Stonature

GIOVANNI CUTOLO

1. Anelli booleani

Per definizione, gli anelli booleani sono gli anelli unitari in cui ogni elemento è idempotente, vale a dire: coincide col proprio quadrato. La definizione ha facili e importanti conseguenze:

1. *Sia R un anello booleano. Allora R è commutativo e, se non nullo, ha caratteristica* 2.

Dimostrazione. Per ogni $a, b \in R$ si ha $a + b = (a + b)^2$, come segue dalla definizione di anello booleano, ma d'altra parte $(a + b)^2 = a^2 + ab + ba + b^2$. Dunque, usando ancora l'idempotenza degli elementi di R, $a + b = a + ab + ba + b$, da cui $0_R = ab + ba$. Abbiamo provato che $ab = -ba$ per ogni $a, b \in R$. Nel caso in cui $a = b$ questa identità fornisce $a^2 = -a^2$, vale a dire $a = -a$, ovvero $2a = 0_R$. Ciò mostra che R ha caratteristica 2, a meno che $|R| = 1$ (vale a dire: $0_R = 1_R$). L'identità $ab = -ba$ provata in precedenza, insieme all'osservazione, appena fatta, che ogni elemento di R coincide col suo opposto prova che R è commutativo. □

2. *Sia R un anello booleano. Allora 1_R è l'unico elemento cancellabile di R; dunque* $\mathrm{Jac}(R) = 0$.

Dimostrazione. Se x è un elemento idempotente in un qualsiasi anello commutativo unitario R, allora $x(x - 1_R) = 0_R$ e quindi x è un divisore dello zero, a meno che $x = 1_R$. Da ciò segue subito la prima parte dell'enunciato. Per concludere la dimostrazione basta ricordare che il radicale di Jacobson di un anello commutativo unitario in cui l'unità sia l'unico invertibile è l'ideale nullo[1]. □

Un ovvio esempio di anello booleano è, per ogni insieme S, l'anello $(\mathcal{P}(S), \triangle, \cap)$ delle parti di S. Se S è infinito, l'insieme delle parti finite di S ne costituisce un sottoanello e fornisce un esempio di anello non unitario ad elementi tutti idempotenti. L'insieme delle parti finite o cofinite[2] di S costituisce invece un sottoanello unitario di $\mathcal{P}(S)$. Se S è numerabile, questo sottoanello è esso stesso numerabile e fornisce così un esempio di anello booleano che, proprio perché numerabile, non è isomorfo a $(\mathcal{P}(X), \triangle, \cap)$ per alcun insieme X.

Se $|S| = 1$ l'anello $(\mathcal{P}(S), \triangle, \cap)$ è isomorfo al campo $\mathbb{Z}_2$. Questo è l'unico esempio di anello booleano che sia integro:

3. *Sia P un ideale primo dell'anello booleano R. Allora P è massimale e $R/P \simeq \mathbb{Z}_2$.*

Dimostrazione. P/R è un dominio di integrità, ma, per 2, tutti i suoi elementi tranne l'identità sono divisori dello zero, vale a dire zero. Dunque, R/P consiste dello zero e dell'unità, quindi $R/P \simeq \mathbb{Z}_2$ e R è massimale. □

Come si vedrà nella prossima sezione, non è un caso che gli esempi di anelli booleani forniti sinora siano (isomorfi a) sottoanelli unitari dell'anello delle parti di un opportuno insieme: non ce ne sono altri.

Somme ed intersezioni tra ideali principali in anelli booleani sono particolarmente semplici da descrivere, vale infatti una sorta di teorema di Bézout per anelli booleani:

4. *Siano a e b elementi di un anello booleano R. Allora:*

(i) $aR + bR = (a + ab + b)R$;
(ii) $aR \cap bR = (aR)(bR) = abR$.

Di conseguenza, l'insieme degli ideali principali di R costituisce un sottoreticolo dell'insieme degli ideali di R. Inoltre, tutti gli ideali finitamente generati di R sono principali.

---

[1] questo è stato visto nella prima parte del corso come applicazione della caratterizzazione del radicale di Jacobson di un anello commutativo unitario R: $\mathrm{Jac}(R) = \{a \in R \mid (\forall x \in R)(1 + ax \in \mathcal{U}(R))\}$.

