Retículos y álgebras de Boole

Manuel Ojeda Aciego

Universidad de Málaga
Dpto. de Matemática Aplicada

Curso 2015-2016

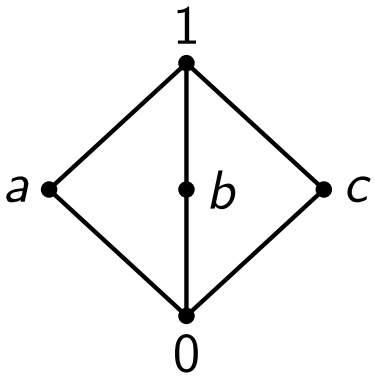
Retículos ordenados

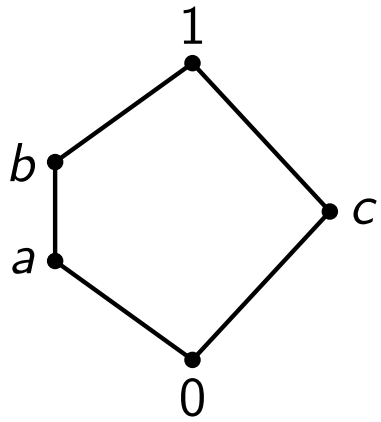
Definición

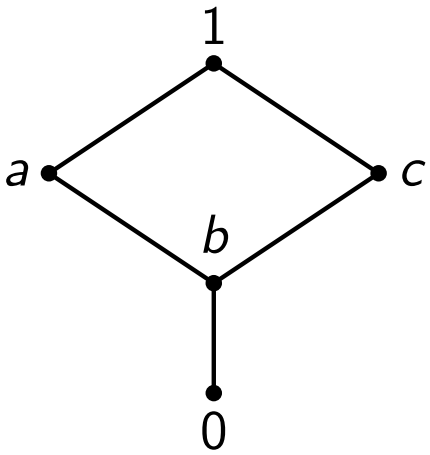
Un conjunto parcialmente ordenado $(\mathcal{L}, \preceq)$ *es un* **retículo** *si cada par de elementos* $a, b \in \mathcal{L}$ *tiene supremo e ínfimo, esto es, existen* $\sup\{a, b\}$ *e* $\inf\{a, b\}$. *El retículo se dice* **completo** *si todo subconjunto* X *tiene supremo e ínfimo.*

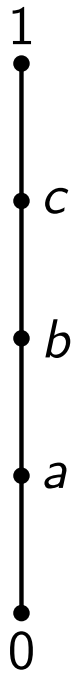
- Ciertos retículos son importantes en teorías abstractas de computación, desarrolladas a partir de la noción de *aproximación*; también pueden usarse para representar el comportamiento de programas.
- Los retículos son especialmente útiles en áreas como optimización combinatoria y criptografía (tanto para romper sistemas existentes como para desarrollar nuevos cifrados).
- Cierto tipo de retículos se usa como generalización de las *álgebras de Boole* en lógicas no clásicas.

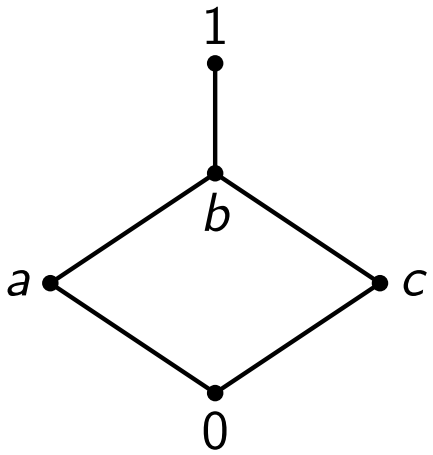
Algunos ejemplos de retículos ordenados I





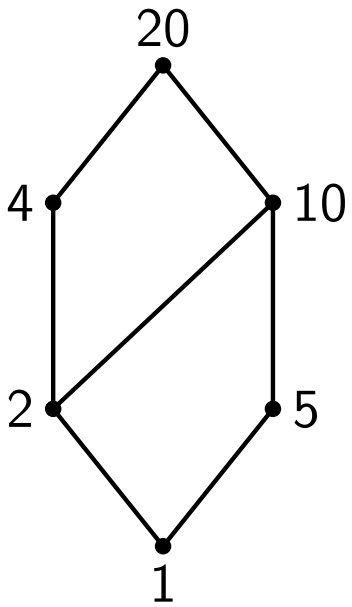




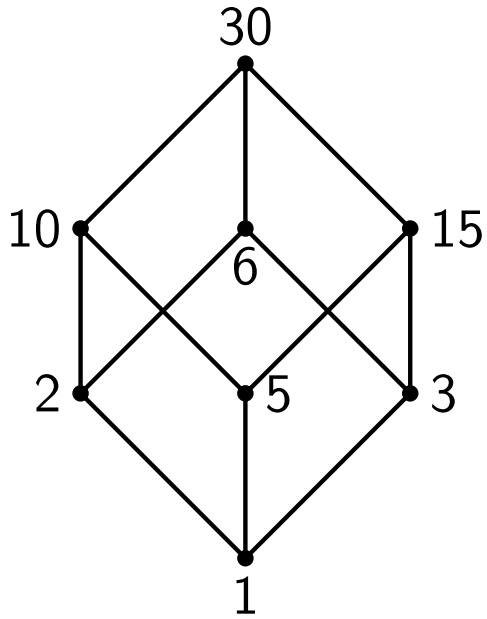


Algunos ejemplos de retículos ordenados II

- $(D_n, |)$, en particular para $n = 20$ y $n = 30$:



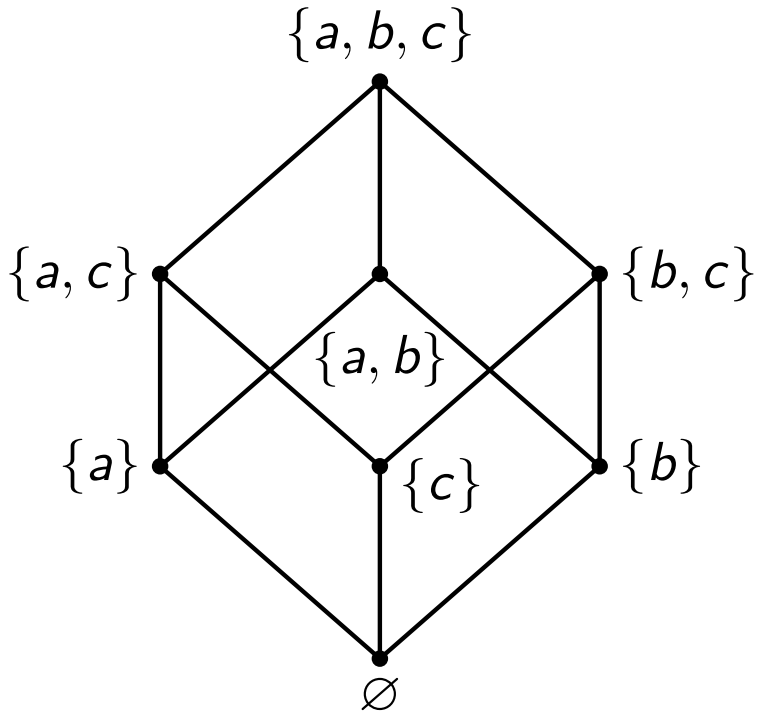
$(D_{20}, |)$



$(D_{30}, |)$

Algunos ejemplos de retículos ordenados III

- $(\mathcal{P}(S), \subseteq)$, en particular para $S = \{a, b, c\}$



Retículos ordenados

Supremo e ínfimo como operaciones algebraicas

Usando la definición de retículo ordenado, en todo retículo $(\mathcal{L}, \preceq)$ se pueden definir dos operaciones binarias $\sqcup$ y $\sqcap$ de la siguiente manera:

