G. Pareschi

RETICOLI

1. Reticoli come insiemi parzialmente ordinati

In questa sezione riprendiamo le nozioni sulle relazioni d'ordine. In particolare, ci occuperemo dei *reticoli*, che non sono altro che insiemi parzialmente ordinati dove il *sup* e l'*inf* di una coppia di elementi esistono sempre.

Definizione 1.1 (Reticolo)**.** Un reticolo è un insieme (parzialmente) ordinato S tale che, per ogni $a, b \in S$, esistono $\inf(a, b)$ e $\sup(a, b)$.

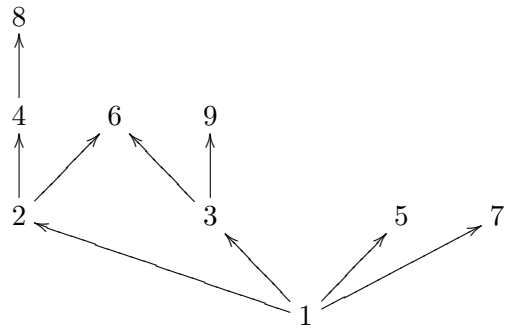
Esercizio 1.2. Dimostrare per induzione che, se S è un reticolo, allora per ogni sottoinsieme *finito* A di S, esistono $\sup A$ e $\inf A$.

Esempio 1.3. Sia A un insieme. Consideriamo il suo insieme delle parti $\mathcal{P}(A)$, ordinato mediante la contenenza. Allora $\mathcal{P}(A)$ è un reticolo. Infatti, dati $B, C \in \mathcal{P}(A)$, $\sup(B, C) = B \cup C$ e $\inf(B, C) = B \cap C$.

Esempio 1.4. L'insieme dei numeri naturali, $\mathbb{N}$, ordinato mediante la divisibilità, è un reticolo. Infatti, dati $h, k \in \mathbb{N}$, si ha che, rispetto alla divisibilità, $\inf(h, k) = mcd(h, k)$ e $\sup(h, k) = mcm(h, k)$ (esercizio).

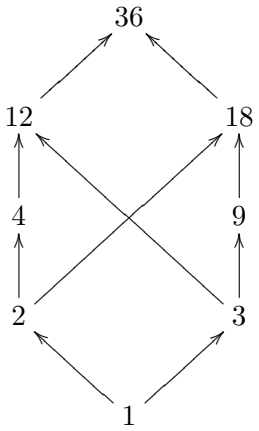
Esempio 1.5. Dato $n \in \mathbb{N}$ l'insieme dei divisori di n, $\mathbf{D}_n$ (vedi dispensa sulle relazioni d'ordine), ordinato mediante la divisibilità, è un reticolo. Infatti, dati due divisori di n, $h, k \in \mathbf{D}_n$, anche $mcm(h, k)$ e $mcd(h, k)$ sono divisori di n, cioè appartengono a $\mathbf{D}_n$.

Esempio 1.6. L'insieme $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, ordinato mediante la divisibilità, non è un reticolo. Infatti, per esempio, $sup(8, 9)$ non esiste.



Esempio 1.7. L'insieme $\{1, 2, 3, 4, 9, 12, 18, 36\}$, ordinato mediante la divisibilità, non è un reticolo. Infatti $\sup(2, 3)$ non esiste: l'insieme dei maggioranti di $\{2, 3\}$ è $\{12, 18, 36\}$, che non

ha minimo.



2. Reticoli come algebre

In questa sezione vedremo i reticoli possono essere definiti, in modo equivalente, come insiemi muniti due operazioni che soddisfano certe proprietà. L'idea è che $(a,b) \mapsto \sup(a,b)$ e $(a,b) \mapsto \inf(a,b)$ sono due operazioni, che possiamo denotare rispettivamente $a \vee b$ e $a \wedge b$. Viceversa, la relazione d'ordine può essere ricavata da queste operazioni, nel modo seguente: $a\,R\,b$ se e solo se $b = a \vee b$ (oppure $a\,R\,b$ se e solo se $a = a \wedge b$).

Proposizione 2.1. Sia S un reticolo. Allora, posto $a \vee b = \sup(a,b)$ e $a \wedge b = \inf(a,b)$, si ha che le operazioni su S: $(a,b) \mapsto a \vee b$ e $(a,b) \mapsto a \wedge b$ verficano le seguenti proprietà:
(a) *Commutatività:* $a \vee b = b \vee a$ e $a \wedge b = b \wedge a$, per ogni $a, b \in S$.
(b) *Associatività*: $a \vee (b \vee c) = (a \vee b) \vee c$ e $a \wedge (b \wedge c) = (a \wedge b) \wedge c$, per ogni $a, b, c \in S$.
(a) *Assorbimento*: $a \wedge (a \vee b) = a$, $a \vee (a \wedge b) = a$ per ogni $a, b \in S$.

Proof. Evidente (esercizio). □

Esaminiamo ora il viceversa della precedente Proposizione

Proposizione 2.2. Sia $(S, \vee, \wedge)$ un insieme munito di due operazioni che verificano le seguenti proprietà:
(a) *Commutatività:* $a \vee b = b \vee a$ e $a \wedge b = b \wedge a$, per ogni $a, b \in S$.
(b) *Associatività*: $a \vee (b \vee c) = (a \vee b) \vee c$ e $a \wedge (b \wedge c) = (a \wedge b) \wedge c$, per ogni $a, b, c \in S$.
(a) *Assorbimento*: $a \wedge (a \vee b) = a$, $a \vee (a \wedge b) = a$ per ogni $a, b \in S$.
Allora la relazione R su S così definita:

$$a\,R\,b \qquad \text{se e solo se} \qquad b = a \vee b$$

è una relazione d'ordine su S. Si ha anche che

$$a\,R\,b \qquad \text{se e solo se} \qquad a = a \wedge b. \tag{1}$$

Inoltre S, munito di tale relazione d'ordine, è un reticolo, e, per ogni $a, b \in S$

$$\sup(a,b) = a \vee b \qquad \text{e} \qquad \inf(a,b) = a \wedge b.$$

Proof. Cominciamo con il dimostrare la (1) Infatti, se $a\,R\,b$, cioè se $b = a \vee b$, allora, per l'assorbimento, $a \wedge b = a \wedge (a \vee b) = a$. Viceversa, se $a = a \wedge b$ allora, ancora per l'assorbimento, e per la commutatività, $a \vee b = (a \wedge b) \vee b = b \vee (a \wedge b) = b$.
Dimostriamo ora che R è una relazione d'ordine.

- *Riflessività:* $a\,R\,a$, cioè $a = a \vee a$. Infatti, usando le due proprietà di assorbimento, per ogni $a, b \in S$ si ha che $a = a \vee (a \wedge (a \vee b) = a \vee a$.
- *Antisimmetria.* Se $a\,R\,b$ e $b\,R\,a$, cioè se $b = a \vee b$ e $a = b \vee a$ allora, per la commutatività, $a = b$.
- *Transitività* Se $a\,R, b$ e $b\,R\,c$, cioè $b = a \vee b$ e $c = b \vee c$ segue che $a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = a \vee c$ (abbiamo usato l'associatività).