[2] una parte X di S è *cofinita* se e solo se $S \smallsetminus X$ è finita

Dimostrazione. È ovvio che $(a + ab + b)R \subseteq aR + bR$. Viceversa, l'idempotenza di a e b comporta $(a + ab + b)a = a + ab + ab = a$ e $(a + ab + b)b = ab + ab + b = b$, dunque $aR + bR \subseteq (a + ab + b)R$. Questo prova (i). Facendo induzione sul numero di generatori è ora facile verificare che tutti gli ideali di R sono principali. Passiamo a provare (ii). Naturalmente $aR \cap bR \supseteq (aR)(bR) = abR$; d'altra parte, se $c \in aR \cap bR$, allora $c = ar = bs$ per opportuni $r, s \in R$ e quindi $ac = a^2r = c$ e $bc = b^2s = c$, quindi $c = abc \in abR$. Così anche (ii) è provata, ed è ora chiaro che gli ideali principali costituiscono un sottoreticolo del reticolo degli ideali di R. □

Esercizi.

1.1. Sia R un anello (non necessariamente unitario) ad elementi tutti idempotenti. Verificare che R è commutativo ed ha caratteristica al più 2. Basta, a questo scopo duplicare la dimostrazione dell'enunciato 1. (Nel caso degli anelli non unitari la caratteristica viene definita come l'esponente del gruppo additivo, se questo esponente è finito, oppure 0, se questo esponente è infinito.)

1.2. Sia R un anello non unitario ad elementi tutti idempotenti. Allora R ha una (ovvia, e univocamente determinata) struttura di $\mathbb{Z}_2$-algebra. Verificare che la consueta costruzione di una $\mathbb{Z}_2$-algebra unitaria (di sostegno $R \times \mathbb{Z}_2$) in cui si immerga R fornisce un anello booleano.

1.3. Sia R un anello booleano. Allora:

- ogni ideale di R coincide col suo radicale;
- ogni ideale primario di R è massimale (e quindi ha indice 2 in R);
- ogni ideale decomponibile (in intersezione finita di ideali primari) ha indice finito (potenza di 2) in R.

2. Il teorema di Stone

Nelle sue varie forme, il teorema di rappresentazione di Stone stabilisce che ogni anello booleano si immerge nell'anello delle parti di un opportuno insieme. Di per sé questo risultato è piuttosto facile da provare. Si può partire dall'osservazione che l'anello delle parti di un insieme è isomorfo ad un prodotto diretto di copie del campo $\mathbb{Z}_2$. Infatti, per ogni insieme S la familiare biezione $\mathcal{P}(S) \to \mathbb{Z}_2^S$ che ad ogni parte di S associa la sua funzione caratteristica, qui considerata come funzione a valori in $\mathbb{Z}_2$, è un isomorfismo di anelli unitari, come è semplice verificare (qui, naturalmente, $\mathbb{Z}_2^S$ ha la usuale struttura di anello di funzioni a valori nel campo $\mathbb{Z}_2$). Dunque

$$(\mathcal{P}(S), \triangle, \cap) \simeq \mathbb{Z}_2^S = \prod_{x \in S} \mathbb{Z}_2. \tag{$*$}$$

Sia ora R un anello booleano. Indichiamo con $\mathcal{M}(R)$ l'insieme dei suoi ideali massimali (cioè, per 3, lo spettro di R). L'omomorfismo

$$\theta \colon x \in R \longmapsto (x + M)_{M \in \mathcal{M}(R)} \in \prod_{M \in \mathcal{M}(R)} R/M$$

ha ovviamente per nucleo $\bigcap \mathcal{M}(R) = \mathrm{Jac}(R)$; ma $\mathrm{Jac}(R) = 0$ per 2, quindi θ è un monomorfismo (di anelli unitari). Inoltre, come mostra 3, si ha $R/M \simeq \mathbb{Z}_2$ per ogni $M \in \mathcal{M}(R)$, quindi $\prod_{M \in \mathcal{M}(R)} R/M \simeq \prod_{M \in \mathcal{M}(R)} \mathbb{Z}_2 \simeq (\mathcal{P}(\mathcal{M}(R)), \triangle, \cap)$, per l'isomorfismo stabilito in $(*)$. Abbiamo così un monomorfismo

$$\mu \colon R \rightarrowtail (\mathcal{P}(\mathcal{M}(R)), \triangle, \cap).$$

Già a questo punto abbiamo dimostrato una forma debole del teorema di Stone: ogni anello booleano è isomorfo ad un sottoanello unitario dell'anello delle parti di un insieme. Nel caso particolare degli anelli booleani finiti questo risultato si può subito migliorare:

5. *Ogni anello booleano finito è isomorfo a $(\mathcal{P}(S), \triangle, \cap)$ per un opportuno insieme finito S.*

Dimostrazione. Torniamo al monomorfismo $\theta \colon R \rightarrowtail \prod_{M \in \mathcal{M}(R)} R/M$ definito sopra. Nel caso in cui l'anello booleano R sia finito, è finito anche l'insieme $\mathcal{M}(R)$ di indici che appare nella descrizione del prodotto diretto $\prod_{M \in \mathcal{M}(R)} R/M$. Per un lemma che dovrebbe essere ben noto (si veda ad esempio la Proposizione 1.10(b) in Atiyah-Macdonald), poiché gli ideali in $\mathcal{M}(R)$ sono (ovviamente!) a due a due comassimali, questo implica che θ è suriettiva. Dunque θ è un isomorfismo e lo stesso vale, di conseguenza, per μ. □

Come è stato già osservato, l'ipotesi che R sia finito non si può rimuovere: esistono anelli booleani infiniti (quelli numerabili, ad esempio) che non sono isomorfi all'anello delle parti di un insieme.

La 5 ha un corollario: un anello booleano finito è determinato, a meno di isomorfismi, dalla sua cardinalità:

6. *Siano R_1 e R_2 due anelli booleani finiti equipotenti. Allora $R_1 \simeq R_2$.*

Dimostrazione. Esistono insiemi finiti S_1 e S_2 tali che $R_1 \simeq \mathcal{P}(S_1)$ e $R_2 \simeq \mathcal{P}(S_2)$. Dunque $|R_1| = 2^{|S_1|}$ e $|R_2| = 2^{|S_2|}$; da $|R_1| = |R_2|$ segue allora $|S_1| = |S_2|$ e quindi $\mathcal{P}(S_1) \simeq \mathcal{P}(S_2)$. Di conseguenza, $R_1 \simeq R_2$. □

Per approfondire lo studio degli anelli booleani infiniti e arrivare ad una versione più sofisticata del teorema di Stone, descriviamo esplicitamente il monomorfismo μ. Abbiamo ottenuto μ dalla composizione degli omomorfismi:

$$R \xrightarrow{\theta} \prod_{M\in\mathcal{M}(R)} R/M \xrightarrow{\psi} \prod_{M\in\mathcal{M}(R)} \mathbb{Z}_2 = \mathbb{Z}_2^{\mathcal{M}(R)} \xrightarrow{\xi} (\mathcal{P}(\mathcal{M}(R)), \triangle, \cap),$$

dove, come al solito, R è un anello booleano, ψ è l'isomorfismo indotto dai singoli (univocamente determinati) isomorfismi $R/M \to \mathbb{Z}_2$, al variare di M in $\mathcal{M}(R)$ e ξ è l'isomorfismo che ad ogni elemento f di $\mathbb{Z}_2^{\mathcal{M}(R)}$ associa la parte di $\mathcal{M}(R)$ di cui f è funzione caratteristica (cioè l'antiimmagine di $\{[1]_2\}$ mediante f). Se $x \in R$, allora $x^{\theta\psi} = (\delta_M)_{M\in\mathcal{M}(R)}$, dove, per ogni M, $\delta_M = [0]_2$ se $x \in M$, e $\delta_M = [1]_2$ se $x \notin M$. Da ciò segue che x^μ non è altro che l'insieme degli ideali massimali di R a cui x non appartiene; volendo non inutilmente complicare le cose: $x^\mu = \mathcal{M}(R) \setminus \mathrm{Var}(xR)$. Per ogni $x, y \in R$, un ideale massimale M di R contiene tra i suoi elementi xy se e solo se contiene uno tra x e y, vale a dire, $\mathrm{Var}(xR) \cup \mathrm{Var}(yR) = \mathrm{Var}(xyR)$, quindi $x^\mu \cap y^\mu = (xy)^\mu$. Analogamente, $x^\mu \cup y^\mu = \{M \in \mathcal{M}(R) \mid x \notin M \vee y \notin M\} = \mathcal{M}(R) \setminus \mathrm{Var}(xR+yR)$, quindi, per la 4, $x^\mu \cup y^\mu = (x + xy + y)^\mu$.