$$\begin{array}{rccl} \sqcup: & \mathcal{L} \times \mathcal{L} & \longrightarrow & \mathcal{L} \\ & (a, b) & \longmapsto & \sup\{a, b\} = a \sqcup b \end{array}$$

$$\begin{array}{rccl} \sqcap: & \mathcal{L} \times \mathcal{L} & \longrightarrow & \mathcal{L} \\ & (a, b) & \longmapsto & \text{ínf}\{a, b\} = a \sqcap b \end{array}$$

Retículos ordenados

Supremo e ínfimo como operaciones algebraicas

Ejemplos

1. En el retículo ordenado $(\mathcal{P}(S), \subseteq)$ se definen las operaciones:

$$\forall A, B \in \mathcal{P}(S),\ A \sqcup B = \sup\{A, B\} = A \cup B \in \mathcal{P}(S),$$

$$A \sqcap B = \inf\{A, B\} = A \cap B \in \mathcal{P}(S)$$

2. En el retículo ordenado $(\mathbb{Z}^+, |)$ se definen las operaciones:

$$\forall a, b \in \mathbb{Z}^+,\ a \sqcup b = \sup\{a, b\} = m.c.m.(a, b) \in \mathbb{Z}^+,$$

$$a \sqcap b = \inf\{a, b\} = m.c.d.(a, b) \in \mathbb{Z}^+$$

Retículos ordenados

Supremo e ínfimo como operaciones algebraicas

Teorema

Sea el retículo $(\mathcal{L}, \preceq)$ *y sea* $(\mathcal{L}, \sqcup, \sqcap)$ *el sistema algebraico que determina. En* $(\mathcal{L}, \sqcup, \sqcap)$ *se verifican las siguientes propiedades:*

1. **Conmutativa** : $a \sqcup b = b \sqcup a$ $\qquad a \sqcap b = b \sqcap a$
2. **Asociativa** : $a \sqcup (b \sqcup c) = (a \sqcup b) \sqcup c$ $\qquad a \sqcap (b \sqcap c) = (a \sqcap b) \sqcap c$
3. **Absorción** : $a \sqcup (a \sqcap b) = a$ $\qquad a \sqcap (a \sqcup b) = a$

Estas propiedades se usan para dar una definición axiomática de **retículo algebraico**.

Retículos algebraicos $(\mathcal{L}, \sqcup, \sqcap)$

Definición

Sean $\sqcup$ y $\sqcap$ dos operaciones binarias definidas en un conjunto $\mathcal{L}$. Se dice que $(\mathcal{L}, \sqcup, \sqcap)$ es un **retículo algebraico** *si para todo $a, b, c \in \mathcal{L}$ se verifican:*

1. Conmutativa:	$a \sqcup b$	$=$	$b \sqcup a$	$a \sqcap b$	$=$	$b \sqcap a$
2. Asociativa:	$a \sqcup (b \sqcup c)$	$=$	$(a \sqcup b) \sqcup c$	$a \sqcap (b \sqcap c)$	$=$	$(a \sqcap b) \sqcap c$
3. Absorción:	$a \sqcup (a \sqcap b)$	$=$	a	$a \sqcap (a \sqcup b)$	$=$	a

Ejemplo

$(\mathcal{P}(S), \cup, \cap)$ es un retículo algebraico, pues verifica:

$A \cup B$	$=$	$B \cup A$	$A \cap B$	$=$	$B \cap A$
$A \cup (B \cup C)$	$=$	$(A \cup B) \cup C$	$A \cap (B \cap C)$	$=$	$(A \cap B) \cap C$
$A \cup (A \cap B)$	$=$	A	$A \cap (A \cup B)$	$=$	A

Principio de Dualidad

Teorema

Dado un conjunto parcialmente ordenado $(A, \preceq)$, para cada $a, b \in A$ se define la relación $a \succeq b$ si y solo si $b \preceq a$. Obviamente, se verifica:

1. $(A, \succeq)$ *también es un conjunto parcialmente ordenado.*
2. *Si* $(A, \preceq)$ *es un retículo, entonces* $(A, \succeq)$ *también lo es.*

Los conjuntos $(A, \preceq)$ y $(A, \succeq)$ están muy relacionados, concretamente:

- la operación $\sqcup$ de $(A, \preceq)$ coincide con la operación $\sqcap$ de $(A, \succeq)$ y
- la operación $\sqcap$ de $(A, \preceq)$ coincide con la operación $\sqcup$ de $(A, \succeq)$.

Principio de Dualidad

Si un enunciado se verifica para un retículo, entonces también se verifica el que resulta al reemplazar la relación $\preceq$ por la relación $\succeq$, la operación $\sqcup$ por la operación $\sqcap$ y la operación $\sqcap$ por la operación $\sqcup$.

Retículos algebraicos $(\mathcal{L}, \sqcup, \sqcap)$

Teorema

Sea $(\mathcal{L}, \sqcup, \sqcap)$ *un retículo algebraico. Se verifican las propiedades:*

4. Idempotencia: $a \sqcup a = a$, $\quad a \sqcap a = a$, *para todo* $a \in \mathcal{L}$

5. $a \sqcup b = b \iff a \sqcap b = a$, *para todo* $a, b \in \mathcal{L}$

- Según hemos visto, a partir de un **retículo ordenado** se puede llegar a un **retículo algebraico**.
- A continuación, se establece que a partir de un **retículo algebraico** podemos obtener un **retículo ordenado**.

Retículo algebraico $\Longrightarrow$ Retículo ordenado

Teorema

Dado el retículo algebraico $(\mathcal{L}, \sqcup, \sqcap)$, *se define una relación* $\ll$ *en* $\mathcal{L}$ *de la siguiente manera:*

$$a \ll b \iff a \sqcup b = b$$

Entonces $(\mathcal{L}, \ll)$ *es un retículo ordenado en el que para todo* $a, b \in \mathcal{L}$, *se verifica que* $\sup\{a, b\} = a \sqcup b$ *e* $\text{ínf}\{a, b\} = a \sqcap b$.

