# Strutture booleane

GIOVANNI CUTOLO

Lo scopo di queste note è quello di presentare in modo unitario anelli booleani, reticoli booleani e algebre di Boole, senza entrare in troppi dettagli ma spiegando come e perché lo studio di ciascuna di queste strutture è equivalente a quello delle altre. Il riquadro che segue contiene un riassunto di questi contenuti; sia bene inteso che questo riassunto non è di per sé sufficiente per la loro comprensione, ma la sua lettura è un utile preliminare a quella del resto di queste note. Nella sezione finale delle note faremo poi qualche osservazione su come si possano inquadrare in questa teoria esempi di algebre di Boole che chi legge ha probabilmente incontrato, o sta per incontrare, in altri corsi.

**In sintesi**

Si definiscono tre tipi di strutture che fanno riferimento nel loro nome a quello di George Boole. Abbiamo gli *anelli booleani*, che sono per definizione gli anelli unitari i cui elementi sono tutti idempotenti, i *reticoli booleani*, che sono invece i reticoli distributivi e complementati, le *algebre di Boole*, che sono particolari strutture algebriche la cui definizione è riportata più avanti, nella terza sezione di queste note.

Ciò che lega queste strutture tra loro è che definire su un insieme una struttura di uno di questi tre tipi (anello booleano, reticolo booleano, algebra di Boole) equivale definirne una di ciascuno degli altri due tipi; in modo che risulti del tutto equivalente lo studio degli anelli booleani, quello delle algebre di Boole e quello dei reticoli booleani.

L'esempio da avere come riferimento è quello dell'insieme $\mathcal{P}(S)$ delle parti di un insieme $S$. Come dovrebbe essere ben noto, $(\mathcal{P}(S), \subseteq)$, cioè l'insieme $\mathcal{P}(S)$ ordinato per inclusione, è un reticolo, che risulta essere un reticolo booleano. Lo stesso insieme, munito delle operazioni di differenza simmetrica ed intersezione, $(\mathcal{P}(S), \triangle, \cap)$, è un anello booleano. Infine, $\mathcal{P}(S)$ si può strutturare come algebra di Boole mediante le operazioni di unione, intersezione e l'operazione unaria di complemento ${}^c\colon X \in \mathcal{P}(S) \mapsto S \smallsetminus X \in \mathcal{P}(S)$; l'algebra di Boole così ottenuta è $(\mathcal{P}(S), \cup, \cap, \varnothing, S, {}^c)$.

Questo esempio è particolarmente importante per almeno due motivi. Uno di tipo pratico: il modo in cui si può, in $\mathcal{P}(S)$, passare da uno dei tre tipi di struttura booleana a ciascuno degli altri due illustra molto bene come si può effettuare l'analogo passaggio a partire da una struttura booleana arbitraria; questo esempio può essere quindi di grande aiuto nello studio della situazione generale. Il secondo motivo, di carattere teorico e di importanza ancora maggiore, è che quello fornito dagli insiemi $\mathcal{P}(S)$ non è un esempio particolare ma, in qualche modo, quello tipico. Infatti un importante teorema (dovuto a M.H. Stone) mostra che ogni anello booleano finito è isomorfo a $(\mathcal{P}(S), \triangle, \cap)$ per un opportuno insieme $S$ (per gli anelli infiniti il teorema è un po' più debole: ogni anello booleano è isomorfo ad un sottoanello unitario di $(\mathcal{P}(S), \triangle, \cap)$, per un opportuno insieme $S$). Analoghi enunciati valgono per i reticoli booleani e per le algebre di Boole. Questo vuol dire, ad esempio, che se sappiamo descrivere il reticolo delle parti degli insiemi finiti, conosciamo, a meno di isomorfismi, tutti i reticoli booleani finiti. Una conseguenza del teorema di Stone è che gli anelli booleani finiti (ma lo stesso vale per i reticoli booleani finiti o per le algebre di Boole finite) hanno per cardinalità una potenza di 2, e che due anelli booleani finiti con lo stesso numero di elementi sono necessariamente isomorfi.

*Avvertenza.* Alcune parti di questo file, in cui appaiono di regola dimostrazioni o verifiche, sono indentate e marcate da un segnale di pericolo. Questo indica che i loro contenuti vanno considerati approfondimenti per chi fosse ad essi interessato ma non fanno parte del programma del corso e non sono richiesti ai fini dell'esame. Altre osservazioni e dimostrazioni possono essere o non essere parte effettiva del programma, a seconda che siano o non siano state trattate a lezione.

## 1. Anelli booleani

Per definizione un *anello booleano* è un anello unitario in cui ogni elemento è *idempotente*, cioè coincide col proprio quadrato.

Ad esempio, l'anello $\mathbb{Z}_2$ degli interi modulo 2 è un anello booleano: è unitario e i suoi due elementi, $\bar{0} = [0]_2$ e $\bar{1} = [1]_2$ sono idempotenti: $\bar{0}^2 = \bar{0}$ e $\bar{1}^2 = \bar{1}$. Un altro esempio significativo è quello dell'anello $(\mathcal{P}(S), \triangle, \cap)$ delle parti di un (arbitrario) insieme $S$. Infatti quest'anello è unitario (di unità $S$) e, dal momento che l'operazione di moltiplicazione nell'anello $\mathcal{P}(S)$ è quella di intersezione, per ogni $X \in \mathcal{P}(S)$ si ha $X^2 = X \cap X = X$.

Prima di dimostrare una semplice proprietà degli anelli booleani è opportuno un richiamo sulla nozione di caratteristica di un anello unitario. Se $R$ è un anello unitario e l'unità $1_R$ di $R$, ha periodo finito $c$ nel gruppo additivo $(R, +)$, si dice che $c$ è la *caratteristica* di $R$. Detto in modo più esplicito, se esiste qualche intero positivo $n$ tale che $n1_R$ (che è la somma $1_R + 1_R + \cdots + 1_R$ con $n$ addendi) è uguale a $0_R$ (lo zero di $R$), allora la caratteristica

di $R$ è il minimo tale intero $n$.[1] Dovrebbe essere chiaro che $R$ ha caratteristica 1 se e solo $1_R = 0_R$; si verifica facilmente che in questo caso $R = \{0_R\}$. Il caso immediatamente successivo è quello degli anelli di caratteristica 2: sono quelli in cui $1_R \neq 0_R$ ma $2 \cdot 1_R = 1_R + 1_R = 0_R$. Notiamo che l'anello $(\mathcal{P}(S), \triangle, \cap)$ ha questa proprietà se $S \neq \varnothing$. Infatti in questo anello l'unità è $S$, lo zero è $\varnothing$, l'addizione è l'operazione di differenza simmetrica e si ha $2 \cdot S = S \triangle S = \varnothing$. Quindi l'anello $\mathcal{P}(S)$ ha caratteristica 2.

Dimostriamo ora che quanto appena visto per $(\mathcal{P}(S), \triangle, \cap)$ vale per tutti gli anelli booleani; verificando inoltre che questi anelli sono sempre commutativi.

**Proposizione 1.** *Sia $R$ un anello booleano. Allora $R$ è commutativo e, se $|R| > 1$, $R$ ha caratteristica 2.*

*Dimostrazione.* Per ogni $a, b \in R$ si ha $a^2 = a$, $b^2 = b$ e $(a+b)^2 = a + b$, perché $R$ è booleano. D'altra parte, come in ogni anello,

$$(a+b)^2 = (a+b)(a+b) = a(a+b) + b(a+b) = a^2 + ab + ba + b^2$$

e quindi

$$a + b = (a+b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b.$$

Da ciò, cancellando $a$ e $b$, si ricava $ab + ba = 0_R$. Dunque:

$$(\forall a, b \in R)\ (ab = -ba). \tag{$*$}$$

Applicando la $(*)$ nel caso in cui $a = b$ si ottiene, per ogni $a \in R$, $a^2 = -a^2$. Ma $a^2 = a$, quindi:

$$(\forall a \in R)\ (a = -a); \qquad \text{ovvero:} \qquad (\forall a \in R)\ (2a = 0_R). \tag{$**$}$$

In particolare, $2 \cdot 1_R = 0_R$, quindi o $1_R = 0_R$ e $R = \{0_R\}$ ha un solo elemento, oppure $|R| > 1$ e la caratteristica di $R$ è 2.

Infine, per ogni $a, b \in R$, applicando la $(**)$ all'elemento $ba$ otteniamo $-ba = ba$, quindi la $(*)$ prova $ab = ba$. È così dimostrato che $R$ è commutativo. □

Enunciamo ma non dimostriamo il teorema di Stone, che è il risultato fondamentale nella teoria degli anelli booleani.

**Teorema di Stone.** *Sia $R$ un anello booleano. Allora:*

(i) *esiste un insieme $S$ tale che $R$ sia isomorfo ad un sottoanello unitario di $(\mathcal{P}(S), \triangle, \cap)$;*
(ii) *se $R$ è finito, esiste un insieme $S$ tale che $R$ sia isomorfo a $(\mathcal{P}(S), \triangle, \cap)$.*

Va notato, a proposito del punto (i), che tutti i sottoanelli unitari di $(\mathcal{P}(S), \triangle, \cap)$ sono booleani. Infatti:

**Esercizio 2.** Se $R$ è un anello booleano ogni sottoanello unitario di $R$ è booleano.

Il teorema di Stone ha un'importante conseguenza:

**Corollario 3.** *Sia $R$ un anello booleano finito. Allora:*

(i) *$|R|$ è un potenza di 2;*
(ii) *se $A$ è un anello booleano e $|A| = |R|$, allora $A \simeq R$.*

*Dimostrazione.* Per il teorema di Stone, esiste un insieme $S$, ovviamente finito, tale che $R$ sia isomorfo a $(\mathcal{P}(S), \triangle, \cap)$. Posto $n = |S|$, allora $|R| = |\mathcal{P}(S)| = 2^n$, il che giustifica la (i). Se poi $A$ è un anello booleano, anch'esso di cardinalità $2^n$, ancora per il teorema di Stone abbiamo $A \simeq (\mathcal{P}(T), \triangle, \cap)$ per un opportuno insieme $T$. Ma allora $|\mathcal{P}(T)| = |A|$, quindi $|\mathcal{P}(T)| = 2^n$ e deduciamo così $|T| = n$. Dunque, $|T| = |S|$; questo comporta (vedi l'esercizio che segue) $(\mathcal{P}(T), \triangle, \cap) \simeq (\mathcal{P}(S), \triangle, \cap)$, quindi $A \simeq R$. □

**Esercizio 4.** Verificare che se $f\colon S \to T$ è un'applicazione biettiva, allora l'applicazione immagine $\vec{f}\colon \mathcal{P}(S) \to \mathcal{P}(T)$ è un isomorfismo di anelli da $(\mathcal{P}(S), \triangle, \cap)$ a $(\mathcal{P}(T), \triangle, \cap)$.

