Università degli Studi Roma Tre
Scuola di Scienze
Dipartimento di Matematica e Fisica

Corso di Laurea Triennale in Matematica

Algebre di Boole e teorema di rappresentazione di Stone

Tesi di Laurea in Logica Matematica

Laureando
Raffaele Di Donna
N. Matr. 523997

Relatore
Chiar.mo Prof.
Lorenzo Tortora de Falco

A.A. 2019/2020

Indice

Introduzione **i**

1 Algebre di Boole **1**
1.1 Definizione e prime proprietà 1
1.2 Algebre di Boole come insiemi ordinati 5
1.3 Omomorfismi e isomorfismi 7
1.4 Ideali 11
1.5 Ideali massimali 13
1.6 Filtri e ultrafiltri 14
1.7 Basi di filtri 16

2 Il teorema di Stone **19**
2.1 Nozioni di topologia 19
2.2 Sottoalgebre di Boole 22
2.3 Spazi di Stone 22
2.4 Il teorema di Stone 25
2.5 Conseguenze in logica 28

Conclusioni **32**

Introduzione

Verso la metà del diciannovesimo secolo nacquero i due campi dell'algebra astratta e della logica simbolica. In effetti, sebbene l'algebra e la logica esistessero da qualche tempo, l'algebra astratta e la logica simbolica erano essenzialmente nuovi sviluppi. L'origine di entrambi i campi è dovuta principalmente all'intuizione che i sistemi formali potessero essere studiati senza far riferimento in maniera esplicita alle loro interpretazioni previste.

Questa intuizione portò George Boole, nella sua opera *Mathematical Analysis of Logic* del 1847, a formulare il primo esempio di algebra non numerica e di logica simbolica al tempo stesso. Egli osservò che l'operazione di congiunzione di due proposizioni aveva delle affinità con il prodotto di due numeri. Vide che indicando le proposizioni con delle lettere, così come si fa per i numeri in algebra, queste similitudini si facevano ancor più evidenti. Quindi $ab = ba$, per esempio, è una legge di questa "algebra della logica" così come è una legge dell'usuale algebra dei numeri. Allo stesso tempo, vi sono alcune discrepanze rispetto all'algebra dei numeri dato che, per esempio, si ha $aa = a$. E le differenze sono importanti quanto le somiglianze. Infatti, mentre le somiglianze suggerivano una logica veramente simbolica, come l'aritmetica "simbolica" che contraddistingue l'algebra ordinaria, le differenze suggerivano che i metodi dell'algebra potessero essere estesi ben oltre l'algebra dei numeri.

Tuttavia, nonostante l'algebra di Boole fosse così legata alle origini sia dell'algebra astratta che della logica simbolica, i due campi si svilupparono per qualche tempo in relativo isolamento. Da un lato, la nozione di algebra di Boole venne perfezionata da Jevons, Schröder, Huntington e altri, andando ad arricchire il campo dell'algebra astratta. D'altra parte, l'idea di una logica simbolica venne sviluppata seguendo linee leggermente diverse dalla formulazione algebrica originale di Boole, partendo dal contributo di Frege fino a raggiungere la sua formulazione classica nel 1910, con i *Principia Mathematica* di Whitehead e Russel. Così Boole, seguendo la tradizione di Leibniz, voleva studiare la matematica della logica, mentre il fine di Frege, Whitehead e Russell era quello di studiare la logica della matematica. Il campo moderno della logica matematica riconosce ambo gli approcci come metodologicamente legittimi e in effetti li abbraccia entrambi sotto l'ambiguità del suo nome, "logica matematica".[1]

A oggi esistono vari modi di approcciare le algebre di Boole. A partire da due presentazioni puramente algebriche, come anelli o insiemi ordinati, scopriremo che è altresì possibile adottare un punto di vista topologico: qualsiasi algebra di Boole può essere identificata con l'insieme dei chiuso-aperti di uno spazio topologico compatto di dimensione zero. Naturalmente, andremo a definire rigorosamente tutte queste nozioni. Si presume tuttavia siano noti i concetti di base come le definizioni di anello, dominio integrale, campo e di spazio topologico. Per le nozioni di base di algebra si rimanda a [7], si veda invece [9] per quelle di topologia.

Nel primo capitolo discuteremo le principali proprietà delle algebre di Boole. Le sezioni 1.1 e 1.2 contengono le definizioni algebriche e le prime proprietà. Un'algebra di Boole è un anello in

[1] Questi e altri riferimenti storici sono reperibili in [5].

cui ogni elemento è uguale al suo quadrato, ma è anche un reticolo distributivo e complementare, vale a dire un insieme ordinato in cui:

- C'è un più piccolo elemento e c'è un più grande elemento.
- A due elementi qualsiasi possiamo associare un estremo superiore e un estremo inferiore.
- Le operazioni di passaggio all'estremo inferiore e all'estremo superiore sono distributive l'una rispetto all'altra.
- Ogni elemento ammette un complemento.

Vedremo che questi due punti di vista sono equivalenti. Nella sezione 1.3 siamo interessati agli omomorfismi tra algebre di Boole. Come sempre in algebra, i nuclei di questi omomorfismi, che qui sono gli ideali, svolgono un ruolo essenziale. Proprio per questo motivo, nella sezione 1.4 ci occuperemo degli ideali e ne studieremo le proprietà, mentre nella sezione 1.5 ci soffermeremo su una classe particolare di ideali, vale a dire gli ideali massimali. Quando consideriamo le algebre di Boole come reticoli preferiamo però studiare i filtri, i quali sono canonicamente associati agli ideali: otteniamo un filtro prendendo i complementi degli elementi di un ideale. Rivolgiamo una particolare attenzione agli ultrafiltri, che naturalmente corrispondono agli ideali massimali. Lo studio dei filtri e degli ultrafiltri è oggetto della sezione 1.6. Nella sezione 1.7, infine, andiamo a introdurre la nozione di "base di un filtro" per poi caratterizzarla grazie al teorema dell'ultrafiltro che, nella dualità tra ideali e filtri, è legato al teorema di Krull sull'esistenza di ideali massimali. In particolare, per fare questo assumeremo l'assioma della scelta.

Il secondo capitolo si apre con dei richiami di topologia, ai quali è dedicata la sezione 2.1. La sezione 2.2 è invece finalizzata a definire e a caratterizzare le sottostrutture di una data algebra di Boole, mentre la sezione 2.3 sposta l'attenzione sugli omomorfismi da una data algebra di Boole $\mathcal{A}$ in $\{0, 1\}$. L'insieme di questi omomorfismi è dotato di una topologia: viene dunque chiamato lo spazio di Stone di $\mathcal{A}$. Nella sezione 2.4 daremo una caratterizzazione topologica delle algebre di Boole tramite il celebre teorema dimostrato nel 1936 dal matematico statunitense M. H. Stone. La sezione 2.5 è infine dedicata alle conseguenze in logica proposizionale. Dopo aver richiamato le nozioni principali, introduciamo il concetto di atomo e studiamo l'algebra di Boole delle classi di formule del calcolo proposizionale, per poi concludere con una dimostrazione del teorema di compattezza per il calcolo proposizionale.

Capitolo 1

Algebre di Boole

1.1 Definizione e prime proprietà

Definizione 1.1. Un anello unitario $\langle A, +, \times, 0, 1\rangle$, con $1 \neq 0$, è detto un'*algebra di Boole* (oppure un *anello di Boole*) se ogni suo elemento è idempotente rispetto all'operazione moltiplicativa, cioè se:

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

In seguito, purché questa scelta non generi ambiguità, il simbolo del prodotto verrà sottinteso allo scopo di semplificare la notazione. Similmente, non specificheremo le operazioni binarie e gli elementi neutri di un'algebra di Boole quando questi saranno evidenti dal contesto. In questi casi, dunque, tenderemo a indicare un'algebra di Boole con una lettera calligrafica $\mathcal{A}$, per distinguerla dal suo supporto A.

Esempio 1.2. L'algebra di Boole più semplice è quella data dall'insieme numerico $\{0, 1\}$ munito delle operazioni di somma $+$ e prodotto $\times$ che andiamo a definire tramite le due seguenti tabelle:

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Tali operazioni si comportano quindi come quelle usuali sugli interi con l'eccezione che $1 + 1 = 0$. Si verifica facilmente che $\{0, 1\}$ con queste operazioni ha una struttura di algebra di Boole. Vale la pena osservare che gli elementi neutri per la somma e per il prodotto sono 0 e 1 rispettivamente.

Esempio 1.3. Un'algebra di Boole assai naturale è l'insieme delle parti di un insieme E non vuoto:

$$\langle \mathcal{P}(E), \triangle, \cap, \varnothing, E\rangle$$

Il simbolo $\triangle$ qui denota l'operazione di differenza simmetrica, cioè la differenza insiemistica tra l'unione e l'intersezione di due insiemi. Precisamente, dati due sottoinsiemi qualsiasi X e Y di E, se indichiamo con $X \setminus Y$ l'insieme differenza tra X e Y, cioè l'insieme $\{x \in X : x \notin Y\}$, la differenza simmetrica tra X e Y risulta definita da:

$$X \triangle Y = (X \cup Y) \setminus (X \cap Y)$$

L'algebra di Boole $\mathcal{P}(E)$ con E insieme non vuoto costituisce un esempio molto significativo, come vedremo nel seguito.

Lemma 1.4. *Ogni algebra di Boole è un anello commutativo nel quale ogni elemento coincide con il proprio opposto.*

Dimostrazione. Consideriamo un'algebra di Boole $\mathcal{A}$ e degli elementi $x, y \in A$. Dalla definizione discende che $(x + y)^2 = x + y$. D'altra parte, per distributività del prodotto rispetto alla somma:

$$(x + y)^2 = x(x + y) + y(x + y) = x^2 + xy + yx + y^2$$

Sfruttando il fatto che $x^2 = x$ e $y^2 = y$ per definizione di algebra di Boole, ne deduciamo quindi:

$$\begin{aligned} & x + y = x + xy + yx + y \\ \implies & 0 = xy + yx \\ \implies & yx = -xy \end{aligned}$$

Prendendo $y = 1$ nella relazione precedente si dimostra che ogni elemento $x \in A$ coincide con il proprio opposto. Una volta osservato questo abbiamo, per x e y qualunque, che $xy = -xy$ e ciò permette di stabilire la commutatività del prodotto, cioè che $\mathcal{A}$ è un anello commutativo. □

Osservazione 1.5. L'anello $\{0, 1\}$ con le operazioni date nell'esempio 1.2 è l'unica algebra di Boole a essere un campo ed è anche l'unica a essere un dominio integrale, cioè a non possedere divisori dello zero sinistri o destri non banali. È infatti immediato verificare che sia un campo (dunque, un dominio integrale), perché l'unico elemento non nullo è 1, che ammette se stesso come inverso moltiplicativo. Inoltre, data un'algebra di Boole $\mathcal{A}$, per un qualsiasi elemento $x \in A$ vale $x^2 = x$, o equivalentemente $x(x - 1) = 0$. Ma sotto l'ipotesi che $\mathcal{A}$ sia un dominio integrale (o addirittura un campo) tale condizione implica $x = 0$ oppure $x = 1$ e dunque $A \subseteq \{0, 1\}$. L'altra inclusione è sempre vera per definizione. Osserviamo però che gli elementi 0 e 1 che compaiono nell'identità da noi ottenuta $A = \{0, 1\}$ sono gli elementi neutri di $\mathcal{A}$ per la somma e per il prodotto e dunque non necessariamente si riferiscono agli elementi numerici dell'algebra di Boole $\{0, 1\}$. Nel caso scegliessimo $\mathcal{A} = \langle \mathbb{Z}/2\mathbb{Z}, +, \times, 0, 1 \rangle$, per esempio, i due elementi $0, 1 \in A$ sarebbero delle classi di equivalenza della relazione di congruenza modulo 2. Per questo motivo parleremo di unicità "a meno di isomorfismo". Tratteremo in modo formale la nozione di isomorfismo nella sezione 1.3.

Se $\mathcal{A}$ è un'algebra di Boole, possiamo definire una relazione binaria $\leq$ su A nella maniera che segue: per ogni $x, y \in A$ poniamo $x \leq y$ se vale $xy = x$. Si vede facilmente che $\leq$ è una relazione d'ordine parziale su A.

Esempio 1.6. Dato un insieme non vuoto E, riprendiamo l'algebra di Boole $\mathcal{P}(E)$ dell'esempio 1.3. Per ogni due sottoinsiemi X e Y di E, per definizione vale $X \leq Y$ se e solo se $X \cap Y = X$, cioè se e solo se $X \subseteq Y$. Di conseguenza, la relazione d'ordine $\leq$ su $\mathcal{P}(E)$ è l'usuale inclusione insiemistica.

Teorema 1.7. *Sia $\mathcal{A}$ un'algebra di Boole.*

(i) *Il minimo di A rispetto alla relazione $\leq$ esiste ed è 0. Anche il massimo esiste ed è 1.*

(ii) *Due elementi qualunque $x, y \in A$ ammettono un estremo inferiore, cioè il massimo dei minoranti comuni a x e a y, denotato $x \frown y$. Tale estremo inferiore è il prodotto xy.*

(iii) *Due elementi qualsiasi $x, y \in A$ ammettono un estremo superiore, cioè il minimo dei maggioranti comuni a x e a y, denotato $x \smile y$. Tale estremo superiore è $x + y + xy$.*

(iv) *Le operazioni binarie $\frown$ e $\smile$ che consistono, rispettivamente, nel passaggio all'estremo inferiore e superiore, sono associative e commutative.*

(v) *L'elemento* 0 *è neutro per l'operazione* $\smile$ *e assorbente per l'operazione* $\frown$. *L'elemento* 1 *è neutro per l'operazione* $\frown$ *e assorbente per l'operazione* $\smile$.

(vi) *Ogni sottoinsieme finito non vuoto* $\{x_1, x_2, \dots, x_k\}$ *di* A *ammette un estremo inferiore, che è dato da* $x_1 \frown x_2 \frown \cdots \frown x_k$ *e un estremo superiore, dato invece da* $x_1 \smile x_2 \smile \cdots \smile x_k$.

(vii) *Le operazioni* $\frown$ *e* $\smile$ *sono distributive l'una rispetto all'altra.*

(viii) *Per ogni* $x \in A$ *esiste un unico elemento* $x^{\mathbf{c}} \in A$, *chiamato complemento (o complementare) di* x, *tale che* $x \smile x^{\mathbf{c}} = 1$ *e* $x \frown x^{\mathbf{c}} = 0$. *Tale elemento è* $1 + x$.

(ix) *L'applicazione* $x \mapsto x^{\mathbf{c}}$ *da* A *in* A *è una biiezione involutiva, cioè coincidente con la sua inversa, che inverte l'ordine.*

Dimostrazione.

(i) Essendo $\mathcal{A}$ un anello unitario, vale $0 \times x = 0$ e $x \times 1 = x$, cioè $0 \leq x$ e $x \leq 1$, per ogni $x \in A$.

(ii) Dati $x, y \in A$, l'elemento xy è un minorante comune a x e a y in virtù delle due condizioni:

$$(xy)x = x^2y = xy$$
$$(xy)y = xy^2 = xy$$

Se inoltre $z \in A$ è un minorante comune a x e a y, cioè se $zx = z$ e $zy = z$, allora abbiamo:

$$z(xy) = (zx)y = zy = z$$

Dunque $z \leq xy$.

(iii) Dati $x, y \in A$, l'elemento $x + y + xy$ è un maggiorante comune a x e a y poiché abbiamo:

$$x(x + y + xy) = x^2 + xy + x^2y = x + xy + xy = x + 0 = x$$
$$y(x + y + xy) = xy + y^2 + xy^2 = xy + y + xy = y + 0 = y$$

Se poi $z \in A$ è un maggiorante comune a x e a y, vale a dire se $xz = x$ e $yz = y$, allora si ha:

$$(x + y + xy)z = xz + yz + xyz = x + y + xy$$

Quindi $x + y + xy \leq z$.

(iv) Si vede facilmente che questo fatto vale per un qualsiasi insieme ordinato che goda delle proprietà (ii) e (iii), escludendo ovviamente le asserzioni finali riguardanti l'elemento che svolge il ruolo di estremo inferiore o superiore.

(v) La verifica di questo fatto per qualsiasi insieme ordinato soddisfacente le proprietà (i), (ii) e (iii), intendendo sempre a meno delle asserzioni finali di queste proprietà, è immediata.

(vi) Sia $\{x_1, x_2, \dots, x_k\}$ un sottoinsieme finito non vuoto di A. Osserviamo preliminarmente che gli elementi $x_1 \frown x_2 \frown \cdots \frown x_k$ e $x_1 \smile x_2 \smile \cdots \smile x_k$ sono ben definiti per il punto (iv), il quale garantisce che le operazioni $\frown$ e $\smile$ sono associative. Ora, naturalmente, ragioniamo per induzione sull'intero $k \geq 1$. Osserviamo che la base di induzione, che corrisponde al

caso $k = 1$, è del tutto banale.[1] Nel passo induttivo assumiamo $k \geq 2$ e supponiamo che la tesi valga per qualsiasi sottoinsieme finito di A di cardinalità $k - 1$. Per associatività, vale:

$$x_1 \frown x_2 \frown \cdots \frown x_k = (x_1 \frown x_2 \frown \cdots \frown x_{k-1}) \frown x_k$$
$$x_1 \smile x_2 \smile \cdots \smile x_k = (x_1 \smile x_2 \smile \cdots \smile x_{k-1}) \smile x_k$$

A questo punto, sfruttando l'ipotesi induttiva e i punti (ii) e (iii) già dimostrati, si giunge molto facilmente alla conclusione. Anche qui, come nei punti (iv) e (v) precedenti, si può osservare che l'asserto continua a valere se si considera non un'algebra di Boole, bensì un insieme ordinato che verifichi, sempre a meno delle asserzioni finali, le proprietà (ii), (iii) e (iv).