L'insieme $\operatorname{im}\mu$, ovvero $\{x^\mu \mid x \in R\}$, è così un sottoreticolo di $(\mathcal{P}(\mathcal{M}(R)), \subseteq)$. Essendo chiuso per intersezioni finite, esso costituisce una base per una topologia su $\mathcal{M}(R)$, che indicheremo con $\mathcal{A}$. La descrizione degli aperti è molto semplice: $\mathcal{A} = \{A_S \mid S \subseteq R\}$, dove, per ogni $S \subseteq R$,

$$A_S = \bigcup S^{\vec{\mu}} = \bigcup_{x\in S} x^\mu = \{M \in \mathcal{M}(R) \mid S \not\subseteq M\} = \mathcal{M}(R) \setminus \mathrm{Var}(SR);$$

ricordiamo che SR è l'ideale di R generato da S. Ci sarà utile riformulare 3 in termini di aperti della base $\operatorname{im}\mu$:

7. *Per ogni $x \in R$, $(1_R + x)^\mu = \mathcal{M}(R) \setminus x^\mu = \mathrm{Var}(xR)$.*

Dimostrazione. Siano $x \in R$ e $M \in \mathcal{M}(R)$. Se $x \in M$, ovviamente $1_R + x \notin M$. Viceversa, se $x \notin M$ allora $1_R + x \in M$ perché $|R/M| = 2$. Abbiamo così verificato che $x \in M$ se e solo se $1 + x \notin M$, il che equivale all'asserto. □

È ora chiaro che gli elementi della base $\operatorname{im}\mu$ sono clopen[3] dello spazio topologico $(\mathcal{M}(R), \mathcal{A})$. Possiamo anche notare che la nostra base $\operatorname{im}\mu$ ha ora una descrizione alternativa: $\operatorname{im}\mu = \{\mathrm{Var}(xR) \mid x \in R\}$. Un'altra osservazione essenziale è la seguente:

8. *Con le notazioni appena stabilite, per ogni $S \subseteq R$ si ha $A_S = A_{SR}$. Inoltre $A_S = \mathcal{M}(R)$ se e solo se $1_R \in SR$.*

Dimostrazione. Che A_S coincida con A_{SR} è evidente dalla descrizione di A_S data sopra. Altrettanto evidenti sono le equivalenze:

$$A_{SR} = \mathcal{M}(R) \iff \mathrm{Var}(SR) = \varnothing \iff SR = R \iff 1_R \in SR,$$

da cui segue l'enunciato. □

Questo basta per determinare diverse proprietà della topologia $\mathcal{A}$:

9. *Lo spazio topologico $(\mathcal{M}(R), \mathcal{A})$ è compatto, di Hausdorff e totalmente sconnesso.*

[3] cioè sottospazi contemporaneamente aperti e chiusi

Dimostrazione. La compattezza segue molto rapidamente da 8. Se $\mathcal{M}(R) = \bigcup\{A_S \mid S \in \mathcal{S}\}$ per un qualche $\mathcal{S} \subseteq \mathcal{P}(R)$, vale a dire: $\mathcal{M}(R) = A_{\bigcup \mathcal{S}}$, allora 1_R appartiene all'ideale di R generato da $\bigcup \mathcal{S}$, quindi all'ideale generato da una parte finita di $\bigcup \mathcal{S}$, e quindi all'ideale generato da $\bigcup \mathcal{S}_0$ per un opportuno sottoinsieme finito $\mathcal{S}_0$ di $\mathcal{S}$. Da ciò segue che $\mathcal{M}(R) = A_{\bigcup \mathcal{S}_0} = \bigcup\{A_S \mid S \in \mathcal{S}_0\}$. Abbiamo così provato che $(\mathcal{M}(R), \mathcal{A})$ è compatto.