Rimane da dimostrare che l'ultima asserzione. Dimostriamo che

$$a \vee b = \sup(a, b)$$

Infatti $a\ R\ (a \vee b)$, perchè per la (1), ciò è equivalente al fatto che $a \wedge (a \vee b) = a$, cosa che è verificata per l'assorbimento. Allo stesso modo, si vede che $b\ R\ (a \vee b)$. Quindi $a \vee b$ è un maggiorante dell'insieme $\{a, b\}$. Rimane da dimostare che è il minimo dell'insieme dei maggioranti. Supponiamo dunque che $a\,R\,c$ e $b\,R\,c$, cioè, $c = a \vee c$ e $c = b \vee c$. Allora $(a \vee b) \vee c = a \vee (b \vee c) = a \vee c = c$. Dunque $(a \vee b)\,R\,c$ e l'asserzione è dimostrata.
Il fatto che $a \wedge b = \inf(a, b)$ si dimostra in modo analogo (esercizio seguente). □

Esercizio 2.3. Dimostrare che $a \wedge b = \inf(a, b)$.

Vista l'equivalenza delle due definizioni di reticolo, nel seguito ci riferiremo indifferentemente all'una o all'altra.

Osservazione 2.4 (Idempotenza)**.** Nel corso della dimostrazione, abbiamo visto che le proprietà di assorbimento implicano che

$$a \vee a = a \qquad \text{per ogni} \quad a \in S \tag{2}$$

Allo stesso modo si può dimostrare (Esercizio!) che

$$a \wedge a = a \qquad \text{per ogni} \quad a \in S \tag{3}$$

Le proprietà (2) e (3) sono dette *proprietà di idempotenza* delle operazioni $\vee$ e $\wedge$.

3. Attributi dei reticoli

3.1. **Limitatezza.**

Definizione 3.1 (Reticolo limitato)**.** Un reticolo S è detto limitato se esistono il minimo ed il massimo di S (denotati rispettivamente 0 e I).
Equivalentemente un reticolo S è limitato se esistono due elementi $0, I \in S$ tali che

$$0 \vee a = a \qquad \text{e} \qquad a \vee I = I,$$

per ogni $a \in A$. Si noti che, per la (1), tale proprietà si può anche esprimere come segue

$$0 \wedge a = 0 \qquad \text{e} \qquad I \wedge a = a$$

Osservazione 3.2. Un reticolo *finito* è limitato. Infatti, se $S = \{a_1, \ldots, a_n\}$, si ha che $I = \sup(a_1, \ldots, a_n)$ e $0 = \inf(a_1, \ldots, a_n)$.

Esempio 3.3. Il viceversa non è vero: ci sono dei reticoli *infiniti* che sono limitati. Ad esempio, anche se A è un insieme infinito, $\mathcal{P}(A)$ è limitato: $\max \mathcal{P}(A) = A$ e $\min \mathcal{P}(A) = \emptyset$. Invece $\mathbb{N}$, ordinato mediante la divisibilità, non è limitato perchè non ha massimo.

3.2. **Complemento.**

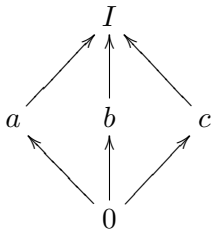
Definizione 3.4 (Complemento)**.** Sia S un reticolo limitato e sia $a \in S$. Un elemento $b \in S$ tale che:

$$a \vee b = I \qquad \text{e} \qquad a \wedge b = 0$$

è detto un complemento di a.

Esempio 3.5. Si osservi che vi può essere più di un complemento. Ad esempio: nel reticolo di diagramma di Hasse

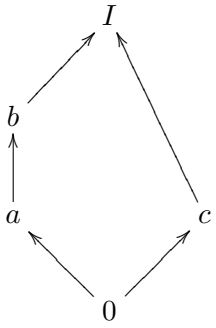
(4)



l'elemento a ha due complementi (b e c). Analogamente, anche b e c hanno due complementi ciascuno.

Esempio 3.6. Si consideri il reticolo di diagramma di Hasse

(5)

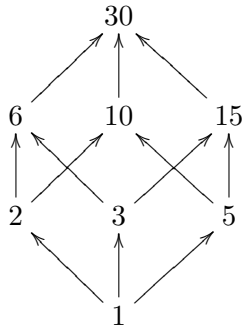


Anche in questo caso vi è un elemento (c) che ha più di un complemento: a e b sono entrambi complementi di c. Invece a e b hanno entrambi un unico complemento (c).

Definizione 3.7 (Reticolo con complemento)**.** Un reticolo limitato S si dice con complemento (o complementato) se ogni $a \in S$ ha un complemento.

Esempio 3.8. (a) I reticoli (4) e (5) sono complementati.
(b) Il reticolo $\mathbf{D}_{30}$ è complementato e il complemento di ogni elemento è unico. Questo si può vedere direttamente dal digramma di Hasse

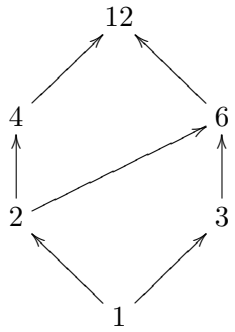
(6)



oppure osservando che, per ogni $k \in \mathbf{D}_{30}$, il suo complemento è $\frac{30}{k}$. Infatti, poichè 30 non ha come fattori potenze maggiori o uguali a due di numeri primi (di solito, per esprimere questa

proprietà si dice che 30 *non ha fattori quadratici*, oppure che 30 è *prodotto di primi distinti*), si ha che $mcm(k, \frac{30}{k}) = 1$ e $mcd(k, \frac{30}{k}) = 30$.
(c) Nel reticolo $\mathbf{D}_{12}$, laddove c'è il complemento, esso è unico, ma non tutti gli elementi hanno complemento:

(7)



Si vede che 2 e 6 non hanno complemento. Questo si può vedere direttamente dal diagramma di Hasse, oppure come segue: se a fosse complemento di 2, si avrebbe che $mcd(a, 2) = 1$, quindi necessariamente $a = 3$, ma $mcm(2, 3)$ è uguale a 6 e non a 12. (analogo ragionamento per 6). Invece 3 e 4 hanno complemento, ed esso è unico (sono l'uno il complemento della altro. Si noti che $3 = \frac{12}{4}$ e che $4 = \frac{12}{3}$).

Esercizio 3.9. Generalizzare gli esempi precedenti dimostrando che $\mathbf{D}_n$ è con complemento se e solo se n è prodotto di primi *distinti*. Nel caso in cui $\mathbf{D}_n$ non sia complementato, descrivere gli elementi che non hanno complemento.