(vii) Siano $x, y, z \in A$ elementi fissati. Da una parte, la distributività dell'operazione $\frown$ rispetto a $\smile$ segue dalle identità:

$$\begin{aligned} x \frown (y \smile z) &= x(y + z + yz) \\ &= xy + xz + xyz \\ &= xy + xz + xyxz = (x \frown y) \smile (x \frown z) \end{aligned}$$

Dall'altra, la distributività di $\smile$ rispetto a $\frown$ deriva facilmente dalle uguaglianze seguenti:

$$\begin{aligned} (x \smile y) \frown (x \smile z) &= (x + y + xy)(x + z + xz) \\ &= x^2 + xz + x^2z + yx + yz + yxz + x^2y + xyz + x^2yz \\ &= x + yz + xyz \\ &= x \smile (yz) \\ &= x \smile (y \frown z) \end{aligned}$$

(viii) È facile verificare che $x \smile (1 + x) = 1$ e che $x \frown (1 + x) = 0$. Questo ci assicura l'esistenza di un elemento x^{c} come nell'enunciato. Per l'unicità basta osservare che, se $x' \in A$ soddisfa le due condizioni $x \smile x' = 1$ e $x \frown x' = 0$, cioè $x + x' + xx' = 1$ e $xx' = 0$, allora $x + x' = 1$, cioè $x' = 1 + x$.

(ix) L'applicazione data è sicuramente una biiezione involutiva in quanto $1 + (1 + x) = x$ per ogni $x \in A$. Per vedere che inverte l'ordine, fissiamo due elementi $x, y \in A$ e notiamo che:

$$\begin{aligned} & 1 + x \leq 1 + y \\ \iff & (1 + x)(1 + y) = 1 + x \\ \iff & 1 + x + y + xy = 1 + x \\ \iff & y + xy = 0 \\ \iff & y = xy \\ \iff & y \leq x \end{aligned}$$

□

Lemma 1.8. *Sia $\mathcal{A}$ un'algebra di Boole e siano $x, y \in A$. Allora $x \leq 1 + y$ se e solo se $xy = 0$.*

Dimostrazione. Per definizione e per distributività del prodotto rispetto alla somma, abbiamo che:

$$\begin{aligned} & x \leq 1 + y \\ \iff & x(1 + y) = x \\ \iff & x + xy = x \\ \iff & xy = 0 \end{aligned}$$

□

[1] Per convenzione, per $k = 1$ definiamo $x_1 \frown x_2 \frown \cdots \frown x_k = x_1 \smile x_2 \smile \cdots \smile x_k = x_1$.

1.2 Algebre di Boole come insiemi ordinati

In questa sezione si intende fornire una caratterizzazione delle algebre di Boole in quanto insiemi parzialmente ordinati soddisfacenti determinate proprietà.

Definizione 1.9. Consideriamo un insieme parzialmente ordinato $\langle A, \leq \rangle$ e le seguenti proprietà:

(a) Esistono il minimo e il massimo di A rispetto alla relazione $\leq$. Tali elementi sono denotati 0 e 1 rispettivamente.

(b) Due elementi qualunque $x, y \in A$ possiedono un estremo inferiore, denotato $x \frown y$ e un estremo superiore, denotato $x \smile y$.

(c) Le operazioni $\frown$ e $\smile$ sono distributive l'una rispetto all'altra.

(d) Per ogni $x \in A$ esiste un elemento $x' \in A$, detto un complemento di x, tale che $x \smile x' = 1$ e $x \frown x' = 0$.

Diremo che $\langle A, \leq \rangle$ è un *reticolo* se verifica le proprietà (a) e (b). Se inoltre $\langle A, \leq \rangle$ è un reticolo che soddisfa la proprietà (c), diremo che è un reticolo *distributivo*. Se invece è un reticolo che verifica la proprietà (d), si dice che è un reticolo *complementare*.

È molto facile dimostrare che in un reticolo distributivo e complementare il complemento di un elemento $x \in A$ è unico. Siano infatti x' e x'' due complementi di x. Consideriamo l'elemento $y = (x \frown x') \smile x''$. Da una parte, risulta $y = 0 \smile x''$ e quindi $y = x''$. Dall'altra, per distributività:

$$y = (x \smile x'') \frown (x' \smile x'') = 1 \frown (x' \smile x'') = x' \smile x''$$

Abbiamo dunque $x'' = x' \smile x''$, cioè $x' \leq x''$. Scambiando i ruoli di x' e x'' si trova anche $x'' \leq x'$ e concludiamo allora che $x' = x''$.

Potremo allora denotare $x^{\mathbf{c}}$ il complemento di x. In un reticolo distributivo e complementare sono inoltre verificate le proprietà (iv), (v) e (vi) del teorema 1.7. Come conseguenza dell'unicità del complemento e del punto (iv) del teorema 1.7, la funzione $x \mapsto x^{\mathbf{c}}$ è una biiezione involutiva.

Lemma 1.10 (Leggi di de Morgan)**.** *Sia $\langle A, \leq \rangle$ un reticolo distributivo e complementare. Dati $x, y \in A$:*

$$(x \frown y)^{\mathbf{c}} = x^{\mathbf{c}} \smile y^{\mathbf{c}}$$
$$(x \smile y)^{\mathbf{c}} = x^{\mathbf{c}} \frown y^{\mathbf{c}}$$

Dimostrazione. La seconda condizione segue immediatamente dalla prima prendendo $x^{\mathbf{c}}$ al posto di x, $y^{\mathbf{c}}$ al posto di y, passando al complemento nei due membri dell'uguaglianza e sfruttando il fatto che la trasformazione $x \mapsto x^{\mathbf{c}}$ è involutiva.

Possiamo dunque concentrarci sulla prima asserzione. Sarà sufficiente mostrare che $x^{\mathbf{c}} \smile y^{\mathbf{c}}$ è un complemento di $x \frown y$ e usare l'unicità del complemento. Per il punto (c) della definizione 1.9 e per la proprietà (iv) del teorema 1.7 si ha:

$$\begin{aligned}
&(x^{\mathbf{c}} \smile y^{\mathbf{c}}) \smile (x \frown y) \\
&= (x^{\mathbf{c}} \smile y^{\mathbf{c}} \smile x) \frown (x^{\mathbf{c}} \smile y^{\mathbf{c}} \smile y) \\
&= (1 \smile y^{\mathbf{c}}) \frown (x^{\mathbf{c}} \smile 1) \\
&= 1 \frown 1 = 1
\end{aligned}
\qquad
\begin{aligned}
&(x^{\mathbf{c}} \smile y^{\mathbf{c}}) \frown (x \frown y) \\
&= (x^{\mathbf{c}} \frown x \frown y) \smile (y^{\mathbf{c}} \frown x \frown y) \\
&= (0 \frown y) \smile (0 \frown x) \\
&= 0 \smile 0 = 0
\end{aligned}$$

□

Le leggi di de Morgan si generalizzano facilmente per ricorsione. Abbiamo allora il seguente enunciato.

Lemma 1.11 (Leggi di de Morgan generalizzate)**.** *Sia $\langle A, \leq \rangle$ un reticolo distributivo e complementare. Allora, per ogni intero $k \geq 1$ e per ogni scelta di $x_1, x_2, \ldots, x_k \in A$, valgono le due condizioni seguenti:*

$$(x_1 \frown x_2 \frown \cdots \frown x_k)^{\mathbf{c}} = x_1^{\mathbf{c}} \smile x_2^{\mathbf{c}} \smile \cdots \smile x_k^{\mathbf{c}}$$
$$(x_1 \smile x_2 \smile \cdots \smile x_k)^{\mathbf{c}} = x_1^{\mathbf{c}} \frown x_2^{\mathbf{c}} \frown \cdots \frown x_k^{\mathbf{c}}$$

Nella dimostrazione del risultato che segue, le parentesi quadre svolgono lo stesso ruolo delle parentesi tonde e vengono introdotte al solo scopo di rendere più agevole la lettura delle formule.

Teorema 1.12. *Sia $\langle A, \leq \rangle$ un reticolo distributivo e complementare. Allora è possibile attribuire ad A una struttura di algebra di Boole $\langle A, +, \times, 0, 1 \rangle$ in maniera tale che l'ordine $\leq$ dato su A coincida con l'ordine associato alla struttura di algebra di Boole. In altre parole, richiediamo che valga $x \leq y$ se e solo se $xy = x$.*

Dimostrazione. Innanzitutto, definiamo le operazioni di prodotto e somma nel modo che segue:

$$x \times y = x \frown y$$
$$x + y = (x \frown y^{\mathbf{c}}) \smile (x^{\mathbf{c}} \frown y)$$

La distributività di $\smile$ rispetto a $\frown$ ci fornisce un'espressione equivalente per la somma:

$$\begin{aligned} x + y &= (x \smile (x^{\mathbf{c}} \frown y)) \frown (y^{\mathbf{c}} \smile (x^{\mathbf{c}} \frown y)) \\ &= (x \smile x^{\mathbf{c}}) \frown (x \smile y) \frown (x^{\mathbf{c}} \smile y^{\mathbf{c}}) \frown (y \smile y^{\mathbf{c}}) \\ &= 1 \frown (x \smile y) \frown (x^{\mathbf{c}} \smile y^{\mathbf{c}}) \frown 1 \\ &= (x \smile y) \frown (x^{\mathbf{c}} \smile y^{\mathbf{c}}) \end{aligned}$$

A questo punto non rimane che verificare la definizione di algebra di Boole con le operazioni di somma e prodotto appena definite, prendendo gli elementi 0 e 1 definiti nella proprietà (a) della definizione 1.9 come elementi neutri per la somma e per il prodotto rispettivamente e osservando che l'ordine $\leq$ dato su A coincide, in effetti, con l'ordine associato alla struttura di algebra di Boole.

- È del tutto evidente che, per ogni $x \in A$, valga $x^2 = x$, perché ovviamente si ha $x \frown x = x$.
- Vediamo che $\langle A, +, 0 \rangle$ è un gruppo abeliano. La stabilità dell'operazione binaria $+$ segue dalla proprietà (b) della definizione 1.9, mentre la commutatività viene ereditata da quella delle operazioni $\frown$ e $\smile$. Dato $x \in A$, è facile convincersi del fatto che 0 è l'elemento neutro:

  $$x + 0 = (x \frown 0^{\mathbf{c}}) \smile (x^{\mathbf{c}} \frown 0) = (x \frown 1) \smile 0 = x \smile 0 = x$$

  Per la commutatività della somma, non serve verificare esplicitamente che $0 + x = x$. Ora notiamo invece che un qualunque $x \in A$ è l'opposto di se stesso, in virtù della condizione:

  $$x + x = (x \frown x^{\mathbf{c}}) \smile (x^{\mathbf{c}} \frown x) = 0 \smile 0 = 0$$

  Rimane da dimostrare solo che la somma è un'operazione associativa. Fissati $x, y, z \in A$, usando l'espressione equivalente per la somma individuata prima, le leggi di de Morgan, la distributività di $\frown$ rispetto a $\smile$ e, infine, il fatto che $\smile$ è un'operazione associativa, si ha:

  $$\begin{aligned} (x + y) + z &= ([x + y] \frown z^{\mathbf{c}}) \smile ([x + y]^{\mathbf{c}} \frown z) \\ &= ([(x \frown y^{\mathbf{c}}) \smile (x^{\mathbf{c}} \frown y)] \frown z^{\mathbf{c}}) \smile ([x + y]^{\mathbf{c}} \frown z) \\ &= ([(x \frown y^{\mathbf{c}}) \smile (x^{\mathbf{c}} \frown y)] \frown z^{\mathbf{c}}) \smile ([(x \smile y) \frown (x^{\mathbf{c}} \smile y^{\mathbf{c}})]^{\mathbf{c}} \frown z) \\ &= ([(x \frown y^{\mathbf{c}}) \smile (x^{\mathbf{c}} \frown y)] \frown z^{\mathbf{c}}) \smile ([(x \smile y)^{\mathbf{c}} \smile (x^{\mathbf{c}} \smile y^{\mathbf{c}})^{\mathbf{c}}] \frown z) \\ &= ([(x \frown y^{\mathbf{c}}) \smile (x^{\mathbf{c}} \frown y)] \frown z^{\mathbf{c}}) \smile ([(x^{\mathbf{c}} \frown y^{\mathbf{c}}) \smile (x \frown y)] \frown z) \\ &= [(x \frown y^{\mathbf{c}} \frown z^{\mathbf{c}}) \smile (x^{\mathbf{c}} \frown y \frown z^{\mathbf{c}})] \smile [(x^{\mathbf{c}} \frown y^{\mathbf{c}} \frown z) \smile (x \frown y \frown z)] \\ &= (x \frown y^{\mathbf{c}} \frown z^{\mathbf{c}}) \smile (x^{\mathbf{c}} \frown y \frown z^{\mathbf{c}}) \smile (x^{\mathbf{c}} \frown y^{\mathbf{c}} \frown z) \smile (x \frown y \frown z) \end{aligned}$$

Per commutatività delle operazioni $\frown$ e $\smile$, qualsiasi permutazione degli elementi x, y e z produce lo stesso risultato. In particolare, per la commutatività della somma, otteniamo:

$$(x + y) + z = (y + z) + x = x + (y + z)$$

- Le proprietà associativa e commutativa del prodotto discendono immediatamente dalla proprietà (iv) del teorema 1.7. È poi evidente che 1 sia l'elemento neutro, perché $x \frown 1 = x$ per ogni $x \in A$.
- Utilizzando ancora la proprietà (iv) del teorema 1.7, la distributività di $\frown$ rispetto a $\smile$ e le leggi di de Morgan, vediamo adesso che vale la proprietà distributiva sinistra di $\times$ rispetto a $+$. Dati $x, y, z \in A$, si ha:

$$\begin{aligned} xy + xz &= (x \frown y) + (x \frown z) \\ &= [(x \frown y) \frown (x \frown z)^{\mathbf{c}}] \smile [(x \frown y)^{\mathbf{c}} \frown (x \frown z)] \\ &= [(x \frown y) \frown (x^{\mathbf{c}} \smile z^{\mathbf{c}})] \smile [(x^{\mathbf{c}} \smile y^{\mathbf{c}}) \frown (x \frown z)] \\ &= [(x \frown y \frown x^{\mathbf{c}}) \smile (x \frown y \frown z^{\mathbf{c}})] \smile [(x^{\mathbf{c}} \frown x \frown z) \smile (y^{\mathbf{c}} \frown x \frown z)] \\ &= 0 \smile (x \frown y \frown z^{\mathbf{c}}) \smile 0 \smile (x \frown y^{\mathbf{c}} \frown z) \\ &= (x \frown y \frown z^{\mathbf{c}}) \smile (x \frown y^{\mathbf{c}} \frown z) \\ &= x \frown [(y \frown z^{\mathbf{c}}) \smile (y^{\mathbf{c}} \frown z)] \\ &= x \frown [y + z] \\ &= x(y + z) \end{aligned}$$

  La proprietà distributiva destra deriva facilmente da quella sinistra e dalla commutatività del prodotto.

Con questo abbiamo mostrato che $\langle A, +, \times, 0, 1 \rangle$ è un'algebra di Boole. Per concludere, dobbiamo solo accertarci che l'ordine $\leq$ fissato su A coincide con quello associato alla struttura di algebra di Boole. Ma ciò è una conseguenza di come si è definito il prodotto. Infatti, per ogni $x, y \in A$, si ha:

$$\begin{aligned} & x \leq y \\ \iff & x \frown y = x \\ \iff & xy = x \end{aligned}$$

□

Possiamo riassumere quanto visto in questa sezione affermando che sono le proprietà (i), (ii), (iii), (vii) e (viii) del teorema 1.7 a caratterizzare le algebre di Boole. Nel seguito capiterà spesso di pensare alle algebre di Boole come a reticoli distributivi e complementari anziché ad anelli in cui ciascun elemento è uguale al proprio quadrato. Il punto di vista che abbiamo appena introdotto si rivela in alcuni casi molto naturale, come nel caso dell'algebra di Boole dell'insieme delle parti di un insieme (esempio 1.3).

1.3 Omomorfismi e isomorfismi

Definizione 1.13. Siano $\mathcal{A} = \langle A, +, \times, 0, 1 \rangle$, $\mathcal{A}' = \langle A', +, \times, 0, 1 \rangle$ algebre di Boole. Una funzione h da A in A' viene detta un *omomorfismo di algebre di Boole da $\mathcal{A}$ in $\mathcal{A}'$* se, per ogni $x, y \in A$, si ha:

$$\begin{aligned} h(x + y) &= h(x) + h(y) \\ h(x \times y) &= h(x) \times h(y) \\ h(1) &= 1 \end{aligned}$$

Bisogna notare che abbiamo commesso l'abuso di notazione che consiste nel non distinguere le operazioni e gli elementi neutri di $\mathcal{A}'$ da quelli di $\mathcal{A}$. Per semplicità, manterremo nel seguito questo abuso, estendendolo anche alle relazioni d'ordine associate alle algebre di Boole. Vediamo ora una precisazione che sarà utile nel seguito.

Osservazione 1.14. Più in generale, se $\mathcal{R} = \langle R, +, \times, 0, 1\rangle, \mathcal{R}' = \langle R', +, \times, 0, 1\rangle$ sono anelli unitari, si dice *omomorfismo di anelli unitari da $\mathcal{R}$ in $\mathcal{R}'$* un'applicazione h da R in R' che soddisfi le proprietà indicate nella definizione precedente. Ne discende che un omomorfismo di algebre di Boole non è altro che un omomorfismo di anelli unitari tra algebre di Boole.

Osservazione 1.15. La condizione $h(0) = 0$ non è menzionata nella definizione di omomorfismo di algebre di Boole (né in quella di omomorfismo di anelli unitari) ma è sempre verificata. Infatti, è il caso particolare nel quale si sceglie $x = 0$ oppure $y = 0$ nella condizione $h(x + y) = h(x) + h(y)$.

A questo punto, vogliamo dare una caratterizzazione degli omomorfismi di algebre di Boole. Prima però abbiamo bisogno di un risultato preliminare.

