n, mcd, mcm) è 1: infatti $1 \in D_n$ e divide tutti gli elementi di D_n;
il limite superiore e massimo del reticolo (D_n, mcd, mcm) è n: infatti $n \in D_n$ e (per definizione) tutti gli elementi di di D_n dividono n.

(b) Sia $n = p_1^{a_1} \ldots p_k^{a_k}$ la decomposizione di n in fattori primi, dove i p_i sono primi distinti e gli a_i sono interi positivi che indicano le potenze con cui appaiono i p_i. Supponiamo che il primo p_i appaia ad una potenza $a_i > 1$. In tal caso, l'elemento $m = n/p_i \in D_n$ non ha complemento in D_n. Infatti nella decomposizione in fattori primi di m compaiono tutti i fattori primi distinti di n e dunque non esiste nessun elemento $a \in D_n$ per cui valga $mcd(a, m) = 1$.
Ad esempio, se $n = 2^3 \cdot 3 = 24$, come nell'Esercizio 15, possiamo verificare che $m = 6$ oppure $m = 12$ non hanno complemento in D_{24}.

Viceversa, sia n prodotto di primi distinti. Innanzitutto è chiaro che $\bar{1} = n$ e $\bar{n} = 1$. Sia m un divisore di n, diverso da 1 e da n. Allora m è il prodotto di un sottoinsieme proprio dei fattori primi di n e il quoziente n/m è il prodotto dei rimanenti. Poiché $\mathrm{mcd}(n, n/m) = 1$ e $\mathrm{mcm}(m, n/m) = n$ si ha che il complemento di m è $\bar{m} = n/m$.

N.B. *In un reticolo distributivo e limitato, se il complemento di un elemento esiste, è unico.*

20. Si consideri il reticolo $L = \{A \in \mathcal{P}(\{1, 2, 3, 4\}) : A \subseteq \{1, 2, 3\}\}$, con le operazioni di unione e intersezione.
    (a) Dimostrare che L è limitato;
    (b) Stabilire se ci sono elementi il cui complemento non è unico;
    (c) Stabilire se L è un reticolo distributivo.

Sol. Siamo nella situazione dell'Esercizio 5, con $X = \{1, 2, 3, 4\}$ e $Y = \{1, 2, 3\}$:

$$L = \{A \in \mathcal{P}(\{1, 2, 3, 4\}) : A \subseteq \{1, 2, 3\}\} = \mathcal{P}(\{1, 2, 3\}) \subset \mathcal{P}(\{1, 2, 3, 4\}).$$

(a) $L = \mathcal{P}(\{1,2,3\})$ è un reticolo loimitato con minimo $\emptyset$ e massimo $\{1,2,3\}$ (vedi Esercizio 18).

(b) Dato un elemento $A \in L = \mathcal{P}(\{1,2,3\})$, cioè un sottoinsieme di $\{1,2,3\}$, il suo complemento $\bar{A}$ è dato dal sottoinsieme complementare di A in $\{1,2,3\}$. Si può verificare che è unico.

(c) In generale, per X insieme arbitrario, il reticolo $\mathcal{P}(X)$ è distributivo:

$$A \cap (B \cup C) = A \cap B \bigcup A \cap C, \qquad A \cup (B \cap C) = A \cup B \bigcap A \cup C, \qquad \forall A, B, C \in \mathcal{P}(X).$$

(la verifica di questi fatti è un esercizio di teoria degli insiemi). Dunque anche $\mathcal{P}(\{1,2,3\})$ è distributivo. Disegnando il diagramma di Hasse di $\mathcal{P}(\{1,2,3\})$, si vede che non contiene né *trirettangoli* né *pentagoni*.

N.B. *In un reticolo distributivo e limitato, se il complemento di un elemento esiste, è unico (vedi (b)).*

21. Quali dei seguenti reticoli sono reticoli con complemento?
    (a) $\mathbf{D}_{70}$;
    (b) $\mathbf{D}_{18}$;
    (c) $\mathcal{P}(\mathcal{P}(\{a\}))$.