Esercizio 3.10. Dimostrare che, dato un insieme A, il reticolo $\mathcal{P}(A)$ è sempre con complemento.

3.3. **Distributività.**

Definizione 3.11 (Reticolo distributivo)**.** Un reticolo S è detto distributivo se valgono le proprietà distributive

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \qquad \text{e} \qquad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

per ogni $a, b, c \in S$.

Esempio 3.12. Gli insiemi delle parti sono sempre distributivi. Infatti

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \qquad \text{e} \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

per ogni scelta di sottoinsiemi A, B e C di un dato insieme.
(b) I reticoli $\mathbb{N}$ e $\mathbf{D}_n$ sono sempre distributivi, cioè per ogni scelta di numeri naturali $a, b, c \in D_n$, valgono le relazioni

$$mcm(a, mcd(b, c)) = mcd(mcm(a, b), mcm(a, c)) \tag{$d1$}$$

$$mcd(a, mcm(b, c)) = mcm(mcd(a, b), mcd(a, c)) \tag{$d2$}$$

• Dimostriamo la relazione (d1):

Scriviamo $n = p_1^{\nu_1} \dots p_k^{\nu_k}$, con $p_1, \dots, p_k$ primi distinti. Allora

$$a = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \qquad b = p_1^{\beta_1} \dots p_k^{\beta_k}, \qquad c = p_1^{\gamma_1} \dots p_k^{\gamma_k},$$

con $0 \leq \alpha_i, \beta_i, \gamma_i \leq \nu_i$, per $i = 1, \dots, k$. Da una parte abbiamo

$$mcd(b, c) = p_1^{min(\beta_1, \gamma_1)} \dots p_k^{min(\beta_k, \gamma_k)},$$

$$mcm(a, mcd(b,c)) = p_1^{max(\alpha_1, min(\beta_1,\gamma_1))} \dots p_k^{max(\alpha_k, min(\beta_k,\gamma_k))};$$

dall'altra

$$mcm(a,b) = p_1^{max(\alpha_1,\beta_1)} \dots p_k^{max(\alpha_k,\beta_k)}, \qquad mcd(a,c) = p_1^{min(\alpha_1,\gamma_1)} \dots p_k^{min(\alpha_k,\gamma_k)}$$

e

$$mcd(mcm(a,b), mcm(a,c)) = p_1^{min(max(\alpha_1,\beta_1), max(\alpha_1,\gamma_1))} \dots p_k^{min(max(\alpha_k,\beta_k), max(\alpha_k,\gamma_k))}.$$

L'uguaglianza desiderata segue dal fatto che dati tre interi non negativi $\alpha,\ \beta,\ \gamma$, vale

$$max(\alpha, min(\beta,\gamma)) = min(max(\alpha,\beta), max(\alpha,\gamma)).$$

• Dimostriamo la relazione (d2):

Da una parte abbiamo

$$mcm(b,c) = p_1^{max(\beta_1,\gamma_1)} \dots p_k^{max(\beta_k,\gamma_k)},$$

$$mcd(a, mcm(b,c)) = p_1^{min(\alpha_1, max(\beta_1,\gamma_1))} \dots p_k^{min(\alpha_k, max(\beta_k,\gamma_k))};$$

dall'altra

$$mcd(a,b) = p_1^{min(\alpha_1,\beta_1)} \dots p_k^{min(\alpha_k,\beta_k)}, \qquad mcd(a,c) = p_1^{min(\alpha_1,\gamma_1)} \dots p_k^{min(\alpha_k,\gamma_k)}$$

e

$$mcm(mcd(a,b), mcd(a,c)) = p_1^{max(min(\alpha_1,\beta_1), min(\alpha_1,\gamma_1))} \dots p_k^{max(min(\alpha_k,\beta_k), min(\alpha_k,\gamma_k))}.$$

L'uguaglianza desiderata segue dal fatto che dati tre interi non negativi $\alpha,\ \beta,\ \gamma$, vale

$$min(\alpha, max(\beta,\gamma)) = max(min(\alpha,\beta), min(\alpha,\gamma)).$$

Proposizione 3.13. *Sia S un reticolo limitato distributivo e sia $a \in S$. Se a ha un complemento, esso è unico.*

Proof. Supponiamo che b e c siano complementi di a. Quindi

$$a \vee b = I \quad a \wedge b = 0 \quad a \vee c = I \quad a \wedge c = 0.$$

Dimostriamo che $c\, R\, b$. Infatti

$$b = b \vee 0 = b \vee (a \wedge c) \overset{distrib.}{=} (b \vee a) \wedge (b \vee c) = I \wedge (b \vee c) = b \vee c$$

Allo stesso modo si dimostra che $c = c \vee b$, cioè che $b\, R\, c$. Dunque, per l'antisimmetria, $b = c$. □

Esempio 3.14. Si evince dalla Proposizione precedente che i reticoli (4) e (5) non sono distributivi. Questo può essere verificato direttamente.
(a) In (4)

$$a \vee (b \wedge c) = a \vee 0 = a \qquad (a \vee b) \wedge (a \vee c) = I \wedge I = I$$

$$a \wedge (b \vee c) = a \wedge I = a \qquad (a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0.$$

(b) In (5)

$$b \wedge (a \vee c) = b \wedge I = b \qquad (b \wedge a) \vee (b \wedge c) = a \vee 0 = a$$

$$a \vee (b \wedge c) = a \vee 0 = a \qquad (a \vee b) \wedge (a \vee c) = b \wedge I = b.$$

4. Elementi irriducibili. Atomi. Decomposizione.

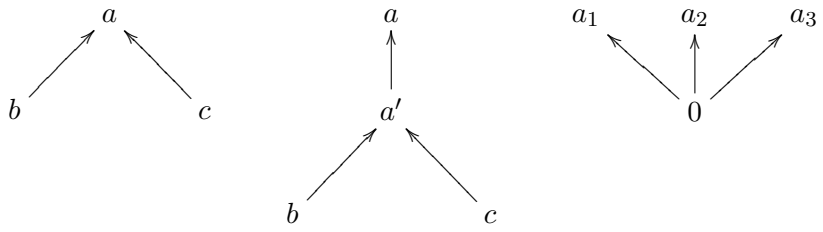
In questa sezione esaminiamo un modo di *decomporre* gli elementi di un reticolo come $\wedge$ di particolari elementi, detti *irriducibili*. Questa decomposizione gioca un po' il ruolo della decomposizione dei numeri naturali in prodotto di numeri primi (in effetti, se si considerano il reticolo $\mathbb{N}$, oppure i reticoli $\mathbf{D}_n$, con le operazioni di *mcm* e *mcd*, la decomposizione che descriveremo coincide con la fattorizzazione in primi).

