RETICOLI ED ALGEBRE DI BOOLE

Abbiamo già introdotto in due modi diversi la nozione di reticolo:

Def.1. Si dice reticolo un insieme (parzialmente) ordinato $(L , \leq)$ tale che per ogni $a,b \in L$ esistano in L inf {a,b} e sup{a,b}.

Def.2. Si dice reticolo una struttura algebrica con due leggi di composizioni (interne) binarie che chiameremo intersezione ed unione ed indicheremo con $\wedge$ e $\vee$, che godono delle seguenti proprietà:

- commutativa	$\forall a,b \in L$	$a\wedge b=b\wedge a$,	$a\vee b=b\vee a$
- associativa	$\forall a,b,c \in L$	$(a\wedge b) \wedge c=a\wedge(b\wedge c)$	$(a\vee b) \vee c=a\vee (b\vee c)$
- di assorbimento	$\forall a,b \in L$	$a\wedge(a\vee b)=a$	$a\vee (a\wedge b)=a$

Si può facilmente passare da una definizione all'altra

Def.1 $\rightarrow$ *Def. 2*

Se $(L , \leq)$ è un insieme (parzialmente) ordinato tale che per ogni $a,b \in L$ esistano in L inf {a,b} e sup{a,b}, possiamo porre

$a\wedge b=$ inf {a,b},

$a\vee b=$ sup{a,b},

poiché per ogni $a,b \in L$, esistono per ipotesi inf {a,b} e sup{a,b} e per come sono definiti sono unici, $\wedge$ e $\vee$ sono leggi di composizioni interne binarie su L.

Ovviamente entrambe le operazioni godono della proprietà commutativa , verifichiamo che godono anche della proprietà associativa: siano $x = (a\wedge b) \wedge c$ e $y = a\wedge(b\wedge c)$quindi, per definizione di $\wedge$, $x=$inf { inf {a,b}, c} e $y=$inf {a, inf {b,c}}.

Ne segue $x\leq$ inf {a,b} e $x\leq c$, ma inf {a,b}$\leq a$ e inf {a,b}$\leq b$, quindi per la transitività della relazione $\leq$, si ha $x\leq a$ e $x\leq b$. Ora $x\leq b$ e $x\leq c$ implicano, per definizione di inf, $x\leq$ inf {b,c} che assieme ad $x\leq a$ implica $x\leq$ inf {a, inf {b,c}}=y. Analogamente si prova che $y\leq x$ e dunque, per la antisimmetria di $\leq$, si ottiene a=b. allo stesso modo si prova l'associatività di $\vee$.

Infine proviamo che le $\wedge$ e $\vee$ che abbiamo introdotto godono anche della proprietà di assorbimento, Sia $z= a\wedge(a\vee b)=$ inf{a, sup {a,b}}, per definizione di inf, abbiamo $z\leq a$.

Inoltre si ha anche $a\leq a$ (per la riflessività di $\leq$) ed $a\leq$ sup {a,b}, per definizione di sup, e quindi a è un minorante di {a, sup {a,b}}, da cui $a\leq z$ perché z è il massimo minorante. Dunque per la antisimmetria a=z. Analogamente si prova che $a\vee (a\wedge b)=a$.

Pertanto $<L, \wedge , \vee>$ è un reticolo secondo la definizione 2.

Def.2 $\rightarrow$ *Def. 1*

Se sull'insieme L sono definite due operazioni interne binari per cui valgono le proprietà commutativa associativa e di assorbimento, si hanno anche queste proprietà

- idempotenza $\forall a \in L$ $a\wedge a= a$, $a\vee a= a$

infatti , utilizzando due volte la proprietà di assorbimento si ha $a\wedge a= a\wedge(a\vee(a\wedge b))=a$ e analogamente $a\vee a= a\vee (a\wedge (a\vee b))=a$

- $a\wedge b=a$ se e solo se $a\vee b=b$

infatti se $a\wedge b=a$ si ha $a\vee b=(a\wedge b)\vee b =b$ (per le proprietà commutativa e di assorbimento), analogamente se $a\vee b=b$ si ha $a\wedge b= a\wedge(a\vee b) =a$.