È bene notare che, nel teorema di Stone il caso degli anelli booleani infiniti differisce effettivamente dal caso degli anelli finiti. Esistono infatti anelli booleani infiniti che non sono isomorfi a $(\mathcal{P}(S), \triangle, \cap)$ per alcun insieme $S$. Un esempio è fornito dall'insieme $P$ costituito da tutti i sottoinsiemi $X$ di $\mathbb{N}$ tali che uno tra $X$ e $\mathbb{N} \smallsetminus X$ sia finito.[2] Non è difficile verificare (ed è un buon esercizio farlo) che $P$ è un sottoanello unitario di $(\mathcal{P}(\mathbb{N}), \triangle, \cap)$ e di conseguenza è un anello booleano. Si può però dimostrare (ma non si tratta in questo caso di un esercizio) che per ogni insieme $S$ non esistono applicazioni biettive da $P$ a $\mathcal{P}(S)$, quindi $P$, come anello, non può essere isomorfo a $(\mathcal{P}(S), \triangle, \cap)$.

---

[1] Se invece non esiste nessun $n \in \mathbb{N}^*$, tale che $n1_R = 0_R$, cioè: se $1_R$ non è periodico in $(R, +)$, allora $R$ ha per definizione caratteristica 0.

[2] una parte $X$ di un insieme $Y$ si dice cofinita in $Y$ se e solo se $Y \smallsetminus X$ è un insieme finito. Dunque, $P$ è l'insieme costituito dalle parti finite e dalle parti cofinite di $\mathbb{N}$.

## 2. Reticoli booleani

Ricordiamo[3] che un reticolo è un insieme ordinato non vuoto $(L, \leq)$ tale che, per ogni $a, b \in L$ esistano l'estremo inferiore $\inf_{(L,\leq)}\{a, b\}$ e l'estremo superiore $\sup_{(L,\leq)}\{a, b\}$ di $\{a, b\}$ in $(L, \leq)$.

Ricordiamo anche che si può, in modo equivalente, riguardare i reticoli anche come strutture algebriche. Infatti, se $(L, \leq)$ è un reticolo, si definiscono in $L$ le due *operazioni reticolari* $\vee$ e $\wedge$, ponendo, per ogni $a, b \in L$,

$$a \vee b = \sup_{(L,\leq)}\{a, b\} \qquad \text{e} \qquad a \wedge b = \inf_{(L,\leq)}\{a, b\}$$

e valgono, per $\vee$ e $\wedge$ queste proprietà algebriche:

(1) $\vee$ e $\wedge$ sono commutative;
(2) $\vee$ e $\wedge$ sono associative;
(3) valgono le leggi di assorbimento: per ogni $a, b \in L$,
   - $a \vee (a \wedge b) = a$;
   - $a \wedge (a \vee b) = a$.

Vale anche per $\vee$ e $\wedge$ una quarta proprietà, l'iteratività: per ogni $a \in L$, $a \vee a = a = a \wedge a$ (vale a dire: ogni elemento di $L$ è idempotente sia rispetto a $\vee$ che rispetto a $\wedge$). Se, viceversa, $(L, \vee, \wedge)$ è una struttura algebrica in cui $\vee$ e $\wedge$ sono due operazioni binarie che verificano (1), (2) e (3), allora si può definire in $L$ una relazione binaria $\preceq$ ponendo, per ogni $a, b \in L$,

$$a \preceq b \iff a = a \wedge b$$

e si verifica che $\preceq$ è una relazione d'ordine che rende $(L, \preceq)$ un reticolo. Inoltre, per ogni $a, b \in L$ si ha $a \vee b = \sup_{(L,\preceq)}\{a, b\}$ e $a \wedge b = \inf_{(L,\preceq)}\{a, b\}$. Dunque, $\vee$ e $\wedge$ risultano essere le operazioni reticolari in $(L, \preceq)$. Allo stesso modo, se $\vee$ e $\wedge$ sono le operazioni reticolari definite in un reticolo $(L, \leq)$, è chiaro che la relazione $\preceq$ definita sopra coincide con $\leq$.

In sintesi, fissato un insieme non vuoto $L$, se $\mathcal{A}$ è l'insieme delle relazioni d'ordine $\leq$ tali che $(L, \leq)$ sia un reticolo e $\mathcal{B}$ è l'insieme delle coppie $(\vee, \wedge)$ di operazioni binarie in $L$ che verificano le condizioni (1), (2) e (3), abbiamo definito due applicazioni tra $\mathcal{A}$ e $\mathcal{B}$. La prima è $\alpha\colon \mathcal{A} \to \mathcal{B}$, che ad una relazione d'ordine $\leq \in \mathcal{A}$ associa la coppia ordinata $(\vee, \wedge) \in \mathcal{B}$, dove $\vee$ e $\wedge$ sono le operazioni reticolari di estremo superiore ed estremo inferiore in $(L, \leq)$. La seconda applicazione è $\beta\colon \mathcal{B} \to \mathcal{A}$, che ad ogni $(\vee, \wedge) \in \mathcal{B}$ associa la relazione d'ordine $\preceq \in \mathcal{A}$ definita come sopra. Quello che abbiamo evidenziato è che $\alpha$ e $\beta$ sono l'una inversa dell'altra, quindi sono biettive.

L'esistenza di queste biezioni fa sì che sia del tutto equivalente lo studio dei reticoli (intesi come particolari insiemi ordinati) e quello delle strutture algebriche $(L, \vee, \wedge)$ per le quali valgano le condizioni (1), (2) e (3). Per questo motivo si fa riferimento a queste strutture chiamandole 'reticoli come strutture algebriche'. D'ora in avanti, dunque, per indicare un reticolo faremo indifferentemente riferimento alla strutture di insieme ordinato (indicando, ad esempio, il reticolo come $(L, \leq)$) o alla struttura algebrica (indicando il reticolo, con un abuso di terminologia, come $(L, \vee, \wedge)$; conveniamo che la prima operazione indicata è quella di estremo superiore, la seconda quella di estremo inferiore). Può essere conveniente, e lo faremo, indicare un reticolo come $(L, \leq, \vee, \wedge)$ per specificare in modo sintetico sia la relazione d'ordine che le operazioni reticolari.

Ricordiamo che anche le due possibili nozioni di isomorfismo per i reticoli (come insiemi ordinati) ed i reticoli come strutture algebriche coincidono. Va però osservato che la nozione di *sottoreticolo* è algebrica, nel senso che può essere definita solo in termini delle operazioni reticolari.

Infatti, se $(L, \leq)$ è un reticolo, un sottoreticolo di $(L, \leq)$ è per definizione un sottoinsieme non vuoto $K$ di $L$ che sia chiuso rispetto alle operazioni reticolari $\vee$ e $\wedge$ di $L$. Le operazioni indotte in $K$ da $\vee$ e $\wedge$ continuano a verificare le condizioni (1), (2) e (3) e quindi rendono $K$ un reticolo rispetto alla relazione d'ordine indotta da $\leq$ su $K$ (quest'ultima osservazione è garantita dal fatto che la relazione d'ordine del reticolo è determinata dalle operazioni reticolari: per ogni $a, b \in L$ si ha $a \leq b \iff a = a \wedge b$).

Se $a$ e $b$ sono elementi di un insieme ordinato $(S, \leq)$, si chiama intervallo chiuso di estremi $a$ e $b$, e si indica con $[a, b]_{(S,\leq)}$ (o semplicemente $[a, b]$ se il riferimento a $(S, \leq)$ può essere sottinteso) l'insieme $\{x \in S \mid a \leq x \leq b\}$, che è diverso dal vuoto se e solo se $a \leq b$ e in questo caso ha $a$ come minimo e $b$ come massimo.

**Lemma 5.** *Siano $a$ e $b$ elementi del reticolo $(L, \leq)$.*

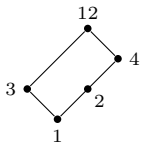
(i) *l'insieme $\{x \in L \mid a \leq x\}$ è un sottoreticolo di $(L, \leq)$;*
(ii) *l'insieme $\{x \in L \mid x \leq b\}$ è un sottoreticolo di $(L, \leq)$;*
(iii) *se $a \leq b$, l'intervallo chiuso $[a, b]$ è un sottoreticolo di $(L, \leq)$.*

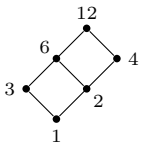
*Dimostrazione.* Sia $X = \{x \in L \mid a \leq x\}$. Certamente $X \neq \varnothing$, perché $a \in X$. Siano $x$ e $y$ elementi di $X$. Allora $a \leq x$ e $a \leq y$, quindi $a$ è un minorante di $\{x, y\}$ in $(L, \leq)$. Dunque $a \leq \inf_{(L,\leq)}\{x, y\} = x \wedge y$ e possiamo concludere $x \wedge y \in X$. Inoltre $a \leq x \leq x \vee y$, quindi $x \vee y \in X$. Abbiamo così provato che $X$ è chiuso rispetto a $\vee$ e $\wedge$, quindi è un sottoreticolo di $(L, \leq)$. È così provata la (i). Per dualità, anche $Y := \{x \in L \mid x \leq b\}$ è un sottoreticolo, quindi anche la (ii) è vera. Infine, si ha ovviamente $[a, b] = X \cap Y$, quindi $[a, b]$ è chiuso rispetto a $\vee$ e $\wedge$, in quanto intersezione di parti chiuse. Se $a \leq b$, allora $[a, b] \neq \varnothing$ e $[a, b]$ è un sottoreticolo di $L$; vale così anche (iii). □

[3] per tutto ciò che qui viene 'ricordato' e non giustificato o comunque spiegato in dettaglio, si rimanda al libro di testo o alle altre fonti a disposizione.