Per completare la dimostrazione, fissiamo due elementi distinti M ed N di $\mathcal{M}(R)$. Allora $N \not\subseteq M$, perché N è massimale. Scelto $x \in N \setminus M$, abbiamo così $M \in x^\mu$ e $N \notin x^\mu$. Poiché x^μ è un clopen, questo basta a provare che $(\mathcal{M}(R), \mathcal{A})$ è totalmente sconnesso e di Hausdorff.[4] □

È un facile esercizio la verifica del fatto che l'insieme dei clopen di un qualsiasi spazio topologico su un insieme S è un sottoanello unitario dell'anello (booleano) delle parti di S, infatti S stesso è un clopen e sia l'intersezione che la differenza simmetrica tra due arbitrari clopen è un clopen. Il teorema di Stone, nella sua forma completa, inverte questa osservazione:

10 (Teorema di Stone)**.** *Sia R un anello booleano. Allora esiste uno spazio topologico T compatto, di Hausdorff e totalmente sconnesso tale che R sia isomorfo all'anello dei clopen di T.*

Dimostrazione. Naturalmente lo spazio topologico dell'enunciato è lo spazio $(\mathcal{M}(R), \mathcal{A})$ definito e discusso in questa sezione. Visti gli enunciati precedenti, per dimostrare il teorema occorre solo verificare che gli insiemi x^μ, al variare di x in R, sono i soli clopen di $(\mathcal{M}(R), \mathcal{A})$. A questo scopo, sia C un clopen in $(\mathcal{M}(R), \mathcal{A})$. Essendo aperto, C sarà uguale ad $A_S = \bigcup\{x^\mu \mid x \in S\}$ per un opportuno $S \subseteq \mathcal{M}(R)$; ma in quanto chiuso in uno spazio compatto, C sarà a sua volta compatto, quindi esiste una parte finita S_0 di S tale che $C = A_{S_0}$. La 4 mostra che S_0R è principale: esiste $y \in R$ tale che $S_0R = yR$; ma allora $C = y^\mu$. Abbiamo così provato che l'immagine di R mediante μ è proprio l'anello dei clopen di $(\mathcal{M}(R), \mathcal{A})$. Questo completa la dimostrazione del teorema di Stone. □

Esercizi.

2.1. Verificare in dettaglio il fatto, notato ed utilizzato nel testo, che l'applicazione che ad una parte X di un insieme S associa la sua funzione caratteristica (da S a $\mathbb{Z}_2$) è un isomorfismo di anelli unitari da $(\mathcal{P}(S), \triangle, \cap)$ a $\mathbb{Z}_2^S$.

2.2. Per quali spazi topologici l'anello (booleano) dei clopen è isomorfo a $\mathbb{Z}_2$?

2.3. Con riferimento alle notazioni del testo ed al monomorfismo $\mu\colon R \rightarrowtail \mathcal{P}(\mathcal{M}(R))$, provare l'equivalenza tra le affermazioni: (i) μ è un isomorfismo; (ii) la topologia $\mathcal{A}$ è discreta; (iii) $\mathcal{M}(R)$ è finito; (iv) R è finito.

2.4. Sia R un arbitrario anello commutativo. Verificare che $\mathcal{Z} := \{\mathrm{Var}(H) \mid H \lhd R\}$ è chiuso per unioni finite e per intersezioni arbitrarie. Dedurne che $\mathcal{Z}$ è l'insieme dei chiusi di una topologia su $\mathrm{Spec}(R)$. Questa si chiama *topologia di Zariski*. Provare che lo spazio topologico $(\mathrm{Spec}(R), \mathcal{Z})$ è compatto. Osservare infine che, nel caso in cui R sia booleano, la topologia di Zariski coincide con quella discussa nel testo (e indicata con $\mathcal{A}$) su $\mathrm{Spec}(R) = \mathcal{M}(R)$.