Subretículos

Definición

Sea $(\mathcal{L}, \sqcup, \sqcap)$ *un retículo y sea* $\mathcal{M}$ *un subconjunto no vacío de* $\mathcal{L}$.
Se dice que $\mathcal{M}$ *es un* **subretículo** *de* $\mathcal{L}$ *si para todo* $x, y \in \mathcal{M}$,

$$x \sqcup y \in \mathcal{M}, \quad x \sqcap y \in \mathcal{M}$$

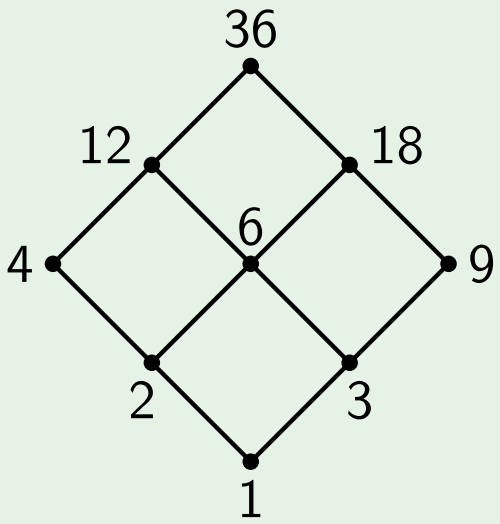
Es decir, $\mathcal{M}$ es **subretículo** de $\mathcal{L}$ si tiene estructura de retículo con respecto a la restricción de las operaciones $\sqcup$ y $\sqcap$ de $\mathcal{L}$ sobre $\mathcal{M}$.

Subretículos

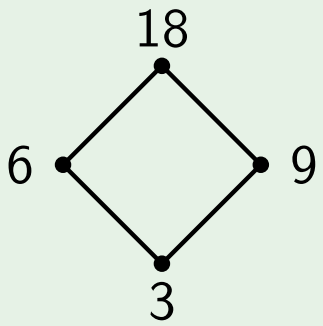
Ejemplos de subretículos

Ejemplos

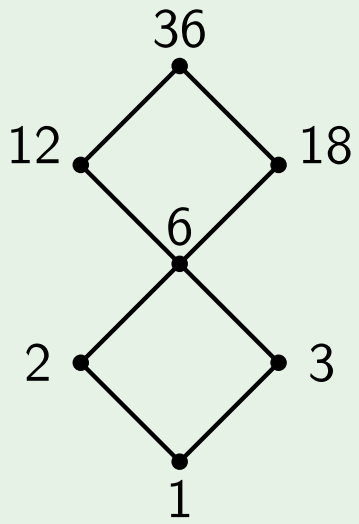
Los subconjuntos parcialmente ordenados $\mathcal{M}_1$ y $\mathcal{M}_2$ son subretículos de D_{36}.



D_{36}



$\mathcal{M}_1$

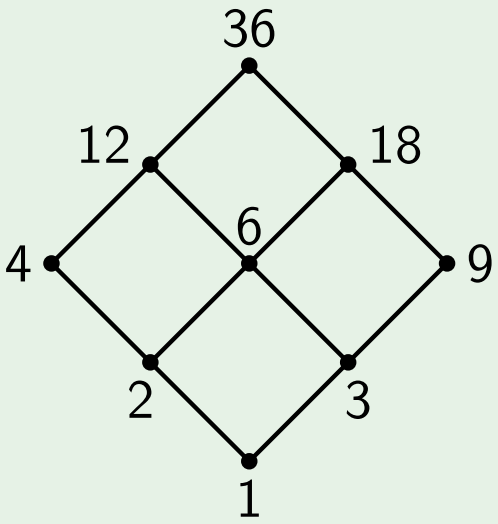


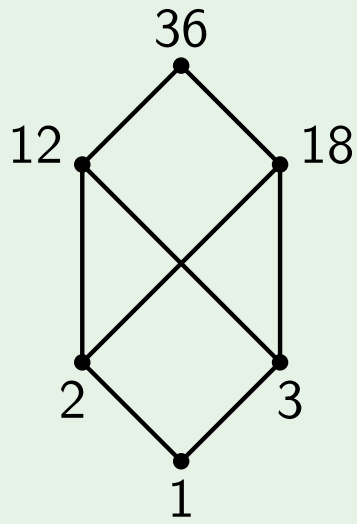
$\mathcal{M}_2$

Subretículos

Contraejemplos de subretículos

Ejemplo



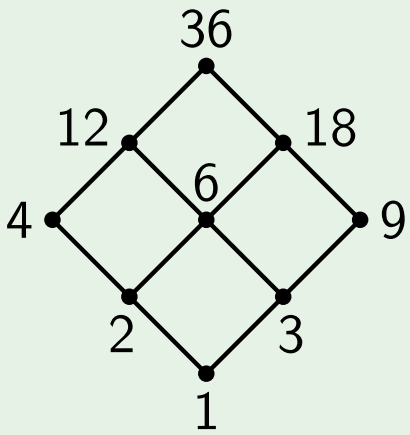


- El subconjunto de la derecha **no** tiene estructura de retículo, puesto que no existe $\sup\{2,3\}$. Por lo tanto, no es un subretículo de D_{36}.

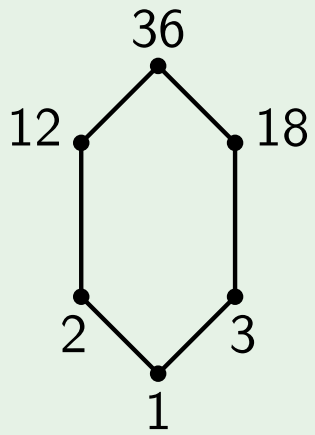
Subretículos

Contraejemplos de subretículo

Ejemplo



D_{36}



$\mathcal{M}_4$

- Aunque $\mathcal{M}_4$ **no** es subretículo de D_{36}, se pueden definir operaciones $\sqcup'$ y $\sqcap'$ que le dan estructura de retículo.

☛ Un subconjunto parcialmente ordenado que sea retículo, puede no ser subretículo.

Retículo producto

Teorema

Sean $(\mathcal{L}_1, \preceq_1)$ y $(\mathcal{L}_2, \preceq_2)$ retículos. Entonces $\mathcal{L}_1 \times \mathcal{L}_2$ es un retículo con la relación de orden producto $\preceq$ y las operaciones $\sqcup$ y $\sqcap$ definidas mediante

$$(x_1, x_2) \preceq (y_1, y_2) \iff x_1 \preceq_1 y_1 \quad \wedge \quad x_2 \preceq_2 y_2$$

$$(x_1, x_2) \sqcup (y_1, y_2) = (x_1 \sqcup_1 y_1,\ x_2 \sqcup_2 y_2)$$

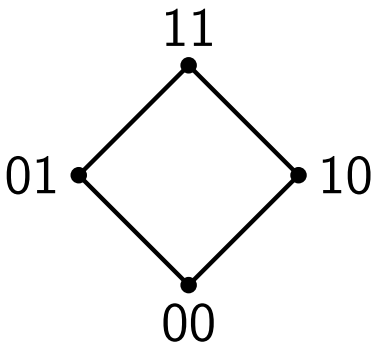
$$(x_1, x_2) \sqcap (y_1, y_2) = (x_1 \sqcap_1 y_1,\ x_2 \sqcap_2 y_2)$$