Ciò posto, si consideri la relazione binaria su L definita da $a \leq b$ se e solo se $a\wedge b=a$ (quindi se e solo se $a\vee b=b$) detto ordinamento indotto su L. Verifichiamo che si tratta di una relazione d'ordine:

proprietà riflessiva: $a \leq a$ per l'idempotenza che abbiamo appena provato,

proprietà antisimmetrica: se $a \leq b$ e $b \leq a$ abbiamo $a\wedge b = a$ e $b\wedge a = b$, quindi per la proprietà commutativa a=b,

proprietà transitiva: se $a \leq b$ e $b \leq c$ abbiamo $a \wedge b = a$ e $b \wedge c = c$, quindi $a \wedge c = a \wedge (b \wedge c) = (a \wedge b) \wedge c = b \wedge c = c$ (dove si è fatto uso della proprietà associativa) e quindi $a \leq b$.
Verifichiamo poi che rispetto alla relazione d'ordine così introdotta per ogni $a,b \in L$ esistono in L $\inf\{a,b\}$ e $\sup\{a,b\}$ e si ha proprio $\inf\{a,b\} = a \wedge b$ e $\sup\{a,b\} = a \vee b$.
Per provare che $\inf\{a,b\} = a \wedge b$ dobbiamo mostrare che $a \wedge b \leq a$ e $a \wedge b \leq b$, infatti $(a \wedge b) \wedge a = a \wedge (a \wedge b) = (a \wedge a) \wedge b = a \wedge b$ e analogamente si prova $(a \wedge b) \wedge b = b$; inoltre dobbiamo provare che se $x \leq a$ e $x \leq b$, allora $x \leq a \wedge b$, infatti abbiamo $x \wedge a = x$, $x \wedge b = x$ da cui $x \wedge (a \wedge b) = (x \wedge a) \wedge b = x \wedge b = x$. Analogamente si prova (utilizzando il fatto che $a \leq b$ se e solo se $a \vee b = b$) che $\sup\{a,b\} = a \vee b$.
Possiamo quindi passare da una all'altra definizione a seconda di quello che ci è utile.

Osserviamo che la relazione d'ordine che abbiamo introdotto è *compatibile con le operazioni*, ovvero se $a \leq b$ $c \leq d$ allora $a \wedge c \leq b \wedge d$ e $a \vee c \leq b \vee d$.
Provarlo per esercizio.

Esempi:

1) Si consideri il reticolo (definito come insieme ordinato) costituito dall'insieme dei naturali N con la relazione d'ordine definita da $n \leq m$ se e solo se n divide m, poiché $\inf\{n,m\}$ = M.C.D.(n,m) e $\sup\{n,m\}$ = m.c.m.(n,m), N con le operazioni interne M.C.D. e m.c.m è un reticolo secondo la definizione 2.
2) Si consideri l'insieme Z degli interi con l'usuale relazione di $\leq$, Z è un reticolo rispetto alle operazioni $\min\{n,m\}$ e $\max\{n,m\}$.
3) Si consideri l'insieme $\wp(A)$ delle parti di un insieme A con le usuali operazioni di unione e intersezione insiemistica, allora su $\wp(A)$ viene indotta come relazione d'ordine la relazione di inclusione insiemistica.

Def. 3. Si dice *zero* di un reticolo $<L, \wedge, \vee>$ l'elemento neutro, se esiste, rispetto all'operazione $\vee$ (che è lo zero rispetto all'operazione $\wedge$ ed è il minimo rispetto alla relazione d'ordine indotta).
Si dice *uno* di un reticolo $<L, \wedge, \vee>$ l'elemento neutro, se esiste, rispetto all'operazione $\wedge$ (che è lo zero rispetto all'operazione $\vee$ ed è il massimo rispetto alla relazione d'ordine indotta).

Ovviamente un reticolo finito ha sempre zero e uno.

Def.4. Un reticolo si dice *distributivo* se e solo se valgono le proprietà distributive di un'operazione rispetto all'altra:

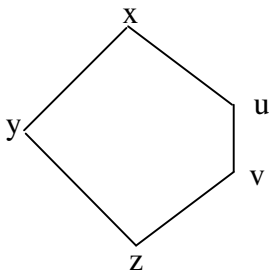
$\forall a,b,c \in L$ $\quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
$\quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

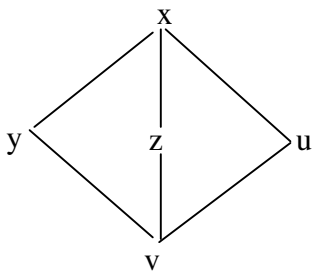
Va osservato che se vale una delle due proprietà precedenti vale anche l'altra e viceversa.

