Estructuras algebraicas

Una **estructura algebraica** es un conjunto no vacío junto con operaciones. Las operaciones pueden ser, por ejemplo, binarias (cuando la operación es sobre dos elementos del conjunto) o unarias (cuando la operación es sobre un elemento del conjunto).

Un **grupo** $(A,*)$ es una estructura algebraica en la cual $*$ es una operación binaria y se cumple que:

- A es **cerrado** con la operación $*$, es decir, que para todo $a, b \in A$, $a * b \in A$.
- La operación $*$ es **asociativa** en A, es decir, para todo $a, b, c \in A$, $(a * b) * c = a * (b * c)$.
- Existe un **neutro** $n \in A$, es decir, un elemento tal que $a * n = n * a = a$
- Para todo elemento $a \in A$, existe un **opuesto** $a' \in A$ tal que $a * a' = a' * a = n$

Un **grupo abeliano/conmutativo** $(A,*)$ es una estructura algebraica en la cual $*$ es una operación binaria y se cumple que:

- A es **cerrado** con la operación $*$, es decir, que para todo $a, b \in A$, $a * b \in A$.
- La operación $*$ es **asociativa** en A, es decir, para todo $a, b, c \in A$, $(a * b) * c = a * (b * c)$.
- Existe un **neutro** $n \in A$, es decir, un elemento tal que $a * n = n * a = a$
- Para todo elemento $a \in A$, existe un **opuesto** $a' \in A$ tal que $a * a' = a' * a = n$
- La operación $*$ es **conmutativa** en A, es decir, para todo $a, b \in A$, $a * b = b * a$

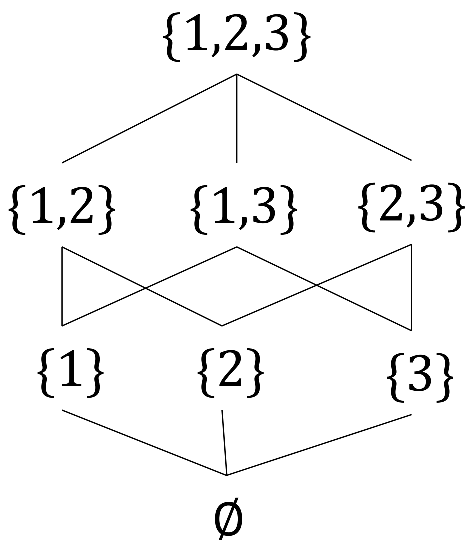
Un anillo $(A,+,\cdot)$ es una estructura algebraica en la cual $+$ y $\cdot$ son operaciones binarias que cumplen que:

- $(A,+)$ es un grupo conmutativo/abeliano.
- Para todo $a,b \in A$, $a \cdot b \in A$
- Para todo $a,b,c \in A$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Para todo $a,b,c \in A$, $a \cdot (b+c) = a \cdot b + a \cdot c$ y $(a+b) \cdot c = a \cdot c + b \cdot c$

Si A es un conjunto, definimos el **conjunto de partes de A,** que escribimos $P(A)$, como $P(A) = \{X : X \subseteq A\}$, es decir el conjunto cuyos elementos son los subconjuntos de A.

Si $A = \{1,2,3\}$, entonces $P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

Diagrama de Hasse



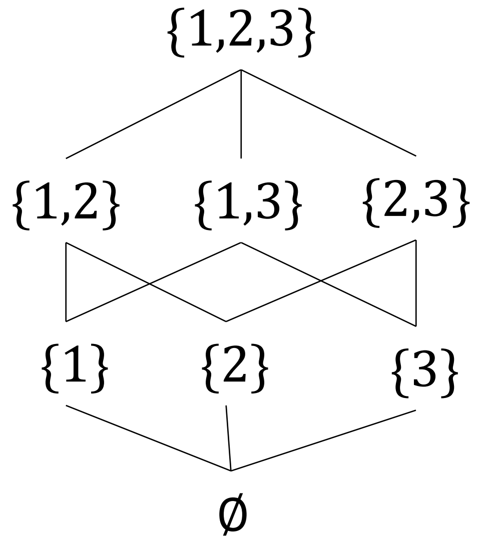
Álgebras de Boole

Un **álgebra de Boole** es una estructura algebraica sobre un conjunto B que tiene **primer** y **último elemento** (que llamaremos 0 y 1), junto con dos operaciones binarias: ∨ (**supremo**) y ∧ (**ínfimo**) y una operación unaria ‘ (**complemento**) que cumplen las siguientes propiedades para $x, y, z \in B$:

- ∨ es conmutativa: $x \vee y = y \vee x$
- ∧ es conmutativa: $x \wedge y = y \wedge x$
- ∨ es distributiva con respecto a ∧: $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$
- ∧ es distributiva con respecto a ∨: $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
- 0 es neutro para ∨: $x \vee 0 = x$
- 1 es neutro para ∧: $x \wedge 1 = x$
- $x \vee x' = 1$
- $x \wedge x' = 0$

En forma abreviada se suele escribir el álgebra de Boole con el conjunto, operaciones, primer y último elemento, como: $\mathcal{B} = (B, \vee, \wedge, ', 0, 1)$

- $\vee$ es conmutativa: $x \vee y = y \vee x$
- $\wedge$ es conmutativa: $x \wedge y = y \wedge x$
- $\vee$ es distributiva con respecto a $\wedge$: $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$
- $\wedge$ es distributiva con respecto a $\vee$: $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
- 0 es neutro para $\vee$: $x \vee 0 = x$
- 1 es neutro para $\wedge$: $x \wedge 1 = x$
- $x \vee x' = 1$
- $x \wedge x' = 0$



¿Cuál sería en este caso el primer elemento?

¿Y el último?

¿Cuál es la operación ínfimo?

¿Cuál es la operación supremo?

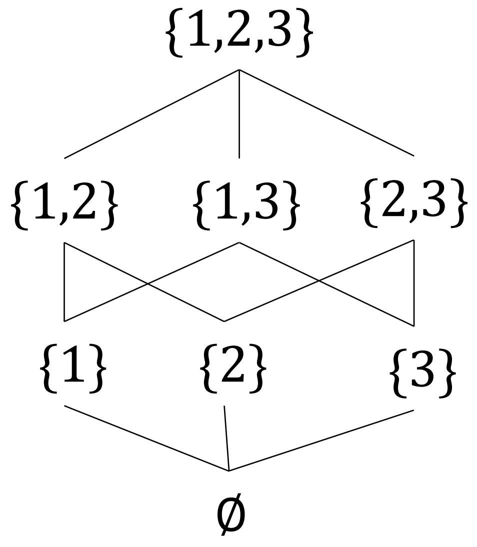
¿Cuál es la operación complemento?

Si cambiamos $\vee$ por $+$ y $\wedge$ por $\cdot$ Obtenemos las siguientes condiciones para un álgebra de Boole $\mathcal{B} = (B, +, \cdot, ', 0, 1)$:

- $+$ es conmutativa: $x + y = y + x$
- $\cdot$ es conmutativa: $x \cdot y = y \cdot x$
- $+$ es distributiva con respecto a $\cdot$: $x + (y \cdot z) = (x + y) \cdot (x + z)$
- $\cdot$ es distributiva con respecto a $+$: $x \cdot (y + z) = (x \cdot y) + (x + z)$
- 0 es neutro para $+$: $x + 0 = x$
- 1 es neutro para $\cdot$: $x \cdot 1 = x$
- $x + x' = 1$
- $x \cdot x' = 0$

Esta es la notación que usaremos en general para las álgebras de Boole. Y, cuando tengamos $x \cdot y$ en muchos casos escribiremos directamente xy.

Toda álgebra de Boole finita admite una representación mediante un **diagrama de Hasse**, donde se ubica el 0 debajo y el 1 encima de todos los elementos. Luego, se ubican siguiendo el orden dado por las operaciones, donde a estará debajo de b si $a \wedge b = a \cdot b = a$



En un diagrama de Hasse los elementos que están por encima del 0 se llaman **átomos**.

Si a es un átomo, entonces para todo $b \in B$ se tiene que $ab = 0$ o $ab = a$.

Si tenemos un álgebra de Boole $\mathcal{B} = (B, +, \cdot, ', 0, 1)$ y $a \in B$, entonces ¿hay un único complemento a' para a?