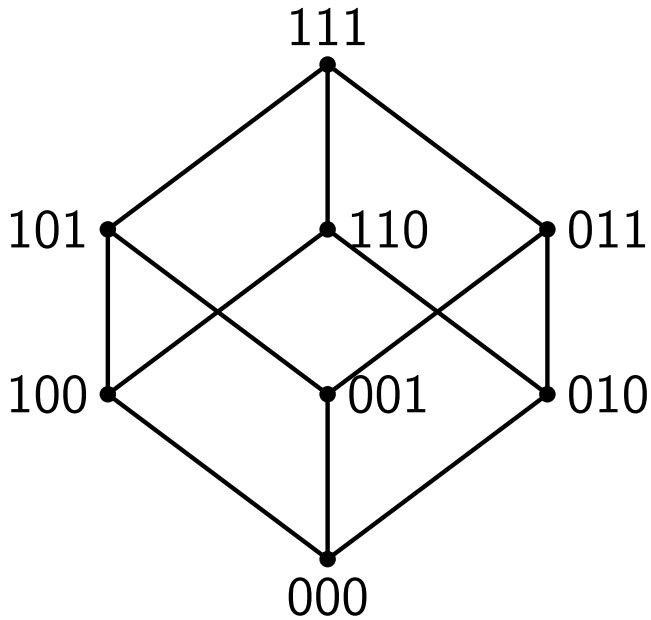
Al retículo $\mathcal{L}_1 \times \mathcal{L}_2$ se le llama **retículo producto**.

Retículo producto

Ejemplos

$\mathcal{L}_1 = \mathbb{B}$, $\mathcal{L}_2 = \mathbb{B}^2$





$\mathcal{L}_1$ $\mathcal{L}_2$ $\mathcal{L}_1 \times \mathcal{L}_2$

Homomorfismos e isomorfismos de retículos

Definición

Sean los retículos $(\mathcal{L}_1, \sqcup_1, \sqcap_1)$ *y* $(\mathcal{L}_2, \sqcup_2, \sqcap_2)$ *y sea* $f : \mathcal{L}_1 \to \mathcal{L}_2$.

Se dice que f *es un*

1. $\sqcup$-**homomorfismo**, *si* $x \sqcup_1 y = z$ *implica que* $f(x) \sqcup_2 f(y) = f(z)$
2. $\sqcap$-**homomorfismo**, *si* $x \sqcap_1 y = z$ *implica que* $f(x) \sqcap_2 f(y) = f(z)$
3. **homomorfismo de orden**, *si* $x \leq_1 y$ *implica que* $f(x) \leq_2 f(y)$

Se dice que f *es un* **homomorfismo** *de retículos si* f *es* $\sqcup$*-homomorfismo y* $\sqcap$*-homomorfismo.*

Los homomorfismos de retículos si son inyectivos, sobreyectivos o biyectivos se llaman **monomorfismos**, **epimorfismos** o **isomorfismos** respectivamente.

Homomorfismos e isomorfismos de retículos

Teorema

Si $f : \mathcal{L}_1 \to \mathcal{L}_2$ es un $\sqcup$-homomorfismo o bien un $\sqcap$-homomorfismo, entonces es un homomorfismo de orden.

El recíproco no es cierto. No toda función entre retículos que conserva el orden, conserva también las operaciones $\sqcup$ y $\sqcap$.

Teorema

Sean $(\mathcal{L}_1, \leq_1)$ y $(\mathcal{L}_2, \leq_2)$ retículos. La función $f : \mathcal{L}_1 \to \mathcal{L}_2$ es un isomorfismo de retículos si y sólo si es biyectiva y $a \leq_1 b \iff f(a) \leq_2 f(b)$ para todo $a, b \in \mathcal{L}_1$.

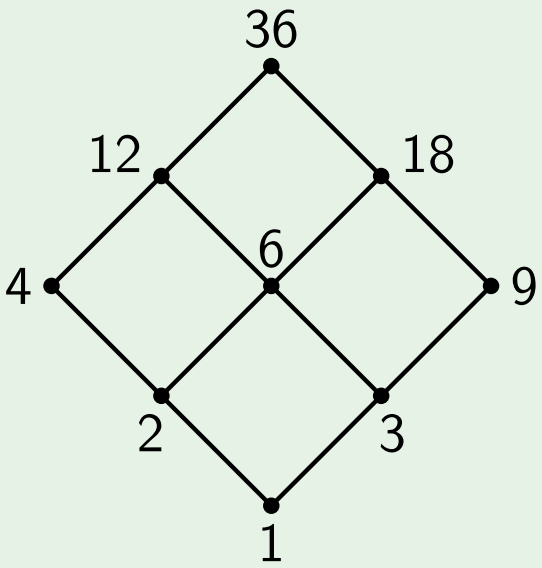
- ☛ Dos retículos isomorfos son **idénticos** tanto algebraicamente como en sus diagramas de Hasse, que sólo se diferenciarán en las etiquetas de los vértices.

Isomorfismos de retículos

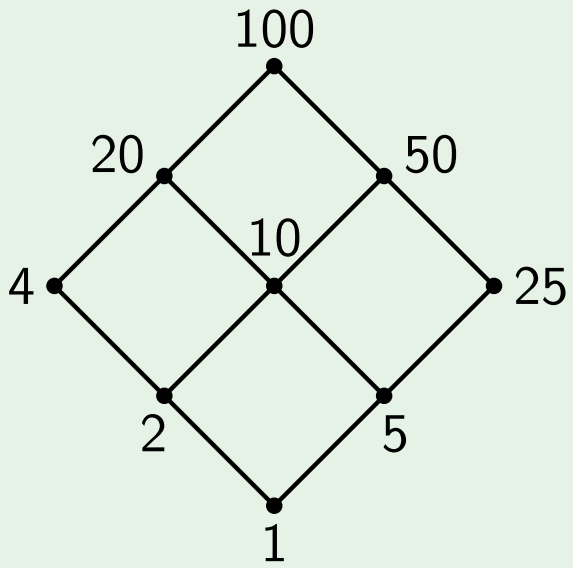
Ejemplo

Ejemplo

$(D_{36}, |)$ y $(D_{100}, |)$ son retículos isomorfos:



D_{36}



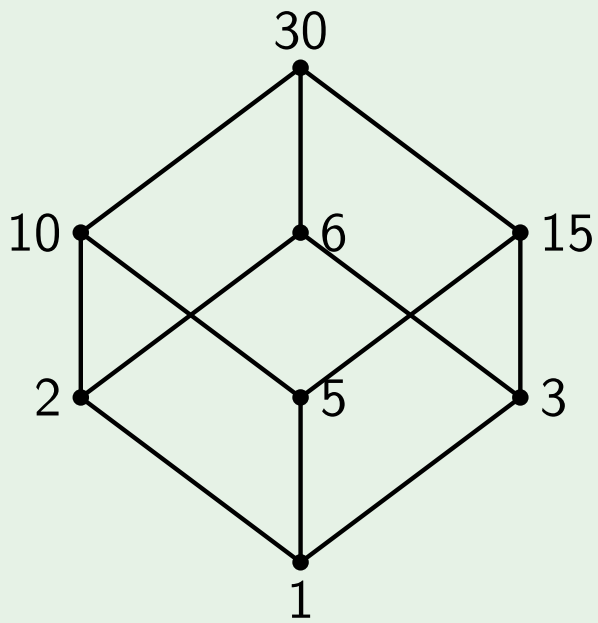
D_{100}

Isomorfismos de retículos

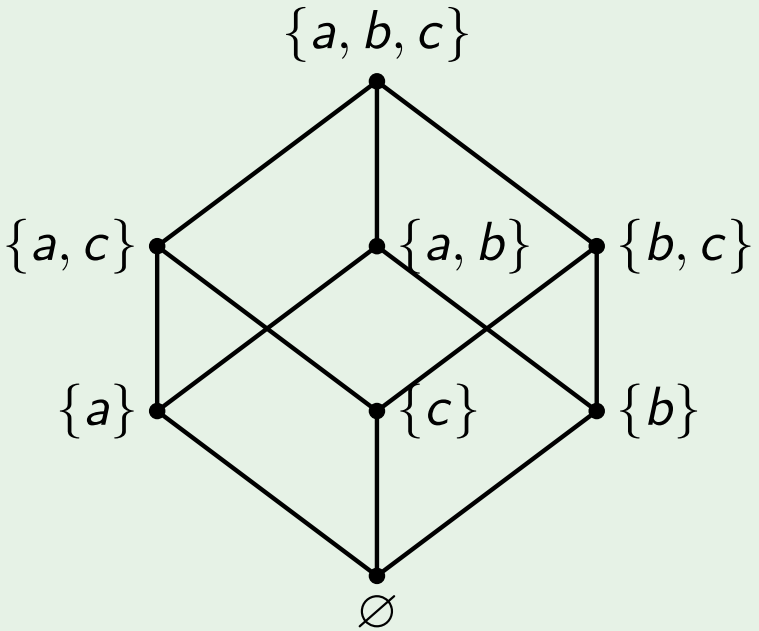
Ejemplo

Ejemplo

$(D_{30}, |)$ y $(\mathcal{P}(\{a, b, c\}), \subseteq)$ son retículos isomorfos:



$(\mathcal{D}_{30}, |)$



$(\mathcal{P}(\{a, b, c\}), \subseteq)$

Retículos distributivos

Definición

Se dice que el retículo $(\mathcal{L}, \sqcup, \sqcap)$ *es* **distributivo** *si para cada* $a, b, c \in \mathcal{L}$ *se verifica:*

$$\begin{aligned} a \sqcap (b \sqcup c) &= (a \sqcap b) \sqcup (a \sqcap c) \\ a \sqcup (b \sqcap c) &= (a \sqcup b) \sqcap (a \sqcup c) \end{aligned}$$

Ejemplos

- $(\mathcal{P}(\{a, b, c\}), \cup, \cap)$ es distributivo.
  En general, $(\mathcal{P}(S), \cup, \cap)$ es un retículo distributivo.
- D_6, D_{12}, D_{36}, ... son retículos distributivos.
  En general, D_n es un retículo distributivo.

Retículos distributivos

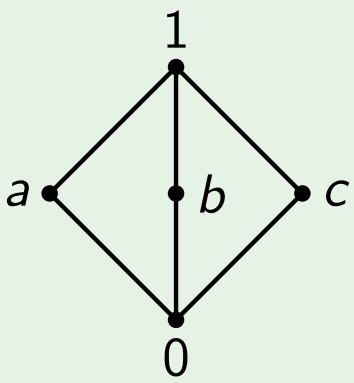
Teorema

Si $\mathcal{L}'$ es un subretículo de un retículo distributivo $(\mathcal{L}, \sqcup, \sqcap)$, entonces $\mathcal{L}'$ también es distributivo.

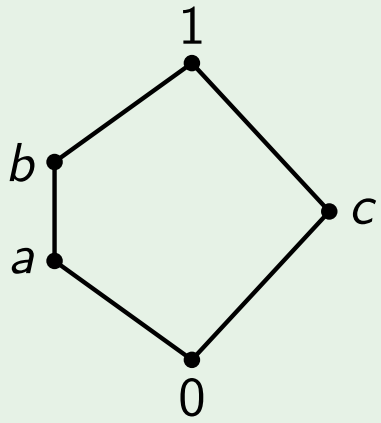
Ejemplo

Los dos casos de retículos no distributivos más representativos son:

Diamante



Pentágono



$$\left\{\begin{array}{rcccc} a \sqcap (b \sqcup c) & = & a \sqcap 1 & = & a \\ (a \sqcap b) \sqcup (a \sqcap c) & = & 0 \sqcup 0 & = & 0 \end{array}\right\} \quad \left\{\begin{array}{rcccc} a \sqcup (b \sqcap c) & = & a \sqcup 0 & = & a \\ (a \sqcup b) \sqcap (a \sqcup c) & = & b \sqcap 1 & = & b \end{array}\right\}$$

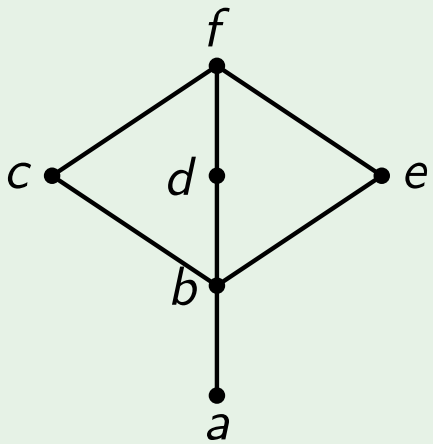
Caracterización de retículos no distributivos

Teorema

Un retículo es no distributivo si y sólo si contiene un subretículo isomorfo a la diamante o al pentágono del ejemplo anterior.

Ejemplo

El siguiente retículo no es distributivo, pues contiene el subretículo $\{b, c, d, e, f\}$ que es isomorfo al diamante.



Retículos distributivos

Teorema

Sea $(\mathcal{L}, \sqcup, \sqcap)$ un retículo distributivo y sean $a, b, c \in \mathcal{L}$ tales que

$$a \sqcup b = a \sqcup c \qquad y \qquad a \sqcap b = a \sqcap c$$

Entonces $b = c$.

Demostración:

$$b \overset{(Abs.)}{=} b \sqcup (b \sqcap a) \overset{(Conm.)}{=} b \sqcup (a \sqcap b) \overset{(Hip.)}{=} b \sqcup (a \sqcap c)$$

$$\overset{(Dist.)}{=} (b \sqcup a) \sqcap (b \sqcup c) \overset{(Conm.)}{=} (a \sqcup b) \sqcap (b \sqcup c)$$

$$\overset{(Hip.)}{=} (a \sqcup c) \sqcap (b \sqcup c) \overset{(Dist.)}{=} (a \sqcap b) \sqcup c \overset{(Hip.)}{=} (a \sqcap c) \sqcup c \overset{(Abs.)}{=} c$$

Retículos Acotados

Definición

Sea $(\mathcal{L}, \preceq)$ *un retículo. Se llama* **mínimo** *de* $\mathcal{L}$ *al elemento que es anterior a todo elemento del retículo, se denota por* 0 *y se le llama también* **primer elemento**.
Se llama **máximo** *de* $\mathcal{L}$ *al elemento que es posterior a todo elemento del retículo. Se denota* 1 *y se le llama también* **último elemento** .