Lemma 1.16. *Siano $\mathcal{A} = \langle A, \leq, 0, 1\rangle, \mathcal{A}' = \langle A', \leq, 0, 1\rangle$ due algebre di Boole e sia h un omomorfismo di algebre di Boole da $\mathcal{A}$ in $\mathcal{A}'$. Scelti due elementi qualunque $x, y \in A$, valgono allora le seguenti proprietà:*

$$h(x \frown y) = h(x) \frown h(y)$$
$$h(x^{\mathbf{c}}) = h(x)^{\mathbf{c}}$$
$$h(x \smile y) = h(x) \smile h(y)$$
$$\text{se } x \leq y, \text{ allora } h(x) \leq h(y)$$

Dimostrazione. La prima proprietà discende immediatamente dalle definizioni di omomorfismo e di prodotto in un reticolo distributivo e complementare (dimostrazione del teorema 1.12). Per il punto (viii) del teorema 1.7, la seconda identità da dimostrare è equivalente a $h(1 + x) = 1 + h(x)$ e quest'ultima è valida per definizione di omomorfismo. La terza proprietà è invece una semplice conseguenza delle precedenti e delle leggi di de Morgan (lemma 1.10). La quarta proprietà deriva infine dalle seguenti implicazioni:

$$\begin{aligned} & x \leq y \\ \Longrightarrow\ & xy = x \\ \Longrightarrow\ & h(xy) = h(x) \\ \Longrightarrow\ & h(x)h(y) = h(x) \\ \Longrightarrow\ & h(x) \leq h(y) \end{aligned}$$

□

Nel seguito, come nella dimostrazione del teorema 1.12, affiancheremo le parentesi quadre a quelle tonde per facilitare la lettura.

Teorema 1.17. *Siano $\mathcal{A} = \langle A, \leq, 0, 1\rangle, \mathcal{A}' = \langle A', \leq, 0, 1\rangle$ due algebre di Boole e sia h una funzione da A in A'. Allora h è un omomorfismo di algebre di Boole da $\mathcal{A}$ in $\mathcal{A}'$ se e solo se, per ogni $x, y \in A$, vale che:*

$$h(x \frown y) = h(x) \frown h(y)$$
$$h(x^{\mathbf{c}}) = h(x)^{\mathbf{c}}$$

Dimostrazione. L'implicazione diretta ci viene data gratuitamente dal lemma precedente e quindi dobbiamo solo occuparci del viceversa. Supponiamo che le condizioni date nell'enunciato siano verificate e consideriamo due qualsiasi elementi $x, y \in A$. Si trovano molto facilmente le identità:

$$h(xy) = h(x \frown y) = h(x) \frown h(y) = h(x)h(y)$$

D'altro canto, per definizione di somma in un reticolo distributivo e complementare, per le leggi di de Morgan e per le due condizioni su h note per ipotesi, abbiamo anche le seguenti relazioni:

$$\begin{aligned} h(x+y) &= h((x \frown y^{\mathbf{c}}) \smile (x^{\mathbf{c}} \frown y)) \\ &= h([(x \frown y^{\mathbf{c}})^{\mathbf{c}} \frown (x^{\mathbf{c}} \frown y)^{\mathbf{c}}]^{\mathbf{c}}) \\ &= [h((x \frown y^{\mathbf{c}})^{\mathbf{c}} \frown (x^{\mathbf{c}} \frown y)^{\mathbf{c}})]^{\mathbf{c}} \\ &= [h((x \frown y^{\mathbf{c}})^{\mathbf{c}}) \frown h((x^{\mathbf{c}} \frown y)^{\mathbf{c}})]^{\mathbf{c}} \\ &= [h(x \frown y^{\mathbf{c}})^{\mathbf{c}} \frown h(x^{\mathbf{c}} \frown y)^{\mathbf{c}}]^{\mathbf{c}} \\ &= h(x \frown y^{\mathbf{c}}) \smile h(x^{\mathbf{c}} \frown y) \\ &= (h(x) \frown h(y^{\mathbf{c}})) \smile (h(x^{\mathbf{c}}) \frown h(y)) \\ &= (h(x) \frown h(y)^{\mathbf{c}}) \smile (h(x)^{\mathbf{c}} \frown h(y)) = h(x) + h(y) \end{aligned}$$

Infine, per l'osservazione 1.15, si hanno anche le seguenti uguaglianze, dalle quali segue l'asserto:

$$h(1) = h(0^{\mathbf{c}}) = h(0)^{\mathbf{c}} = 0^{\mathbf{c}} = 1$$ □

Osservazione 1.18. Si noti che, nell'enunciato del teorema 1.17, la doppia implicazione continua a valere se, anziché porre una condizione sull'immagine dell'estremo inferiore di due elementi, si richiede la condizione analoga per l'estremo superiore. Infatti, l'implicazione diretta è fornita dal lemma 1.16 anche in questo caso, mentre per il viceversa usiamo la condizione sull'immagine di un complemento e le leggi di de Morgan per recuperare l'ipotesi mancante sull'estremo inferiore:

$$\begin{aligned} h(x \frown y) &= h([(x \frown y)^{\mathbf{c}}]^{\mathbf{c}}) \\ &= [h((x \frown y)^{\mathbf{c}})]^{\mathbf{c}} \\ &= [h(x^{\mathbf{c}} \smile y^{\mathbf{c}})]^{\mathbf{c}} \\ &= [h(x^{\mathbf{c}}) \smile h(y^{\mathbf{c}})]^{\mathbf{c}} \\ &= [h(x^{\mathbf{c}})]^{\mathbf{c}} \frown [h(y^{\mathbf{c}})]^{\mathbf{c}} \\ &= h([x^{\mathbf{c}}]^{\mathbf{c}}) \frown h([y^{\mathbf{c}}]^{\mathbf{c}}) = h(x) \frown h(y) \end{aligned}$$

Definizione 1.19. Un omomorfismo di algebre di Boole biiettivo prende il nome di *isomorfismo di algebre di Boole*. Due algebre di Boole $\mathcal{A}$ e $\mathcal{A}'$ si dicono *isomorfe* se esiste un isomorfismo di algebre di Boole da $\mathcal{A}$ in $\mathcal{A}'$. In tal caso scriveremo $\mathcal{A} \cong \mathcal{A}'$.

Questa definizione permette finalmente di attribuire un significato preciso all'unicità "a meno di isomorfismo" cui avevamo accennato nell'osservazione 1.5. Si dirà infatti che una data algebra di Boole $\mathcal{A}$ è l'unica, a meno di isomorfismo, a godere di determinate proprietà se ogni algebra di Boole soddisfacente quelle stesse proprietà è isomorfa ad $\mathcal{A}$.

Esempio 1.20. Si vede assai facilmente che $\{0,1\} \cong \mathbb{Z}/2\mathbb{Z}$. Infatti, basta associare agli interi 0 e 1 le classi di equivalenza delle quali sono rappresentanti in $\mathbb{Z}/2\mathbb{Z}$. Più in generale, ogni algebra di Boole costituita dai soli elementi neutri della somma e del prodotto è isomorfa a $\{0,1\}$. Quanto visto nell'osservazione 1.5 ci permette dunque di affermare che $\{0,1\}$ è l'unica algebra di Boole, a meno di isomorfismo, a essere un campo ed è anche l'unica, sempre a meno di isomorfismo, a essere un dominio integrale.

Teorema 1.21. *Siano $\mathcal{A} = \langle A, \leq, 0, 1\rangle$, $\mathcal{A}' = \langle A', \leq, 0, 1\rangle$ due algebre di Boole e sia h un'applicazione suriettiva da A in A'. Perché h sia un isomorfismo di algebre di Boole da $\mathcal{A}$ in $\mathcal{A}'$ è necessario e sufficiente che, per ogni $x, y \in A$, valga $x \leq y$ se e solo se $h(x) \leq h(y)$.*

Dimostrazione. Vediamo innanzitutto l'implicazione diretta. Il lemma 1.16 afferma che, se $x \leq y$, allora $h(x) \leq h(y)$. D'altra parte, l'ipotesi che h sia un isomorfismo di algebre di Boole ci fornisce le seguenti implicazioni:

$$\begin{aligned} & h(x) \leq h(y) \\ \implies & h(x)h(y) = h(x) \\ \implies & h(xy) = h(x) \\ \implies & xy = x \\ \implies & x \leq y \end{aligned}$$

Per dimostrare il viceversa faremo vedere che h è biiettiva, dopodiché ci serviremo del teorema precedente. La condizione che assumiamo per ipotesi ci permette di affermare immediatamente che h è iniettiva, dunque biiettiva perché, comunque fissati due elementi $u, v \in A$, abbiamo che:

$$\begin{aligned} & h(u) = h(v) \\ \implies & h(u) \leq h(v) \text{ e } h(v) \leq h(u) \\ \implies & u \leq v \text{ e } v \leq u \\ \implies & u = v \end{aligned}$$

Consideriamo ora due elementi $x, y \in A$ e poniamo $t = h(x) \frown h(y)$. Poiché h è suriettiva, esiste un elemento $z \in A$ tale che valga $t = h(z)$. Vogliamo mostrare che $z = x \frown y$. Questo fatto segue dalle ipotesi e dalla definizione di estremo inferiore, come si evince dalle seguenti implicazioni:

$$\begin{aligned} & h(z) = h(x) \frown h(y) \\ \implies & h(z) \leq h(x) \text{ e } h(z) \leq h(y) \\ \implies & z \leq x \text{ e } z \leq y \\ \implies & z \leq x \frown y \end{aligned} \qquad \begin{aligned} & x \frown y \leq x \text{ e } x \frown y \leq y \\ \implies & h(x \frown y) \leq h(x) \text{ e } h(x \frown y) \leq h(y) \\ \implies & h(x \frown y) \leq h(x) \frown h(y) = h(z) \\ \implies & x \frown y \leq z \end{aligned}$$

Abbiamo dunque dimostrato che $h(x \frown y) = h(x) \frown h(y)$ per ogni $x, y \in A$. Per poter applicare il teorema 1.17, ci rimane da mostrare che $h(x^{\mathbf{c}}) = h(x)^{\mathbf{c}}$ per un qualsiasi $x \in A$. Osserviamo allora che, ripetendo l'argomento precedente con $\smile$ e $\geq$ al posto di $\frown$ e $\leq$,[2] si ricava in modo immediato la condizione $h(x \smile y) = h(x) \smile h(y)$ per ogni $x, y \in A$. Notiamo inoltre che, per ogni $u \in A'$, se t è l'immagine inversa di u tramite la biiezione h, allora abbiamo $0 \leq t$ e $t \leq 1$ per la proprietà (a) della definizione 1.9. La condizione nota per ipotesi ci garantisce quindi che $h(0) \leq u$ e $u \leq h(1)$. Concludiamo, per arbitrarietà nella scelta di $u \in A'$, che $h(0)$ e $h(1)$ sono il minimo e il massimo di A', cioè che $h(0) = 0$ e $h(1) = 1$. Fatte queste considerazioni, possiamo finalmente affermare che, comunque fissato un elemento $x \in A$, vale $h(x^{\mathbf{c}}) = h(x)^{\mathbf{c}}$. Infatti, abbiamo le seguenti condizioni:

$$\begin{aligned} h(x) \frown h(x^{\mathbf{c}}) &= h(x \frown x^{\mathbf{c}}) = h(0) = 0 \\ h(x) \smile h(x^{\mathbf{c}}) &= h(x \smile x^{\mathbf{c}}) = h(1) = 1 \end{aligned}$$ □

Corollario 1.22. *Siano $\mathcal{A}$, $\mathcal{A}'$ e $\mathcal{A}''$ algebre di Boole e siano φ, ψ isomorfismi di algebre di Boole da $\mathcal{A}$ in $\mathcal{A}'$, da $\mathcal{A}'$ in $\mathcal{A}''$ rispettivamente. Allora l'applicazione composta $\psi \circ \varphi$ e l'applicazione inversa φ^{-1} sono isomorfismi di algebre di Boole da $\mathcal{A}$ in $\mathcal{A}''$, da $\mathcal{A}'$ in $\mathcal{A}$ rispettivamente.*

[2] Si intende che la relazione $\geq$ sul supporto A di una qualunque algebra di Boole $\mathcal{A}$ è definita ponendo $x \geq y$ se $y \leq x$.

Dimostrazione. Poiché le applicazioni $\psi \circ \varphi$ e φ^{-1} sono chiaramente suriettive, basta verificare la condizione fornita dal teorema 1.21. Osserviamo dunque che, per ogni $x, y \in A$, $u, v \in A'$, si ha:

$$\begin{aligned} & x \leq y \\ \iff & \varphi(x) \leq \varphi(y) \\ \iff & \psi(\varphi(x)) \leq \psi(\varphi(y)) \end{aligned} \qquad \begin{aligned} & u \leq v \\ \iff & \varphi(\varphi^{-1}(u)) \leq \varphi(\varphi^{-1}(v)) \\ \iff & \varphi^{-1}(u) \leq \varphi^{-1}(v) \end{aligned}$$ □

1.4 Ideali

Definizione 1.23. Sia $\mathcal{R} = \langle R, +, \times, 0, 1\rangle$ un anello commutativo e unitario con $1 \neq 0$. Diremo che un sottoinsieme I di R è un *ideale di* $\mathcal{R}$ se soddisfa le condizioni che seguono:

- Vale che $\langle I, +, 0\rangle$ è un sottogruppo di $\langle R, +, 0\rangle$.
- Per ogni $x \in I$ e per ogni $y \in R$, vale che $xy \in I$.
- Si ha che $I \neq R$ oppure, equivalentemente, che $1 \notin I$.

Solitamente in algebra non si richiede la terza condizione, che contraddistingue invece ciò che viene comunemente chiamato "ideale proprio". L'equivalenza tra $I \neq R$ e $1 \notin I$ si giustifica come segue. Da una parte, se $I = R$, allora si ha $1 \in I$ ovviamente. Dall'altra, se assumiamo $1 \in I$, per la seconda condizione della definizione vale $I = R$ perché, per ogni $y \in R$, si ha $1 \times y \in I$. Diamo ora una caratterizzazione degli ideali nel contesto delle algebre di Boole.

Teorema 1.24. *Sia $\mathcal{A} = \langle A, \leq, 0, 1\rangle$ un'algebra di Boole e sia I un sottoinsieme di A. Allora I è un ideale di $\mathcal{A}$ se e solo se sono soddisfatte le tre condizioni seguenti:*

(i) $0 \in I$ *e* $1 \notin I$.

(ii) *Per ogni $x, y \in I$, vale che $x \smile y \in I$.*

(iii) *Per ogni $x \in I$ e per ogni $y \in A$, se $y \leq x$, allora $y \in I$.*

Dimostrazione. Supponiamo innanzitutto che I sia un ideale di $\mathcal{A}$. La condizione (i) è banalmente soddisfatta perché I è in particolare un sottogruppo di $\langle A, +, 0\rangle$ e $1 \notin I$ per definizione di ideale. La condizione (ii) è conseguenza immediata del fatto che $x \smile y = x + y + xy$ per la proprietà (iii) del teorema 1.7. Osserviamo poi che, se $x \in I$ e se $y \in A$, allora $xy \in I$ per definizione di ideale e, se inoltre $y \leq x$, allora $xy = y$ e di conseguenza $y \in I$. Dunque abbiamo anche la condizione (iii).

Occupiamoci ora del viceversa. Dati due qualsiasi elementi $x, y \in I$, per la condizione (ii) si ha che $x \smile y \in I$ ma, come è immediato verificare, vale la disuguaglianza $x + y \leq x \smile y$ e inoltre, per il lemma 1.4, sappiamo che $x + y = x - y$. La condizione (iii) ci garantisce allora che $x - y \in I$ e questo fatto, assieme all'ipotesi che $0 \in I$ data dalla condizione (i), ci permette di affermare che $\langle I, +, 0\rangle$ è un sottogruppo di $\langle A, +, 0\rangle$.[3] Osserviamo adesso che, se $x \in I$ e se $y \in A$ allora, poiché in un'algebra di Boole vale sempre $xy \leq y$, per la condizione (iii) si ha $xy \in I$. Essendo infine $1 \notin I$ per la condizione (i), possiamo concludere che I è un ideale di $\mathcal{A}$. □

Corollario 1.25. *Sia $\mathcal{A}$ un'algebra di Boole e sia I un ideale di $\mathcal{A}$. Allora non esiste alcun elemento $x \in A$ tale che $x \in I$ e $1 + x \in I$.*

[3] Se H è un sottoinsieme non vuoto di un gruppo $\langle G, +, 0\rangle$, vale che $\langle H, +, 0\rangle$ è un sottogruppo di $\langle G, +, 0\rangle$ se e solo se $a - b \in H$ per ogni $a, b \in H$. Per una dimostrazione, si veda [7].

Dimostrazione. Osserviamo che, se esistesse un tale $x \in A$ allora, per la proprietà (ii) del teorema precedente, avremmo $1 \in I$ in quanto $x \smile (1 + x) = 1$. Ma questo contraddice la proprietà (i). □

La condizione (ii) del teorema 1.24 si generalizza facilmente, per induzione sul numero degli elementi. Per la convenzione $x_1 \smile x_2 \smile \cdots \smile x_k = x_1$ introdotta nella nota 1, possiamo includere anche il caso $k = 1$.

Corollario 1.26. *Sia $\mathcal{A}$ un'algebra di Boole e sia I un ideale di $\mathcal{A}$. Allora, per qualsiasi intero $k \geq 1$ e per ogni $x_1, x_2, \ldots, x_k \in I$, vale che $x_1 \smile x_2 \smile \cdots \smile x_k \in I$.*

Esempio 1.27. Sia $\mathcal{A}$ un'algebra di Boole. Dato un elemento $a \in A$ con $a \neq 1$ si verifica facilmente, sfruttando il teorema 1.24, che l'insieme $I_a = \{x \in A : x \leq a\}$ è un ideale di $\mathcal{A}$. Si veda [2] per una dimostrazione esplicita. L'ideale I_a di $\mathcal{A}$ prende il nome di *ideale principale generato da a*.

Consideriamo ora un anello commutativo e unitario $\mathcal{R} = \langle R, +, \times, 0, 1 \rangle$ con $1 \neq 0$ e un ideale I di $\mathcal{R}$. Definiamo su R una relazione di equivalenza, detta *congruenza modulo I*, nel modo seguente: per ogni $x, y \in R$, poniamo $x \equiv_I y$ se $x - y \in I$. Denotiamo $\overline{x}$ la classe di equivalenza di un certo elemento $x \in R$. Definiamo le seguenti operazioni binarie che, commettendo un piccolo abuso di notazione, indichiamo ancora con i simboli + e ×:

$$\overline{x} + \overline{y} = \overline{x + y}$$
$$\overline{x} \times \overline{y} = \overline{x \times y}$$

L'insieme quoziente $R/\equiv_I$ acquisisce, con queste operazioni, una struttura di anello commutativo e unitario, nota come *anello quoziente di $\mathcal{R}$ rispetto a I* e indicata con $\mathcal{R}/I$.[4] Gli elementi neutri della somma e del prodotto sono, naturalmente, le classi $\overline{0}$ e $\overline{1}$.