Supongamos que a' y b son los dos complementos de a, es decir, cumplen que

$$aa' = 0 \quad \text{y} \quad a + a' = 1$$

$$ab = 0 \quad \text{y} \quad a + b = 1$$

Como tenemos que 0 es neutro para +, tenemos que

$$b = b + 0$$

Pero, además, $0 = aa'$, por lo que la igualdad anterior la podemos escribir como

$$b = b + aa'$$

Ahora, como sabemos que en un álgebra de Boole $+$ distribuye en $\cdot$, podemos reescribir la igualdad anterior como sigue::

$$b = (b + a)(b + a')$$

Al ser conmutativa la operación $+$, esto equivale a:

$$b = \underbrace{(a + b)}_{=1\ (por\ hip)} (b + a')$$

$$b = b + a'$$

Por otro lado, y razonando de forma análoga, tenemos que:

$$a' = a' + 0 = a' + ab = (a' + a)(a' + b) = \underbrace{(a + a')}_{=1}(a' + b) = a' + b = b + a'$$

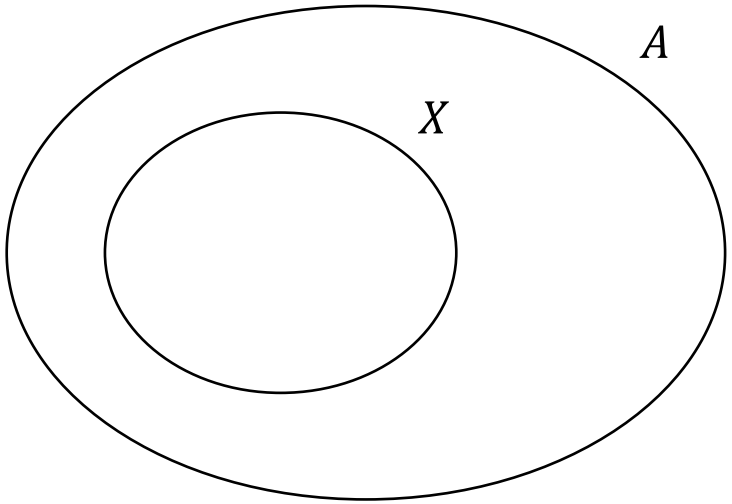
Por lo tanto, probamos que $b = a'$ y queda probado que el complemento es único.

Álgebra de Boole del Conjunto de Partes

Si tenemos un conjunto A, entonces el conjunto $P(A)$ con las operaciones binarias de unión e intersección ∪ y ∩, la operación unaria de complemento y los conjuntos ∅ y A forman un álgebra de Boole $(P(A), \cup, \cap, {}^{C}, \emptyset, A)$.

Si $X, Y, Z \in P(A)$, tenemos que:

- ∪ es conmutativa: $X \cup Y = Y \cup X$
- ∩ es conmutativa: $X \cap Y = Y \cap X$
- ∪ es distributiva con respecto a ∩: $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$
- ∩ es distributiva con respecto a ∪: $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
- ∅ es neutro para ∪: $X \cup \emptyset = X$
- A es neutro para ∩: $X \cap A = X$
- $X \cup X^C = A$
- $X \cap X^C = \emptyset$



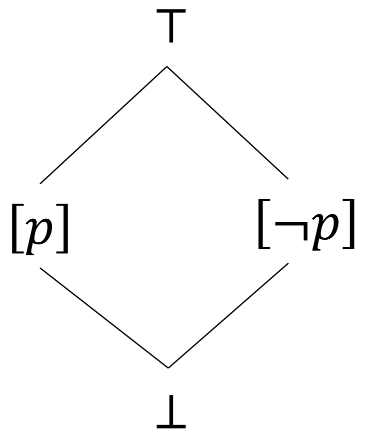
Álgebra de Boole del Cálculo Proposicional

Vamos a escribir $[p]$ para referirnos al conjunto de todas las proposiciones que son equivalentes a la proposición p. Por ejemplo $p \wedge p \in [p]$ y $p \vee p \in [p]$, pero $\neg p \notin [p]$.

Tenemos entonces que, por ejemplo, $[p \to q] = [\neg p \vee q]$.

Si escribimos, además $\top$ para referirnos a las proposiciones que son tautologías, donde, por ejemplo, $[p \vee \neg p] = \top$ y $\bot$ para referirnos a las proposiciones que son una contradicción, es decir, que $[p \wedge \neg p] = \bot$, entonces podemos formar el álgebra de Boole del cálculo proposicional: $\Phi = (\{[p], [\neg p], \top, \bot\}, \vee, \wedge, \neg, \bot, \top)$.