2.5. Descrivere la topologia di Zariski, definita nell'esercizio precedente, nel caso in cui R sia l'anello degli interi.

2.6. Sia R un anello commutativo. $\mathrm{Spec}(R)$, munito della topologia di Zariski, è necessariamente di Hausdorff? È totalmente sconnesso?

2.7. Sia $R = (\mathcal{P}(X), \triangle, \cap)$, per un arbitrario insieme X. Allora:

- per ogni $Y \subseteq X$, l'ideale di R generato da Y è $\mathcal{P}(Y)$. Questo ideale è massimale se e solo se $X \setminus Y$ è un singleton;
- se X è finito, ogni ideale di R è principale;
- se X è infinito, l'insieme $\mathcal{P}_\mathcal{F}(X)$ delle parti finite di X costituisce un ideale (proprio) di R. Questo ideale non è contenuto in nessun ideale principale proprio di R. Dunque $\mathrm{Var}(\mathcal{P}_\mathcal{F}(X))$ (che non è vuoto) è l'insieme degli ideali massimali non principali di R.

[4] forse è il caso di ricordarlo: uno spazio topologico è totalmente sconnesso quando le sue componenti connesse sono singleton. Se, scelti comunque due punti distinti a e b di uno spazio topologico T, esiste un clopen X di T contenente a ma non b, allora lo spazio è di Hausdorff (a e b sono separati da X e da $T \setminus X$, entrambi aperti) e totalmente sconnesso: se a e b appartengono allo stesso sottospazio Y di T, allora $Y \cap X$ è un clopen non banale di Y, quindi Y non è connesso.

3. Altri punti di vista

Esistono presentazioni alternative, ma equivalenti, alla teoria degli anelli booleani ed al teorema di Stone. Senza entrare in dettagli, e solo a titolo di informazione, forniamo qui una panoramica di alcune delle possibilità.

La nozione di anello booleano equivale a quella di reticolo booleano, ovvero a quella di algebra di Boole. Vediamo le definizioni: un reticolo booleano è semplicemente un reticolo che sia distributivo e complementato. La definizione di algebra di Boole è più involuta: si tratta di una struttura algebrica $(B, \wedge, \vee, ', 1, 0)$, dove $\wedge$ e $\vee$ sono operazioni binarie associative e commutative, ciascuna distributiva rispetto all'altra, $'$ è un'operazione unaria e 1 e 0 sono due operazioni nullarie (in altri termini, 1 e 0 sono elementi preselezionati in B) che individuino elementi neutri, rispettivamente, per $\wedge$ e $\vee$; inoltre si richiede che, per ogni $a, b \in B$ valgano le seguenti uguaglianze: $a \vee (a \wedge b) = a = a \wedge (a \vee b)$ (leggi di assorbimento), $1 = a \vee a'$ e $0 = a \wedge a'$ (leggi di complementazione).

Chi ha familiarità con la definizione di reticolo come struttura algebrica, e con l'equivalenza tra questa definizione e quella di reticolo come struttura ordinata non avrà difficoltà a riconoscere che la definizione data di algebra di Boole non è altro che la definizione di reticolo come struttura algebrica arricchita con le condizioni di distributività e complementazione richieste dalla definizione di reticolo booleano. Dunque è chiaro che lo studio dei reticoli booleani e quello delle algebre di Boole sono equivalenti ed i rispettivi linguaggi sono perfettamente interscambiabili.

Vale la pena di menzionare il fatto la definizione data di algebra di Boole è ridondante: la neutralità di 0 e 1 segue facilmente dalle leggi di assorbimento e di complementazione; inoltre la distributività di $\wedge$ rispetto a $\vee$ implica la distributività di $\vee$ rispetto a $\wedge$, e viceversa, basterebbe quindi richiedere una sola delle due distributività. Altra osservazione che aiuta a non fare confusione: a differenza di quanto accade per reticoli arbitrari, nei reticoli distributivi ogni elemento ha al massimo un complemento, quindi, per ogni elemento a dell'algebra di Boole B, indicata come sopra, a' è l'*unico* complemento di a in B.