Ad esempio, per ogni $n \in \mathbb{N}$ sia l'insieme $\mathrm{Div}_{\mathbb{N}}(n)$ dei divisori di $n$ che quello, $n\mathbb{N}$, dei multipli di $n$ (in $\mathbb{N}$) costituiscono sottoreticoli di $(\mathbb{N}, |\,)$. Similmente, se $S$ è un insieme e $T \subseteq S$, allora sia $\mathcal{P}(T)$ che l'insieme delle parti di $S$ contenenti $T$ costituiscono sottoreticoli di $(\mathcal{P}(S), \subseteq)$.

**Esempio 6.** Sia $L = \mathrm{Div}_{\mathbb{N}}(12)$ il reticolo dei divisori di 12, rappresentato dal diagramma di Hasse a destra. Il sottoinsieme $K = L \smallsetminus \{6\}$ non è un sottoreticolo di $L$, infatti $K$ non è chiuso rispetto all'operazione reticolare $\vee$, dal momento che 2 e 3 appartengono a $K$ ma $6 = 2 \vee 3 \notin K$. Se però consideriamo $K$ come insieme ordinato dall'ordinamento indotto da quello di $L$, quindi ordinato per divisibilità, non è difficile verificare che, rispetto a questo ordinamento, $K$ è un reticolo; il suo diagramma di Hasse è rappresentato a sinistra.




Questo esempio mostra che anche se un sottoinsieme ordinato di un reticolo $L$ è, rispetto all'ordinamento indotto, a sua volta un reticolo, non è detto che esso sia un sottoreticolo di $L$.

Anche le nozioni di minimo e massimo hanno un'interpretazione algebrica.

**Lemma 7.** *Sia $(L, \leq, \vee, \wedge)$, un reticolo. Per ogni $a \in L$, $a$ è il minimo in $L$ se e solo se $a$ è elemento neutro rispetto a $\vee$; $a$ è il massimo in $L$ se e solo se $a$ è elemento neutro rispetto a $\wedge$.*

*Dimostrazione.* Si ha $a = \min L$ se e solo se $a \leq b$ per ogni $b \in L$; ma $a \leq b$ equivale a $a \vee b = b$. Dunque, $a = \min L$ se e solo se, per ogni $b \in L$ si ha $a \vee b = b$, cioè: se e solo se $a$ è neutro in $(L, \vee)$. È così provata la prima parte dell'enunciato. La seconda è duale. □

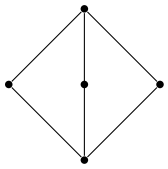
Dunque, se $(L, \leq, \vee, \wedge)$ è un un reticolo limitato (cioè dotato di minimo e massimo) sia $(L, \vee)$ che $(L, \wedge)$ sono monoidi commutativi.

Ad esempio, il reticolo $(\mathcal{P}(S), \subseteq)$ delle parti di un insieme $S$ ha minimo e massimo, rispettivamente $\varnothing$ e $S$, ed operazioni reticolari $\cup$ e $\cap$. In effetti, $\varnothing$ è l'elemento neutro del monoide $(S, \cup)$, $S$ è l'elemento neutro del monoide $(S, \cap)$.

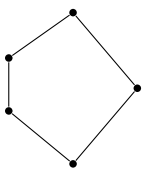
**Definizione.** Sia $(L, \leq, \vee, \wedge)$ un reticolo limitato e sia $a \in L$. Per ogni $b \in L$, $b$ è un *complemento* di $a$ in $L$ se e solo se $a \vee b = \max L$ e $a \wedge b = \min L$.

Dovrebbe essere chiaro che, con le notazioni della definizione, dire che $b$ è un complemento di $a$ equivale a dire che $a$ è un complemento di $b$. Altrettanto ovvio è che $\min L$ e $\max L$ sono l'uno complemento dell'altro (anzi, $\min L$ è l'unico complemento di $\max L$ in $L$ e, dualmente, $\max L$ è l'unico complemento di $\min L$ in $L$.) Altri esempi:

- nel reticolo $(\mathcal{P}(S), \subseteq)$ delle parti di un insieme $S$, ogni elemento ha uno ed un solo complemento. Infatti, per ogni $X \in \mathcal{P}(S)$, $X \cup (S \smallsetminus X) = S = \max \mathcal{P}(S)$ e $X \cap (S \smallsetminus X) = \varnothing = \min \mathcal{P}(S)$, quindi $S \smallsetminus X$ è un complemento di $X$ in $\mathcal{P}(S)$. L'unicità è facile da verificare direttamente, ma segue anche da considerazioni che faremo più avanti (Proposizione 9).
- Nel reticolo dei divisori di 12, visto nell'Esempio 6, gli elementi 1 e 12 (minimo e massimo del reticolo) sono l'uno complemento dell'altro, 3 e 4 sono l'uno complemento dell'altro ma né 2 né 6 hanno complemento.
- Come si vede facilmente, se $L$ è un insieme non vuoto totalmente ordinato (e quindi un reticolo) limitato, in $L$ gli unici elementi che hanno complemento sono il minimo ed il massimo.
- Anche in $(\mathbb{N}, |\,)$, gli unici elementi che hanno complemento sono il minimo, 0, ed il massimo, 1. Sia infatti $a \in \mathbb{N}$ e sia $b$ un complemento di $a$ in $(\mathbb{N}, |\,)$. Ricordando che le operazioni reticolari in $(\mathbb{N}, |\,)$ sono descritte dal minimo comune multiplo e dal massimo comun divisore, abbiamo $0 = \mathrm{mcm}(a, b)$ e $1 = \mathrm{MCD}(a, b)$. Se $a \neq 0$, allora da $\mathrm{mcm}(a, b) = 0$ segue $b = 0$, ma se $b = 0$ allora $1 = \mathrm{MCD}(a, b) = \mathrm{MCD}(a, 0) = a$. Dunque, se $a \notin \{0, 1\}$, $a$ non ha complementi in $(\mathbb{N}, |\,)$.
- Un elemento in un reticolo (limitato) può anche avere più di un complemento. Questi due esempi sono di grande importanza:



reticolo trirettangolo



reticolo pentagonale

Come si vede immediatamente, nel reticolo trirettangolo ciascuno dei tre elementi diversi dal minimo e dal massimo ha gli altri due come complementi; nel reticolo pentagonale l'elemento rappresentato più a destra ha due complementi.

Ovviamente è possibile modificare questi esempi in modo da ottenenere reticoli finiti (e quindi limitati) con elementi dotati di un numero arbitrario di complementi. (Come?)

**Definizione.** Un reticolo $L$ si dice *complementato* se e solo se ogni suo elemento ha in $L$ almeno un complemento.

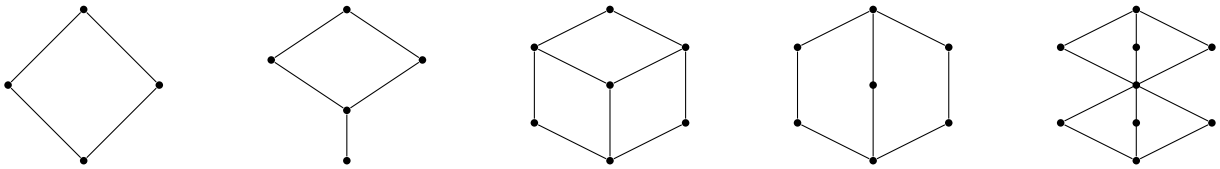
È chiaro che un reticolo, per essere complementato deve essere, in primo luogo, limitato, altrimenti in esso non possono esistere elementi dotati di complementi. Dagli esempi forniti a proposito della nozione di complemento vediamo subito che:

- per ogni insieme $S$, il reticolo $(\mathcal{P}(S), \subseteq)$ è complementato;
- un insieme non vuoto totalmente ordinato è complementato se e solo se ha al massimo due elementi;
- né $(\mathbb{N}, |\,)$ né il reticolo dei divisori di 12 sono complementati;
- il reticolo trirettangolo e quello pentagonale sono complementati.

**Esercizio 8.** Per ogni $n \in \mathbb{N}$, sia $D_n$ il reticolo dei divisori di $n$ in $\mathbb{N}$ (che è, ricordiamo, un sottoreticolo di $(\mathbb{N}, |\,)$). Lo scopo di questo esercizio è riconoscere che $D_n$ è complementato se e solo se $n$ è un intero *libero da quadrati*, cioè un intero non divisibile per il quadrato di alcun primo.[(4)]

(i) Sia $d$ un divisore (in $\mathbb{N}$) di $n$. Se $d$ e $n/d$ sono coprimi, allora $n/d$ è un complemento di $d$ in $D_n$. [*Suggerimento: basta calcolare MCD e mcm tra $d$ e $n/d$.*]
(ii) Dedurre dal punto precedente che se $n$ è libero da quadrati allora $D_n$ è complementato. [*Suggerimento: pensare alla scomposizione di $n$ in fattori primi e descrivere i divisori di $n$.*]
(iii) Supponiamo che esista un primo $p$ tale che $p^2$ divida $n$. Allora $p$ non ha complemento in $D_n$. [*Suggerimento: se $a$ è un complemento di $p$, $p$ divide o non divide $a$?*]
(iv) A questo punto la conclusione è facile: $D_n$ è complementato se e solo se $n$ è libero da quadrati.

Ulteriori esempi: dei reticoli qui rappresentati sono complementati il primo, ed il quarto, non gli altri tre.



Un'altra proprietà di natura algebrica riferita a reticoli è la distributività.

**Definizione.** Un reticolo $(L, \leq, \vee, \wedge)$ si dice *distributivo* se e solo ciascuna delle due operazioni reticolari $\vee$ e $\wedge$ è distributiva rispetto all'altra.

In termini più espliciti, $(L, \leq, \vee, \wedge)$ è distributivo se e solo se, per ogni $a, b, c \in L$ si ha:

$(d_1)$: $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$; e
$(d_2)$: $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

In realtà è possibile dimostrare che se, in un reticolo $L$, è verificata almeno una delle due condizioni $(d_1)$ e $(d_2)$ *per ogni terna $(a, b, c)$ di elementi di $L$*, allora anche l'altra è verificata e quindi $L$ è distributivo.

Ad esempio, l'operazione insiemistica di unione binaria è distributiva rispetto all'intersezione, e viceversa l'intersezione è distributiva rispetto all'unione, quindi, per ogni insieme $S$, il reticolo $(\mathcal{P}(S), \subseteq)$ è distributivo.