Def.5. Si dice *sottoreticolo* di un reticolo $<L, \wedge, \vee>$ un sottoinsieme H di L chiuso rispetto alle operazioni $\wedge$ e $\vee$.

Ad esempio l'insieme dei numeri pari è un sottoreticolo del reticolo < N, M.C.D., m.c.m>.
L'insieme $H = \{1,2,3,12\}$ non è un sottoreticolo di < N, M.C.D., m.c.m> (pur essendo un reticolo quando si consideri su H la relazione di divisibilità come relazione d'ordine, notate che in questo caso $\sup\{2,3\}$ è 12, non m.c.m (2,3))

Osservazione: Un reticolo è distributivo se e solo se non contiene sottoreticoli il cui diagramma di Hasse ha una delle seguenti forme:





Def. 6. Un reticolo L con 0 ed 1 si dice *complementato* se per ogni a ∈ L esiste un a'∈ L tale che a∧a'=0 e a∨a'=1. L'elemento a' (che non è necessariamente unico) si dice *complemento* di a.

Un reticolo distributivo e complementato è *unicamente complementato* (ovvero ogni elemento ammette un unico complemento).
Provarlo per esercizio.

Def. 7. Si dice *algebra di Boole* un reticolo con 0 ed 1, distributivo e complementato. Un'algebra di Boole viene spesso indicata con <L, ∧ ,∨, '> o con <L, ∧ ,∨,0,1, '> (per indicare rispettivamente che ha una operazione interna unaria, il complemento , o che ha due operazioni interne zeroarie, la scelta di 0 ed 1 , ed una operazione interna unaria, il complemento)
Osserviamo che per ogni a,b ∈ L si ha (a')'=a , 0'=1, (a∧b)'=a'∨b', (a∨b)'=a'∧b'.
Dimostrarlo per esercizio.

Es. L'insieme $\wp(A)$ con unione ed intersezione insiemistica è un'algebra di Boole. (Lo 0 è l'insieme vuoto, l'1 è l'insieme A, il complemento di un insieme B è il complemento insiemistico).

Prop.1. In un'algebra di Boole la relazione d'ordine indotta può essere anche definita ponendo a≤ b se e solo se a∧b'=0.
Infatti, se a≤ b, si ha a∧b=a, ma è per definizione di 0, 0=a∧0=a∧(b∧b'), da cui per la proprietà associativa 0=(a∧b) ∧b'= a∧b'.
Se invece a∧b'=0, da a=a∧1= a∧(b∨b') si ha per la proprietà distributiva a=(a∧b)∨(a∧b')=(a∧b)∨0 = a∧b, cioè a≤ b.

Def. 8. Si dice *atomo* di un reticolo <L, ∧ ,∨> con 0 un elemento a∈ L e diverso da 0 tale che per ogni b∈ L si abbia a∧b=0 o a∧b=a, in altre parole a è un elemento tale che 0<a e non esiste b con 0<b<a (dove con il simbolo < intendiamo la relazione binaria su L definita da a<b se e solo se a≤b e a≠b); questo viene spesso indicato dicendo che l'elemento a *copre* lo 0.

Prop. 2. In un reticolo finito per ogni b∈ L e diverso da 0 esiste almeno un atomo a tale che a≤b.
Infatti o b è un atomo e allora b≤b, o esiste un elemento b_1∈ L tale che b_1≤b e o b_1 è un atomo o esiste un elemento b_2∈ L tale che b_2≤b_1≤b e o b_2 è un atomo o esiste un elemento b_3∈ L tale che b_3≤b_2≤b_1≤b, etc…; poiché gli elementi di L sono finiti questa sequenza deve finire in un numero finito di passi, ma termina solo quando si trova un b_i∈ L tale che b_i≤…≤b_1≤b e b_i è un atomo.

Di conseguenza ogni reticolo finito <L, ∧ ,∨> , non ridotto a un solo elemento, contiene un insieme non vuoto di atomi.