Definizione 4.1 (Elementi irriducibili, atomi)**.** (a) Sia S un reticolo. Un elemento $a \in S$ è detto irriducibile se vale la proprietà: se $a = b \vee c$ allora $a = b$ oppure $a = c$.
(b) Sia S un reticolo limitato. Un elemento $a \in S$ è detto un atomo se 0 è un suo predecessore immediato (cioè vale la proprietà: se $b\,R\,a$ allora $b = 0$ oppure $b = a$).

Proposizione 4.2. Sia S un reticolo limitato.
(a) Un elemento a di S è irriducibile se e solo se ha un solo predecessore immediato.
(b) Un atomo è sempre irriducibile.

Proof. (a) Supponiamo che a abbia un unico predecessore immediato, diciamo a'. Se fosse che $a = b \vee c = \sup(b, c)$, con $a \neq b, c$ allora b e c sarebbero predecessori di a, e quindi anche di a', e quindi non potrebbe essere che $\sup(b, c) = a$. Dunque a è irriducibile. Viceversa, supponiamo che b abbia almeno due predeccori immediati, diciamo b e c. Allora è evidente che $a = \sup(b, c) = a \vee c$. Dunque a non è irriducibile.
(b) Se 0 è un predecessore immediato di a, è necessariamente *l'unico* predecessore di a (un eventuale altro predecessore di a, diciamo b, è sempre tale che $0\,R\,b\,R\,a$, quindi 0 non sarebbe un predecessore immediato). □

Le seguenti figure possono servire, rispettivamente, a chiarire i concetti di elemento non-irriducibile, irriducibile, atomi:



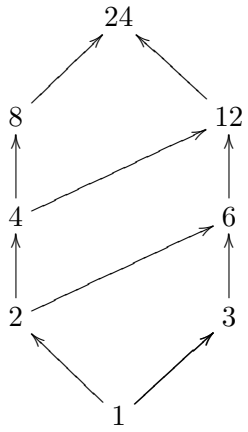
Proposizione 4.3 (Esistenza della decomposizione)**.** Sia S un reticolo finito, e sia $a \in S$. Allora esistono elementi irriducibili $a_1, .., a_k \in S$ tali che a_i non precede a_j se $i \neq j$, e tali che

$$a = a_1 \vee \cdots \vee a_k.$$

Proof. Se a è irriducibile, non c'è niente da dimostrare. Altrimenti, $a = b \vee c$. Se b e c sono irriducibili, abbiamo finito. Altrimenti $b = d \vee e$ e $c = f \vee g$ e dunque $a = d \vee e \vee f \vee g$. Se d, e, f, g sono irriducibili, abbiamo finito. Altrimenti continuiamo così. Visto che S è finito, dopo un numero finito di passi avremo la decomposizione in irruducibili $a = a_1 \vee \cdots a_k$. Se c'è qualche a_i che precede qualche a_j, lo eliminiamo. □

Esempio 4.4. Nel reticolo $\mathbf{D}_{24}$

(8)



decomponiamo 24 in irriducibili:

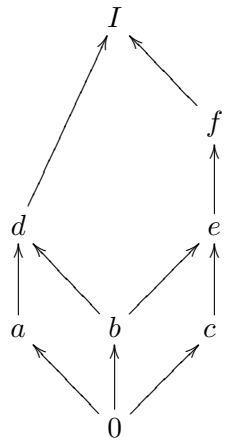
$$24 = 8 \vee 12 = 8 \vee 4 \vee 6 = 8 \vee 4 \vee 2 \vee 3$$

adesso togliamo gli elementi *ridondanti* (cioè gli irriducibili che sono minori di qualche altro elemento della decomposizione) e risulta

$$24 = 8 \vee 3$$

Esempio 4.5. Si consideri il reticolo

(9)



Decomponiamo I in irriducibili e poi eliminiamo gli elementi ridondanti:

$$I = d \vee f = a \vee b \vee f = a \vee f$$

Si osservi c'è anche un'altra decomposizione:

$$I = a \vee b \vee c$$

Quindi, in questo esempio, ci sono due decomposizioni diverse dello stesso elemento.

Proposizione 4.6. Sia S un reticolo finito distributivo. Allora una decomposizione come in Prop. 4.3 è unica (a meno di riordinamento degli elementi della decomposizione).

Proof. Supponiamo che $a = a_1 \vee \cdots a_k = b_1 \vee \cdots b_h$. Dato $i \in \{1, .., k\}$, si ha che

$$a_i = a_i \wedge a = a_i \wedge (b_1 \vee \cdots b_h) \overset{distrib.}{=} (a_i \wedge b_1) \vee \cdots \vee (a_i \wedge b_h)$$

Poichè a_i è irriducibile, esisterà un $j \in \{1, ..., h\}$ tale che $a_i = a_i \wedge b_j$. Quindi $a_i \, R \, b_j$. Abbiamo quindi dimostrato che, per ogni $i \in \{1, \ldots, k\}$ esiste un $j \in \{1, \ldots, h\}$ tale che $a_i \, R \, b_j$. Allo stesso modo, si mostra che, per ogni $j \in \{1, ..., h\}$, esiste un $i \in \{1, ..., h\}$ tale che $b_j \, R \, a_i$. Da ciò si deduce facimente che per ogni i esiste uno ed un solo j tale che $a_i = b_j$ e viceversa. □

Proposizione 4.7. Sia S un reticolo con complemento tale che ogni elemento ha un unico complemento. Allora ogni elemento irriducibile di S è un atomo.

Proof. Sia $a \in S$ un elemento irriducibile. Vogliamo dimostrare che l'unico predecessore di a è 0. A tale scopo, consideriamo l'uico predecessore immediato b di a, e supponiamo che $b \neq 0$. Se dimostriamo che $b = a$ la Proposizione è dimostrata. A tale scopo, consideriamo il complemento (unico) di b, e denotiamolo c. Allora

$$a \vee c = I$$

perchè, dal fatto che, per ipotesi, $I = b \vee c$, e $b \, R \, a$ segue che $I = (b \vee c) \; R \, (a \vee c)$. Inoltre

$$a \wedge c = 0.$$

Infatti, poichè $(a \wedge c) \, R \, a$, si ha che $(a \wedge c) \, R \, b$ (perchè b è l'unico predecessore di a). Poi, ovviamente, $(a \wedge c) \, R \, c$. Mettendo insieme, si ha che $(a \wedge c) \, R \, (b \wedge c)$. Ma, per ipotesi, $b \wedge c = 0$. Dunque $a \wedge c = 0$, come asserito.