Non è difficile verificare (è un utile esercizio di aritmetica) che anche il reticolo $(\mathbb{N}, |\,)$ è distributivo, così come sono distributivi i reticoli totalmente ordinati (quest'ultimo fatto segue anche dal criterio di distributività di Birkhoff, che incontreremo tra poco).

Invece, non sono distributivi né il reticolo trirettangolo né il reticolo pentagonale. Questo fatto segue dal prossimo risultato, perché come abbiamo visto, in questi due reticoli esistono elementi con più complementi.

**Proposizione 9.** *Sia $(L, \leq, \vee, \wedge)$ un reticolo distributivo. Allora ogni elemento di $L$ ha al più un complemento in $L$.*

*Dimostrazione.* Sia $a \in L$, e siano $x$ e $y$ complementi di $a$ in $L$. Per provare l'enunciato occorre (e basta) verificare che $x = y$.

Indicando con 1 e 0, nell'ordine, il massimo e il minimo di $L$, si ha $a \wedge x = a \wedge y = 0$ e $a \vee x = a \vee y = 1$. Usando la proprietà distributiva abbiamo:

$$x = x \vee 0 = x \vee (a \wedge y) = (x \vee a) \wedge (x \vee y) = 1 \wedge (x \vee y) = x \vee y.$$

Analogamente, scambiando i ruoli tra $x$ e $y$, possiamo ottenenere $y = y \vee x$. Ma allora $y = y \vee x = x \vee y = x$. □

Dovrebbe essere evidente dalla definizione che ogni sottoreticolo di un reticolo distributivo è a sua volta distributivo. Di conseguenza, un reticolo distributivo non può avere sottoreticoli che siano isomorfi al reticolo trirettangolo o quello pentagonale. Un risultato notevole della teoria dei reticoli, che non dimostreremo, mostra che vale anche il viceversa: l'assenza di tali sottoreticoli basta a provare che un reticolo è distributivo.

**Criterio di distributività di Birkhoff.** *Sia $L$ un reticolo. $L$ è distributivo se e solo se non ha sottoreticoli isomorfi a uno tra il reticolo trirettangolo e il reticolo pentagonale.*

(4) i numeri naturali liberi da quadrati sono dunque 1 ed i numeri naturali che si possono scrivere come prodotti di primi a due a due distinti.

Vediamo qualche esempio di applicazione del criterio di Birkhoff. Poiché i sottoreticoli dei reticoli totalmente ordinati sono certamente totalmente ordinati, e nessuno dei due reticoli trirettangolo o pentagonale lo è, il criterio di Birkhoff fornisce una maniera per dimostrare che i reticoli totalmente ordinati sono distributivi. Siccome sia il reticolo trirettangolo che quello pentagonale sono costituiti da cinque elementi, il criterio di Birkhoff mostra anche che i reticoli con meno di cinque elementi sono sicuramente distributivi, quelli di cardinalità cinque sono distributivi se e solo se non sono isomorfi né al reticolo trirettangolo né al pentagonale. Se torniamo ai cinque reticoli esaminati come esempi dopo l'Esercizio 8, vediamo così che i primi due sono distributivi, gli altri tre no. Evidenziamo sottoreticoli trirettangoli (in blu) o pentagonali (in rosso) nei tre reticoli non distributivi:

È necessario fare attenzione al fatto che il criterio di Birkhoff esclude l'esistenza di sottoreticoli isomorfi al reticolo trirettangolo o a quello pentagonale in un reticolo distributivo $L$, ma non esclude che un sottoinsieme di $L$, munito dell'ordinamento indotto, possa essere un reticolo di uno di questi due tipi. Consideriamo il reticolo $L$ dei divisori di 12 ed il suo sottoinsieme $K = L \smallsetminus \{6\}$ discusso nell'Esempio 6. Come sappiamo, $L$ è un reticolo distributivo (è un sottoreticolo di $(\mathbb{N}, |\,)$) e, come si può vedere, $K$ è isomorfo al reticolo pentagonale. Questo non contraddice il criterio di Birkhoff, perché $K$ non è un sottoreticolo di $L$.

**Definizione.** Un reticolo si dice *booleano* se e solo se è distributivo e complementato.

Ad esempio, per ogni insieme $S$, il reticolo $(\mathcal{P}(S), \subseteq)$ è booleano. In conseguenza della definizione e della Proposizione 9, *se $L$ è un reticolo booleano, ogni elemento di $L$ ha uno ed un solo complemento in $L$.*

Osserviamo che un reticolo $L$ è complementato, distributivo o booleano, allora anche il duale di $L$ ha la stessa proprietà. Quindi vale per i reticoli con queste proprietà il principio di dualità: se una certa affermazione è verificata da ogni reticolo complementato, allora anche l'affermazione duale varrà in ogni reticolo complementato. Lo stesso è vero se nella frase precedente sostituiamo "complementato" con "distributivo" o con "booleano".

## 3. Algebre di Boole

Come sappiamo, si può dare la nozione di reticolo in termini puramente algebrici, cioè esclusivamente in termini di operazioni, senza fare riferimento a relazioni d'ordine: stiamo parlando dei reticoli 'come strutture algebriche'. Sia $(L, \wedge, \vee)$ una struttura algebrica di reticolo; vediamo quali condizioni sulle operazioni dobbiamo imporre affinché il reticolo $L$ sia booleano. Oltre alle proprietà commutativa, associativa ed alle leggi di assorbimento, che già conosciamo, devono valere le proprietà distributive (di $\vee$ rispetto a $\wedge$ e di $\wedge$ rispetto a $\vee$), che fanno sì che il reticolo $L$ sia distributivo. Sappiamo poi dal Lemma 7 che il fatto che $L$ sia limitato equivale all'esistenza di elementi neutri per $\vee$ e $\wedge$. Infine, come abbiamo visto, in un reticolo booleano ogni elemento ha un unico complemento; possiamo allora considerare l'applicazione $'\colon L \to L$ che ad ogni $a \in L$ associa il suo complemento $a'$ in $L$. Queste considerazioni suggeriscono la seguente definizione:

**Definizione.** Si dice *algebra di Boole* una struttura algebrica $(L, \vee, \wedge, 0, 1, ')$ , dove $\vee$ e $\wedge$ sono operazioni binarie, 0 e 1 operazioni nullarie e $'$ un'operazione unaria, tale che:

(1) $(L, \vee, 0)$ e $(L, \wedge, 1)$ siano monoidi commutativi;
(2) valgano le leggi di assorbimento: per ogni $a, b \in L$, $a \vee (a \wedge b) = a = a \wedge (a \vee b)$;
(3) $\vee$ sia distributiva rispetto a $\wedge$ e $\wedge$ sia distributiva rispetto a $\vee$;
(4) per ogni $a \in L$, $a \vee a' = 1$ e $a \wedge a' = 0$,

dove abbiamo indicato con $a'$ l'immagine di $a$ rispetto a $'$.

Per quanto detto sopra, ogni reticolo booleano dà luogo ad un'algebra di Boole, viceversa un'algebra di Boole si può sempre riguardare come reticolo booleano. Infatti, la (1) e la (2) esprimono esattamente il fatto che $(L, \wedge, \vee)$ è un reticolo limitato, con minimo 0 e massimo 1, come segue dal Lemma 7; la (3) dice che questo reticolo è distributivo e la (4) garantisce che ogni elemento $a$ di $L$ ha un complemento: $a'$.

Possiamo dunque dire che la nozione di algebra di Boole è la versione 'puramente algebrica' della nozione di reticolo booleano.

Abbiamo, come per tutti tipi di strutture algebriche, una nozione di isomorfismo tra algebre di Boole: un'isomorfismo da un'algebra di Boole $(L_1, \vee_1, \wedge_1, 0_1, 1_1, ')$ ad un'algebra di Boole $(L_2, \vee_2, \wedge_2, 0_2, 1_2, '')$ è un'applicazione biettiva $f\colon L_1 \to L_2$ che 'conservi le operazioni', tale cioè che, per ogni $a, b \in L_1$ si abbia

i.) $f(a \vee_1 b) = f(a) \vee_2 f(b)$ e $f(a \wedge_1 b) = f(a) \wedge_2 f(b)$;
ii.) $f(0_1) = 0_2$ e $f(1_1) = 1_2$;
iii.) $f(a') = (f(a))''$.

Ora, la i.), cioè il proprietà che $f$ conservi le operazioni reticolari, equivale al fatto che la biezione $f$ sia un isomorfismo di reticoli. Se questa proprietà è verificata valgono però anche la ii.) e la iii.). Infatti, se $f$ è un isomorfismo di reticoli da $L_1$ a $L_2$, allora $f$ deve mandare il minimo $0_1$ di $L_1$ nel minimo $0_2$ di $L_2$ e, analogamente, $1_1 = \max L_1$ in $1_2 = \max L_2$. Vale così la ii.). Inoltre, per ogni $a \in L_1$, poiché $a'$ è un complemento di $a$ in $L_1$,

la sua immagine $f(a')$ deve essere un complemento di $f(a)$ in $L_2$. Ma, poiché $L_2$ è booleano, $(f(a))''$ è l'unico complemento di $f(a)$ in $L_2$, quindi $f(a') = (f(a))''$. Quello che abbiamo verificato è che gli isomorfismi di algebre di Boole da $L_1$ a $L_2$ sono tutti e soli gli isomorfismi di reticoli da $L_1$ a $L_2$. In particolare due algebre di Boole sono isomorfe (come algebre di Boole) se e solo se sono isomorfe come reticoli. A questo punto possiamo davvero concludere che lo studio delle algebre di Boole equivale allo studio dei reticoli booleani.

**Definizione.** Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole. Una parte non vuota $K$ di $L$ ne costituisce una *sottoalgebra di Boole* se e solo se $K$ è un sottomonoide sia di $(L, \vee)$ che di $(L, \wedge)$ e contiene il complemento in $L$ di ogni suo elemento.

In modo più esplicito, $K$ costituisce una sottoalgebra di Boole di $(L, \vee, \wedge, 0, 1, ')$ se e solo se $K \subseteq L$ e sono verificate queste condizioni: per ogni $a, b \in K$,

- $a \vee b \in K$ e $a \wedge b \in K$;
- $0 \in K$ e $1 \in K$;
- $a' \in K$.