Lemma 1.28. *Sia $\mathcal{A}$ un'algebra di Boole e sia I un ideale di $\mathcal{A}$. Allora l'anello $\mathcal{A}/I$ è un'algebra di Boole.*

Dimostrazione. Basta osservare che, per come è definita la moltiplicazione in $\mathcal{A}/I$, gli elementi di $\mathcal{A}/I$ ereditano da quelli di $\mathcal{A}$ la proprietà di essere idempotenti rispetto al prodotto. Si ha infatti:

$$\overline{x}^2 = \overline{x} \times \overline{x} = \overline{x \times x} = \overline{x}$$ □

Teorema 1.29. *Sia $\mathcal{A}$ un'algebra di Boole e sia I un sottoinsieme di A. Allora le seguenti affermazioni sono equivalenti:*

(1) Vale che I è un ideale di $\mathcal{A}$.

(2) Esiste un omomorfismo di algebre di Boole h da $\mathcal{A}$ tale che I sia il nucleo di h, cioè tale che valga:

$$I = h^{-1}(\{0\}) = \{x \in A : h(x) = 0\}$$

(3) Esiste un omomorfismo di anelli unitari h da $\mathcal{A}$ tale che I sia il nucleo di h.

Dimostrazione. Sarà sufficiente dimostrare che (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) $\Longrightarrow$ (1). Osserviamo subito che l'implicazione (2) $\Longrightarrow$ (3) è banale per l'osservazione 1.14. Vediamo ora le altre due implicazioni.

- (1) $\Longrightarrow$ (2). Se I è un ideale di $\mathcal{A}$, allora l'anello quoziente $\mathcal{A}/I$ è un'algebra di Boole per il lemma 1.28. Consideriamo la mappa quoziente h da $\mathcal{A}$ in $\mathcal{A}/I$, detta anche omomorfismo canonico, la quale è per definizione la funzione che manda ciascun elemento $x \in A$ nella

[4] Per una dimostrazione dettagliata, si rimanda a [7].

sua classe di congruenza modulo I. Il teorema 1.17 garantisce che h sia un omomorfismo di algebre di Boole. Infatti abbiamo, per qualsiasi $x, y \in A$, le due condizioni che seguono:

$$h(x \frown y) = h(xy) = \overline{xy} = \overline{x} \times \overline{y} = h(x) \times h(y) = h(x) \frown h(y)$$
$$h(x^{\mathbf{c}}) = h(1 + x) = \overline{1 + x} = \overline{1} + \overline{x} = \overline{1} + h(x) = h(x)^{\mathbf{c}}$$

D'altra parte è del tutto evidente che I sia il nucleo di h perché $x \in I$ se e solo se $x \equiv_I 0$, cioè se e solo se $h(x) = \overline{0}$.

- (3) $\Longrightarrow$ (1). Per ipotesi esistono un anello unitario $\mathcal{R} = \langle R, +, \times, 0, 1 \rangle$ e un omomorfismo di anelli unitari h da $\mathcal{A}$ in $\mathcal{R}$ tale che I sia il nucleo di h. Per concludere che I è un ideale di $\mathcal{A}$, sarà sufficiente verificare le condizioni date dal teorema 1.24. Siccome $h(0) = 0$ per l'osservazione 1.15 e $h(1) = 1$ per definizione di omomorfismo di anelli unitari, si ha che $0 \in I$ e $1 \notin I$, cioè la condizione (i). Se $x, y \in I$, cioè se $h(x) = 0$ e $h(y) = 0$, allora abbiamo:

$$h(x \smile y) = h(x + y + xy) = h(x) + h(y) + h(x)h(y) = 0$$

Dunque anche $x \smile y \in I$ e la condizione (ii) è soddisfatta. Se infine $x \in I$, $y \in A$ e $y \leq x$, allora $h(x) = 0$ e $xy = y$. Ne segue che $y \in I$, cioè che la condizione (iii) è verificata, infatti:

$$h(y) = h(xy) = h(x)h(y) = 0$$ □

1.5 Ideali massimali

Secondo le nostre convenzioni, un ideale è sempre un "ideale proprio" e di conseguenza un *ideale massimale* di un anello $\mathcal{R}$ sarà semplicemente un ideale che non è contenuto strettamente in alcun altro ideale di $\mathcal{R}$, cioè un elemento massimale, rispetto all'inclusione insiemistica, nell'insieme di tutti gli ideali di $\mathcal{R}$. Adesso si vogliono caratterizzare gli ideali massimali delle algebre di Boole.

Teorema 1.30. *Sia $\mathcal{A}$ un'algebra di Boole e sia I un ideale di $\mathcal{A}$. Le seguenti affermazioni sono equivalenti:*

(1) Vale che I è un ideale massimale di $\mathcal{A}$.

(2) L'anello quoziente $\mathcal{A}/I$ è isomorfo all'algebra di Boole $\{0, 1\}$.

(3) L'ideale I è il nucleo di un omomorfismo da $\mathcal{A}$ in $\{0, 1\}$.

(4) Per ogni $x \in A$, vale che $x \in I$ oppure $1 + x \in I$.

(5) Per ogni $x, y \in A$, se $xy \in I$, allora $x \in I$ oppure $y \in I$.[5]

(6) Per ogni $k \geq 1$ e per ogni $x_1, x_2, \ldots, x_k \in A$, se $x_1 x_2 \cdots x_k \in I$, allora $x_i \in I$ per un certo indice $i \in \{1, 2, \ldots, k\}$.

Dimostrazione. Basta dimostrare che (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) $\Longrightarrow$ (4) $\Longrightarrow$ (5) $\Longrightarrow$ (1) e che (5) $\Longleftrightarrow$ (6).

- (1) $\Longrightarrow$ (2). Un ben noto risultato di algebra ci garantisce che, dati un anello commutativo e unitario $\mathcal{R}$ con $1 \neq 0$ e un ideale I di $\mathcal{R}$, l'anello quoziente $\mathcal{R}/I$ è un campo se e solo se I è un ideale massimale di $\mathcal{R}$. Per una dimostrazione di questo fatto si veda [2] o [7]. Tuttavia abbiamo anche osservato, nell'esempio 1.20, che $\{0, 1\}$ è l'unica algebra di Boole, a meno di isomorfismo, a essere anche un campo. Se dunque I è un ideale massimale di $\mathcal{A}$, allora $\mathcal{A}/I$ è un campo e quindi $\mathcal{A}/I \cong \{0, 1\}$.

[5] In letteratura, un ideale di un anello $\mathcal{R}$ soddisfacente tale proprietà viene spesso chiamato un *ideale primo di $\mathcal{R}$*.

- (2) $\Longrightarrow$ (3). Basta osservare che I è il nucleo della mappa quoziente h da $\mathcal{A}$ in $\mathcal{A}/I$. Questo fatto lo abbiamo già giustificato nella dimostrazione del teorema 1.29. Poiché abbiamo per ipotesi un isomorfismo φ da $\mathcal{A}/I$ in $\{0,1\}$, l'ideale I sarà il nucleo dell'omomorfismo $\varphi \circ h$ da $\mathcal{A}$ in $\{0,1\}$.

- (3) $\Longrightarrow$ (4). Per ipotesi, possiamo considerare un omomorfismo h da $\mathcal{A}$ in $\{0,1\}$ di cui I sia il nucleo. Per qualsiasi $x \in A$, abbiamo $h(x) = 0$ oppure $h(x) = 1$. Osserviamo quindi che:

$$\begin{aligned} & h(x) = 0 \\ & \Longrightarrow\ x \in I \end{aligned} \qquad\qquad \begin{aligned} & h(x) = 1 \\ & \Longrightarrow\ 1 + h(x) = 0 \\ & \Longrightarrow\ h(1+x) = 0 \\ & \Longrightarrow\ 1 + x \in I \end{aligned}$$

- (4) $\Longrightarrow$ (5). Fissiamo due elementi $x, y \in A$ e mostriamo che, se $x \notin I$ e $y \notin I$, allora $xy \notin I$. Se $x \notin I$ e $y \notin I$ allora, per la condizione (4), dobbiamo avere $1 + x \in I$ e $1 + y \in I$ e quindi $(1 + x) \smile (1 + y) \in I$ per la proprietà (ii) del teorema 1.24. Ma $(1 + x) \smile (1 + y) = 1 + xy$ e dunque $1 + xy \in I$. Dal corollario 1.25 discende quindi che $xy \notin I$.

- (5) $\Longrightarrow$ (1). Si procede per contrapposizione logica e cioè si dimostra che, se non vale (1), allora non vale nemmeno (5). Supponiamo allora che I non sia un ideale massimale di $\mathcal{A}$ e consideriamo un ideale J di $\mathcal{A}$ che contenga strettamente I. Esiste dunque un elemento $a \in J$ tale che $a \notin I$. Per il corollario 1.25 dobbiamo avere $1 + a \notin J$ e anche $1 + a \notin I$ in virtù dell'inclusione $I \subseteq J$. D'altra parte, si ha $a(1 + a) = 0$. Ne deduciamo che la proprietà (5) non è soddisfatta in quanto $a \notin I$ e $1 + a \notin I$, mentre $a(1 + a) \in I$ per definizione di ideale.

- (5) $\Longrightarrow$ (6). Si procede per induzione sull'intero $k \geq 1$. La base, vale a dire il caso $k = 1$, è ovvia. Nel passo induttivo assumiamo $k \geq 2$, supponiamo che la proprietà da dimostrare sia vera per $k - 1$ e facciamo vedere che vale anche per k. Siano quindi $x_1, x_2, \ldots, x_k \in A$ degli elementi fissati tali che $x_1 x_2 \cdots x_k \in I$. Per il punto (5) si ha $x_1 x_2 \cdots x_{k-1} \in I$ oppure $x_k \in I$. Ma, per ipotesi induttiva, la condizione $x_1 x_2 \cdots x_{k-1} \in I$ implica $x_i \in I$ per qualche indice $i \in \{1, 2, \ldots, k-1\}$ e allora concludiamo che $x_i \in I$ per un qualche $i \in \{1, 2, \ldots, k\}$.

- (6) $\Longrightarrow$ (5). Basta restringersi al caso $k = 2$ della proprietà che assumiamo per ipotesi. □

Osservazione 1.31. Dal teorema appena dimostrato e, in particolare, dall'equivalenza (1) $\Longleftrightarrow$ (3) discende che, in un'algebra di Boole $\mathcal{A}$, l'insieme degli ideali massimali di $\mathcal{A}$ è in corrispondenza biunivoca con l'insieme degli omomorfismi di algebre di Boole da $\mathcal{A}$ in $\{0,1\}$. Infatti, associamo a un omomorfismo da $\mathcal{A}$ in $\{0,1\}$ il suo nucleo che, grazie all'implicazione (3) $\Longrightarrow$ (1), è un ideale massimale di $\mathcal{A}$. Abbiamo così una mappa ben definita che è anche suriettiva per l'implicazione (1) $\Longrightarrow$ (3) e iniettiva perché, se g e h sono omomorfismi di algebre di Boole da $\mathcal{A}$ in $\{0,1\}$ con lo stesso nucleo I, allora g e h sono identici. Infatti, per ogni $x \in A$, vale $x \in I$ oppure $x \notin I$, dunque $g(x) = 0$ e $h(x) = 0$ oppure $g(x) = 1$ e $h(x) = 1$.

1.6 Filtri e ultrafiltri

Introduciamo ora la nozione duale di quella di ideale in un'algebra di Boole.

Definizione 1.32. Sia $\mathcal{A}$ un'algebra di Boole. Un sottoinsieme F di A tale che $\{x \in A : x^c \in F\}$ sia un ideale di $\mathcal{A}$ viene detto un *filtro di* $\mathcal{A}$.

Osservazione 1.33. Conseguenza immediata della definizione precedente è che, dato un filtro F in un'algebra di Boole $\mathcal{A}$, l'ideale $I = \{x \in A : x^c \in F\}$ a esso associato è univocamente determinato. Si dice allora che I è l'*ideale duale di* F. Osserviamo che, se due filtri F e G di $\mathcal{A}$ hanno uno stesso ideale duale I, allora $F = G$. Infatti, poiché l'operazione $x \mapsto x^c$ di passaggio al complementare è involutiva (punto (ix) del teorema 1.7), abbiamo $x \in F$ se e solo se $x^c \in I$, essendo $x = (x^c)^c$, e per lo stesso motivo $x^c \in I$ se e solo se $x \in G$. Ragionando allo stesso modo, si vede facilmente che un qualsiasi ideale I di $\mathcal{A}$ è l'ideale duale del filtro $F = \{x \in A : x^c \in I\}$. Per questo diremo anche che F è il *filtro duale di* I. Abbiamo dunque ottenuto una corrispondenza biunivoca tra l'insieme degli ideali di $\mathcal{A}$ e l'insieme dei filtri di $\mathcal{A}$.

Come conseguenza della dualità descritta nell'osservazione precedente, otteniamo per i filtri dei risultati analoghi al teorema 1.24 e ai corollari 1.25 e 1.26.

Teorema 1.34. *Sia $\mathcal{A} = \langle A, \leq, 0, 1\rangle$ un'algebra di Boole e sia F un sottoinsieme di A. Allora F è un filtro di $\mathcal{A}$ se e solo se sono soddisfatte le tre condizioni seguenti:*

(f) $0 \notin F$ *e* $1 \in F$.

(ff) *Per ogni* $x, y \in F$, *vale che* $x \frown y \in F$.

(fff) *Per ogni* $x \in F$ *e per ogni* $y \in A$, *se* $x \leq y$, *allora* $y \in F$.

Dimostrazione. Sia $I = \{x \in A : x^c \in F\}$. Se F è un filtro, allora I è l'ideale duale di F e dunque le condizioni (i), (ii) e (iii) del teorema 1.24 sono tutte verificate. Le condizioni (f), (ff) e (fff) di questo enunciato seguono allora, rispettivamente, dal fatto che $0^c = 1$ e $1^c = 0$, dalle leggi di de Morgan e dal teorema 1.7-(ix). Viceversa, per le stesse ragioni di prima, le proprietà (f), (ff) e (fff) implicano i punti (i), (ii) e (iii) del teorema 1.24 e questi forniscono una condizione sufficiente perché I sia un ideale di $\mathcal{A}$. Dunque F è un filtro di $\mathcal{A}$. □

Corollario 1.35. *Sia $\mathcal{A}$ un'algebra di Boole e sia F un filtro di $\mathcal{A}$. Allora non esiste alcun elemento $x \in A$ tale che $x \in F$ e $1 + x \in F$.*

Corollario 1.36. *Sia $\mathcal{A}$ un'algebra di Boole e sia F un filtro di $\mathcal{A}$. Allora, per qualsiasi intero $k \geq 1$ e per ogni $x_1, x_2, \ldots, x_k \in F$, vale che $x_1 \frown x_2 \frown \cdots \frown x_k \in F$.*

Esempio 1.37. Sia $\mathcal{A}$ un'algebra di Boole. Dato un qualunque elemento non nullo $a \in A$, il filtro duale dell'ideale principale generato da $1 + a$, cioè $F_a = \{x \in A : a \leq x\}$, è detto il *filtro principale generato da* a.

Definizione 1.38. Sia $\mathcal{A}$ un'algebra di Boole. Un filtro di $\mathcal{A}$ che non è strettamente contenuto in alcun altro filtro, cioè un elemento massimale, rispetto all'inclusione insiemistica, nell'insieme di tutti i filtri di $\mathcal{A}$, si dice un *ultrafiltro di* $\mathcal{A}$.

È del tutto evidente che la corrispondenza biunivoca ottenuta nell'osservazione 1.33 tra filtri e ideali induce, per restrizione, una biiezione tra ultrafiltri e ideali massimali. Abbiamo infatti che il filtro duale di un ideale massimale è un ultrafiltro, mentre l'ideale duale di un ultrafiltro è un ideale massimale. E allora abbiamo anche l'analogo per i filtri del teorema 1.30.

Teorema 1.39. *Sia $\mathcal{A}$ un'algebra di Boole e sia F un filtro di $\mathcal{A}$. Le seguenti affermazioni sono equivalenti:*

(1′) *Vale che F è un ultrafiltro di $\mathcal{A}$.*

(3′) *Esiste un omomorfismo h da $\mathcal{A}$ in $\{0, 1\}$ tale che $F = \{x \in A : h(x) = 1\}$.*

(4′) *Per ogni $x \in A$, vale che $x \in F$ oppure $1 + x \in F$.*

(5′) *Per ogni $x, y \in A$, se $x \smile y \in F$, allora $x \in F$ oppure $y \in F$.*

(6′) *Per ogni $k \geq 1$ e per ogni $x_1, x_2, \ldots, x_k \in A$, se $x_1 \smile x_2 \smile \cdots \smile x_k \in F$, allora $x_i \in F$ per qualche indice $i \in \{1, 2, \ldots, k\}$.*

Dimostrazione. Sia $I = \{x \in A \colon x^c \in F\}$. L'asserto è una semplice conseguenza del teorema 1.30 e dell'equivalenza dei punti (1), (3), (4), (5) e (6) del risultato che abbiamo appena menzionato con i punti (1′), (3′), (4′), (5′) e (6′) di questo enunciato. La verifica di tale equivalenza è immediata. □

Osservazione 1.40. Le disgiunzioni che compaiono nel punto (4) del teorema 1.30 e nel punto (4′) del teorema 1.39 sono in effetti delle disgiunzioni esclusive a causa dei corollari 1.25 e 1.35. Come conseguenza di questo fatto, se F è un ultrafiltro di un'algebra di Boole $\mathcal{A}$ e se I è l'ideale duale di F, allora I e F formano una partizione di A. Infatti $A = I \cup F$ perché, dato un elemento $x \in A$, se $x \notin I$, allora $1 + x \in I$ e dunque $x \in F$. Inoltre, gli insiemi I e F sono disgiunti perché $x \in I$ se e solo se $1 + x \notin I$, cioè se e solo se $x \notin F$. Possiamo allora concludere che I e F sono al tempo stesso:

- L'uno il complementare dell'altro, in quanto sottoinsiemi di A.
- L'uno l'insieme dei complementi degli elementi dell'altro.