Sia ora R un anello booleano. Indichiamo con $|$ la relazione di divisibilità in R; dunque, per ogni $a, b \in R$, $a|b$ se e solo se esiste $c \in R$ tale che $b = ac$. Notiamo subito che quest'ultima uguaglianza implica $ab = a(ac) = a^2c = ac = b$, dunque:

$$(\forall\, a, b \in R)(a|b \iff ab = b).$$

È facile dedurre che $|$ è una relazione d'ordine in R. A questo punto, segue subito da 4 che $(R, |)$ è un reticolo: se $a, b \in R$, $ab = \sup_{(R,|)}\{a, b\}$ e $a + ab + b = \inf_{(R,|)}\{a, b\}$ (in altri termini ab e $a + ab + b$ sono rispettivamente minimo comune multiplo e massimo comun divisore tra a e b). È chiaro che questo reticolo è limitato (con massimo 0_R e minimo 1_R) e che ogni $a \in R$ ha complemento, precisamente $1_R + a$, in $(R, |)$. Infine, che le operazioni reticolari siano distributive l'una rispetto all'altra segue dalla verifica diretta delle identità $a(b+bc+c) = ab+(ab)(ac)+ac$ e $a(b+bc+c) = ab+(ab)(ac)+ac$, che valgono per ogni $a, b, c \in R$.[5] Dunque, $(R, |)$ è un reticolo booleano. In verità si preferisce, abitualmente, associare all'anello booleano R il reticolo duale a $(R, |)$, vale a dire $(R, \leq)$, dove la relazione $\leq$ è definita da $a \leq b$ se e solo se $b|a$ ("a è multiplo di b"), vale a dire: $ab = a$. Non cambia niente di essenziale: ogni reticolo booleano è isomorfo al suo duale (tramite l'isomorfismo che associa ad ogni elemento il suo complemento). Ricaviamo però due piccoli vantaggi: in primo luogo, in questo modo l'applicazione definita da $a \mapsto aR$ stabilisce un isomorfismo tra il reticolo booleano associato ad R ed il reticolo degli ideali principali di R (vedi 4). In secondo luogo, il più tipico degli esempi può essere formulato con linguaggio più scorrevole: è un semplicissimo esercizio la verifica del fatto che, scelto comunque un insieme S, il reticolo booleano associato all'anello $(\mathcal{P}(S), \triangle, \cap)$ è $(\mathcal{P}(S), \subseteq)$.

Queste costruzioni si invertono: se $(B, \leq)$ è un reticolo booleano, indicata con $(B, \wedge, \vee, ', 1, 0)$ la corrispondente algebra di Boole, si può definire in B un'operazione di addizione, ponendo $a+b = (a \wedge b') \vee (a' \wedge b)$ per ogni $a, b \in B$ (la definizione ricalca quella della differenza simmetrica). Si verifica, con un pò di pazienza, che $(R, +, \wedge)$ è un anello booleano, con zero 0 e unità 1. Non solo, il reticolo booleano costruito a partire da questo anello come illustrato sopra è proprio $(B, \leq)$. Viceversa, dato un anello booleano $(R, +, \cdot)$, l'anello definito, come appena specificato, dal reticolo booleano corrispondente a $(R, +, \cdot)$ è proprio $(R, +, \cdot)$. Detto in termini più precisi, per ogni insieme R abbiamo costruito due applicazioni biettive, l'una inversa dell'altra, tra l'insieme delle coppie di operazioni binare che strutturano R come anello booleano e quello delle relazioni d'ordine su R che lo strutturano come reticolo booleano. Per questo motivo, come accennato all'inizio di questa sezione, la teoria degli anelli booleani è perfettamente

[5] come accennato sopra, in realtà basta verificare solo una delle due identità.

equivalente a quella dei reticoli booleani e a quella delle algebre di Boole, e si può liberamente passare, senza perdere alcuna informazione, dall'uno all'altro dei corrispondenti linguaggi.[6]

Un'altra breve discussione che vale la pena di fare riguarda il teorema di Stone. Soprattutto quando il teorema viene presentato nel linguaggio delle algebre di Boole, piuttosto che in quello degli anelli booleani, la dimostrazione viene espressa in termini di *ultrafiltri* piuttosto che di ideali massimali. Ma, di nuovo, queste due nozioni sono essenzialmente interscambiabili.