È evidente che in queste condizioni $K$, munita delle operazioni indotte da quelle di $L$ è a sua volta un'algebra di Boole.

La nozione di sottoalgebra di Boole differisce da quella di sottoreticolo. Infatti, un sottoreticolo $K$ di un reticolo booleano $L$ deve essere chiuso rispetto alle due operazioni reticolari (quindi deve verificare la prima delle tre condizioni appena elencate), ma non contiene necessariamente il massimo o il minimo del reticolo né, tanto meno, i complementi dei suoi elementi.

**Esempio 10.** Dato un insieme $S \neq \varnothing$, consideriamo il reticolo booleano $(\mathcal{P}(S), \subseteq)$. Questo si struttura come algebra di Boole nella forma $(\mathcal{P}(S), \cup, \cap, \varnothing, S, ^c)$, dove $^c$ è l'applicazione "complemento" che manda ogni $X \in \mathcal{P}(S)$ in $X^c = S \smallsetminus X \in \mathcal{P}(S)$. Se $T$ è una parte propria di $S$, allora $\mathcal{P}(T)$ costituisce un sottoreticolo di $\mathcal{P}(S)$ (ad esempio, per il Lemma 5), ma non una sottoalgebra di Boole di $\mathcal{P}(S)$, dal momento che $S \notin \mathcal{P}(T)$.

Nel caso appena considerato, $(\mathcal{P}(T), \subseteq)$ è comunque un reticolo booleano, quindi si struttura come algebra di Boole. Ma in altri casi la situazione puo' essere diversa. Ad esempio, se supponiamo $\varnothing \neq T \subset S$, allora $\{\varnothing, T, S\}$ forma un sottoreticolo di $(\mathcal{P}(S), \subseteq)$ che non è complementato e quindi non è booleano.

**Esercizio 11.** Provare che un parte di un'algebra di Boole ne è una sottoalgebra di Boole se e solo se è un sottoreticolo che contenga il complemento di ogni suo elemento.

Il prossimo enunciato elenca alcune identità che valgono nelle algebre di Boole. La terza si esprime dicendo che l'operazione di complemento è involutoria, cioè coincide con l'applicazione inversa di sé stessa (e, in particolare, è biettiva); le ultime due sono le note come leggi di De Morgan per algebre di Boole.

**Proposizione 12.** *Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole. Allora, per ogni $a, b \in L$,*

(i) $1 \vee a = 1$ *e* $0 \wedge a = 0$;
(ii) $1' = 0$ *e* $0' = 1$;
(iii) $(a')' = a$;
(iv) $(a \vee b)' = a' \wedge b'$;
(v) $(a \wedge b)' = a' \vee b'$.

*Dimostrazione.* La (i) e la (ii) sono immediate: visto $L$ come reticolo, e quindi come insieme ordinato, 1 e 0 ne sono il massimo e il minimo e le operazioni $\vee$ e $\wedge$ forniscono estremi superiori e inferiori, dunque $1 \vee a = \sup\{1, a\} = 1$ e $0 \wedge a = \inf\{0, a\} = 0$;[(5)] inoltre, come sappiamo, minimo e massimo sono sempre l'uno il complemento dell'altro.

Anche la (iii) è pressoché ovvia: essendo $a'$ un complemento di $a$, $a$ è un complemento di $a'$. Anche $(a')'$ è un complemento di $a'$; l'unicità dei complementi nei reticoli booleani comporta $a = (a')'$.

Sempre per l'unicità del complemento, per provare la (iv) basterà mostrare che $a' \wedge b'$ è un complemento di $a \vee b$, cioè $(a \vee b) \vee (a' \wedge b') = 1$ e $(a \vee b) \wedge (a' \wedge b') = 0$. Usando la distributività e la (i), abbiamo $(a \vee b) \vee (a' \wedge b') = (a \vee b \vee a') \wedge (a \vee b \vee b') = (a \vee a' \vee b) \wedge (a \vee b \vee b') = (1 \vee b) \wedge (a \vee 1) = 1 \wedge 1 = 1$ e, in modo simmetrico, $(a \vee b) \wedge (a' \wedge b') = (a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') = (a \wedge a' \wedge b') \vee (b \wedge b' \wedge a') = (0 \wedge b') \vee (0 \wedge a') = 0 \vee 0 = 0$. È così provata la (iv). La (v) segue per dualità. □

Ad illustrazione della Proposizione 12, leggiamo le identità appena provate nel caso in cui l'algebra di Boole $L$ che appare nell'enunciato sia l'algebra delle parti di un insieme $S$, cioè $(\mathcal{P}(S), \cup, \cap, \varnothing, S, ^c)$, dove, come nell'Esempio 10 $^c$: $X \in \mathcal{P}(S) \mapsto S \smallsetminus X \in \mathcal{P}(S)$. In questo caso la Proposizione 12 esprime cinque ben note formule insiemistiche elementari: per ogni $a, b \in \mathcal{P}(S)$, (i): $S \cup a = S$ e $\varnothing \cap a = \varnothing$; (ii): $S \smallsetminus S = \varnothing$ e $S \smallsetminus \varnothing = S$; (iii): $S \smallsetminus (S \smallsetminus a) = a$; (iv): $S \smallsetminus (a \cup b) = (S \smallsetminus a) \cap (S \smallsetminus b)$ e (v): $S \smallsetminus (a \cap b) = (S \smallsetminus a) \cup (S \smallsetminus b)$.

**Esercizio 13.** Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole. Allora anche $(L, \wedge, \vee, 1, 0, ')$ è un'algebra di Boole, quella costruita a partire dal reticolo booleano $(L, \wedge, \vee)$, il duale di $(L, \vee, \wedge)$. Verificare che l'applicazione $'$ è un isomorfismo tra queste due algebre di Boole. Questa è una riformulazione della Proposizione 12. Notare la conseguenza: ogni reticolo booleano è isomorfo al suo duale.

[(5)] oppure, per via algebrica: dal momento che 1 è neutro rispetto a $\wedge$, $1 \wedge a = a$, quindi, per una delle leggi di assorbimento, $1 = 1 \vee (1 \wedge a) = 1 \vee a$; analogamente si procede per 0.

## 4. Anelli booleani e algebre di Boole

In questa sezione arriveremo a provare che le nozioni di anello booleano e di reticolo booleano (ovvero di algebra di Boole) sono in sostanza interscambiabili, nel senso che si può costruire una struttura di reticolo booleano su ogni anello booleano e, viceversa, una struttura di anello booleano su ogni reticolo booleano, in modo che queste due costruzioni siano l'una inversa dell'altra.

In primo luogo, partendo da un anello booleano $(R, +, \cdot)$ vogliamo definire una struttura di reticolo booleano su $R$. L'esempio dell'anello delle parti di un insieme può suggerirci in che modo procedere. Fissato un insieme $S$, infatti, $(\mathcal{P}(S), \triangle, \cap)$ è un anello booleano ma $\mathcal{P}(S)$ è anche un reticolo booleano, con operazioni reticolari $\cup$ e $\cap$. La seconda operazione reticolare è proprio l'operazione di moltiplicazione nell'anello. Anche la prima operazione reticolare si può esprimere in termini delle operazioni dell'anello: per ogni $A, B \in \mathcal{P}(S)$ abbiamo infatti $A \cup B = (A \triangle B) \cup (A \cap B) = (A \triangle B) \triangle (A \cap B)$. Inoltre il minimo ed il massimo del reticolo sono $\varnothing$ e $S$, cioè lo zero e l'unità dell'anello, e ciascun $A \in \mathcal{P}(S)$ ha come complemento, nel reticolo $(\mathcal{P}(S), \subseteq)$, l'insieme $S \smallsetminus A = S \triangle A = 1_{\mathcal{P}(S)} \triangle A$.

Passando ora ad un arbitrario anello booleano $(R, +, \cdot, 0_R, 1_R)$, dove $0_R$ e $1_R$ sono lo zero l'unità dell'anello, l'esempio di $\mathcal{P}(S)$ suggerisce di definire in $R$ l'operazione binaria $\vee$ ponendo, per ogni $a, b \in R$,

$$a \vee b := a + b + ab$$

e l'applicazione $'\colon a \in R \mapsto 1_R + a \in R$ da utilizzare come operazione unaria di complemento.

**Proposizione 14.** *Con le notazioni appena fissate, $(R, \vee, \cdot, 0_R, 1_R, ')$ è un'algebra di Boole.*

*Dimostrazione.* Dobbiamo verificare che $(R, \vee, 0_R)$ e $(R, \cdot, 1_R)$ siano monoidi commutativi, che valgano per $\vee$ e $\cdot$ le leggi di assorbimento e le proprietà distributive,[(6)] ed infine che l'applicazione $'$ verifichi la condizione richiesta dalla definizione di complemento.

Che $\vee$ sia commutativa è evidente, ed è anche chiaro che $a \vee 0_R = a + 0_R + a0_R = a$ per ogni $a \in R$, quindi $0_R$ è neutro rispetto a $\vee$. Proviamo l'associatività di $\vee$: per ogni $a, b, c \in R$ si ha $(a \vee b) \vee c = (a + b + ab) \vee c = (a+b+ab)+c+(a+b+ab)c = a+b+c+ab+ac+bc+abc$. Si ha quindi $a \vee (b \vee c) = (b \vee c) \vee a = b+c+a+bc+ba+ca+bca$; dunque $(a \vee b) \vee c = a \vee (b \vee c)$. È così provato che $\vee$ è associativa; $(R, \vee, 0_R)$ è quindi un monoide commutativo. Che lo sia anche $(R, \cdot, 1_R)$ è già noto in partenza, dal momento che $R$ è un anello booleano.

Verifichiamo le leggi di assorbimento. Per ogni $a, b \in R$, $a \vee (ab) = a + ab + a(ab)$. Dal momento che $R$ è booleano, $a(ab) = a^2b = ab$ e $ab + ab = 0_R$, quindi $a \vee (ab) = a + ab + ab = a$. Inoltre $a(a \vee b) = a(a + b + ab) = a^2 + ab + a^2b = a + ab + ab = a$. Le leggi di assorbimento sono così provate. A questo punto già possiamo concludere che $(R, \vee, \cdot)$ è un reticolo limitato.