Osservazione 1.41. Riprendendo quanto avevamo detto prima di enunciare il teorema precedente, possiamo completare l'osservazione 1.31 dicendo che, in una qualunque algebra di Boole $\mathcal{A}$, sono in corrispondenza biunivoca gli insiemi degli ideali massimali di $\mathcal{A}$, degli ultrafiltri di $\mathcal{A}$ e degli omomorfismi di algebre di Boole da $\mathcal{A}$ in $\{0, 1\}$. Se indichiamo con h_I l'omomorfismo di algebre di Boole da $\mathcal{A}$ in $\{0, 1\}$ associato a un ideale massimale I di $\mathcal{A}$, ovvero tale che I sia il suo nucleo, allora possiamo scrivere in maniera più esplicita la corrispondenza biunivoca sopra menzionata:

$$
\begin{array}{ccccc}
\{\text{Ideali massimali di } \mathcal{A}\} & \longleftrightarrow & \{\text{Ultrafiltri di } \mathcal{A}\} & \longleftrightarrow & \left\{\begin{array}{c}\text{Omomorfismi di}\\ \text{algebre di Boole}\\ \text{da } \mathcal{A} \text{ in } \{0,1\}\end{array}\right\} \\
I & \longmapsto & A \setminus I & & \\
A \setminus F & \longmapsfrom & F & \longmapsto & h_{A\setminus F} \\
 & & \{x \in A \colon h(x) = 1\} & \longmapsfrom & h \\
I & \longmapsto & & & h_I \\
\{x \in A \colon h(x) = 0\} & \longmapsfrom & & & h
\end{array}
$$

1.7 Basi di filtri

Definizione 1.42. Sia $\mathcal{A} = \langle A, \leq, 0, 1\rangle$ un'algebra di Boole. Diremo che un sottoinsieme X di A è una *base di un filtro di $\mathcal{A}$* se verifica la proprietà dell'intersezione finita cioè se, per ogni intero $k \geq 1$ e per ogni $x_1, x_2, \ldots, x_k \in X$, abbiamo che $x_1 \frown x_2 \frown \cdots \frown x_k \neq 0$. In altre parole, una base di un filtro di $\mathcal{A}$ è un sottoinsieme di A tale che ogni suo sottoinsieme finito non vuoto abbia estremo inferiore non nullo.

Lemma 1.43. *Sia $\mathcal{A} = \langle A, \leq, 0, 1\rangle$ un'algebra di Boole e sia X un sottoinsieme di A. Allora X è una base di un filtro di $\mathcal{A}$ se e solo se esiste un filtro di $\mathcal{A}$ che contiene X.*

Dimostrazione. Il viceversa si dimostra facilmente. Supponiamo infatti che X sia contenuto in un filtro F di $\mathcal{A}$, consideriamo un intero $k \geq 1$ ed elementi $x_1, x_2, \ldots, x_k \in X$. Siccome in particolare $x_1, x_2, \ldots, x_k \in F$, il corollario 1.36 garantisce che anche $x_1 \frown x_2 \frown \cdots \frown x_k \in F$. D'altra parte, ci è noto che $0 \notin F$ per la condizione (f) del teorema 1.34 e dunque abbiamo che $x_1 \frown x_2 \frown \cdots \frown x_k \neq 0$. Questo dimostra che X è una base di un filtro di $\mathcal{A}$.

Dimostriamo ora l'implicazione diretta. Osserviamo subito che, se X è vuoto, allora $\{1\} = F_1$ è un filtro di $\mathcal{A}$ contenente X. Possiamo dunque ridurci al caso in cui X è non vuoto. Definiamo:

$$F_X = \{x \in A \colon x_1 \frown x_2 \frown \cdots \frown x_k \leq x \text{ per qualche intero } k \geq 1 \text{ e per certi } x_1, x_2, \ldots, x_k \in X\}$$

È del tutto evidente che F_X contiene X e quindi, per concludere, sarà sufficiente dimostrare che F_X è un filtro di $\mathcal{A}$, ma questa è una semplice conseguenza del teorema 1.34. Delle tre condizioni da verificare, la più significativa e interessante è senz'altro la (f). Notiamo infatti che $0 \notin F_X$ perché, se fosse $0 \in F_X$, allora si avrebbe una contraddizione con l'ipotesi che X sia una base di un filtro di $\mathcal{A}$ e osserviamo che $1 \in F_X$ perché X è non vuoto e 1 è il massimo di A rispetto alla relazione d'ordine $\leq$. La condizione (ff) del teorema 1.34, invece, è valida in virtù del fatto che, se abbiamo le condizioni $x_1 \frown x_2 \frown \cdots \frown x_h \leq x$ e $y_1 \frown y_2 \frown \cdots \frown y_k \leq y$, allora:

$$x_1 \frown x_2 \frown \cdots \frown x_h \frown y_1 \frown y_2 \frown \cdots \frown y_k \leq x \frown y$$

La condizione (fff) del teorema 1.34, infine, vale perché le due condizioni $x_1 \frown x_2 \frown \cdots \frown x_h \leq x$ e $x \leq y$ implicano $x_1 \frown x_2 \frown \cdots \frown x_h \leq y$. □

Ricordiamo ora un importante risultato di teoria degli anelli sull'esistenza di ideali massimali. La dimostrazione, che utilizza il lemma di Zorn, viene trattata in [2] e in [7].

Teorema 1.44 (di Krull). *Sia $\mathcal{R} = \langle R, +, \times, 0, 1\rangle$ un anello unitario con $1 \neq 0$. Allora ogni ideale di $\mathcal{R}$ è contenuto in un ideale massimale di $\mathcal{R}$.*

In effetti, il teorema di Krull è addirittura equivalente al lemma di Zorn, come dimostrato dal matematico britannico W. Hodges nella pubblicazione [6]. Non è dunque possibile fare a meno del lemma di Zorn per stabilire questo risultato, perché il lemma di Zorn non è derivabile dagli altri assiomi della teoria degli insiemi di Zermelo-Fraenkel. È infatti ben nota l'equivalenza delle tre formulazioni seguenti dell'assioma della scelta, delle quali una è appunto il lemma di Zorn.

Formulazione 1 (Teorema del buon ordinamento)**.** Sia X un insieme. Allora X ammette un buon ordinamento, cioè esiste una relazione d'ordine parziale $\leq$ su X tale che ogni sottoinsieme $Y \subseteq X$ non vuoto abbia un minimo.

Formulazione 2 (Lemma di Zorn)**.** Sia $\langle X, \leq\rangle$ un insieme parzialmente ordinato tale che ciascun sottoinsieme totalmente ordinato di X ammetta un maggiorante. Allora esiste in X un elemento massimale.

Formulazione 3 (Funzione di scelta)**.** Sia $\{X_i\}$ una famiglia di insiemi non vuoti indicizzata su un insieme I. Allora il prodotto $\prod X_i$ è un insieme non vuoto, cioè è possibile scegliere un elemento $x_i \in X_i$ per ogni $i \in I$.

Non richiamiamo le definizioni basilari sulle relazioni d'ordine, per le quali si rimanda a [3]. Vale invece la pena ricordare le nozioni di famiglia di insiemi e di prodotto, in quanto ci saranno utili per il capitolo successivo.

Definizione 1.45. Sia I un insieme. Una funzione f di dominio I che a ciascun indice $i \in I$ associa un insieme X_i si dice una *famiglia di insiemi* e si denota $\{X_i\}$. Se inoltre f ha immagine finita, cioè se gli insiemi X_i distinti, con $i \in I$, sono in numero finito, diremo che la famiglia $\{X_i\}$ è *finita*. La restrizione di f su un sottoinsieme di I viene invece detta una *sottofamiglia di* $\{X_i\}$. Infine, se X_i è costituito da un unico elemento x_i per ogni $i \in I$, la famiglia di insiemi $\{X_i\}$ si indica con $\{x_i\}$ ed è detta una *successione*.

Non specificheremo di volta in volta l'insieme I degli indici, purché questa scelta non produca ambiguità. Quando diremo che $\{X_i\}$ è una famiglia di insiemi sarà dunque sottintesa l'esistenza di un insieme I sul quale la famiglia è indicizzata.

Definizione 1.46. Sia $\{X_i\}$ una famiglia di insiemi indicizzata su un qualche insieme I. L'insieme delle successioni $\{x_i\}$ tali che $x_i \in X_i$ per ogni $i \in I$ si dice il *prodotto della famiglia* $\{X_i\}$ e si denota $\prod X_i$.

Non ci occuperemo di giustificare l'equivalenza delle formulazioni 1, 2 e 3 e rimandiamo per questo a [1]. La dimostrazione del fatto che l'assioma della scelta è indipendente, vale a dire non derivabile, dalla teoria di Zermelo-Fraenkel risale invece al 1963 e utilizza la tecnica del "forcing" dovuta al matematico statunitense P. Cohen. Essa è reperibile in [4] e in [8].

Conseguenza immediata del teorema di Krull e della dualità tra ultrafiltri e ideali massimali è il seguente risultato.

Teorema 1.47 (dell'ultrafiltro)**.** *Sia $\mathcal{A} = \langle A, +, \times, 0, 1\rangle$ un'algebra di Boole. Allora ogni filtro di $\mathcal{A}$ è contenuto in un ultrafiltro di $\mathcal{A}$.*

Dimostrazione. Sia F un filtro di $\mathcal{A}$. Per il teorema di Krull, l'ideale duale di F è contenuto in un ideale massimale I di $\mathcal{A}$. Ne segue che il filtro duale di I è un ultrafiltro di $\mathcal{A}$ contenente F. □

Il teorema dell'ultrafiltro ci permette di fornire una formulazione alternativa del lemma 1.43.

Lemma 1.48. *Sia $\mathcal{A} = \langle A, \leq, 0, 1\rangle$ un'algebra di Boole e sia X un sottoinsieme di A. Allora X è una base di un filtro di $\mathcal{A}$ se e solo se esiste un ultrafiltro di $\mathcal{A}$ che contiene X.*

Dimostrazione. Il viceversa deriva banalmente dal lemma 1.43 perché gli ultrafiltri sono filtri. Per l'implicazione diretta basta invece osservare che da una parte il lemma 1.43 garantisce l'esistenza di un filtro F di $\mathcal{A}$ che contiene X, dall'altra il teorema dell'ultrafiltro fornisce un ultrafiltro di $\mathcal{A}$ che contiene F e dunque X. □

Capitolo 2

Il teorema di Stone

2.1 Nozioni di topologia

Ricordiamo alcuni fatti di topologia di cui avremo bisogno nel seguito.

Innanzitutto, dato uno spazio topologico X, ogni suo sottoinsieme Y può essere munito di una topologia, detta la *topologia indotta su* Y, prendendo come insiemi aperti di Y le intersezioni con Y degli aperti di X. In tal caso, diremo che Y è un *sottospazio di* X.

Un'applicazione tra due spazi topologici che è continua e biiettiva con inversa continua si dice un *omeomorfismo*. Due spazi topologici X_1 e X_2 si dicono *omeomorfi* se esiste un omeomorfismo da X_1 a X_2 e in tal caso scriveremo $X_1 \approx X_2$.

Una famiglia $\{\Omega_i\}$ di insiemi aperti di uno spazio topologico X si dice una *base di aperti di* X se ogni aperto di X si può esprimere come unione di aperti di $\{\Omega_i\}$. Una volta fissata una base di aperti di X, chiameremo *aperti elementari di* X i suoi elementi e parleremo di *chiusi elementari di* X per riferirci ai complementari degli aperti elementari di X. Il risultato che segue è senza dubbio prevedibile.

Lemma 2.1. *Sia X uno spazio topologico e sia Y un sottospazio di X. Se $\{\Omega_i\}$ è una base di aperti di X, allora $\{\Omega_i \cap Y\}$ è una base di aperti di Y.*

Dimostrazione. Sia V un insieme aperto di Y. Poiché per ipotesi Y è un sottospazio di X, anche Y è uno spazio topologico e ha la topologia indotta. Esiste allora un insieme aperto U di X tale che $V = U \cap Y$. Sia ora I l'insieme che indicizza la famiglia di insiemi $\{\Omega_i\}$. Dall'assunzione che $\{\Omega_i\}$ sia una base di aperti di X segue l'esistenza di un sottoinsieme J di I tale che $U = \bigcup_{j\in J} \Omega_j$. Ora, passando all'intersezione con Y, abbiamo che $V = \bigcup_{j\in J}(\Omega_j \cap Y)$ perché, come si vede facilmente per doppia inclusione, vale $(\bigcup_{j\in J} \Omega_j) \cap Y = \bigcup_{j\in J}(\Omega_j \cap Y)$. Avendo espresso un insieme aperto di Y qualsiasi come unione di elementi di $\{\Omega_i \cap Y\}$ ed essendo tali elementi insiemi aperti di Y per definizione di topologia indotta, concludiamo che $\{\Omega_i \cap Y\}$ è una base di aperti di Y. □

Uno spazio topologico X si dice uno *spazio di Hausdorff* se, comunque presi due punti distinti $x, y \in X$, esistono due insiemi aperti disgiunti U e V di X tali che $x \in U$ e $y \in V$.

Una famiglia $\{E_i\}$ di sottoinsiemi di uno spazio topologico X viene detta un *ricoprimento di* X se l'unione degli insiemi E_i è uguale a X. Se inoltre tali insiemi E_i sono aperti di X, allora diremo che la famiglia $\{E_i\}$ è un *ricoprimento aperto di* X. Una sottofamiglia di un ricoprimento $\{E_i\}$ di X che è essa stessa un ricoprimento di X si dice un *sottoricoprimento di* $\{E_i\}$.

Uno spazio topologico X si dice *compatto* se è uno spazio di Hausdorff e se ogni ricoprimento aperto di X ammette un sottoricoprimento finito. Uno spazio topologico compatto ammette varie caratterizzazioni.

Lemma 2.2. *Sia X uno spazio di Hausdorff. Allora X è compatto se e solo se ogni famiglia di chiusi di X la cui intersezione è vuota ammette una sottofamiglia finita la cui intersezione è ancora vuota.*

Dimostrazione. Basta osservare che, se $\{F_i\}$ è una famiglia di insiemi chiusi di X, indicizzata su un insieme I, la cui intersezione è vuota, allora la famiglia $\{U_i\}$ dei complementari in X degli insiemi della famiglia $\{F_i\}$ è un ricoprimento aperto di X. Precisamente, definiamo $U_i = X \setminus F_i$ per ogni indice $i \in I$. Di conseguenza, la condizione espressa nell'enunciato è equivalente alla definizione di compattezza. □

Lemma 2.3. *Sia X uno spazio di Hausdorff e sia $\{\Omega_i\}$ una base di aperti di X. Allora X è compatto se e solo se ogni ricoprimento di X costituito da aperti elementari di X ammette un sottoricoprimento finito.*

Dimostrazione. La condizione data è banalmente necessaria per definizione di spazio topologico compatto. Mostriamo allora che è anche sufficiente. Supponiamo che la base di aperti $\{\Omega_i\}$ di X sia indicizzata su un insieme I e consideriamo un ricoprimento aperto $\{U_k\}$ di X indicizzato su un insieme K. Per ogni $k \in K$, l'insieme U_k si può esprimere come unione di aperti elementari di X e dunque esiste un sottoinsieme J di I tale che la famiglia $\{\Omega_j\}$ indicizzata sull'insieme J sia un ricoprimento aperto di X e tale che, per ogni $j \in J$, si abbia $\Omega_j \subseteq U_k$ per un qualche indice $k \in K$. Per ipotesi esiste allora un sottoricoprimento finito del ricoprimento aperto $\{\Omega_j\}$, ovvero esistono indici $j_1, j_2, \ldots, j_n \in J$ tali che $X = \Omega_{j_1} \cup \Omega_{j_2} \cup \cdots \cup \Omega_{j_n}$. Per come si è scelto l'insieme J possiamo selezionare degli indici $k_1, k_2, \ldots, k_n \in K$ tali che $X = U_{k_1} \cup U_{k_2} \cup \cdots \cup U_{k_n}$. Abbiamo estratto un sottoricoprimento finito del ricoprimento $\{U_k\}$ fissato inizialmente e possiamo allora concludere che X è compatto. □

Lemma 2.4. *Sia X uno spazio di Hausdorff e sia $\{\Omega_i\}$ una base di aperti di X. Allora X è compatto se e solo se ogni famiglia di chiusi elementari di X la cui intersezione è vuota ammette una sottofamiglia finita la cui intersezione è ancora vuota.*

Dimostrazione. Con lo stesso argomento della dimostrazione del lemma 2.2 si vede subito che la condizione data nell'enunciato è del tutto equivalente alla condizione fornita dal lemma 2.3. □

Inoltre, è ben noto che gli spazi topologici compatti godono delle seguenti proprietà. Sebbene non presentino particolari difficoltà, non vedremo le dimostrazioni, ma queste sono trattate, per esempio, in [9].

Lemma 2.5. *Sia X uno spazio topologico compatto e sia Y un sottospazio di X. Se Y è anche un chiuso di X, allora Y è compatto.*

Lemma 2.6. *Siano X_1 uno spazio topologico compatto, X_2 uno spazio di Hausdorff e sia f un'applicazione continua e biiettiva da X_1 a X_2. Allora f è un omeomorfismo.*

Un sottoinsieme di uno spazio topologico X che sia al tempo stesso un aperto e un chiuso di X si dice un *chiuso-aperto di X*. Inoltre, se esiste una base di aperti di X costituita da chiuso-aperti di X, diremo che X è uno spazio topologico di *dimensione zero*. Abbiamo ora i due seguenti risultati.