Quindi a è un complementare di c. Per l'unicità del complemento $a = b$. □

Come conseguenza si ha il seguente

Corollario 4.8. Sia S un reticolo finito, distributivo, con complemento. Allora ogni elemento si S può essere decomposto in modo unico in atomi. In altre parole, per ogni $a \in S$ esistono e sono unici atomi $a_1, \ldots, a_k$ tali che

$$a = a_1 \vee \cdots \vee a_k$$

Proof. Per la Prop. 4.3 esiste sempre una decomposizione in irriducibili. Poichè il reticolo è distributivo e con complemento, per la Prop. 3.13 il complemento eiste sempre ed è unico. Per la Prop. 4.7 gli irriducibili sono atomi, quindi la decomposizione è in atomi. Infine, ancora usando la distributività, la Prop. 4.6 implica che la decomposizione è unica. □

5. Sottoreticoli

In matematica si incontra spesso la nozione di "sotto"-oggetto: sottospazio vettoriale, sottogruppo, sottoanello,... In questi esempi, si tratta di un insieme "ambiente" munito di operazioni, e un "sotto"-oggetto è un sottoinsieme chiuso rispetto alle operazioni. La nozione di sottoreticolo è del tutto analoga:

Definizione 5.1 (Sottoreticolo)**.** Dato un reticolo S, un sottoinsieme $T \subset S$ è detto un sottoreticolo si S se $a \vee b \in T$ e $a \wedge b \in T$ per ogni $a, b \in T$.

È chiaro che un sottoreticolo è esso stesso un reticolo. Invece il viceversa non è necessariamente vero: dato un reticolo S, esso può avere sottoinsiemi che sono reticoli rispetto alle operazioni di S ma non sono sottoreticoli di S.

Esempio 5.2. Nel reticolo (7) – oltre ai sottoreticoli *banali* ($\mathbf{D}_{12}$ stesso e i sottoinsiemi con un solo elemento) – abbiamo i seguenti sottoreticoli: $\{1, 2, 3, 6\}$ e $\{2, 4, 6, 12\}$.

Si osservi, ad esempio, che anche $\{1, 2, 3, 4, 12\}$ è un sottoinsieme di $\mathbf{D}_{12}$ che è a sua volta un reticolo, ma non è un sottoreticolo si $\mathbf{D}_{12}$ (perchè?)

Esercizio 5.3. (a) Determinare tutti i sottoreticoli non banali di $\mathcal{P}(\{1, 2, 3\})$.
(b) Determinare tutti i sottoreticoli non banali di $\mathbf{D}_{30}$ e di $\mathbf{D}_{24}$.

6. Isomorfismo di insiemi parzialmente ordinati

In matematica si usa spesso il terminini *isomorfismo* e *isomorfi*. Si potrebbe tradurre dal greco che due oggetti *isomorfi* sono *fatti in modo uguale*. Nel contesto degli insiemi parzialmente ordinati si da' la seguente

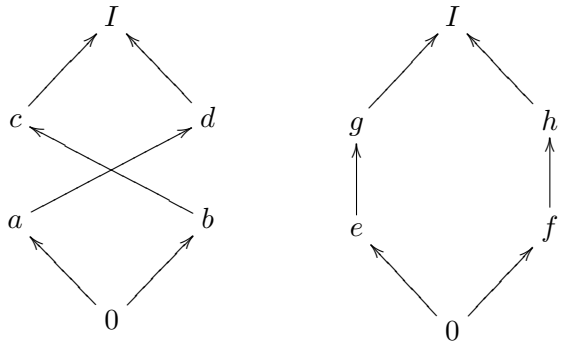
Definizione 6.1 (Isomorfismo di insiemi (parzialmente) ordinati)**.** Sia S_1 (rispettivamente, S_2) un insieme munito di una relazione d'ordine R_1 (rispettivamente, R_2). Una funzione

$$f : S_1 \to S_2$$

tale che:
(a) f è biettiva;
(2) dati $s, t \in S_1$, $\quad f(s)\, R_2\, f(t) \quad$ se e solo se $\quad s\, R_1\, t$.
è detta un *isomorfismo di insiemi (parzialmente) ordinati*. Se tale funzione esiste i due insiemi parzialmente ordinati sono detti *isomorfi*.

Si osservi che due insiemi parzialmente ordinati isomorfi hanno necessariamente la stessa cardinalità. Per due insiemi parzialmente ordinati *finiti*, essere isomorfi significa avere "diagramma di Hasse della stessa forma" (espressione che va presa con beneficio d'inventario, perchè i diagrammi di Hasse di due insiemi parzialmente ordinati isomorfi possono sembrare diversi solo perchè *disegnati* in modo diverso).

Esempio 6.2.



sono isomorfi. Quanti isomorfismi ci sono?

La definizione di isomorfismo di insiemi parzialmente ordinati vale, in particolare, per reticoli.

Definizione/Proposizione 6.3 (Isomorfismo di reticoli)**.** Siano S_1 e S_2 due reticoli. Un isomorfismo di insiemi parzialemente ordinati tra S_1 e S_2 è detto un isomorfismo di reticoli. Equivalentemente, un isomorfismo di reticoli è una funzione biettiva $f : S_1 \to S_2$ tale che $f(a \vee b) = f(a) \vee f(b)$ e $f(a) \wedge f(b)$ per ogni $a, b \in S_1$.

Proof. Si tratta di dimostrare l'ultima parte. Ciò segue immediatamente dalla seguente asserzione, da dimostrare per esercizio: *la condizione:*

$$\inf(f(a), f(b)) = f(\inf(a, b)) \qquad e \qquad \sup(f(a), f(b)) = f(\sup(a, b)), \qquad \text{per ogni } a, b \in S_1$$

è equivalente alla condizione

$$\text{per ogni } a, b \in S_1, \quad f(a)\, R\, f(b) \quad \text{se e solo se} \quad a\, R\, b$$

□

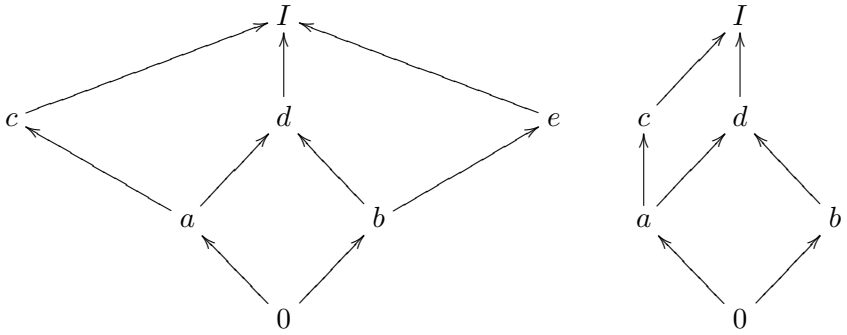
Esempio 6.4. I reticoli $\mathbf{D}_{30}$, $\mathbf{D}_{42}$ e $\mathcal{P}(\{1, 2, 3\})$ sono isomorfi. Un isomorfismo f tra i primi due si ottiene mandando 1 in 1 (cioè il minimo nel minimo) e l'insieme $\{2, 3, 5\}$ in $\{2, 3, 7\}$. Ad esempio, $f(2) = 7$, $f(3) = 3$, $f(5) = 2$. Questo determina le immagini degli altri elementi: ad esempio, $f(6) = f(2 \vee 3) = f(2) \vee f(3) = 7 \vee 3 = 21$. Ne consegue che gli isomorfismi di reticolo tra $\mathbf{D}_{30}$ e $\mathbf{D}_{42}$ sono 3! (come le funzioni biettive tra $\{2, 3, 5\}$ e $\{2, 3, 7\}$).