Prima le definizioni: se $(X, \leq)$ è un insieme ordinato, un *filtro* in $(X, \leq)$ è un sottoinsieme proprio e non vuoto di X che contenga tutti i maggioranti dei suoi elementi ed almeno un minorante di ogni sua parte finita. Più esplicitamente, F è un filtro di $(X, \leq)$ se e solo se $\varnothing \neq F \subset X$ e valgono:

(F.1) $(\forall x \in F)(\forall z \in X)(x \leq z \Rightarrow z \in F)$
(F.2) $(\forall\, x, y \in F)(\exists z \in F)(z \leq x \wedge z \leq y)$.

Un ultrafiltro è filtro che sia massimale rispetto all'inclusione. Ora consideriamo il caso in cui $(X, \leq) = (\mathcal{P}(S), \subseteq)$ per un insieme S. È un facile esercizio riconoscere che i filtri di $(\mathcal{P}(S), \subseteq)$ sono precisamente gli insiemi della forma $\bar{H} := \{S \smallsetminus x \mid x \in H\}$ al variare di H nell'insieme degli ideali propri di $(\mathcal{P}(S), \triangle, \cap)$. Ovviamente $\bar{H}$ risulta essere un ultrafiltro precisamente quando H è un ideale massimale di $(\mathcal{P}(S), \triangle, \cap)$. Lo stesso vale per un arbitrario anello booleano R: l'assegnazione $H \mapsto 1_R + H = \{1_R + x \mid x \in H\}$ definisce una biezione dall'insieme degli ideali propri di R a quello dei filtri del reticolo booleano corrispondente a R, e questa biezione fa corrispondere ideali massimali ad ultrafiltri. È dunque possibile sostituire, nella dimostrazione del teorema di Stone fornita nella sezione precedente, lo spazio topologico $(\mathcal{M}(R), \mathcal{A})$ con uno spazio, ad esso omoeomorfo, con sostegno l'insieme degli ultrafiltri di un reticolo booleano; questa è la strada che segue la maggior parte delle trattazioni in letteratura.

Esercizi.

3.1. Sia S un insieme. Per ogni $x \in S$, l'insieme $\{X \in \mathcal{P}(S) \mid x \in X\}$ è un ultrafiltro di $(\mathcal{P}(S), \subseteq)$. Gli ultrafiltri di questa forma si dicono ultrafiltri principali (o anche banali) di $(\mathcal{P}(S), \subseteq)$. Verificare che gli ultrafiltri principali di $(\mathcal{P}(S), \subseteq)$ corrispondono precisamente (nel senso indicato nel testo) agli ideali massimali principali di $(\mathcal{P}(S), \triangle, \cap)$. Dedurre, utilizzando l'esercizio 2.7, l'esistenza di ultrafiltri non principali in $(\mathcal{P}(S), \subseteq)$ nel caso in cui S sia infinito.

3.2. Una nota caratterizzazione degli ultrafiltri di un reticolo booleano $(B, \leq)$ è questa: un filtro F di $(B, \leq)$ è un ultrafiltro se e solo se, per ogni $x \in B$, se $x \notin F$ allora $x' \in F$ (come di consueto, x' indica il complementare di x). Dimostrare questa caratterizzazione come conseguenza (immediata!) dell'enunciato 3.

[6] con le dovute accortezze a proposito delle sottostrutture. Ad esempio, se $(R, +, \cdot)$ è un anello booleano, corrispondente al reticolo booleano $(R, \leq)$ ed all'algebra di Boole $(R, \wedge, \vee, ', 1, 0)$, una parte X di R costituisce una sottoalgebra di $(R, \wedge, \vee, ', 1, 0)$ se e solo se costituisce un sottoanello unitario di $(R, +, \cdot)$, ma può costituire un sottoreticolo di $(R, \leq)$ anche in altri casi. Ad esempio, ogni ideale principale di $(R, +, \cdot)$ costituisce un sottoreticolo, e un sottoreticolo di $(R, \leq)$ può addirittura non essere booleano.