Lemma 2.7. *Sia X uno spazio topologico. Allora X è di dimensione zero se e solo se la famiglia di tutti i suoi chiuso-aperti è una base di aperti di X.*

Dimostrazione. La condizione data è necessaria in quanto ogni famiglia di aperti contenente una base di aperti di X è essa stessa una base di aperti di X. In particolare, se esiste una base di aperti di X costituita da chiuso-aperti di X, anche la famiglia di tutti i chiuso-aperti di X è una base di aperti di X. Il viceversa è una conseguenza immediata della definizione di spazio topologico di dimensione zero. □

Lemma 2.8. *Sia X uno spazio topologico di dimensione zero e sia Y un suo sottospazio. Allora anche Y è uno spazio topologico di dimensione zero.*

Dimostrazione. Per ipotesi, esiste una base di aperti $\{\Omega_i\}$ di X costituita da chiuso-aperti di X. La famiglia di insiemi $\{\Omega_i \cap Y\}$ è quindi una base di aperti di Y per il lemma 2.1, ma tali aperti sono anche chiusi di Y in quanto essi si ottengono dall'intersezione con Y di insiemi chiusi di X. □

Uno spazio topologico compatto di dimensione zero viene detto uno *spazio di Boole*.

Data adesso una famiglia $\{X_i\}$ di spazi topologici, indicizzata su un insieme I, definiamo sul prodotto $\prod X_i$ una topologia prendendo come aperti elementari i sottoinsiemi della forma $\prod U_i$, dove U_i è un aperto di X_i per ogni $i \in I$ e $U_i = X_i$ per ogni $i \in I$ tranne che per un numero finito di tali indici i. La topologia così definita viene chiamata *topologia prodotto*. Enunciamo adesso un risultato molto importante, la cui dimostrazione usa il lemma di Zorn ed è reperibile nel testo [9].

Teorema 2.9 (di Tychonoff)**.** *Sia $\{X_i\}$ una famiglia di spazi topologici compatti. Allora $\prod X_i$ è compatto.*

Consideriamo ora il caso particolare in cui ciascuno degli spazi topologici X_i è lo spazio $\{0,1\}$ munito della topologia discreta, cioè della topologia in cui ogni sottoinsieme di $\{0,1\}$ è un aperto. Nel nostro caso, il prodotto $\prod X_i$ è semplicemente l'insieme $\{0,1\}^I$ delle funzioni da I in $\{0,1\}$.

Lemma 2.10. *Lo spazio topologico $\{0,1\}^I$ è di dimensione zero.*

Dimostrazione. Come già detto, un aperto elementare Ω della topologia prodotto è un prodotto di aperti di $\{0,1\}$, i quali sono diversi da tutto $\{0,1\}$ soltanto in numero finito. In simboli, esistono un intero $n \geq 0$, degli indici $i_1, i_2, \ldots, i_n \in I$ e degli insiemi aperti $U_1, U_2, \ldots, U_n$ di $\{0,1\}$, diversi dall'insieme $\{0,1\}$, tali che:

$$\Omega = \{f \in \{0,1\}^I \colon f(i_1) \in U_1, f(i_2) \in U_2, \ldots, f(i_n) \in U_n\}$$

Dobbiamo far vedere che Ω è un sottoinsieme chiuso di $\{0,1\}^I$. Naturalmente, se U_k è l'insieme vuoto per un certo $k \in \{1,2,\ldots,n\}$, allora anche Ω è vuoto e in particolare Ω è chiuso. Possiamo dunque ridurci al caso in cui U_k è non vuoto per ogni $k = 1,2,\ldots,n$ ma, poiché abbiamo scelto la topologia discreta su $\{0,1\}$, ci stiamo in realtà riducendo al caso in cui $U_k = \{0\}$ oppure $U_k = \{1\}$ per ogni $k = 1,2,\ldots,n$. Per opportuni $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \{0,1\}$, possiamo dunque scrivere:

$$\Omega = \{f \in \{0,1\}^I \colon f(i_1) = \varepsilon_1, f(i_2) = \varepsilon_2, \ldots, f(i_n) = \varepsilon_n\}$$

Un aperto elementare non vuoto di $\{0,1\}^I$ è dunque l'insieme delle applicazioni da I in $\{0,1\}$ che prendono determinati valori su un numero finito di punti dati. A questo punto basta notare che:

$$\{0,1\}^I \setminus \Omega = \bigcup_{k=1}^{n} \{f \in \{0,1\}^I \colon f(i_k) = 1 - \varepsilon_k\}$$

Il complementare di Ω in $\{0,1\}^I$ è quindi un aperto di $\{0,1\}^I$ essendo unione di aperti elementari. Abbiamo allora ottenuto che Ω è un chiuso, quindi un chiuso-aperto, di $\{0,1\}^I$ e questo conclude la dimostrazione. □

Osserviamo infine che lo spazio topologico $\{0,1\}$ è ovviamente compatto. Come immediata conseguenza del teorema di Tychonoff e del lemma precedente, si ha allora il seguente risultato.

Teorema 2.11. *Lo spazio topologico $\{0,1\}^I$ è uno spazio di Boole.*

2.2 Sottoalgebre di Boole

Definizione 2.12. Sia $\mathcal{A} = \langle A, +, \times, 0, 1\rangle$ un'algebra di Boole e sia B un sottoinsieme di A. Si dice che $\langle B, +, \times, 0, 1\rangle$ è una *sottoalgebra di Boole di* $\mathcal{A}$ se B contiene gli elementi neutri ed è stabile per le operazioni di somma e prodotto, cioè se $0 \in B$, $1 \in B$ e se $x + y \in B$, $xy \in B$ per ogni $x, y \in B$.

Teorema 2.13. *Sia $\mathcal{A} = \langle A, +, \times, 0, 1\rangle$ un'algebra di Boole e sia B un sottoinsieme di A. Allora, perché $\langle B, +, \times, 0, 1\rangle$ sia una sottoalgebra di Boole di $\mathcal{A}$, è necessario e sufficiente che $0 \in B$ e che B sia stabile per le operazioni $x \mapsto x^{\mathbf{c}}$ e $(x, y) \mapsto x \frown y$.*

Dimostrazione. La condizione è chiaramente necessaria dal momento che, per il punto (viii) del teorema 1.7 e per definizione del prodotto in un reticolo distributivo e complementare, abbiamo $x^{\mathbf{c}} = 1 + x$ e $x \frown y = xy$.

Facciamo vedere allora che la condizione è sufficiente. Osserviamo, innanzitutto, che $1 \in B$ in quanto $1 = 0^{\mathbf{c}}$. Notiamo anche che, grazie alle leggi di de Morgan, si ha $x \smile y = (x^{\mathbf{c}} \frown y^{\mathbf{c}})^{\mathbf{c}}$ per ogni $x, y \in A$ ma allora l'ipotesi che B sia stabile per le operazioni di passaggio al complemento e di passaggio all'estremo inferiore ci garantisce la stabilità per l'operazione $(x, y) \mapsto x \smile y$. Ora basta ricordare che somma e prodotto in un'algebra di Boole possono essere definiti a partire dalle operazioni $\frown$, $\smile$ e di passaggio al complemento (dimostrazione del teorema 1.12). Concludiamo che B è stabile per la somma e per il prodotto e quindi $\langle B, +, \times, 0, 1\rangle$ è una sottoalgebra di Boole di $\mathcal{A}$. □

Esempio 2.14. Sia X uno spazio topologico. Denotiamo $\mathcal{B}(X)$ il sottoinsieme dell'insieme delle parti $\mathcal{P}(X)$ costituito dai sottoinsiemi chiuso-aperti per la topologia di X. Poiché l'insieme vuoto è un chiuso-aperto di X e siccome anche il complementare di un chiuso-aperto e l'intersezione di due chiuso-aperti sono ancora chiuso-aperti di X, il teorema 2.13 ci dice che $\langle \mathcal{B}(X), \triangle, \cap, \varnothing, X\rangle$ è una sottoalgebra di Boole di $\mathcal{P}(X)$. D'ora in avanti, con un piccolo abuso di linguaggio, si dirà che $\mathcal{B}(X)$ è una sottoalgebra di Boole di $\mathcal{P}(X)$.

2.3 Spazi di Stone

In questa sezione supporremo sempre che $\mathcal{A} = \langle A, +, \times, 0, 1\rangle$ sia un'algebra di Boole.

Definizione 2.15. L'insieme degli omomorfismi di algebre di Boole da $\mathcal{A}$ in $\{0, 1\}$ si chiama *spazio di Stone di* $\mathcal{A}$ e si denota $S(\mathcal{A})$.

Alla luce dell'osservazione 1.41, lo spazio di Stone di $\mathcal{A}$ è in biiezione con l'insieme degli ideali massimali di $\mathcal{A}$ e con l'insieme degli ultrafiltri di $\mathcal{A}$. Se adesso consideriamo $\{0, 1\}$ come spazio topologico munito della topologia discreta e se dotiamo $\{0, 1\}^A$ della topologia prodotto, allora possiamo pensare a $S(\mathcal{A})$ come a uno spazio topologico munito della topologia indotta da quella di $\{0, 1\}^A$. Come conseguenza immediata dei lemmi 2.8 e 2.10, abbiamo ora il seguente risultato.

Lemma 2.16. *Lo spazio topologico $S(\mathcal{A})$ è di dimensione zero.*

Nella dimostrazione del lemma 2.10 si era sottolineato che un aperto elementare non vuoto di $\{0, 1\}^A$ è l'insieme delle applicazioni da A in $\{0, 1\}$ che assumono valori fissati su un numero finito di punti dati e abbiamo visto che un tale insieme è un chiuso-aperto di $\{0, 1\}^A$. Un aperto elementare non vuoto di $S(\mathcal{A})$ sarà allora l'intersezione di un tale insieme con $S(\mathcal{A})$, cioè l'insieme degli omomorfismi di algebre di Boole da $\mathcal{A}$ in $\{0, 1\}$ che assumono valori fissati su un numero finito di punti dati. Inoltre un siffatto aperto elementare sarà, per definizione di topologia indotta, un chiuso-aperto di $S(\mathcal{A})$.

Lemma 2.17. *Sia Δ un sottoinsieme di $S(\mathcal{A})$. Allora Δ è un aperto elementare di $S(\mathcal{A})$ se e solo se esiste un elemento $a \in A$ tale che:*

$$\Delta = \{h \in S(\mathcal{A}) \colon h(a) = 1\}$$

Se inoltre questa condizione è verificata, allora un tale elemento $a \in A$ è unico.

Dimostrazione. Innanzitutto, osserviamo che la condizione è sufficiente perché Δ è l'insieme degli omomorfismi di algebre di Boole da $\mathcal{A}$ in $\{0,1\}$ che assumono valore 1 sul punto a.

Vediamo allora che la condizione è necessaria. Supponiamo che Δ sia un aperto elementare di $S(\mathcal{A})$ e notiamo che, se Δ è l'insieme vuoto, allora $\Delta = \{h \in S(\mathcal{A}) \colon h(0) = 1\}$. Se invece $\Delta = S(\mathcal{A})$, allora $\Delta = \{h \in S(\mathcal{A}) \colon h(1) = 1\}$. Possiamo dunque ridurci al caso in cui Δ è non vuoto e diverso da $S(\mathcal{A})$. Per quanto detto prima, esistono un intero $n \geq 1$, degli elementi $a_1, a_2, \ldots, a_n \in A$ e dei valori $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \{0,1\}$ tali che:

$$\Delta = \{h \in S(\mathcal{A}) \colon h(a_1) = \varepsilon_1, h(a_2) = \varepsilon_2, \ldots, h(a_n) = \varepsilon_n\}$$

Per ogni $k = 1, 2, \ldots, n$, definiamo:

$$b_k = \begin{cases} a_k & \text{se } \varepsilon_k = 1 \\ 1 + a_k & \text{se } \varepsilon_k = 0 \end{cases}$$

Allora, per ogni $h \in S(\mathcal{A})$ e per ogni $k = 1, 2, \ldots, n$, abbiamo:

$$h(b_k) = \begin{cases} h(a_k) & \text{se } \varepsilon_k = 1 \\ 1 + h(a_k) & \text{se } \varepsilon_k = 0 \end{cases}$$

Ne deduciamo che, per ogni $h \in S(\mathcal{A})$, valgono le seguenti equivalenze:

$$\begin{aligned} & h \in \Delta \\ \iff & h(a_k) = \varepsilon_k \quad \forall k = 1, 2, \ldots, n \\ \iff & h(b_k) = 1 \quad \forall k = 1, 2, \ldots, n \\ \iff & h(b_1) \curlywedge h(b_2) \curlywedge \cdots \curlywedge h(b_n) = 1 \\ \iff & h(b_1 \curlywedge b_2 \curlywedge \cdots \curlywedge b_n) = 1 \end{aligned}$$

Prendendo adesso $a = b_1 \curlywedge b_2 \curlywedge \cdots \curlywedge b_n$, otteniamo allora che Δ è un insieme della forma voluta.

Rimane da dimostrare l'unicità. Per fare questo, consideriamo due elementi distinti $a, b \in A$. Allora, essendo $a + b \neq 0$, possiamo considerare il filtro principale generato da $a + b$. Il teorema dell'ultrafiltro afferma che tale filtro è contenuto in un ultrafiltro F di $\mathcal{A}$, mentre il punto (3′) del teorema 1.39 garantisce l'esistenza di un omomorfismo $\varphi \in S(\mathcal{A})$ tale che $F = \{x \in A \colon \varphi(x) = 1\}$. Poiché $a + b \in F$, vale che $\varphi(a + b) = 1$, cioè che $\varphi(a) + \varphi(b) = 1$ e di conseguenza uno e uno solo tra $\varphi(a)$ e $\varphi(b)$ vale 1. Questo dimostra che $\{h \in S(\mathcal{A}) \colon h(a) = 1\} \neq \{h \in S(\mathcal{A}) \colon h(b) = 1\}$ perché φ appartiene a uno di questi due insiemi ma non all'altro. □

Corollario 2.18. *L'insieme dei chiusi elementari di $S(\mathcal{A})$ coincide con l'insieme dei suoi aperti elementari.*

Dimostrazione. Avendo già osservato che gli aperti elementari di $S(\mathcal{A})$ sono chiuso-aperti, basterà convincersi del fatto che ogni chiuso elementare di $S(\mathcal{A})$ è un aperto elementare. Sia allora Γ un chiuso elementare di $S(\mathcal{A})$. Il complementare di Γ in $S(\mathcal{A})$ sarà un aperto elementare e dunque, per il lemma precedente, esiste $a \in A$ tale che:

$$S(\mathcal{A}) \setminus \Gamma = \{h \in S(\mathcal{A}) \colon h(a) = 1\}$$

Lo stesso risultato ci permette di concludere che Γ stesso è un aperto elementare, infatti abbiamo:

$$\begin{aligned}\Gamma &= \{h \in S(\mathcal{A})\colon h(a) \neq 1\}\\ &= \{h \in S(\mathcal{A})\colon h(a) = 0\}\\ &= \{h \in S(\mathcal{A})\colon h(1+a) = 1\}\end{aligned}$$ □

Lemma 2.19. *Lo spazio topologico $S(\mathcal{A})$ è compatto.*

Dimostrazione. Dal teorema 2.11 segue in particolare che $\{0,1\}^A$ è uno spazio di Hausdorff ed è facile verificare che anche il suo sottospazio topologico $S(\mathcal{A})$ è di Hausdorff. Per dimostrare che è compatto, ci serviremo del lemma 2.4, ma nel nostro caso particolare, alla luce del corollario 2.18, sarà sufficiente mostrare che ogni famiglia di aperti elementari di $S(\mathcal{A})$ la cui intersezione è vuota ammette una sottofamiglia finita la cui intersezione è ancora vuota. Sia allora $\{\Omega_i\}$ una famiglia di aperti elementari di $S(\mathcal{A})$, indicizzata su un insieme I, tale che l'intersezione di tutti gli Ω_i sia l'insieme vuoto. Applicando il lemma 2.17 otteniamo, per ogni $i \in I$, un elemento $x_i \in A$ tale che:

$$\Omega_i = \{h \in S(\mathcal{A})\colon h(x_i) = 1\}$$

Sia allora $X = \{x_i\colon i \in I\}$. Poiché l'intersezione degli Ω_i è vuota, nessun omomorfismo $h \in S(\mathcal{A})$ può assumere valore 1 su tutti i punti di X e siccome gli ultrafiltri di $\mathcal{A}$ sono, per il punto (3') del teorema 1.39, insiemi di punti di A che vengono mappati in 1 da un certo omomorfismo $h \in S(\mathcal{A})$, nessun ultrafiltro di $\mathcal{A}$ può contenere X. Questo equivale a richiedere, per il lemma 1.48, che X non sia una base di un filtro di $\mathcal{A}$. Per definizione, esistono dunque degli indici $i_1, i_2, \ldots, i_n \in I$ tali che $x_{i_1} \frown x_{i_2} \frown \cdots \frown x_{i_n} = 0$. Ne segue, per il punto (f) del teorema 1.34 e per il corollario 1.36, che nessun ultrafiltro di $\mathcal{A}$ può contenere tutti i punti $x_{i_1}, x_{i_2}, \ldots, x_{i_n}$ oppure, equivalentemente, che questi punti non vengono mappati in 1 da nessun omomorfismo $h \in S(\mathcal{A})$. Abbiamo dunque mostrato che:

$$\Omega_{i_1} \cap \Omega_{i_2} \cap \cdots \cap \Omega_{i_n} = \varnothing$$

Avendo individuato una sottofamiglia finita di $\{\Omega_i\}$ la cui intersezione è vuota, concludiamo. □

Dai lemmi 2.16 e 2.19 discende immediatamente il seguente risultato.