Definición

Un retículo $\mathcal{L}$ *se dice* **acotado** *si tiene primer y último elemento.*

Ejemplos

- $\left(\mathcal{P}(S), \subseteq\right)$ es retículo acotado, con mínimo $\varnothing$ y máximo S.
- Dado un entero positivo n, en el retículo $(D_n, |)$ el primer elemento es 1 y el último elemento es n.
- En $\left(\mathcal{F}(\mathbb{B}^2, \mathbb{B}), \preceq\right)$ el primer elemento es la función cero y el último elemento es la función uno.

Retículos acotados

Teorema

Sea $(\mathcal{L}, \preceq)$ un retículo acotado. Para todo elemento $a \in \mathcal{L}$ se verifica:

1. $a \sqcup 0 = a \qquad a \sqcap 0 = 0$
2. $a \sqcap 1 = a \qquad a \sqcup 1 = 1$

Teorema

Todo retículo finito es acotado.

En general, no todos los retículos infinitos serán acotados:

- Si S es un conjunto infinito, entonces $\mathcal{P}(S)$ también es infinito. Por lo tanto, tenemos que $\left(\mathcal{P}(S), \subseteq\right)$ es un **retículo infinito acotado**
- Por ejemplo, $(\mathbb{Z}, \leq)$ no es acotado, ya que no tiene primer ni último elemento.

Retículos acotados

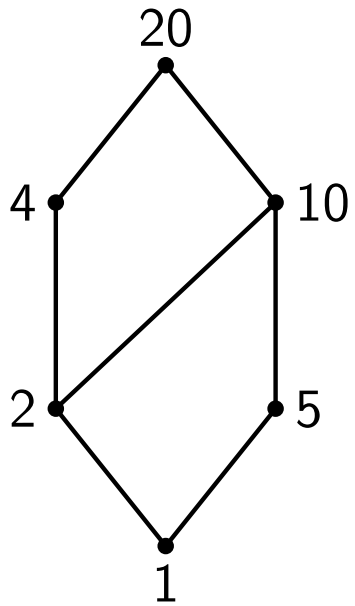
Átomos y superátomos

Definición

Sea $(\mathcal{L}, \preceq)$ un retículo acotado. Se llama **átomo** *a cada elemento que es sucesor inmediato del primer elemento. Se llama* **superátomo** *a cada elemento cuyo sucesor inmediato es el último elemento.del retículo.*

Ejemplos

- Los átomos del retículo D_{20} son 2 y 5; sus superátomos son 4 y 10.

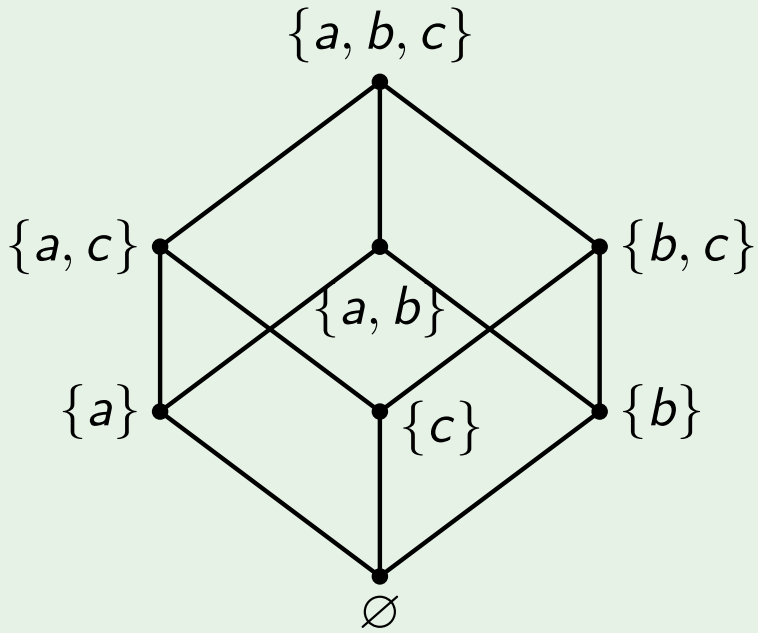


Retículos acotados

Átomos y superátomos

Ejemplos

- En $P(S)$ los átomos son los subconjuntos unitarios; los superátomos los que subconjuntos con **dos** elementos.



- Los átomos de $F(S, \mathbb{B})$ son las funciones que toman el valor 1 exactamente en **un** elemento del dominio; los superátomos son las que toman el valor 0 exactamente en **un** elemento.

Retículos acotados

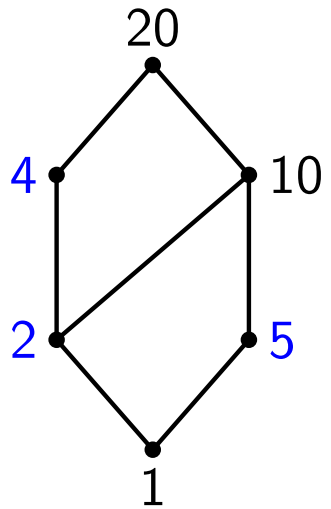
Elementos $\sqcup$-irreducibles

Definición

Se dice que $x \in \mathcal{L}$ es un elemento $\sqcup$-**irreducible** *si no se puede expresar como el supremo de otros elementos, es decir:*

$$\textit{Si} \quad x = y \sqcup z \quad \textit{entonces o bien} \quad x = y \quad \textit{o bien} \quad x = z$$

Ejemplos Los elementos $\sqcup$-irreducibles de D_{20} son 2, 4 y 5.



Retículos acotados

Elementos $\sqcup$-irreducibles

Teorema

Sea $x \neq 0 \in \mathcal{L}$, se tiene que x es un elemento $\sqcup$-irreducible si y solo si es sucesor inmediato de exactamente un elemento .

Corolario

Los átomos son elementos $\sqcup$-irreducibles.

El recíproco no es cierto.

Contraejemplo

En el retículo $(D_{36}, |)$, el elemento 4 es $\sqcup$-irreducible, pero **no** es un átomo ya que no es sucesor inmediato del primer elemento.

Retículos acotados

Descomposición en unión de elementos $\sqcup$-irreducibles no redundantes

Teorema

Sea $(\mathcal{L}, \sqcup, \sqcap)$ un retículo finito. Entonces cada $a \in \mathcal{L}$ se puede expresar

$$a = d_1 \sqcup d_2 \sqcup \cdots \sqcup d_t$$

donde los d_i son elementos $\sqcup$-irreducibles no redundantes.

¿Qué quiere decir que los elementos d_i son **no redundantes**?

- ✓ Si $d_j \preceq d_k$, es decir, $d_j \sqcup d_k = d_k$, entonces se puede suprimir d_j de la descomposición de a.
- ✓ Así, la expresión es **no redundante** si todos los d_j son incomparables en $\preceq$.