Verifichiamo ora che $\cdot$ è distributiva rispetto a $\vee$. Per ogni $a, b, c \in R$ si ha $a(b \vee c) = a(b + c + bc) = ab + ac + abc$ e $(ab) \vee (ac) = ab + ac + (ab)(ac) = ab + ac + abc$, dunque $a(b \vee c) = (ab) \vee (ac)$. Pertanto, utilizzando anche la proprietà commutativa, possiamo concludere che $\cdot$ è distributiva rispetto a $\vee$.

Anche se non è strettamente necessario, verifichiamo anche che $\vee$ è distributiva rispetto a $\cdot$. Per ogni $a, b, c \in R$ abbiamo $a \vee (bc) = a + bc + abc$ e $(a \vee b)(a \vee c) = (a + b + ab)(a + c + ac) = a + ac + ac + ab + bc + abc + ab + abc + abc = a + bc + abc = a \vee (bc)$. Dunque, $\vee$ è distributiva rispetto a $\cdot$.

Resta infine da dimostrare che, per ogni $a \in R$, l'immagine di $a$ mediante l'applicazione $'$, vale a dire $a' := 1_R + a$, verifica le condizioni $a \vee (1_R + a) = 1_R$ e $aa' = 0_R$. Questo è molto facile: per ogni $a \in R$ si ha $aa' = a(1_R + a) = a + a = 0_R$ e $a \vee a' = a + a' + aa' = a + (1_R + a) + 0_R = 1_R$, come richiesto. Con questo la dimostrazione è completa □

Descriviamo ora la costruzione inversa: quella di un anello booleano a partire da un'algebra di Boole. Anche in questo caso ci facciamo guidare dall'esempio dell'algebra $(\mathcal{P}(S), \cup, \cap, \varnothing, S, ^c)$ delle parti di un insieme $S$ (come nell'Esempio 10, il simbolo $^c$ rappresenta l'operazione unaria di complemento in $S$). Delle due operazioni binarie dell'anello (booleano) $(\mathcal{P}(S), \triangle, \cap)$, quella di moltiplicazione, $\cap$, è già tra le operazioni dell'algebra di Boole. Per esprimere l'altra, la differenza simmetrica, utilizzando le operazioni dell'algebra di Boole ci è utile osservare che se $A$ e $B$ sono parti di $S$, allora $A \smallsetminus B = A \cap (S \smallsetminus B) = A \cap B^c$. Dunque $A \triangle B$ può essere scritta come $(A \smallsetminus B) \cup (B \smallsetminus A) = (A \cap B^c) \cup (B \cap A^c)$ o anche come $(A \cup B) \smallsetminus (A \cap B) = (A \cup B) \cap (A \cap B)^c$. Queste esempio suggerisce due possibili modi per definire, in un'arbitraria algebra di Boole $(L, \vee, \wedge, 0, 1, ')$, un'operazione binaria di addizione $+$ analoga alla differenza simmetrica in $\mathcal{P}(S)$. Il prossimo lemma mostra che queste due possibilità portano allo stesso risultato.

**Lemma 15.** *Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole. Allora, per ogni $a, b \in L$ si ha $(a \wedge b') \vee (a' \wedge b) = (a \vee b) \wedge (a \wedge b)'$.*

*Dimostrazione.* Usando la proprietà distributiva di $\vee$ rispetto a $\wedge$, abbiamo:

$$(a \wedge b') \vee (a' \wedge b) = (a \vee a') \wedge (a \vee b) \wedge (b' \vee a') \wedge (b' \vee b) = 1 \wedge (a \vee b) \wedge (b' \vee a') \wedge 1 = (a \vee b) \wedge (a' \vee b') = (a \vee b) \wedge (a \wedge b)',$$

avendo utilizzato, per l'ultimo passaggio, una delle leggi di De Morgan (Proposizione 12 (v)). □

(6) in realtà, per un'osservazione fatta a margine della definizione di reticolo distributivo, basterebbe dimostrare una sola delle due proprietà distributive.

Anche quest'altra osservazione può essere utile:

**Lemma 16.** *Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole. Allora, per ogni $a, b \in L$ si ha $(a \wedge b)' \wedge (a \wedge c) = a \wedge b' \wedge c$.*

*Dimostrazione.* Utilizzando una delle formule di De Morgan, $(a \wedge b)' \wedge (a \wedge c) = (a' \vee b') \wedge a \wedge c = \big((a' \wedge a) \vee (b' \wedge a)\big) \wedge c = \big(0 \vee (b' \wedge a)\big) \wedge c = a \wedge b' \wedge c$. □

**Proposizione 17.** *Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole. Se $+$ è l'operazione binaria definita in $L$ ponendo, per ogni $a, b \in L$, $a + b = (a \wedge b') \vee (a' \wedge b)$, allora $(L, +, \wedge)$ è un anello booleano, con zero $0$ e unità $1$.*

*Dimostrazione.* Iniziamo col verificare che $(L, +)$ è un gruppo abeliano. Poiché $\vee$ e $\wedge$ sono commutative, è evidente che $+$ è commutativa. Per ogni $a, b, c \in L$ abbiamo:

$$\begin{aligned}
(a+b)+c &= \big((a \wedge b') \vee (a' \wedge b)\big) + c \\
&= \big(\big((a \wedge b') \vee (a' \wedge b)\big) \wedge c'\big) \vee \big(\big((a \wedge b') \vee (a' \wedge b)\big)' \wedge c\big) \\
&= \big(\big((a \wedge b') \vee (a' \wedge b)\big) \wedge c'\big) \vee \big(\big((a \vee b) \wedge (a \wedge b)'\big)' \wedge c\big) && \text{[usando il Lemma 15]} \\
&= \big(\big((a \wedge b') \vee (a' \wedge b)\big) \wedge c'\big) \vee \big(\big((a' \wedge b') \vee (a \wedge b)\big) \wedge c\big) && \text{[usando la Proposizione 12]} \\
&= \big((a \wedge b' \wedge c') \vee (a' \wedge b \wedge c')\big) \vee \big((a' \wedge b' \wedge c) \vee (a \wedge b \wedge c)\big) \\
&= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c) \vee (a \wedge b \wedge c).
\end{aligned}$$

Poiché $+$ è commutativa, abbiamo quindi anche $a+(b+c) = (b+c)+a = (b \wedge c' \wedge a') \vee (b' \wedge c \wedge a') \vee (b' \wedge c' \wedge a) \vee (b \wedge c \wedge a)$ ed allora, per la commutatività di $\wedge$ e $\vee$, $a + (b + c) = (a + b) + c$. Pertanto $+$ è associativa. Per ogni $a \in L$ vale $a + 0 = (a \wedge 0') \vee (a' \wedge 0) = (a \wedge 1) \vee 0 = a \vee 0 = a$, quindi $0$ è neutro rispetto a $+$. Inoltre, sempre per ogni $a \in L$, $a + a = (a \wedge a') \vee (a' \wedge a) = 0 \vee 0 = 0$, quindi ogni elemento di $L$, rispetto a $+$, è il simmetrico di sé stesso. Dunque $(L, +)$ è un gruppo abeliano, con elemento neutro $0$.
Sappiamo dalla definizione di algebra di Boole che $(L, \wedge, 1)$ è un monoide commutativo. Verifichiamo la distributività di $\wedge$ rispetto a $+$. Per ogni $a, b, c \in L$ abbiamo:

$$a \wedge (b + c) = a \wedge \big((b \wedge c') \vee (b' \wedge c)\big) = (a \wedge b \wedge c') \vee (a \wedge b' \wedge c)$$

e, utilizzando due volte il Lemma 16,

$$(a \wedge b) + (a \wedge c) = \big((a \wedge b) \wedge (a \wedge c)'\big) \vee \big((a \wedge b)' \wedge (a \wedge c)\big) = (a \wedge b \wedge c') \vee (a \wedge b' \wedge c),$$

quindi $a \wedge (b + c) = (a \wedge b) + (a \wedge c)$.
A questo punto abbiamo dimostrato che $(L, +, \wedge)$ è un anello (commutativo) unitario, con $0$ e $1$ come zero e unità. Per ogni $a \in L$ vale $a^2 = a \wedge a = a$, quindi questo anello è booleano. La dimostrazione è così completa. □

Abbiamo così visto che ogni anello booleano $(R, +, \cdot)$ determina una struttura di algebra di Boole sul suo stesso sostegno: $(R, \vee, \cdot, 0_R, 1_R, ')$, definita come nella Proposizione 14. Per la Proposizione 17, questa definisce a sua volta un anello booleano, indichiamolo come $(R, \oplus, \cdot)$, con operazione additiva $\oplus$ definita da: per ogni $a, b \in R$

$$a \oplus b = (ab') \vee (a'b) \in R.$$

Ora, scelti comunque $a, b \in R$, poiché, in accordo con la Proposizione 14, per ogni $u, v \in R$, abbiamo $u' = 1_R + u$ (e $uu' = 0_R$) e $u \vee v = u + v + uv$,

$$(ab') \vee (a'b) = (ab') + (a'b) + (ab')(a'b) = (ab') + (a'b) + aa'bb' = a(1_R + b) + (1_R + a)b + 0_R = a + ab + b + ab = a + b,$$

ricordando che $ab + ab = 0_R$. Dunque, l'operazione additiva $\oplus$ dell'anello booleano costruito a partire da $(R, \vee, \cdot, 0_R, 1_R, ')$ non è altro che l'originale addizione in $(R, +, \cdot)$.

Questo significa che, dato un anello booleano $R$, se si costruisce un'algebra di Boole su $R$ come indicato nella Proposizione 14 e poi, a partire da quest'ultima, si costruisce un anello booleano come indicato nella Proposizione 17, questo anello è precisamente l'anello $R$ da cui si era partiti.

Lo stesso vale se si fa il discorso inverso. Se, partendo da un'algebra di Boole $(L, \vee, \wedge, 0, 1, ')$, si definisce l'anello booleano $(L, +, \wedge)$ come nella Proposizione 17 e poi si usa la Proposizione 14 per costruire un'algebra di Boole $(L, \curlyvee, \wedge, 0, 1, '')$ a partire da questo anello, l'algebra così ottenuta è quella originaria. Per provarlo, basta verificare che l'operazione $\curlyvee$ coincide con $\vee$. Infatti, una volta stabilito ciò, si ha che le due strutture di reticolo booleano su $L$, l'originale $(L, \vee, \wedge)$ e la "nuova" $(L, \curlyvee, \wedge)$, coincidono, quindi lo stesso è vero per le corrispondenti algebre di Boole.