Corollario 2.20. *Lo spazio topologico $S(\mathcal{A})$ è uno spazio di Boole.*

Lemma 2.21. *L'insieme dei chiuso-aperti di $S(\mathcal{A})$ coincide con l'insieme dei suoi aperti elementari.*

Dimostrazione. Sappiamo già che gli aperti elementari di $S(\mathcal{A})$ sono chiuso-aperti. Consideriamo dunque un chiuso-aperto qualsiasi Γ di $S(\mathcal{A})$. Poiché $S(\mathcal{A})$ è uno spazio topologico compatto e Γ è un suo sottoinsieme chiuso, per il lemma 2.5 anche Γ è compatto. Ma siccome Γ è aperto, esiste una famiglia $\{\Gamma_i\}$ di aperti elementari di $S(\mathcal{A})$ la cui unione sia Γ. Supponiamo che tale famiglia sia indicizzata su un insieme I. Essa costituisce un ricoprimento aperto di Γ e di conseguenza, per compattezza, essa ammette un sottoricoprimento finito, ovvero esistono $i_1, i_2, \ldots, i_n \in I$ tali che:

$$\Gamma = \Gamma_{i_1} \cup \Gamma_{i_2} \cup \cdots \cup \Gamma_{i_n}$$

Per il lemma 2.17, esistono $x_1, x_2, \ldots, x_n \in A$ tali che, per ogni $k = 1, 2, \ldots, n$, valga la condizione:

$$\Gamma_{i_k} = \{h \in S(\mathcal{A})\colon h(x_k) = 1\}$$

Definiamo $x = x_1 \smile x_2 \smile \cdots \smile x_n$, $\Delta = \{h \in S(\mathcal{A})\colon h(x) = 1\}$ e dimostriamo che $\Gamma = \Delta$. Una volta fatto questo, il lemma 2.17 permette di concludere la dimostrazione. Osserviamo allora che ogni elemento di Γ è un omomorfismo $h \in S(\mathcal{A})$ con $h(x_k) = 1$ per un qualche $k \in \{1, 2, \ldots, n\}$, quindi:

$$h(x) = h(x_1 \smile x_2 \smile \cdots \smile x_n) = h(x_1) \smile h(x_2) \smile \cdots \smile h(x_n) = 1$$

Vale quindi l'inclusione $\Gamma \subseteq \Delta$. D'altra parte, un omomorfismo $h \in S(\mathcal{A})$ che non appartiene a Γ è tale che $h(x_k) = 0$ per ogni $k = 1, 2, \ldots, n$ e di conseguenza non appartiene nemmeno a Δ perché:

$$h(x) = h(x_1 \smile x_2 \smile \cdots \smile x_n) = h(x_1) \smile h(x_2) \smile \cdots \smile h(x_n) = 0$$

È dunque dimostrata anche l'inclusione $\Delta \subseteq \Gamma$. □

2.4 Il teorema di Stone

Come abbiamo già osservato all'inizio, uno degli esempi più naturali di algebre di Boole è quello fornito dall'insieme delle parti di un insieme dato. È dunque ragionevole porsi questa domanda: è vero che ogni algebra di Boole è isomorfa all'algebra di Boole dei sottoinsiemi di un insieme? La risposta è negativa e ne daremo una giustificazione nella sezione successiva. Tuttavia il teorema di rappresentazione di Stone, al quale dedichiamo questa sezione, ci assicura che esiste sempre un legame tra un'algebra di Boole e l'algebra di Boole dei sottoinsiemi di un insieme. Vedremo infatti che ogni algebra di Boole è isomorfa a una sottoalgebra di Boole dell'algebra dei sottoinsiemi di un insieme.

Teorema 2.22 (di rappresentazione di Stone)**.** *Sia $\mathcal{A}$ un'algebra di Boole. Allora $\mathcal{A} \cong \mathcal{B}(S(\mathcal{A}))$, cioè $\mathcal{A}$ è isomorfa all'algebra di Boole dei chiuso-aperti del suo spazio di Stone.*

Dimostrazione. Consideriamo la funzione H da A in $\mathcal{B}(S(\mathcal{A}))$ che, a ogni elemento $a \in A$, associa:

$$H(a) = \{h \in S(\mathcal{A}) \colon h(a) = 1\}$$

Per concludere, basterà dimostrare che H è un isomorfismo di algebre di Boole da $\mathcal{A}$ in $\mathcal{B}(S(\mathcal{A}))$. I lemmi 2.17 e 2.21 garantiscono che H sia effettivamente un'applicazione a valori in $\mathcal{B}(S(\mathcal{A}))$ e che la sua immagine sia esattamente $\mathcal{B}(S(\mathcal{A}))$. Si tratta cioè di una funzione di codominio $\mathcal{B}(S(\mathcal{A}))$ e suriettiva.

Per il teorema 1.21 dobbiamo soltanto assicurarci che, per ogni $x, y \in A$, valga $x \leq y$ se e solo se $H(x) \subseteq H(y)$. Fissati $x, y \in A$ supponiamo, in un primo momento, che $x \leq y$. Il lemma 1.16 ci garantisce che $h(x) \leq h(y)$ per ogni $h \in S(\mathcal{A})$ e quindi, se $h(x) = 1$, allora anche $h(y) = 1$. Questo mostra l'inclusione $H(x) \subseteq H(y)$. Assumiamo ora $x \not\leq y$. Per il lemma 1.8, vale allora $x(1 + y) \neq 0$ e il filtro principale generato da $x(1 + y)$ risulta ben definito. Per il teorema dell'ultrafiltro, si può considerare un ultrafiltro F di $\mathcal{A}$ che lo contenga. Sia $h \in S(\mathcal{A})$ l'omomorfismo associato a F, cioè tale che $F = \{x \in A \colon h(x) = 1\}$. Abbiamo allora che:

$$\begin{aligned}
& x(1 + y) \in F \\
\implies\ & h(x(1 + y)) = 1 \\
\implies\ & h(x) = 1 \text{ e } h(1 + y) = 1 \\
\implies\ & h(x) = 1 \text{ e } h(y) = 0 \\
\implies\ & h \in H(x) \text{ e } h \notin H(y) \\
\implies\ & H(x) \not\subseteq H(y)
\end{aligned}$$

□

La domanda che abbiamo posto a inizio sezione ha risposta affermativa se ci restringiamo alle algebre di Boole finite, ovvero con supporto finito. È questo il contenuto del risultato che segue.

Corollario 2.23. *Sia $\mathcal{A}$ un'algebra di Boole finita. Allora $\mathcal{A}$ è isomorfa all'algebra di Boole dell'insieme delle parti di un insieme.*

Dimostrazione. Se A è un insieme finito allora, poiché abbiamo attribuito la topologia discreta allo spazio $\{0,1\}$, anche la topologia prodotto su $\{0,1\}^A$ risulta essere la topologia discreta. Ciò è vero in quanto i singleton di $\{0,1\}^A$, cioè i sottoinsiemi costituiti da un unico elemento, sono insiemi aperti. Si ricordi che questa è una condizione sufficiente perché la topologia su $\{0,1\}^A$ sia quella discreta, perché qualunque sottoinsieme di $\{0,1\}^A$ è unione di singleton e un'unione arbitraria di aperti è un insieme aperto. In effetti, i singleton di $\{0,1\}^A$ sono addirittura aperti elementari. Se infatti f è una funzione da A in $\{0,1\}$, allora $\{f\}$ è l'insieme delle funzioni che prendono gli stessi valori di f sui punti di A, i quali sono in numero finito e dunque $\{f\}$ soddisfa la caratterizzazione degli aperti elementari non vuoti di $\{0,1\}^A$ che abbiamo dato nella dimostrazione del lemma 2.10.

In particolare, la topologia indotta sul sottospazio $S(\mathcal{A})$ di $\{0,1\}^A$ è quella discreta e dunque ogni sottoinsieme di $S(\mathcal{A})$ è un chiuso-aperto di $S(\mathcal{A})$. L'algebra di Boole $\mathcal{B}(S(\mathcal{A}))$ coincide allora con $\mathcal{P}(S(\mathcal{A}))$ e, per il teorema di rappresentazione di Stone, concludiamo che $\mathcal{A} \cong \mathcal{P}(S(\mathcal{A}))$. □

La dimostrazione del risultato precedente non si può estendere alle algebre di Boole infinite. Infatti, nel caso generale la topologia prodotto su $\{0,1\}^A$ non coincide con quella discreta. Prima di vederne il motivo, facciamo alcune considerazioni preliminari.

Osservazione 2.24. Se E è un insieme finito di cardinalità n, allora $\mathcal{P}(E)$ ha cardinalità 2^n. Questo fatto si dimostra facilmente ragionando per induzione sull'intero $n \geq 0$. La base di induzione è il caso $n = 0$, cioè il caso in cui E è l'insieme vuoto. L'unico sottoinsieme di E è E stesso, quindi $\mathcal{P}(E)$ ha cardinalità pari a $2^0 = 1$. Nel passo induttivo assumiamo $n \geq 1$ e supponiamo che qualunque sottoinsieme finito di cardinalità $n-1$ abbia 2^{n-1} sottoinsiemi. Dato che $n \geq 1$, l'insieme E è non vuoto e dunque possiamo considerare un particolare elemento $x \in E$. Osserviamo che l'insieme $F = E \setminus \{x\}$ ha cardinalità $n-1$ e inoltre $E = F \cup \{x\}$. Tra i sottoinsiemi di E possiamo distinguere quelli che non contengono x e quelli che lo contengono. I primi sono esattamente i sottoinsiemi di F e, per ipotesi induttiva, ve ne sono 2^{n-1}. I secondi sono invece insiemi del tipo $G \cup \{x\}$, dove $G \in \mathcal{P}(F)$. Poiché vi sono 2^{n-1} scelte possibili per G, anche gli insiemi di questo tipo devono essere in numero di 2^{n-1}. E allora concludiamo che $\mathcal{P}(E)$ contiene $2^{n-1} + 2^{n-1} = 2^n$ elementi.

Osservazione 2.25. Se X è uno spazio topologico finito, allora X è compatto. Si osservi infatti che, in vista dell'osservazione precedente, l'insieme $\mathcal{P}(X)$ è finito. Ma allora ogni ricoprimento aperto di X sarà esso stesso un ricoprimento finito dal momento che i ricoprimenti di X sono famiglie di sottoinsiemi di X e questi ultimi sono in numero finito. Ne ricaviamo che X è, in effetti, compatto.

Osservazione 2.26. Se X è uno spazio topologico compatto e discreto, cioè munito della topologia discreta, allora X è finito. Per dimostrarlo, poniamo $E_x = \{x\}$ per ogni $x \in X$. Poiché per ipotesi X è discreto, la famiglia di insiemi $\{E_x\}$ indicizzata su X è un ricoprimento aperto di X. Essendo però X uno spazio compatto, deve esistere un sottoricoprimento $\{E_y\}$ di $\{E_x\}$ indicizzato su un sottoinsieme finito $Y \subseteq X$. Ne deduciamo, per le definizioni di ricoprimento e sottoricoprimento, che $Y = X$ e questo dimostra che X è, come Y, un insieme finito.

A questo punto, il motivo per cui la dimostrazione del corollario 2.23 non si estende al caso in cui A è un insieme infinito è evidente. Infatti, se A è infinito, anche $\{0,1\}^A$ è infinito in quanto è iniettiva l'applicazione da A in $\{0,1\}^A$ che a ogni elemento $a \in A$ associa la funzione $f_a \in \{0,1\}^A$ seguente:

$$f_a(x) = \begin{cases} 0 & \text{se } x \neq a \\ 1 & \text{se } x = a \end{cases}$$

D'altra parte, il teorema 2.11 garantisce che $\{0,1\}^A$ è uno spazio di Boole e quindi, in particolare, uno spazio topologico compatto. E allora dall'osservazione 2.26 si deduce, per contrapposizione logica, che $\{0,1\}^A$ non è discreto, cioè che la topologia prodotto su $\{0,1\}^A$ non coincide con quella discreta.

Dal corollario 2.23 e dall'osservazione 2.24 deduciamo immediatamente il seguente risultato.

Corollario 2.27. *Ogni algebra di Boole finita ha per cardinalità una potenza di* 2*.*

Dimostrazione. Se $\mathcal{A}$ è un'algebra di Boole finita allora, per il corollario 2.23, esiste un insieme E tale che $\mathcal{A} \cong \mathcal{P}(E)$. In particolare, l'insieme delle parti $\mathcal{P}(E)$ ha cardinalità finita e dunque anche E è un insieme finito. Se allora E ha cardinalità n, per l'osservazione 2.24 la cardinalità di $\mathcal{P}(E)$, quindi quella di A, è pari a 2^n. □

Il teorema di rappresentazione di Stone ci ha permesso di associare uno spazio di Boole a ogni algebra di Boole. Ora è del tutto naturale chiedersi se sia possibile associare un'algebra di Boole a ogni spazio di Boole. La risposta a questo problema è affermativa e ci viene fornita dal seguente risultato.

Teorema 2.28. *Sia X uno spazio di Boole. Allora $X \approx S(\mathcal{B}(X))$, cioè X è omeomorfo allo spazio di Stone dell'algebra di Boole dei chiuso-aperti di X.*

Dimostrazione. Consideriamo la funzione f da X in $S(\mathcal{B}(X))$ che, a ciascun punto $x \in X$, associa l'omomorfismo di algebre di Boole f_x da $\mathcal{B}(X)$ in $\{0,1\}$ definito per casi nella maniera seguente:

$$f_x(\Omega) = \begin{cases} 1 & \text{se } x \in \Omega \\ 0 & \text{se } x \notin \Omega \end{cases}$$

Bisogna innanzitutto convincersi della buona definizione di f e questo richiede di verificare che f_x sia effettivamente un omomorfismo di algebre di Boole. Notiamo allora che, dati due qualsiasi chiuso-aperti Ω e Δ di X, si hanno le condizioni $f_x(\Omega \cap \Delta) = f_x(\Omega) f_x(\Delta)$ e $f_x(X \setminus \Omega) = 1 + f_x(\Omega)$ in virtù delle seguenti equivalenze:

$$\begin{aligned} & f_x(\Omega \cap \Delta) = 1 \\ \iff & x \in \Omega \cap \Delta \\ \iff & x \in \Omega \text{ e } x \in \Delta \\ \iff & f_x(\Omega) = 1 \text{ e } f_x(\Delta) = 1 \\ \iff & f_x(\Omega) f_x(\Delta) = 1 \end{aligned} \qquad \begin{aligned} & f_x(X \setminus \Omega) = 1 \\ \iff & x \in X \setminus \Omega \\ \iff & x \notin \Omega \\ \iff & f_x(\Omega) = 0 \\ \iff & 1 + f_x(\Omega) = 1 \end{aligned}$$

Dal teorema 1.17 segue allora che f_x è un omomorfismo di algebre di Boole. Essendo X e $S(\mathcal{B}(X))$ spazi di Boole, per poter concludere che f è un omeomorfismo da X in $S(\mathcal{B}(X))$ sarà sufficiente dimostrare, grazie al lemma 2.6, che f è un'applicazione continua e biiettiva. Vediamo allora che:

- *f è iniettiva.* Siano $x, y \in X$ due elementi distinti. Dato che X è uno spazio di Hausdorff, esiste un aperto $U \subseteq X$ tale che $x \in U$ e $y \notin U$. Ricordiamo adesso che X è di dimensione zero, quindi $\mathcal{B}(X)$ è una base di aperti di X per il lemma 2.7. Esiste allora un chiuso-aperto Ω di X tale che $x \in \Omega$ e $y \notin \Omega$. Questo ci permette di affermare che f_x e f_y sono distinte in quanto $f_x(\Omega) = 1$ mentre $f_y(\Omega) = 0$.

- *f è suriettiva.* Sia h un omomorfismo di algebre di Boole da $\mathcal{B}(X)$ in $\{0,1\}$. Consideriamo l'ultrafiltro associato a h, cioè:

  $$F = \{\Omega \in \mathcal{B}(X) \colon h(\Omega) = 1\}$$

  Si noti che F è una base di un filtro di $\mathcal{B}(X)$ per il lemma 1.48, quindi gode della proprietà dell'intersezione finita. Ogni sottofamiglia finita di F ammette dunque intersezione non

vuota ma allora, dato che F è una famiglia di chiusi dello spazio topologico compatto X possiamo affermare, per il lemma 2.2, che anche l'intersezione di tutti i chiusi di F è non vuota. Di conseguenza, possiamo considerare un elemento x di tale intersezione. Per un chiuso-aperto $\Omega \in \mathcal{B}(X)$ vi sono due possibilità: se $\Omega \in F$, allora $x \in \Omega$, quindi $f_x(\Omega) = 1$ e $h(\Omega) = 1$, altrimenti $\Omega \notin F$ e allora, per il punto (4') del teorema 1.39, abbiamo $X \setminus \Omega \in F$, dunque $x \in X \setminus \Omega$, o equivalentemente $x \notin \Omega$ e allora $f_x(\Omega) = 0$, $h(\Omega) = 0$. Ne deduciamo che $f_x = h$.

- *f è continua.* Sia G un qualsiasi aperto elementare di $S(\mathcal{B}(X))$. Per il lemma 2.17, esiste un chiuso-aperto $\Omega \in \mathcal{B}(X)$ tale che $G = \{h \in S(\mathcal{B}(X)) \colon h(\Omega) = 1\}$. E allora la preimmagine di G tramite f è un aperto di X perché:

$$\begin{aligned} f^{-1}(G) &= \{x \in X \colon f_x \in G\} \\ &= \{x \in X \colon f_x(\Omega) = 1\} \\ &= \{x \in X \colon x \in \Omega\} = \Omega \end{aligned}$$

□

2.5 Conseguenze in logica

Ricordiamo alcune nozioni di logica proposizionale.

Un *alfabeto proposizionale* è un insieme di simboli che è unione disgiunta dei seguenti insiemi:

- L'insieme dei *connettivi proposizionali*, costituito dai simboli di *negazione* $\neg$, di *disgiunzione* $\vee$, di *congiunzione* $\wedge$, di *implicazione* $\rightarrow$ e di *equivalenza* $\leftrightarrow$.
- L'insieme dei *simboli ausiliari*, costituito dalla parentesi aperta (e dalla parentesi chiusa).
- Un insieme non vuoto P di *variabili proposizionali*, che indicheremo con le lettere maiuscole dell'alfabeto latino.

L'insieme $\mathcal{F}$ delle *formule proposizionali* su un alfabeto $\mathcal{L}$ si definisce induttivamente come segue:

1. (Base della definizione). Se X è una variabile proposizionale, allora X è una formula su $\mathcal{L}$.
2. (Passo della definizione). Se A è una formula su $\mathcal{L}$, allora $\neg A$ è una formula su $\mathcal{L}$. Se A e B sono formule su $\mathcal{L}$, allora anche $(A \vee B)$, $(A \wedge B)$, $(A \rightarrow B)$ e $(A \leftrightarrow B)$ sono formule su $\mathcal{L}$.
3. (Clausola finale). Nient'altro è una formula su $\mathcal{L}$.