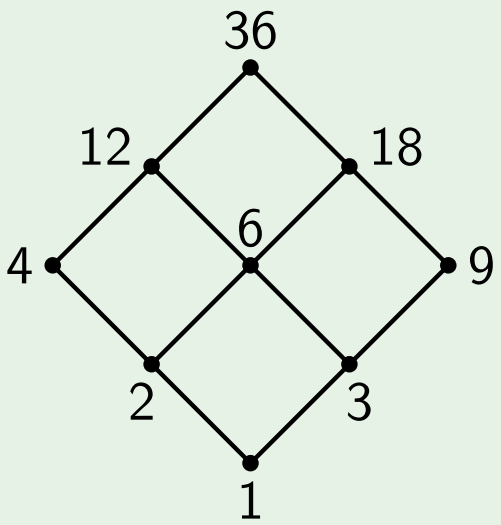
Retículos acotados

Descomposición como suma de elementos $\sqcup$-irreducibles no redundantes

Ejemplo

En D_{36} el elemento 18 se expresa de la forma:

$$18 = \sup(6, 9) = \sup(\sup(2, 3), 9) = \sup(2, \sup(3, 9))$$



$$18 = 6 \sqcup 9 = (2 \sqcup 3) \sqcup 9 = 2 \sqcup (3 \sqcup 9) = 2 \sqcup 9$$

Elementos Complementarios

Definición

Sea $(\mathcal{L}, \sqcup, \sqcap)$ *un retículo acotado, y sean* $a, b \in \mathcal{L}$. *Se dice que* a *y* b *son* **complementarios** *(uno es el complemento del otro) si:*

$$a \sqcup b = 1 \quad y \quad a \sqcap b = 0$$

También se dice que b *es* **complemento** *de* a *y que* a *es* **complemento** *de* b.

En todo retículo acotado se verifica que 0 e 1 son complementarios.

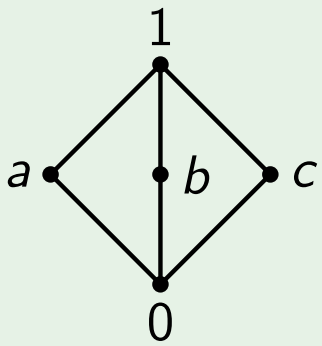
Observación

En un retículo acotado un elemento $x \in \mathcal{L}$ puede no tener complemento, tener un único complemento o puede tener más de un complemento.

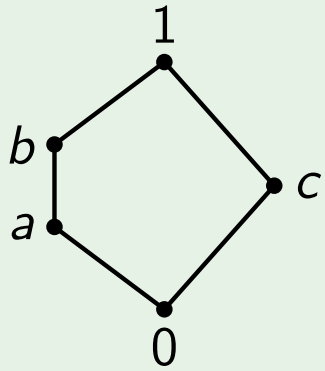
Elementos Complementarios

Ejemplos

- En el diamante
  - a y b son complementarios, ya que $a \sqcup b = 1$ y $a \sqcap b = 0$
  - a y c son complementarios, ya que $a \sqcup c = 1$ y $a \sqcap c = 0$
  - b y c son complementarios, ya que $b \sqcup c = 1$ y $b \sqcap c = 0$



diamante



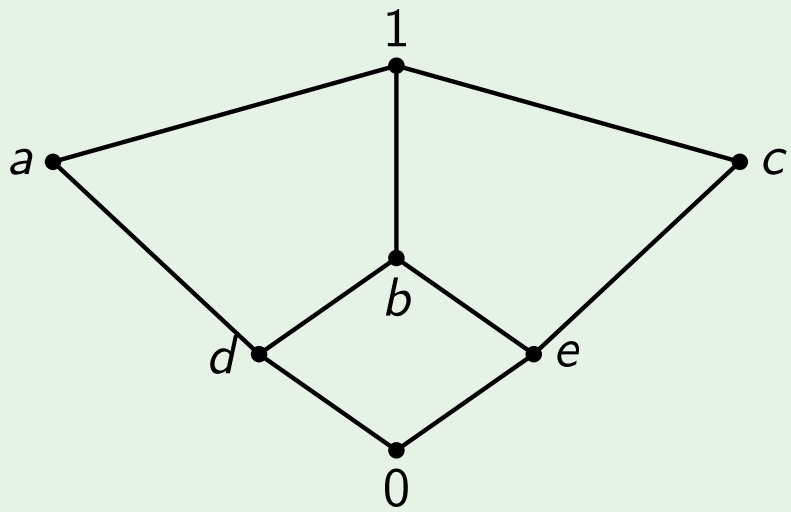
pentágono

- En el pentágono:
  - a y c son complementarios, ya que $a \sqcup c = 1$ y $a \sqcap c = 0$
  - b y c son complementarios, ya que $b \sqcup c = 1$ y $b \sqcap c = 0$

Elementos Complementarios

Ejemplo

- En el retículo



  - 0 y 1 son complementarios.
  - a y c son complementarios, ya que $a \sqcup c = 1$ y $a \sqcap c = 0$.
  - a y e son complementarios, ya que $a \sqcup e = 1$ y $a \sqcap e = 0$.
  - d y c son complementarios, ya que $d \sqcup c = 1$ y $d \sqcap c = 0$.
  - b no tiene complemento.

Retículos complementados

Definición

Un retículo $(\mathcal{L}, \sqcup, \sqcap)$ *se llama* **complementado** *si cada elemento tiene al menos un complemento.*

Ejemplo

- $(D_n, m.c.m., m.c.d.)$ es complementado para $n = 6$.
  Sin embargo no lo es para $n = 12$, ya que 2 no tiene complemento en D_{12}.

Teorema

Sea $(\mathcal{L}, \sqcup, \sqcap)$ *un retículo distributivo y acotado con* 0 *y* 1. *Entonces cada elemento* $a \in \mathcal{L}$ *tiene a lo sumo un complemento.*

Complemento de un elemento

Ejemplo

$\left(\mathcal{F}(\mathbb{B}^2, \mathbb{B}), \leq\right)$ es un retículo complementado.

En el retículo $\left(\mathcal{F}(\mathbb{B}^2, \mathbb{B}), \leq\right)$ cada elemento tiene un único complemento.