- $\vee$ es conmutativa: $[p] \vee [q] = [q] \vee [p]$
- $\wedge$ es conmutativa: $[p] \wedge [q] = [q] \wedge [p]$
- $\vee$ es distributiva con respecto a $\wedge$: $[p] \vee ([q] \wedge [r]) = ([p] \vee [q]) \wedge ([p] \vee [r])$
- $\wedge$ es distributiva con respecto a $\vee$: $[p] \wedge ([q] \vee [r]) = ([p] \wedge [q]) \vee ([p] \wedge [r])$
- $\bot$ es neutro para $\vee$: $[p] \vee \bot = [p]$
- $\top$ es neutro para $\wedge$: $[p] \wedge \top = [p]$
- $[p] \vee [\neg p] = \top$
- $[p] \wedge [\neg p] = \bot$



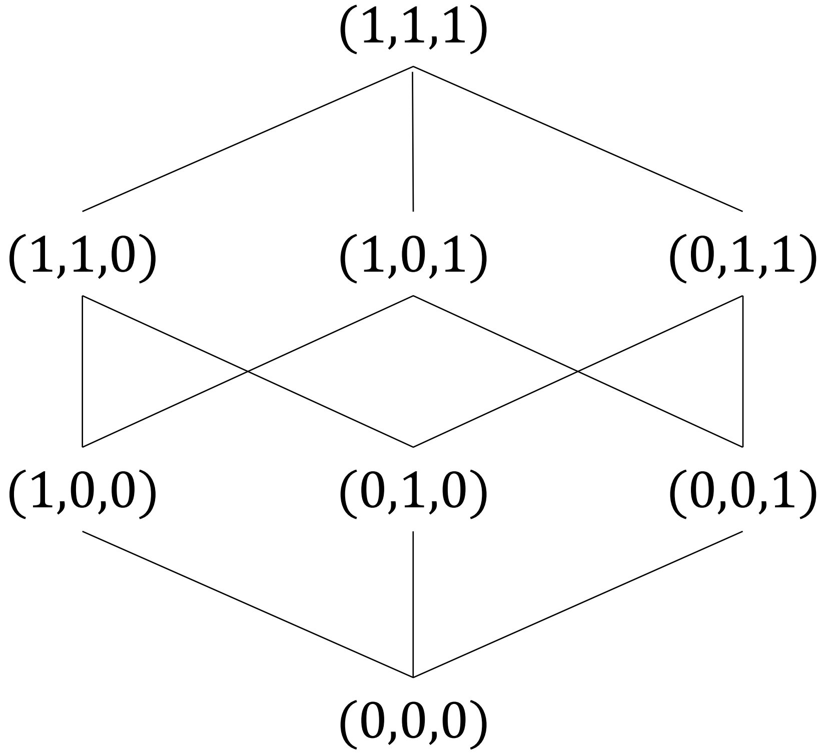
Si tomamos el conjunto $\{0,1\}^3 = \{(x_1, x_2, x_3) : x_i \in \{0,1\}\}$ junto con las operaciones

$$(x_1, x_2, x_3) \vee (y_1, y_2, y_3) = (x_1 \vee y_1, x_2 \vee y_2, x_3 \vee y_3)$$

$$(x_1, x_2, x_3) \wedge (y_1, y_2, y_3) = (x_1 \wedge y_1, x_2 \wedge y_2, x_3 \wedge y_3)$$

$$(x_1, x_2, x_3)' = (x_1', x_2', x_3')$$

donde el primer elemento es $(0,0,0)$ y el último elemento $(1,1,1)$, tenemos un álgebra de Boole.



Principio de dualidad

Si tenemos un álgebra de Boole $\mathcal{B} = (B, +, \cdot, ', 0, 1)$, podemos obtener su álgebra **dual** si intercambiamos las operaciones $+$ y $\cdot$ y los elementos 0 y 1. Las proposiciones correspondientes se llaman duales y serán verdaderas si y solo si su dual lo es.