Un'applicazione da P in $\{0, 1\}$ si dice una *distribuzione di valori di verità*. Se pensiamo $\{0, 1\}$ con la usuale struttura di algebra di Boole allora, presa una distribuzione di valori di verità δ, possiamo definirne il prolungamento $\bar{\delta}$ su $\mathcal{F}$ nel modo che segue, per induzione sull'altezza della formula:

- Se X è una variabile proposizionale, allora $\bar{\delta}(X) = \delta(X)$.
- Se F e G sono formule su $\mathcal{L}$, allora:
  - (i) $\bar{\delta}(\neg F) = 1 + \bar{\delta}(F)$.
  - (ii) $\bar{\delta}((F \vee G)) = \bar{\delta}(F) + \bar{\delta}(G) + \bar{\delta}(F)\bar{\delta}(G)$.
  - (iii) $\bar{\delta}((F \wedge G)) = \bar{\delta}(F)\bar{\delta}(G)$.
  - (iv) $\bar{\delta}((F \rightarrow G)) = 1 + \bar{\delta}(F) + \bar{\delta}(F)\bar{\delta}(G)$.
  - (v) $\bar{\delta}((F \leftrightarrow G)) = 1 + \bar{\delta}(F) + \bar{\delta}(G)$.

Le cinque condizioni date nel passo della definizione induttiva si possono esprimere sotto forma di tabelle, dette *tavole di verità*, nel modo seguente:

F	$\neg F$
0	1
1	0

F	G	$(F \vee G)$	$(F \wedge G)$	$(F \to G)$	$(F \leftrightarrow G)$
0	0	0	0	1	1
0	1	1	0	1	0
1	0	1	0	0	0
1	1	1	1	1	1

Dalla definizione precedente si deduce immediatamente che, se F e G sono formule su $\mathcal{L}$, allora:

(i') $\bar{\delta}(\neg F) = 1$ se e solo se $\bar{\delta}(F) = 0$.

(ii') $\bar{\delta}((F \vee G)) = 0$ se e solo se $\bar{\delta}(F) = \bar{\delta}(G) = 0$.

(iii') $\bar{\delta}((F \wedge G)) = 1$ se e solo se $\bar{\delta}(F) = \bar{\delta}(G) = 1$.

(iv') $\bar{\delta}((F \to G)) = 0$ se e solo se $\bar{\delta}(F) = 1$ e $\bar{\delta}(G) = 0$.

(v') $\bar{\delta}((F \leftrightarrow G)) = 1$ se e solo se $\bar{\delta}(F) = \bar{\delta}(G)$.

Se F è una formula su $\mathcal{L}$, si dice che δ *soddisfa* F se $\bar{\delta}(F) = 1$. Diremo inoltre che F è una *tautologia* se assume il valore 1 su tutte le distribuzioni di valori di verità, cioè se $\bar{\delta}(F) = 1$ per ogni $\delta \in \{0,1\}^P$. Una tautologia è dunque una formula "sempre vera". Similmente, diremo che F è un'*antilogia* se assume il valore 0 su tutte le distribuzioni di valori di verità, ovvero un'antilogia è una formula "sempre falsa".

Due formule F e G su $\mathcal{L}$ si dicono *logicamente equivalenti* e si scrive $F \sim G$ se la formula $(F \leftrightarrow G)$ è una tautologia. Osserviamo che, come conseguenza immediata della proprietà (v'), si ha $F \sim G$ se e solo se $\bar{\delta}(F) = \bar{\delta}(G)$ per ogni $\delta \in \{0,1\}^P$. Se ne deduce facilmente che la relazione binaria $\sim$ è una relazione di equivalenza. La classe di equivalenza di una formula F nell'insieme quoziente, denotato $\mathcal{F}/\!\sim$, si indica con $\mathrm{cl}(F)$. Da quanto si è detto finora deduciamo immediatamente che le formule logicamente equivalenti a una tautologia sono tutte tautologie e che quelle logicamente equivalenti a un'antilogia sono tutte antilogie. La classe delle tautologie si denota $\mathbf{1}$, quella delle antilogie si denota $\mathbf{0}$.

Date due formule F e G su $\mathcal{L}$, definiamo ora:

- $\neg\,\mathrm{cl}(F) = \mathrm{cl}(\neg F)$.
- $\mathrm{cl}(F) \vee \mathrm{cl}(G) = \mathrm{cl}((F \vee G))$.
- $\mathrm{cl}(F) \wedge \mathrm{cl}(G) = \mathrm{cl}((F \wedge G))$.
- $\mathrm{cl}(F) \to \mathrm{cl}(G) = \mathrm{cl}((F \to G))$.
- $\mathrm{cl}(F) \leftrightarrow \mathrm{cl}(G) = \mathrm{cl}((F \leftrightarrow G))$.
- $\mathrm{cl}(F) \nleftrightarrow \mathrm{cl}(G) = \mathrm{cl}(\neg(F \leftrightarrow G))$.

Così facendo, abbiamo definito un'operazione unaria e delle operazioni binarie su $\mathcal{F}/\!\sim$, cioè una funzione di arietà 1 e delle applicazioni di arietà 2 su $\mathcal{F}/\!\sim$ a valori in $\mathcal{F}/\!\sim$. Si noti che abbiamo commesso un abuso di notazione in quanto abbiamo riutilizzato i simboli destinati ai connettivi proposizionali. Utilizzando le tavole di verità, si vede facilmente che $\mathcal{F}/\!\sim$ è un'algebra di Boole

con le operazioni di somma e prodotto date da $\nleftrightarrow$ e $\wedge$ rispettivamente. L'elemento neutro per la somma è la classe **0** delle antilogie, mentre l'identità è la classe **1** delle tautologie. In particolare, si può definire una relazione d'ordine $\leq$ su $\mathcal{F}/\sim$ ponendo $\mathrm{cl}(F) \leq \mathrm{cl}(G)$ se vale $\mathrm{cl}(F) \wedge \mathrm{cl}(G) = \mathrm{cl}(F)$, cioè se $((F \wedge G) \leftrightarrow F)$ è una tautologia. Con le tavole di verità si verifica che è del tutto equivalente richiedere che la formula $(F \rightarrow G)$ sia una tautologia:

F	G	$(F \wedge G)$	$(F \rightarrow G)$	$((F \wedge G) \leftrightarrow F)$
0	0	0	1	1
0	1	0	1	1
1	0	0	0	0
1	1	1	1	1

Introduciamo adesso la nozione di atomo in un'algebra di Boole.

Definizione 2.29. Sia $\mathcal{A} = \langle A, \leq, 0, 1\rangle$ un'algebra di Boole. Un elemento $a \in A$ si dice un *atomo* se $a \neq 0$ e se, per ogni $b \in A$ con $b \leq a$, si ha che $b = a$ oppure $b = 0$. In altre parole, un atomo è un elemento non nullo che non possiede minoranti stretti non nulli.

Esempio 2.30. Sia E un insieme non vuoto. È facile verificare che gli atomi dell'algebra di Boole $\mathcal{P}(E)$ sono i singleton, cioè i sottoinsiemi di E costituiti da un unico elemento.

Esempio 2.31. Esistono algebre di Boole senza atomi. Infatti, un esempio ci è fornito dall'algebra di Boole $\mathcal{F}/\sim$ delle classi di formule del calcolo proposizionale quando l'insieme P delle variabili proposizionali è infinito. Per convincerci di questo fatto, dobbiamo mostrare che ogni elemento non nullo in $\mathcal{F}/\sim$ ammette almeno un minorante stretto non nullo. Sia allora F una formula che non è un'antilogia, ovvero tale che $\mathrm{cl}(F) \neq \mathbf{0}$. Esiste dunque una distribuzione di valori di verità δ che soddisfa F. Sia inoltre X una variabile proposizionale che non occorre in F. Una tale scelta è senza dubbio possibile in quanto P è per ipotesi un insieme infinito, mentre le formule sono per definizione successioni finite di simboli. Vediamo che la formula $((F \wedge X) \rightarrow F)$ è una tautologia:

F	X	$(F \wedge X)$	$((F \wedge X) \rightarrow F)$
0	0	0	1
0	1	0	1
1	0	0	1
1	1	1	1

Quindi $\mathrm{cl}((F \wedge X)) \leq \mathrm{cl}(F)$. Consideriamo adesso la distribuzione di valori di verità λ definita da:

$$\lambda(Y) = \begin{cases} \delta(Y) & \text{se } Y \neq X \\ 1 & \text{se } Y = X \end{cases}$$

Per costruzione essa soddisfa sia X sia F, perché X non occorre in F. Dunque soddisfa $(F \wedge X)$ e di conseguenza si ha $\mathrm{cl}((F \wedge X)) \neq \mathbf{0}$. Sia invece μ la distribuzione di valori di verità definita da:

$$\mu(Y) = \begin{cases} \delta(Y) & \text{se } Y \neq X \\ 0 & \text{se } Y = X \end{cases}$$

Allora μ non soddisfa X ma soddisfa F, di nuovo perché X non occorre in F. Ne deduciamo che μ soddisfa F e non soddisfa $(F \wedge X)$, quindi che non soddisfa $((F \wedge X) \leftrightarrow F)$. Questo dimostra che $\mathrm{cl}((F \wedge X)) \neq \mathrm{cl}(F)$ e allora concludiamo che $\mathrm{cl}((F \wedge X))$ è un minorante stretto non nullo di $\mathrm{cl}(F)$.

Osservazione 2.32. Siano $\mathcal{A} = \langle A, \leq, 0, 1\rangle$, $\mathcal{A}' = \langle A', \leq, 0, 1\rangle$ algebre di Boole, sia $a \in A$ un atomo e sia φ un isomorfismo di algebre di Boole da $\mathcal{A}$ in $\mathcal{A}'$. Allora $\varphi(a)$ è un atomo. Preso infatti un qualsiasi elemento $b' \in A'$ con $b' \leq \varphi(a)$, esiste $b \in A$ tale che $\varphi(b) = b'$ in quanto φ è suriettiva, dunque $\varphi(b) \leq \varphi(a)$. Dal teorema 1.21 deduciamo dunque che $b \leq a$ e quindi si deve avere $b = a$ oppure $b = 0$ perché a è un atomo. Otteniamo allora che $\varphi(b) = \varphi(a)$ oppure $\varphi(b) = \varphi(0)$, ovvero che $b' = \varphi(a)$ oppure $b' = 0$. D'altra parte, si ha $\varphi(a) \neq 0$ perché $a \neq 0$ e dunque $\varphi(a)$ è un atomo.

Abbiamo quindi una risposta negativa alla domanda posta all'inizio della sezione precedente: non tutte le algebre di Boole sono isomorfe all'algebra di Boole dei sottoinsiemi di un insieme, in quanto non può esistere un isomorfismo tra $\mathcal{F}/\!\sim$ con infinite variabili proposizionali e $\mathcal{P}(E)$ con E insieme non vuoto. Infatti, nell'esempio 2.30 abbiamo visto che i singleton sono atomi di $\mathcal{P}(E)$, quindi un eventuale isomorfismo da $\mathcal{P}(E)$ in $\mathcal{F}/\!\sim$ dovrebbe mandare i singleton in atomi di $\mathcal{F}/\!\sim$ per l'osservazione 2.32, ma questo non può succedere perché $\mathcal{F}/\!\sim$ non ha atomi, come abbiamo mostrato nell'esempio 2.31. Notiamo inoltre che $\mathcal{F}/\!\sim$ non è un'algebra di Boole finita, quindi non abbiamo una contraddizione con il corollario 2.23.

Servendoci delle nozioni che abbiamo sviluppato fino a questo punto, presentiamo infine una dimostrazione del teorema di compattezza per il calcolo proposizionale. Prima però ricordiamo che un sottoinsieme T di formule del calcolo proposizionale si dice *soddisfacibile* se esiste almeno una distribuzione di valori di verità che soddisfa tutte le formule di T, è invece detto *finitamente soddisfacibile* se ogni suo sottoinsieme finito è soddisfacibile.

Teorema 2.33 (di compattezza)**.** *Sia T un sottoinsieme di formule del calcolo proposizionale finitamente soddisfacibile. Allora T è soddisfacibile.*

Dimostrazione. Per qualsiasi sottoinsieme S di formule del calcolo proposizionale, definiamo un sottoinsieme di $\mathcal{F}/\!\sim$ nella maniera seguente:

$$S/\!\sim = \{\mathrm{cl}(F) \colon F \in S\}$$

Asserisco che $T/\!\sim$ è una base di un filtro di $\mathcal{F}/\!\sim$. Dato un numero finito di formule $F_1, F_2, \ldots, F_k$ di T, l'insieme $T_0 = \{F_1, F_2, \ldots, F_k\}$ è infatti un sottoinsieme finito di T e dunque, per ipotesi, esso è soddisfacibile. Se λ è una distribuzione di valori di verità che soddisfa le formule di T_0, allora:

$$\begin{aligned}
&\bar{\lambda}(F_i) = 1 \quad \forall i = 1, 2, \ldots, k \\
&\implies \bar{\lambda}((F_1 \wedge F_2 \wedge \cdots \wedge F_k)) = 1 \\
&\implies \mathrm{cl}((F_1 \wedge F_2 \wedge \cdots \wedge F_k)) \neq \mathbf{0} \\
&\implies \mathrm{cl}(F_1) \wedge \mathrm{cl}(F_2) \wedge \cdots \wedge \mathrm{cl}(F_k) \neq \mathbf{0}
\end{aligned}$$

Si noti che, per associatività dell'operazione $\wedge$, abbiamo omesso alcune coppie di parentesi. Con questo abbiamo dunque dimostrato che $T/\!\sim$ è una base di un filtro di $\mathcal{F}/\!\sim$ in quanto soddisfa la proprietà dell'intersezione finita. Dal lemma 1.48 segue allora che esiste un ultrafiltro U di $\mathcal{F}/\!\sim$ contenente $T/\!\sim$. Per l'osservazione 1.41 possiamo considerare l'omomorfismo h da $\mathcal{F}/\!\sim$ in $\{0, 1\}$ associato all'ultrafiltro U che, per il punto (3′) del teorema 1.39, manda ogni elemento di U in 1. Di conseguenza, se q è la mappa quoziente da $\mathcal{F}$ in $\mathcal{F}/\!\sim$, per ogni formula F di T abbiamo che:

$$(h \circ q)(F) = h(\mathrm{cl}(F)) = 1$$

Concludiamo allora che la restrizione di $h \circ q$ sulle lettere proposizionali è una distribuzione di valori di verità δ tale che valga $\bar{\delta} = h \circ q$ e in particolare δ soddisfa tutte le formule di T. Dunque T è soddisfacibile. □

Conclusioni

Abbiamo discusso le principali proprietà delle algebre di Boole, caratterizzandole sia come anelli unitari i cui elementi sono idempotenti rispetto alla moltiplicazione, sia come reticoli distributivi e complementari.

Abbiamo poi ripreso le nozioni tipicamente algebriche di omomorfismo, isomorfismo, ideale e ideale massimale, inserendole nel contesto delle algebre di Boole, per poi introdurre i concetti di filtro e ultrafiltro. Abbiamo messo in luce la dualità tra ideali e filtri di un'algebra di Boole $\mathcal{A}$, nonché la corrispondenza biunivoca tra ideali massimali, ultrafiltri e omomorfismi di algebre di Boole da $\mathcal{A}$ in $\{0,1\}$:

$$\begin{array}{ccccc}
\{\text{Ideali massimali di } \mathcal{A}\} & \longleftrightarrow & \{\text{Ultrafiltri di } \mathcal{A}\} & \longleftrightarrow & S(\mathcal{A}) \\
I & \longmapsto & A \setminus I & & \\
A \setminus F & \longmapsfrom & F & \longmapsto & h_{A\setminus F} \\
 & & \{x \in A \colon h(x) = 1\} & \longmapsfrom & h \\
I & \multicolumn{3}{c}{\longmapsto} & h_I \\
\{x \in A \colon h(x) = 0\} & \multicolumn{3}{c}{\longmapsfrom} & h
\end{array}$$

Con il teorema dell'ultrafiltro, abbiamo tradotto il teorema sull'esistenza di ideali massimali, dovuto a Krull, in termini di filtri e ultrafiltri, per poi fornire una caratterizzazione delle basi di filtri in quanto sottoinsiemi di ultrafiltri.

Con l'ausilio di qualche risultato di topologia, tutte queste nozioni ci hanno poi consentito di dimostrare che lo spazio di Stone $S(\mathcal{A})$ di un'algebra di Boole $\mathcal{A}$ è uno spazio di Boole, cioè uno spazio topologico compatto di dimensione zero.

Abbiamo quindi stabilito, grazie anche al teorema di rappresentazione di Stone, una biiezione tra algebre di Boole e spazi di Boole:

$$\begin{array}{ccc}
\{\text{Algebre di Boole}\} & \longleftrightarrow & \{\text{Spazi di Boole}\} \\
\mathcal{A} & \longmapsto & S(\mathcal{A}) \\
\mathcal{B}(X) & \longmapsfrom & X
\end{array}$$

In particolare:

- Ogni algebra di Boole è l'algebra di Boole dei chiuso-aperti di uno spazio di Boole, a meno di isomorfismo.
- Ogni spazio di Boole è lo spazio di Stone di un'algebra di Boole, a meno di omeomorfismo.

Per concludere, ci siamo dedicati alle conseguenze in logica proposizionale, dando anche una dimostrazione del teorema di compattezza per il calcolo proposizionale.

Bibliografia

[1] Vito Michele Abrusci and Lorenzo Tortora de Falco. *Logica: Volume 2-Incompletezza, teoria assiomatica degli insiemi*, volume 111. Springer, 2018.

[2] René Cori and Daniel Lascar. *Logique mathématique: cours et exercices. Calcul propositionnel, algèbres de Boole, calcul des prédicats*. Masson, 1993.

[3] Lorenzo Tortora de Falco and Vito Michele Abrusci. *Logica: Dimostrazioni e modelli al primo ordine*. Springer, 2014.

[4] Patrick Dehornoy. *La théorie des ensembles*. Calvage & Mounet, Paris, 2017.

[5] J Michael Dunn and Gary Hardegree. *Algebraic methods in philosophical logic*. OUP Oxford, 2001.

[6] Wilfrid Hodges. Krull implies zorn. *Journal of the London Mathematical Society*, 2(2):285–287, 1979.

[7] Thomas W Hungerford. *Abstract algebra: an introduction*. Cengage Learning, 2012.

[8] Jean-Louis Krivine. *Théorie des ensembles*. Cassini, 1998.

[9] Marco Manetti. *Topologia*, volume 78. Springer Science & Business Media, 2014.