Verifichiamo $\curlyvee = \vee$. Scelti comunque $a, b \in L$, le costruzioni in Proposizione 17 e Proposizione 14 dànno $a \curlyvee b = a + b + (a \wedge b)$ e $a + b = (a \wedge b') \vee (a' \wedge b)$. Come caso particolare, per ogni $c \in L$ si ha $c + 1 = (c \wedge 1') \vee (c' \wedge 1) = (c \wedge 0) \vee (c' \wedge 1) = c'$, perché $1$ e $1' = 0$ sono l'unità e lo zero di $(L, +\wedge)$. Allora $a \curlyvee b = (a + b) + (a \wedge b) = ((a + b + 1) \wedge (a \wedge b)) \vee ((a + b) \wedge ((a \wedge b) + 1))$, ma $(a + b) \wedge (a \wedge b) = 2(a \wedge b) = 0$ perché $(L, +\wedge)$ è booleano,[7] dunque $a \curlyvee b = (a \wedge b) \vee (a + b) = (a \wedge b) \vee (a' \wedge b) \vee (a \wedge b') = a \vee b$, perché se $x \in \{a, b\}$, $y \in \{a', b\}$ e $z \in \{a, b'\}$, si ha $x \vee y \vee z = 1$ a meno che $(y, z) = (b, a)$, nel qual caso $x \vee y \vee z = a \vee b$. Quindi, effettivamente, $\curlyvee$ coincide con $\vee$. Possiamo sintetizzare quanto abbiamo dimostrato nel seguente teorema.

[7] usando le notazioni consuete per gli anelli, quindi $\cdot$ al posto di $\wedge$, $(a + b) \wedge (a \wedge b)$ si scrive come $(a + b)ab = a^2b + ab^2 = 2ab = 0$.

**Teorema 18.** *Sia $L$ un insieme. Sia $\mathcal{A}$ l'insieme delle coppie ordinate $(\vee, \wedge)$ di operazioni binarie in $L$ che strutturano $L$ come algebra di Boole, e sia $\mathcal{B}$ l'insieme delle coppie ordinate $(+, \cdot)$ di operazioni binarie in $L$ che strutturano $L$ come anello booleano. Allora le costruzioni descritte dalla Proposizione 14 e dalla Proposizione 17 definiscono due applicazioni, da $\mathcal{B}$ a $\mathcal{A}$ e da $\mathcal{A}$ a $\mathcal{B}$, che sono l'una inversa dell'altra, quindi biettive.*

Questa corrispondenza tra algebre di Boole e anelli booleani conserva la nozione di isomorfismo.

**Proposizione 19.** *Siano $(L_1, \vee_1, \wedge_1, 0_1, 1_1, ')$ e $(L_2, \vee_2, \wedge_2, 0_2, 1_2, '')$ algebre di Boole e $(L_1, +_1, \wedge_1)$ e $(L_2, +_2, \wedge_2)$ i corrispondenti (nel senso del Teorema 18) anelli booleani. Sia poi $f\colon L_1 \to L_2$ un'applicazione biettiva. Allora $f$ è un isomorfismo di algebre di Boole se e solo se è un isomorfismo di anelli booleani.*

*Dimostrazione.* Sia $f$ un isomorfismo di algebre di Boole. Allora, per ogni $a, b \in L_1$ si ha

$$f(a +_1 b) = f\big((a \vee_1 b') \wedge_1 (a' \vee_1 b)\big) = \big(f(a) \vee_2 f(b)''\big) \wedge_2 \big(f(a)'' \vee_2 f(b)\big) = f(a) +_2 f(b)$$

e, ovviamente, $f(a \wedge_1 b) = f(a) \wedge_2 f(b)$. Quindi $f$ è un isomorfismo di anelli booleani. Viceversa, se $f$ è un isomorfismo di anelli booleani, allora, per ogni $a, b \in L_1$ si ha $f(a \wedge_1 b) = f(a) \wedge_2 f(b)$ e

$$f(a \vee_1 b) = f\big(a +_1 b +_1 (a \wedge_1 b)\big) = f(a) +_2 f(b) +_2 \big(f(a) \wedge_2 f(b)\big) = f(a) \vee_2 f(b).$$

Dunque $f$ conserva le operazioni reticolari ed è quindi un isomorfismo di reticoli da $L_1$ a $L_2$. Come già sappiamo dalla sezione 4, da ciò segue che $f$ è un isomorfismo di algebre di Boole. □

A questo punto possiamo concludere che lo studio degli anelli booleani equivale a quello delle algebre di Boole, e quindi a quello dei reticoli booleani. Vediamo anche che le sottoalgebre di Boole corrispondono precisamente ai sottoanelli unitari.

**Proposizione 20.** *Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole e sia $(L, +, \wedge)$ il corrispondente anello booleano (nel senso del Teorema 18). Sia $K \subseteq L$. Allora $K$ è una sottoalgebra di Boole di $(L, \vee, \wedge, 0, 1, ')$ se e solo se è un sottoanello unitario di $(L, +, \wedge)$.*

*Dimostrazione.* Sia $K$ una sottoalgebra di Boole. Allora, per ogni $a, b \in K$, si ha $a + b = (a \wedge b') \vee (a' \wedge b) \in K$, quindi $K$ è chiusa rispetto a $+$. Dal momento che $(L, +, \wedge)$ è booleano, ogni elemento di $L$ coincide col suo opposto. Da ciò segue che $K$ è un sottogruppo di $(L, +)$. Ovviamente, poiché $K$ è una sottoalgebra, $K$ è un sottomonoide di $(K, \wedge, 1)$. Dunque, $K$ è un sottoanello unitario di $(L, +, \wedge)$.

Viceversa, se $K$ è un sottoanello unitario di $(L, +, \wedge)$, allora $K$ è un sottomonoide di $(L, \wedge, 1)$. Inoltre $0 \in K$, per ogni $a \in K$ si ha $a' = 1 + a \in K$ e dunque, per ogni $a, b \in K$, $a \vee b = (a \wedge b') + (a' \wedge b) \in K$. Concludiamo che $K$ è anche un sottomonoide di $(L, \vee, 0)$ e contiene il complemento in $L$ di ogni suo elemento. Dunque, $K$ è una sottoalgebra di Boole di $(L, \vee, \wedge, 0, 1, ')$. □

Da questi ultimi risultati e dal teorema di Stone per anelli booleani seguono subito i teoremi di Stone per algebre di Boole e per reticoli booleani.

**Teorema di Stone** (per algebre di Boole)**.** *Sia $L$ un'algebra di Boole. Allora:*

(i) *esiste un insieme $S$ tale che $L$ sia isomorfa ad una sottoalgebra di Boole dell'algebra delle parti $(\mathcal{P}(S), \cup, \cap, \varnothing, S, ^c)$ di $S$;*
(ii) *se $L$ è finita, esiste un insieme $S$ tale che $L$ sia isomorfa all'algebra delle parti $(\mathcal{P}(S), \cup, \cap, \varnothing, S, ^c)$ di $S$.*

**Teorema di Stone** (per reticoli booleani)**.** *Sia $L$ un reticolo booleano. Allora:*

(i) *esiste un insieme $S$ tale che $L$ sia isomorfo ad un sottoreticolo del reticolo $(\mathcal{P}(S), \subseteq)$ delle parti di $S$;*
(ii) *se $L$ è finito, esiste un insieme $S$ tale che $L$ sia isomorfo al reticolo $(\mathcal{P}(S), \subseteq)$ delle parti di $S$.*

Naturalmente, in conseguenza di questi teoremi, valgono anche per le algebre di Boole finite ed i reticoli booleani finiti le conseguenze osservate nel Corollario 3 per gli anelli booleani: tutte le algebre di Boole finite e tutti i reticoli booleani finiti hanno per cardinalità una potenza di 2; se due algebre di Boole finite sono equipotenti (cioè hanno lo stesso numero di elementi) allora esse sono isomorfe; se due reticoli booleani finiti sono equipotenti allora essi sono isomorfi.

## 5. Anelli booleani, stringhe di zeri e uno ed operazioni bit a bit

In questa sezione faremo alcune osservazioni ed esempi su una delle situazioni in cui, in informatica, capita di incontrare strutture booleane.

Iniziamo da un accenno ad una costruzione generale. Fissiamo un anello $R$ ed un intero positivo $n$. L'insieme $R^n$ delle $n$-ple di elementi di $R$ si può strutturare come anello definendo operazioni binarie di addizione e moltiplicazione "componente per componente", cioè in questo modo: per ogni $\underline{a} = (a_1, a_2, \dots, a_n)$ e $\underline{b} = (b_1, b_2, \dots, b_n)$ appartenenti a $R$ si pone

$$\underline{a} + \underline{b} = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n) \qquad \text{e} \qquad \underline{a} \cdot \underline{b} = (a_1 b_1, a_2 b_2, \dots, a_n b_n); \tag{$*$}$$

abbiamo indicato con $+$ e $\cdot$ sia le operazioni in $R$ che quelle in $R^n$. È un semplice esercizio la verifica del fatto che in questo modo $R^n$ si struttura come anello (con $(0_R, 0_R, \dots, 0_R)$ come zero e, se $R$ è unitario, $(1_R, 1_R, \dots, 1_R)$ come unità) e che $R^n$ è booleano se $R$ è booleano.

Consideriamo il caso in cui $R$ è l'anello $\mathbb{Z}_2$ degli interi modulo 2. Dal momento che $\mathbb{Z}_2$ è booleano, anche $\mathbb{Z}_2^n$ è booleano. I suoi elementi sono le $n$-ple di elementi di $\mathbb{Z}_2$, quindi le $n$-ple $(a_1, a_2, \dots, a_n)$ dove ciascuno degli $a_i$ è uno dei due elementi di $\mathbb{Z}_2$: o $[0]_2$ oppure $[1]_2$. Ovviamente $|\mathbb{Z}_2^n| = 2^n$. Per semplificare la notazione possiamo scrivere 0 e 1 per $[0]_2$ e $[1]_2$ e rappresentare le $n$-ple come stringhe di lunghezza $n$, vale a dire, se, ad esempio, $n = 5$, scriviamo '$a_1a_2a_3a_4a_5$' piuttosto che $(a_1, a_2, a_3, a_4, a_5)$. Per esempio, sempre per $n = 5$, la stringa '10100' sta per $([1]_2, [0]_2, [1]_2, [0]_2, [0]_2) \in \mathbb{Z}_2^5$.