- $+$ es conmutativa: $x + y = y + x$
- $\cdot$ es conmutativa: $x \cdot y = y \cdot x$
- $+$ es distributiva con respecto a $\cdot$: $x + (y \cdot z) = (x + y) \cdot (x + z)$
- $\cdot$ es distributiva con respecto a $+$: $x \cdot (y + z) = (x \cdot y) + (x + z)$
- 0 es neutro para $+$: $x + 0 = x$
- 1 es neutro para $\cdot$: $x \cdot 1 = x$
- $x + x' = 1$
- $x \cdot x' = 0$

Teorema 1 – Leyes de idempotencia

Si $\mathcal{B} = (B, +, \cdot, ', 0, 1)$ es un álgebra de Boole entonces para cualquier $x \in B$ se cumple que $x + x = x$ y $x \cdot x = x$

Demostración

Como 0 es el neutro de $+$ tenemos que

$$x \cdot x = x \cdot x + 0$$

Además, como $x \cdot x' = 0$, podemos reemplazar en la igualdad anterior y obtener:

$$x \cdot x = x \cdot x + x \cdot x'$$

Por otro lado, como $\cdot$ es distributivo con respecto a $+$ obtenemos:

$$x \cdot x = x \cdot (x + x')$$

Y ahora, como $x + x' = 1$, tenemos:

$$x \cdot x = x \cdot 1$$

Como 1 es el neutro de $\cdot$ tenemos que

$$x \cdot x = x$$

Como 1 es el neutro de $\cdot$ tenemos que

$$x + x = (x + x) \cdot 1$$

Además, como $x + x' = 1$, podemos reemplazar en la igualdad anterior y obtener:

$$x + x = (x + x) \cdot (x + x')$$

Por otro lado, como $+$ es distributiva con respecto a $\cdot$ obtenemos:

$$x + x = x + (x \cdot x')$$

Y ahora, como $x \cdot x' = 0$, tenemos:

$$x + x = x + 0$$

Como 0 es el neutro de $+$ tenemos que

$$x + x = x$$

Teorema 2 – Leyes de acotación

Si $\mathcal{B} = (B, +, \cdot, ', 0, 1)$ es un álgebra de Boole entonces para cualquier $x \in B$ se cumple que $x + 1 = 1$ y $x \cdot 0 = 0$

Demostración

Como $x \cdot x' = 0$, tenemos que:

$$x \cdot 0 = x \cdot (x \cdot x')$$

Como la operación $\cdot$ es asociativa vale que:

$$x \cdot 0 = (x \cdot x) \cdot x'$$

Por el Teorema 1 tenemos que $x \cdot x = x$

$$x \cdot 0 = x \cdot x'$$

Como $x \cdot x' = 0$,

$$x \cdot 0 = 0$$

Como $x + x' = 1$, tenemos que:

$$x + 1 = x + (x + x')$$

Como la operación $+$ es asociativa vale que:

$$x + 1 = (x + x) + x'$$

Por el Teorema 1 tenemos que $x + x = x$

$$x + 1 = x + x'$$

Como $x + x' = 1$,

$$x + 1 = 1$$

Teorema 3 – Leyes de absorción

Si $\mathcal{B} = (B, +, \cdot, ', 0, 1)$ es un álgebra de Boole entonces para cualquier par de elementos $x, y \in B$ se cumple que $x + (x \cdot y) = x$ y $x \cdot (x + y) = x$

Demostración

Como 1 es el neutro de $\cdot$ tenemos que

$$x + (x \cdot y) = x \cdot 1 + (x \cdot y)$$

Por otro lado, como $\cdot$ es distributivo con respecto a $+$ obtenemos:

$$x + (x \cdot y) = x \cdot (1 + y)$$

Por el Teorema 2 tenemos que $1 + y = 1$, por lo que la igualdad nos queda

$$x + (x \cdot y) = x \cdot 1$$

Como 1 es el neutro de $\cdot$ tenemos que

$$x + (x \cdot y) = x$$

Como 0 es el neutro de $+$ tenemos que

$$x \cdot (x + y) = (x + 0) \cdot (x + y)$$

Por otro lado, como $+$ es distributiva con respecto a $\cdot$ obtenemos:

$$x \cdot (x + y) = x + (0 \cdot y)$$

Por el Teorema 2 tenemos que $0 \cdot y = 0$, por lo que la igualdad nos queda

$$x \cdot (x + y) = x + 0$$

Como 0 es el neutro de $+$ tenemos que

$$x \cdot (x + y) = x$$