Sol. (a) $\mathbf{D}_{70} = \{1,2,5,7,10,14,35,70\}$. Poiché $70 = 2 \cdot 5 \cdot 7$ è prodotto di primi distinti, $\mathbf{D}_{70}$ è un reticolo complementato (vedi Esercizio 19). Precisamente: $\bar{1} = 70$, $\bar{2} = 35$, $\bar{5} = 14$, $\bar{7} = 10$.

N.B. In generale, se $n = p_1 \dots p_k$ è prodotto di primi distinti, $\mathbf{D}_n$ è un reticolo booleano, cioè un reticolo limitato, distributivo, complementato (e quindi con complemento unico). Ogni reticolo booleano è anche un'algebra di Boole.

(b) $\mathbf{D}_{18} = \{1,2,3,6,9,18\}$. Poiché $18 = 2 \cdot 3^2$ non è prodotto di primi distinti, $\mathbf{D}_{18}$ non è un reticolo complementato (vedi Esercizio 19).

(c) Abbiamo che $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$ e $\mathcal{P}(\mathcal{P}(\{a\})) = \{\emptyset, \{\emptyset\}, \{\{a\}\}, \{\emptyset, \{a\}\}\}$. $\mathcal{P}(\mathcal{P}(\{a\}))$ è un reticolo complementato: $\overline{\emptyset} = \{\emptyset, \{a\}\}$ e $\overline{\{\emptyset\}} = \{\{a\}\}$.

22. Stabilire se i seguenti reticoli sono reticoli distributivi, reticoli con complemento, reticoli con complemento unico:
    (a) $\{1,2,3,4,6,9,12,18,36\}$, munito delle operazioni *mcd* e *mcm*;
    (b) $\mathbf{D}_{12}$;
    (c) $\mathcal{P}(\{a,b,c\})$;
    (d) $\mathbf{D}_{30}$;
    (e) $\{1,6,10,15,30,60,90,180\}$, munito delle operazioni *mcd* e *mcm*.

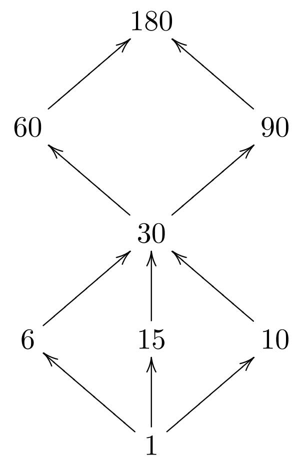
Sol. (a) L'insieme $\{1,2,3,4,6,9,12,18,36\}$ coincide con D_{36}. Quindi, munito delle operazioni *mcd* e *mcm*, è un reticolo limitato, con minimo 1 e massimo 36. Dal suo diagramma di Hasse si vede che è distributivo. Poiché $36 = 2^2 \cdot 3^2$, non è prodotto di primi distinti, D_{36} non è un reticolo complementato (vedi Esercizio 19).

(b) $\mathbf{D}_{12}$: è limitato con con minimo 1 e massimo 12. Dal suo diagramma di Hasse si vede che è distributivo. Poiché $12 = 2^2 \cdot 3$, non è prodotto di primi distinti, D_{12} non è un reticolo complementato (vedi Esercizio 19).

(c) $\mathcal{P}(\{a,b,c\})$: è limitato, distributivo, complementato con complemento unico (vedi sopra....).

(d) $\mathbf{D}_{30}$ pure, perché è isomorfo a $\mathcal{P}(\{a,b,c\})$ (vedi sopra....).

(e) $L = \{1,6,10,15,30,60,90,180\}$ è limitato con con minimo 1 e massimo 180. Dal suo diagramma di Hasse si vede che non è distributivo (contiene un trirettangolo). Non è complementato: ad esempio 30 non ha complemento in L.



Il reticolo L.

23. Considerare l'esercizio 14.80 del libro di Schaum. Verificare che il diagramma di Hasse del reticolo D_{60} contenuto nella figura 14–29 a pag. 475 è sbagliato.