Prop. 3. In un'algebra di Boole finita <L, ∧ ,∨, '>, ogni b∈ L e diverso da 0 si scrive come unione di tutti e soli gli atomi di L minori o eguali a b.
Sia b∈ L e diverso da 0, sappiamo che esiste un insieme non vuoto A_b={a∈ L|a è un atomo e a≤b}.

Sia $c= \bigcup_{a\in A_b} a$, si ha $c\leq b$ (perché $\leq$ è compatibile con l'unione). Supponiamo $c<b$ allora $c'\wedge b\neq 0$ ($c'\wedge b=0$ implicherebbe $b\leq c$ e quindi $c=b$), esiste quindi un atomo $a\leq c'\wedge b$, da cui $a\leq c$ c' e $a\leq b$ cioè $a\in A_b$, ma da quest'ultima si ha $a\leq c$ e quindi $a\leq c\wedge c'=0$, assurdo. Dunque $c=b$.

Prop. 4. Sia $<L, \wedge, \vee, '>$ un'algebra di Boole finita , se $b=a_1\vee a_2\vee\ldots\vee a_n$ ed a è un atomo L minore o eguale a b, allora esiste un i, con $1\leq i \leq n$, tale che $a= a_i$.
Essendo $a\leq b$ si ha $a=a\wedge b$ e quindi $a=a\wedge(a_1\vee a_2\vee\ldots\vee a_n)= (a\wedge a_1)\vee (a\wedge a_2)\vee\ldots\vee (a\wedge a_n)$, per la distributività. Ora per ogni j, essendo a un atomo, si ha $a\wedge a_j=0$ oppure $a\wedge a_j=a$; se fosse sempre $a\wedge a_j=0$ si avrebbe l'assurdo $a=0$, dunque esiste un i tale che $a\wedge a_i=a$, ma essendo anche a_i un atomo si deduce $a= a_i$.

Si può a questo punto osservare che ogni elemento b di un'algebra di Boole finita è completamente individuato dall'insieme A_b.

Siamo quindi in grado di provare il
Teor.1. Ogni algebra di Boole finita $<L, \wedge, \vee, '>$ è isomorfa all'algebra di Boole $<\wp(A),\cap,\cup, '>$, dove A è l'insieme degli atomi di L, $\cap$, $\cup$, ' sono unione, intersezione e complemento insiemistici.
Consideriamo la corrispondenza $f: L\rightarrow\wp(A)$ definita da $f(b)= A_b$. Le proposizioni 3 e 4 garantiscono che f è biunivoca.
E' facile provare che f conserva l'operazione di unione. Infatti per ogni b,c in L, $A_{b\vee c}\supseteq A_b \cup A_c$; inoltre se $a \in A_{b\vee c}$, abbiamo $a= a\wedge(b\vee c)=(a\wedge b)\vee(a\wedge c)$, da cui tenuto conto della definizione di atomo, si ricava $a=a\wedge b$ o $a=a\wedge c$, cioè $a \in A_b$ o $a \in A_c$, da cui $A_{b\vee c}\subseteq A_b \cup A_c$.
Proviamo ora che f conserva l'operazione di intersezione. Per ogni b,c in L, $A_{b\wedge c}\subseteq A_b \cap A_c$; inoltre se $a \in A_b \cap A_c$, abbiamo $a=a\wedge b$ e $a=a\wedge c$ da cui $a\wedge(b\vee c)=(a\wedge b)\vee(a\wedge c)=a$, da cui $A_{b\wedge c}\supseteq A_b \cap A_c$.
Banalmente si ha che $f(0)=\varnothing$ e $f(1)=A$.
Consideriamo ora $f(a')$. Poiché f conserva l'intersezione, si ha $f(a\wedge a')= A_a\cap A_{a'}$, ma $f(a\wedge a')=f(0)= \varnothing$, dunque $A_a\cap A_{a'}=\varnothing$; analogamente si prova che $A_a\cup A_{a'}=S$; dunque $A_{a'}= A_a$', quindi $f(a')=f(a)$ '.
Ne segue che f è un isomorfismo di $<L, \wedge, \vee, '>$ su $<\wp(A),\cap,\cup, '>$.

Corollario. 1. Un'algebra di Boole finita $<L, \wedge, \vee, '>$ ha ordine 2^n per qualche intero naturale n.
Corollario. 2. Per ogni intero naturale n esiste un'algebra di Boole $<L, \wedge, \vee, '>$ di ordine 2^n .