Esercizio 6.5. Dimostrare che $\mathbf{D}_n$ e $\mathbf{D}_m$ sono isomorfi se e solo se la fattorizzazione in primi di n e m "ha la stessa struttura", cioè $n = p_1^{r_1} \cdots p_k^{r_k}$ e $m = q_1^{r_1} \cdots q_k^{r_k}$. In tale caso, quanto isomorfismi ci sono?

Abbiamo il seguente Teorema, di cui omettiamo la dimostrazione

Teorema 1. *Sia S un reticolo finito. Allora S è distributivo se e solo se S non ha sottoreticoli isomorfi a (4) o a (5).*

Esercizio 6.6. Stabilire se i seguenti reticoli sono distributivi.



7. Algebre di Boole come reticoli

Le Algebre di Boole saranno oggetto del prossimo file. Esse possono essere definite in almeno tre modi diversi ma equivalenti. Ciascuno di essi mette in luce un diverso aspetto del concetto di Algebra di Boole. Cominciamo qui con la definizione di Algebra di Boole come reticolo, rimandando altre definizioni al capitolo successivo.

Definizione 7.1 (Algebra di Boole come reticolo)**.** Un reticolo limitato, distributivo, complementato è detto un'algebra di Boole.

Esempio 7.2. L'insieme delle parti di un dato insieme (finito o infinito) è un'Algebra di Boole. Nel Teorema successivo vedremo che un'Algebra di Boole *finita* è necessariamente isomorfa (come reticolo) all'insieme delle parti di un dato insieme finito.

Il seguente Teorema è detto *Teorema di rappresentazione per le Algebre di Boole finite*:

Teorema 2. *Sia S un'algebra di Boole finita e siano $a_1, .., a_n$ i suoi atomi. Allora S è isomorfo, come reticolo, al reticolo $\mathcal{P}(\{a_1, ..., a_n\})$. In particolare, $|S| = 2^n$.*

Proof. Dal Corollario 4.8 sappiamo che ogni elemento $a \in S$ si decompone in modo unico come "somma" di atomi:

$$a = a_{i_1} \vee .... \vee a_{i_k}, \qquad \text{con} \quad \{i_1, \dots i_k\} \subseteq \{1, \dots, n\}$$

Consideriamo quindi la funzione

$$F : S \to \mathcal{P}(\{a_1, \dots, a_n\}) \qquad a \mapsto \{i_1, \dots, i_n\}$$

Poichè ad ogni elemento di S corrisponde un'unica decomposizione e viceversa, la funzione F è biettiva. E' chiaro che F è un isomorfismo di reticoli. Infatti, se $b = a_{j_1} \vee \cdots \vee a_{j_h}$, denotando $I = \{a_{i_1}, \dots, a_{i_k}\}$ e $J = \{a_{j_1}, \dots, a_{i_n}\}$, si ha che

$$F(a \vee b) = I \cup J = F(a) \cup F(b) \qquad e \qquad F(a \wedge b) = I \cap J = F(a) \cap F(j)$$

□

8. Raccolta di alcuni esercizi tratti da compiti d'esame su: reticoli.

Attenzione: questi sono alcuni esercizi d'esame, sugli argomenti di questa dispensa. Non sono una selezione di quelli che ritengo più significativi, ma solamente quelli tratti dagli appelli di cui sono in possesso del file sorgente. Siete quindi invitati a cercare di risolvere gli esercizi, su questi argomenti, tratti dai TUTTI gli esami degli anni passati (oltre agli esercizi assegnati, naturalmente).

Esercizio 8.1. Si consideri il reticolo $\mathbf{D}_{60}$. (a) Esibire esplicitamente (motivando) due elementi $h, k \in \mathbf{D}_{60}$ tali che h ha complemento e k non ha complemento.
(b) Stabilire (motivando) se qualcuno tra i seguenti sottoinsiemi di $\mathbf{D}_{60}$ è un sottoreticolo: (i) $A = \{1, 2, 4, 5, 20\}$; (ii) $B = \{1, 3, 4, 6, 12\}$; (iii) $C = \{1, 2, 3, 5, 30\}$.
(c) Stabilire se $\mathbf{D}_{60}$ è isomorfo a $\mathbf{D}_{90}$ e, in caso affermativo, esibire esplicitamente un isomorfismo e stabilire quanti sono gli isomorfismi di reticolo.

Soluzione. (a) L'elemento 3 ha complemento 20. Infatti $mcd(3, 20) = 1$ e $mcm(3, 20) = 60$. L'elemento 2 non ha complemento. Infatti, se esistesse un complemento di 2, chiamiamolo a, sarebbe $mcd(2, a) = 1$. Quindi a dovrebbe essere: 3, oppure 5, oppure 15. Ma $mcm(2, 3) = 6$, $mcm(2, 5) = 10$, $mcm(2, 15) = 30$.

(b) Nessuno dei tre sottoinsiemi è un sottoreticolo di $\mathbf{D}_{60}$. Infatti: $2 \vee 5 = mcm(2, 5) = 10 \notin A$. $4 \wedge 6 = mcd(4, 6) = 2 \notin B$. $\quad 2 \vee 3 = mcm(2, 3) = 6 \notin C$.

(c) Fattorizzando 60 e 90 in numeri primi, si ha che $60 = 2^2 \cdot 3 \cdot 5$ e $90 = 2 \cdot 3^2 \cdot 5$. Dunque entrambi sono della forma $p^2 \cdot q \cdot r$, con p, q, r primi distinti. Quindi sono isomorfi, perchè entranbi della forma $\{1, p, q, r, p^2, pq, pr, p^2q, p^2r, p^2qr\}$. Un isomorfismo dovrà mandare 2 in 3, 3 in 2 (oppure in 5) e 5 in 5 (oppure in 2). Gli altri valori sono determinati. Vi sono quindi due isomorfismi, corrispondenti alla scelta $f(3) = 2$, $f(5) = 5$, oppure $f(3) = 5$, $f(5) = 2$. Il primo isomorfismo è:

$f : \mathbf{D}_{60} \to \mathbf{D}_{90}$, $f(1) = 1$, $f(2) = 3$, $f(3) = 2$, $f(5) = 5$, $f(6) = f(2 \vee 3) = f(2) \vee f(3) = 3 \vee 2 = 6$, $f(10) = f(2 \vee 5) = f(2) \vee f(5) = 3 \vee 5 = 15$, $f(15) = f(3 \vee 5) = f(3) \vee f(5) = 2 \vee 5 = 10$, $f(4) = 9$, $f(12) = f(4) \vee f(3) = 9 \vee 2 = 18$, $f(20) = f(4) \vee f(5) = 9 \vee 5 = 45$, $f(60) = 90$.