Con queste notazioni, dette $\underline{a} =$ '$a_1a_2 \dots a_n$' e $\underline{b} =$ '$b_1b_2 \dots b_n$' due stringhe appartenenti a $\mathbb{Z}_2^n$, abbiamo $\underline{a} + \underline{b} =$ '$s_1s_2 \dots s_n$' e $\underline{a} \cdot \underline{b} =$ '$p_1p_2 \dots p_n$', dove, per ogni $i \in \{1, 2, \dots, n\}$, $s_i$ è la somma e $p_i$ il prodotto di $a_i$ e $b_i$ in $\mathbb{Z}_2$, quindi $s_i = 0$ se $a_i = b_i$ e $s_i = 1$ se $a_i \neq b_i$, mentre $p_i = 1$ se $a_i = b_i = 1$ e $p_i = 0$ negli altri casi.

Molto probabilmente, chi legge riconosce in queste regole di calcolo le operazioni 'bit a bit' su "stringhe di zeri e uno" di fissata lunghezza con cui funzionano gli elaboratori elettronici, associate ai connettivi (operatori) logici XOR e AND. Quello che stiamo qui dicendo è che

*queste operazioni 'bit a bit' non sono altro che le due operazioni binarie dell'anello booleano $\mathbb{Z}_2^n$.*

Naturalmente lo stesso discorso si può estendere alle operazioni che, ai sensi della Proposizione 14, strutturano $\mathbb{Z}_2^n$ come algebra di Boole. Indicando con $\underline{1}$ la stringa '$11 \dots 1$' (di lunghezza $n$), che è l'unità di $\mathbb{Z}_2^n$, il complemento di $\underline{a} =$ '$a_1a_2 \dots a_n$' in $\mathbb{Z}_2^n$ sarà $\underline{1} + \underline{a}$ che, come si verifica subito, è la stringa ottenuta sostituendo in $\underline{a}$ ogni 0 con 1 ed ogni 1 con 0; quello che abbiamo descritto è l'operatore NOT. Se poi $\underline{b} =$ '$b_1b_2 \dots b_n$' $\in \mathbb{Z}_2^n$, è facile verificare che $\underline{a} \vee \underline{b} =$ '$l_1l_2 \dots l_n$', dove, per ogni $i$, $l_i = 0$ se $a_i = b_i = 0$ e $l_i = 1$ altrimenti; un modo per farlo è osservare che per le leggi di De Morgan (Proposizione 12) $\underline{a} \vee \underline{b} = \underline{1} + \big((\underline{1} + \underline{a})(\underline{1} + \underline{b})\big)$. Dunque $\vee$ coincide con l'operatore OR bit a bit.

**Esercizio 21.** Verificare la correttezza della definizione dell'anello $R^n$ data all'inizio di questa sezione e le proprietà di $R^n$ lì indicate.

Più in generale, siano $n$ un intero positivo e $(R_1, +_1, \cdot_1)$, $(R_2, +_2, \cdot_2), \dots, (R_n, +_n, \cdot_n)$ anelli. Sia $P$ il prodotto cartesiano $R_1 \times R_2 \times \cdots \times R_n$ e definiamo in $P$ due operazioni binarie $+$ e $\cdot$ ponendo, per ogni $\underline{a} = (a_1, a_2, \dots, a_n), \underline{b} = (b_1, b_2, \dots, b_n) \in P$, come in $(*)$, $\underline{a} + \underline{b} = (a_1 +_1 b_1, a_2 +_2 b_2, \dots, a_n +_n b_n)$ e $\underline{a} \cdot \underline{b} = (a_1 \cdot_1 b_1, a_2 \cdot_2 b_2, \dots, a_n \cdot_n b_n)$. Verificare che $(P, +, \cdot)$ è un anello e che questo anello è unitario (rispettivamente, commutativo, booleano) se ciascuno degli anelli $R_i$ ha la stessa proprietà.

Infine, vediamo cosa di altro possiamo dire sull'anello $\mathbb{Z}_2^n$ alla luce del teorema di Stone. Innanzitutto, (continuando a indicare con $n$ un intero positivo fissato) cosa sono le $n$-ple di elementi di $\mathbb{Z}_2$? Una maniera per rispondere è assumere che, per definizione, una $n$-pla di elementi di $\mathbb{Z}_2$ sia un'applicazione da $S := \{1, 2, \dots, n\}$ a $\mathbb{Z}_2$: la $n$-pla $\underline{a} =$ '$a_1a_2 \dots a_n$' è l'applicazione $i \in S \mapsto a_i \in \mathbb{Z}_2$. Quindi l'insieme $\mathbb{Z}_2^n$ è l'insieme $\mathbb{Z}_2^S$ delle applicazioni da $S$ a $\mathbb{Z}_2$.

A questo punto ci viene in aiuto la nozione insiemistica di funzione caratteristica. Se $X$ è una parte di $S$, la funzione caratteristica di $X$ in $S$ (a valori in $\mathbb{Z}_2$) è l'applicazione

$$\chi_{X,S} \colon i \in S \longmapsto \begin{cases} 1, & \text{se } i \in X \\ 0, & \text{se } i \notin X \end{cases} \in \mathbb{Z}_2.$$

Si ricorda che l'applicazione $X \in \mathcal{P}(S) \mapsto \chi_{X,S} \in \mathbb{Z}_2^S$ è biettiva; l'applicazione inversa è quella che associa, ad ogni applicazione $f \colon S \to \mathbb{Z}_2$, l'antiimmagine di $\{1\}$ mediante $f$. Dunque, ricordano anche che $\mathbb{Z}_2^S = \mathbb{Z}_2^n$ e continuando a scrivere gli elementi di questo insieme come stringhe di lunghezza $n$, la stringa (funzione) caratteristica di una parte di $S$ è la stringa '$a_1a_2 \dots a_n$', dove per ogni $i \in S$ si ha $a_i = 1$ se $i \in X$ e $a_i = 0$ se $i \notin X$; viceversa, una stringa '$a_1a_2 \dots a_n$' corrisponde all'insieme degli $i \in S$ tali che $a_i = 1$.

Facciamo un esempio per chiarire ulteriormente questa coppia di applicazioni biettive. Assumendo $n = 7$,

| la stringa | è | la 7-pla | e corrisponde a | l'insieme |
|---|---|---|---|---|
| '1011010' | | $([1]_2, [0]_2, [1]_2, [1]_2, [0]_2, [1]_2, [0]_2)$ | | $\{1, 3, 4, 6\}$ |

Ora, per il teorema di Stone l'anello $(\mathbb{Z}_2^n, +, \cdot)$ è isomorfo all'anello delle parti di un insieme. Poiché $|\mathbb{Z}_2^n| = 2^n$ e $|S| = n$, dobbiamo avere $\mathbb{Z}_2^n \simeq (\mathcal{P}(S), \triangle, \cap)$. In effetti, possiamo verificare che l'applicazione biettiva appena descritta è un isomorfismo.

**Proposizione 22.** *Siano $n$ un intero positivo e $S = \{1, 2, \dots, n\}$. L'applicazione $\varphi$ che ad ogni parte $X$ di $S$ associa la stringa che rappresenta la funzione caratteristica di $X$ in $S$ è un isomorfismo di anelli booleani da $(\mathcal{P}(S), \triangle, \cap)$ a $(\mathbb{Z}_2^n, +, \cdot)$.*

⚠ *Dimostrazione.* Siano $A$ e $B$ parti di $S$, e siano $\underline{a} =$ '$a_1a_2 \dots a_n$' $= \varphi(A)$ e $\underline{b} =$ '$b_1b_2 \dots b_n$' $= \varphi(B)$. Allora, per ogni $i \in S$, $a_i = 1$ se e solo se $i \in A$ (risultando $a_i = 0$ altrimenti); similmente $b_i = 1$ se e solo se $i \in B$. Sia $\underline{c} =$ '$c_1c_2 \dots c_n$' $= \varphi(A \cap B)$. Allora, per ogni $i$, $c_i = 1$ se e solo se $i \in A \cap B$, cioè se e solo se $a_i = b_i = 1$. Da ciò è chiaro che $\underline{c} = \underline{a} \cdot \underline{b}$. Sia poi $d =$ '$d_1d_2 \dots d_n$' $= \varphi(A \triangle B)$. Allora, per ogni $i \in S$, $d_i = 1$ se e solo se $i \in A \triangle B$, cioè se e solo se vale esattamente una tra $i \in A$ e $i \in B$, cioè se e solo se, tra $a_i$ e $b_i$ uno è 1 e l'altro è 0. Se ne ricava: $\underline{d} = \underline{a} + \underline{b}$. Abbiamo così provato che $\varphi$ è un isomorfismo. □

Possiamo in definitiva concludere che lavorare su stringhe di zeri e uno di fissata lunghezza $n$ utilizzando le operazioni 'bit a bit' è del tutto equivalente a lavorare nell'anello (booleano) delle parti dell'insieme $S$. La

moltiplicazione 'bit a bit' (operatore AND) corrisponde all'operazione di intersezione, l'addizione (modulo 2, operatore XOR) corrisponde all'operazione di differenza simmetrica.

Ad esempio, se, come sopra, $n = 7$ e $\underline{a} =$ '1011010', ed inoltre $\underline{b} =$ '0011100', allora $\underline{a}$ e $\underline{b}$ corrispondono ai sottoinsiemi $A = \{1, 3, 4, 6\}$ e $B = \{3, 4, 5\}$ di $\{1, 2, 3, 4, 5, 6, 7\}$, e possiamo completare come segue una tabella in cui le stringhe al primo rigo corrispondono ad insiemi al secondo rigo:

| | | | |
|---|---|---|---|
| $\underline{a} =$ '1011010' | $\underline{b} =$ '0011100' | $\underline{a} + \underline{b} =$ '1000110' | $\underline{a} \cdot \underline{b} =$ '0011000' |
| $A = \{1, 3, 4, 6\}$ | $B = \{3, 4, 5\}$ | $A \triangle B = \{1, 5, 6\}$ | $A \cap B = \{3, 4\}$ |