Esercizio 8.2. Si consideri il reticolo $L = \{1, 2, 4\} \times \{1, 2, 4\}$, ordinato tramite la relazione d'ordine "$\leq$" cosi' definita: dati $(a, b) \in L$ e $(c, d) \in L$, $(a, b) \leq (c, d)$ se a divide c e b divide d.
(a) Si considerino i seguenti sottoinsiemi di L: $A = \{(1, 2), (1, 4), (2, 2), (2, 4)\}$,

$B = \{(1,2),(1,4),(2,2),(4,2),(4,4)\}$. Stabilire se A è un sottoreticolo di L. Stabilire se B è un sottoreticolo di L.
(b) Determinare, se possibile, un elemento $x \in L$, diverso dal massimo e dal minimo, che ha complemento. Determinare, se possibile, un elemento $y \in L$ che non ha complemento.
(c) Determinare gli elementi irriducibili di L e determinare una decomposizione irridondante in irriducibili dell'elemento $(4,4)$.

Soluzione. (a) A è un sottoreticolo, perchè $(1,4)\wedge(2,2) = (1,2) \in A$ e $(1,4)\vee(2,2) = (2,4) \in A$ (le altre condizioni sono banali, perchè le altre coppie di elementi si A sono in relazione). B non è un sottoreticolo, perchè, ad esempio $(1,4) \vee (2,2) = (2,4) \notin B$.

(b) Ad esempio, $(1,4)$ ha complemento: $(1,4)' = (4,1)$. Infatti $(1,4) \wedge (4,1) = (1,1) = min\, L$, e
$(1,4) \vee (4,1) = (4,4) = max\, L$.
Invece, ad esempio, $(1,2)$ non ha complemento. Infatti, le uniche coppie (a,b) tali che $(1,2) \wedge (a,b) = (1,1)$ sono $(2,1)$ e $(4,1)$, ma $(1,2) \vee (2,1) = (2,2) \neq max\, L$ e $(1,2) \vee (4,1) = (4,2) \neq max\, L$.

(c) Gli irriducibili di L sono: $(1,2)$, $(2,1)$ (atomi) e $(1,4)$, $(4,1)$.

$(4,4) = (2,4) \vee (4,2) = \big((1,4) \vee (2,2)\big) \vee \big((2,2), \vee (4,1)\big) = (1,4) \vee (2,2) \vee (4,1) = (1,4) \vee (1,2) \vee (2,1) \vee (4,1) = (1,4) \vee (4,1)$. La decomposizione richiesta è

$$(4,4) = (1,4) \vee (4,1)$$

Esercizio 8.3. Si consideri il reticolo $L = \mathcal{P}(\{0\}) \times \mathcal{P}(\{a,b\})$, ordinato mediante la relazione $(A,B) \leq (C,D)$ se $A \subseteq C$ e $B \subseteq D$. Si consideri anche il reticolo $M = \{1,2,3,4,9,15,60,180\}$, ordinato mediante la divisibilità.
(a) Stabilire se L o M è isomorfo a $\mathcal{P}(\{a,b,c\})$ e, in tal caso, esibire esplicitamente un isomorfismo e determinare quanti sono gli isomorfismi.

Soluzione. Innanzitutto è utile elencare esplicitamente gli elementi di L:

$$L = \{(\emptyset,\emptyset),(\emptyset,\{a\}),(\emptyset,\{b\}),(\emptyset,\{a,b\}),(\{0\},\emptyset),(\{0\},\{a\}),(\{0\},\{b\}),(\{0\},\{a,b\})$$

Si vede che L è isomorfo a $\mathcal{P}(a,b,c)$. Un isomorfismo è $f : L \to \mathcal{P}(\{a,b,c\})$, così definito: $f((\emptyset,\emptyset)) = \emptyset$, $f((\emptyset,\{a\})) = \{a\}$, $f((\emptyset,\{b\})) = \{b\}$, $f((\{0\},\emptyset)) = \{c\}$, $f((\emptyset,\{a,b\})) = \{a,b\}$, $f((\{0\},\{a\})) = \{a,c\}$, $f((\{0\},\{b\})) = \{b,c\}$, $f((\{0\},\{a,b\})) = \{a,b,c\}$. Gli isomorfismi devono mandare biettivamente gli atomi in atomi. Poichè gli atomi sono tre, ci sono $3! = 6$ modi di fare ciò. Dunque gli isomorfismi tra L e $\mathcal{P}(\{a,b,c\})$ sono sei.

Il reticolo M non è isomorfo a $\mathcal{P}(\{a,b,c\})$ (ad esempio, M ha solamente due atomi).

Esercizio 8.4. Si consideri il reticolo $A = \mathbf{D}_4 \times \mathbf{D}_6$, ordinato mediante la relazione "$\leq$" seguente: dati (a,b) e (c,d) in A, $(a,b) \leq (c,d)$ se a divide c e b divide d.
(a) Determinare gli elementi irriducibili e gli atomi di A. (b) Stabilire quali dei seguenti reticoli sono isomorfi tra loro: A, $\mathbf{D}_{60}$, $\mathbf{D}_{72}$ e, in caso di reticoli isomorfi, stabilire quanti sono gli isomorfismi ed esibirne esplicitamente uno. (c) Esibire, se esiste, un elemento di A senza complemento.

Soluzione. (a) Atomi: $(1,2)$, $(1,3)$, $(2,1)$. Irriducibili: $(1,2)$, $(1,3)$, $(2,1)$, $(4,1)$.

(b) $\mathbf{D}_{60}$ e $\mathbf{D}_{72}$ non sono isomorfi, perchè hanno fattorizzazioni in primi di tipo diverso: $60 = 2^2 \cdot 3 \cdot 5$, $72 = 2^3 \cdot 3^2$. Oppure, più semplicemente, perchè, ad esempio, $\mathbf{D}_{60}$ ha tre atomi, mentre $\mathbf{D}_{72}$ solo due.

Si vede invece che A e $\mathbf{D}_{60}$ sono isomorfi. Gli isomorfismi sono due. Per vedere ciò, si osservi che l'atomo $(2,1)$ di A deve corrispondere necessariamente all'atomo 2 di $\mathbf{D}_{60}$, in quanto, al di sopra di esso c'è l'irriducibile (non atomo) $(4,1)$ di A , che deve corrispondere necessariamente all'irriducibile (non atomo) 4 di $\mathbf{D}_{60}$. Quindi un isomorfismo tra A e $\mathbf{D}_{60}$ deve mandare $(1,2)$ in 3 e $(1,3)$ in 5 o, viceversa, $(1,2)$ in 5 e $(1,3)$ in 2. Vi sono quindi solo due possibilità.

Esplicitamente, nel primo caso, si ottiene l'isomorfismo $f : A \to \mathbf{D}_{60}$ così definito: $f((1,1)) = 1$, $f((1,2)) = 3$, $f((1,3)) = 5$, $f((2,1)) = 2$, $f((4,1)) = 4$, $f((1,6)) = 15$, $f((2,2)) = 6$, $f((2,3)) = 10$, $f((2,6)) = 30$, $f((4,2)) = 24$, $f((4,3)) = 20$, $f((4,6)) = 60$.

(c) Ad esempio, $(2,1)$ (se non lo si vede direttamente, ci si può aiutare usando quanto si sa sul reticolo $\mathbf{D}_{60}$).

Esercizio 8.5. Per $n \in \mathbb{N}$, indichiamo con $\mathbf{D}_n = \{m \in \mathbb{N} \mid m \text{ divide } n\}$ il reticolo dei divisori di n con le operazioni di massimo comun divisore e di minimo comune multiplo. Si considerino i seguenti reticoli:

$$\mathbf{D}_{30}, \quad \mathbf{D}_{24}, \quad \mathbf{D}_{54}, \quad \mathcal{P}(\{a,b,c\})$$

(a) Stabilire quali tra questi reticoli sono isomorfi tra loro, mostrando esplicitamente un isomorfismo o dimostrando che non esiste nessun isomorfismo.

(b) In caso i reticoli siano isomorfi, stabilire se esiste più di un isomorfismo. In tal caso, esibirne almeno due.

(a) Osserviamo innanzitutto che tutti i reticoli in questione hanno lo stesso numero di elementi

$$|\mathbf{D}_{24}| = |\mathbf{D}_{54}| = |\mathbf{D}_{30}| = |\mathcal{P}(\{a,b,c\})| = 8.$$

Tuttavia risulta che $\mathbf{D}_{24}$ e $\mathbf{D}_{54}$ sono reticoli isomorfi, e lo stesso vale per $\mathbf{D}_{30}$ e $\mathcal{P}(\{a,b,c\})$. Invece $\mathbf{D}_{24}$ e $\mathcal{P}(\{a,b,c\})$ non sono reticoli isomorfi. (I rispettivi diagrammi di Hasse hanno infatti forma diversa).

(b) Esiste un unico isomorfismo di reticoli fra $\mathbf{D}_{24}$ e $\mathbf{D}_{54}$, ed è quello che manda

$$1 \mapsto 1,\ 2 \mapsto 3,\ 3 \mapsto 2,\ 4 \mapsto 9,\ 8 \mapsto 27,\ 6 \mapsto 6,\ 12 \mapsto 18,\ 24 \mapsto 54.$$

Invece esistono $3! = 6$ isomorfismi fra $\mathbf{D}_{30}$ e $\mathcal{P}(\{a,b,c\})$. Ognuno di essi è determinato dalle immagini di $2, 3, 5$ in $\{a\}, \{b\}, \{c\}$. Due isomorfismi sono ad esempio

$$1 \mapsto \emptyset,\ 2 \mapsto \{a\},\ 3 \mapsto \{b\},\ 5 \mapsto \{c\},\ 6 \mapsto \{a,b\},\ 15 \mapsto \{b,c\},\ 10 \mapsto \{a,c\},\ 30 \mapsto \{a,b,c\};$$

$$1 \mapsto \emptyset,\ 2 \mapsto \{b\},\ 3 \mapsto \{a\},\ 5 \mapsto \{c\},\ 6 \mapsto \{a,b\},\ 15 \mapsto \{a,c\},\ 10 \mapsto \{b,c\},\ 30 \mapsto \{a,b,c\}.$$

Esercizio 8.6. Si consideri il reticolo $(\mathbf{D_{405}}, \text{mcd}, \text{mcm})$, dove $\mathbf{D_{405}} = \{n \in \mathbb{N} \mid n \text{ divide } 405\}$.

(a) Verificare che $\mathbf{D_{405}}$ è un reticolo limitato.

(b) Determinare se $\mathbf{D_{405}}$ è un reticolo complementato (verificare che ogni elemento ammette complemento oppure esibire almeno un elemento che non ammette complemento).

(c) Enunciare la proposizione "*Il reticolo* $\mathbf{D_{405}}$ *è distributivo*" usando quantificatori e connettivi logici.

(d) Verificare se l'enunciato formulato al punto (c) è vero o falso sulla terna $x = 9$, $y = 5$, $z = 45$. Poiché $405 = 3^4 \cdot 5$, il reticolo $\mathbf{D_{405}}$ è dato da

$$\mathbf{D_{405}} = \{1, 3, 9, 27, 81, 5, 15, 45, 135, 405\}.$$

L'ordinamento parziale sul reticolo è dato da: $m \leq n$ *se* m *divide* n.

(a) Il reticolo $\mathbf{D_{405}}$ è limitato:

il minimo è 1: infatti 1 divide tutti gli elementi di $\mathbf{D_{405}}$ e dunque $1 \leq n$, per ogni $n \in \mathbf{D_{405}}$.

il massimo è 405: infatti ogni gli elemento di $\mathbf{D_{405}}$ divide 405 e dunque $n \leq 405$, per ogni $n \in \mathbf{D_{405}}$.

(b) Il reticolo $\mathbf{D_{405}}$ non è complementato:

l'elemento 15 non ha complemento in $\mathbf{D_{405}}$: infatti se $m \in \mathbf{D_{405}}$ ha la proprietà che $\mathrm{mcd}(15, m) = 1$, allora necessariamente $m = 1$. D'altra parte $\mathrm{mcm}(15, 1) = 15 \neq 405$ ed $m = 1$ non è un complemento di 15.

(c)

$$\forall x, y, z \in \mathbf{D_{405}} \quad \mathrm{mcd}(x, \mathrm{mcm}(y, z)) = \mathrm{mcm}(\mathrm{mcd}(x, y), \mathrm{mcd}(x, z));$$
$$\forall x, y, z \in \mathbf{D_{405}} \quad \mathrm{mcm}(x, \mathrm{mcd}(y, z)) = \mathrm{mcd}(\mathrm{mcm}(x, y), \mathrm{mcm}(x, z)).$$

(d)

$$\mathrm{mcd}(9, \mathrm{mcm}(5, 45)) = \mathrm{mcm}(\mathrm{mcd}(9, 5), \mathrm{mcd}(9, 45)), \quad \mathrm{mcd}(9, 45) = 9 = \mathrm{mcm}(1, 9);$$
$$\mathrm{mcm}(9, \mathrm{mcd}(5, 45)) = \mathrm{mcd}(\mathrm{mcm}(9, 5), \mathrm{mcm}(9, 45)), \quad \mathrm{mcm}(9, 5) = 45 = \mathrm{mcd}(45, 45).$$