El complemento de la función $f : \mathbb{B}^2 \to \mathbb{B}$ es la función

$$\overline{f} : \mathbb{B}^2 \to \mathbb{B}$$

definida como

$$\overline{f}(x) = \begin{cases} 0, & \text{si} \quad f(x) = 1 \\ 1, & \text{si} \quad f(x) = 0 \end{cases}$$

Operación complemento

Definición

Sea $(\mathcal{L}, \sqcup, \sqcap)$ *un retículo complementado y distributivo y sea* $x \in \mathcal{L}$.
El **complemento** *del elemento* $a \in \mathcal{L}$ *es el único elemento* $\overline{a} \in \mathcal{L}$ *tal que*

$$a \sqcup \overline{a} = 1 \qquad y \qquad a \sqcap \overline{a} = 0$$

En todo retículo distributivo y complementado podemos definir una función de $\mathcal{L}$ en sí mismo que asigna a cada elemento $a \in \mathcal{L}$ su complemento $\overline{a}$.

$$\begin{array}{ccccc} - & : & \mathcal{L} & \to & \mathcal{L} \\ & & a & \mapsto & \overline{a} \end{array}$$

Ejemplo

En $\left(\mathcal{P}(S), \cup, \cap\right)$ el complemento de cada $X \subseteq S$ es el conjunto $\overline{X} = S \setminus X$.

$$\begin{array}{ccccc} - & : & \mathcal{P}(S) & \to & \mathcal{P}(S) \\ & & X & \mapsto & \overline{X} = S \setminus X \end{array}$$

Retículos de Boole

Definición

Se llama **retículo de Boole** *a un retículo distributivo y complementado.*

Ejemplo

- $\mathbb{B} = \{0, 1\}$ con su orden habitual $\leq$ es un retículo ordenado. Las operaciones $\sqcup$ y $\sqcap$ asociadas son las siguientes:

$\sqcup$	0	1
0	0	1
1	1	1

$\sqcap$	0	1
0	0	0
1	0	1

  Se puede demostrar fácilmente que $(\mathbb{B}, \sqcup, \sqcap)$ es un retículo distributivo y complementado.

Retículos de Boole

Propiedades

Un retículo de Boole es un conjunto con dos operaciones binarias $\sqcup$ y $\sqcap$ y una operación unaria $-$ que verifica las propiedades que hemos visto. Además, se tiene:

Teorema

Sea $(\mathcal{L}, \sqcup, \sqcap, -)$ un retículo de Boole. Para todo $a, b \in \mathcal{L}$ se verifican las propiedades:

- *De Morgan* $\quad \overline{(a \sqcup b)} = \overline{a} \sqcap \overline{b} \qquad \overline{a \sqcap b} = \overline{a} \sqcup \overline{b}$
- *Involución* $\quad \overline{\overline{a}} = a$

A los retículos de Boole se les llama también **álgebras de Boole**.
Se usa el término **retículo de Boole** para hacer hincapié en el orden parcial subyacente, mientras que se usa **álgebra de Boole** cuando se quiere resaltar las operaciones algebraicas $\sqcup$, $\sqcap$ y $-$.

Álgebras de Boole

Definición algebraica

Definición

Sea $\mathcal{A}$ un conjunto no vacío con dos elementos distintos especiales, $0 \neq 1$, junto con dos operaciones binarias $+$ y $\cdot$ y una operación unaria $-$.
Se dice que $(\mathcal{A}, +, \cdot, -, 0, 1)$ es un **álgebra de Boole** *si para todo $a, b, c \in \mathcal{A}$ se cumple:*

Identidad :	$a + 0$	$=$	a		$a \cdot 1$	$=$	a
Conmutativa :	$a + b$	$=$	$b + a$		$a \cdot b$	$=$	$b \cdot a$
Distributiva :	$a + (b \cdot c)$	$=$	$(a + b) \cdot (a + c)$		$a \cdot (b + c)$	$=$	$a \cdot b + a \cdot c$
Complemento :	$a + \overline{a}$	$=$	1		$a \cdot \overline{a}$	$=$	0

Teorema

Todo retículo de Boole es un álgebra de Boole y viceversa.

Retículo/Álgebra de Boole

Listado de propiedades

1.	**Conmutativa** :	$a+b$	$=$	$b+a$	$a\cdot b$	$=$	$b\cdot a$
2.	**Asociativa** :	$a+(b+c)$	$=$	$(a+b)+c$	$(a\cdot b)\cdot c$	$=$	$a\cdot(b\cdot c)$
3.	**Absorción:**	$a+(a\cdot b)$	$=$	a	$a\cdot(a+b)$	$=$	a
4.	**Idempotencia** :	$a+a$	$=$	a	$a\cdot a$	$=$	a

5.	**Cotas** :	$a\preceq b$	$\iff$	$a+b=b$	$\iff$	$a\cdot b=a$
6.	**Extremos**	$0,\ 1\in\mathcal{A}$				$0\ \preceq a\preceq 1$

7	**Identidad:**	$0+a$	$=$	a	$a\cdot 1$	$=$	a
8	**Dominancia**	$a+1$	$=$	1	$0\cdot a$	$=$	0
9.	**Distributiva**	$a+(b\cdot c)$	$=$	$(a+b)\cdot(a+c)$	$a\cdot(b+c)$	$=$	$(a\cdot b)+(a\cdot c)$
10.	**Complemento** :	$a+\overline{a}$	$=$	1	$a\cdot\overline{a}$	$=$	0
11.	**DeMorgan**	$\overline{(a+b)}$	$=$	$\overline{a}\cdot\overline{b}$	$\overline{a\cdot b}$	$=$	$\overline{a}+\overline{b}$
12.	**Involución :**	$\overline{\overline{a}}$	$=$	a			

Isomorfismos de Álgebras de Boole

Definición

Un **isomorfismo** *entre dos álgebras de Boole* $(\mathcal{A}, +, \cdot, -, 0_A, 1_A)$ *y* $(\mathcal{B}, \vee, \wedge, -, 0_B, 1_B)$ *es una función biyectiva* $\phi\colon \mathcal{A} \to \mathcal{B}$ *y tal que, para todo* $a, b \in \mathcal{A}$*, verifica:*

1. $\phi(a + b) = \phi(a) \vee \phi(b)$
2. $\phi(a \cdot b) = \phi(a) \wedge \phi(b)$
3. $\phi(\overline{a}) = \overline{\phi(a)}$

Teorema de representación

Lema

Sea $(\mathcal{A}, +, \cdot, -, 0_{\mathcal{A}}, 1_{\mathcal{A}})$ un álgebra de Boole finita. Si b es cualquier elemento distinto de cero en $\mathcal{A}$, y $a_1, a_2, \ldots, a_k$ son todos los átomos de $\mathcal{A}$ tales que $a_i \preceq b$, entonces $b = a_1 + a_2 + \cdots + a_k$ de forma única.

- Del lema se deduce que hay una biyección, de hecho un isomorfismo, de $(\mathcal{A}, \preceq)$ en $(\mathcal{P}(S), \subseteq)$, donde S es el conjunto de átomos de A.

Teorema

Toda álgebra de Boole finita $(\mathcal{A}, +, \cdot, -, 0_{\mathcal{A}}, 1_{\mathcal{A}})$ es isomorfa al álgebra de Boole $(\mathcal{P}(S), \cup, \cap, -, \varnothing, S)$, donde S es el conjunto de átomos de $\mathcal{A}$.

Corolario

Si $(\mathcal{A}, +, \cdot, -, 0_{\mathcal{A}}, 1_{\mathcal{A}})$ es un álgebra de Boole finita con n átomos, entonces $\mathcal{A}$ tiene 2^n elementos.

El álgebra de Boole $\mathcal{F}_n$

Definición

Se llama **función booleana** *de n* **variables** *a una función* $f : \mathbb{B}^n \to \mathbb{B}$. *El conjunto de todas las funciones booleanas de n variables se denota* $\mathcal{F}_n$, *y tiene estructura de álgebra de Boole con las operaciones naturales.*

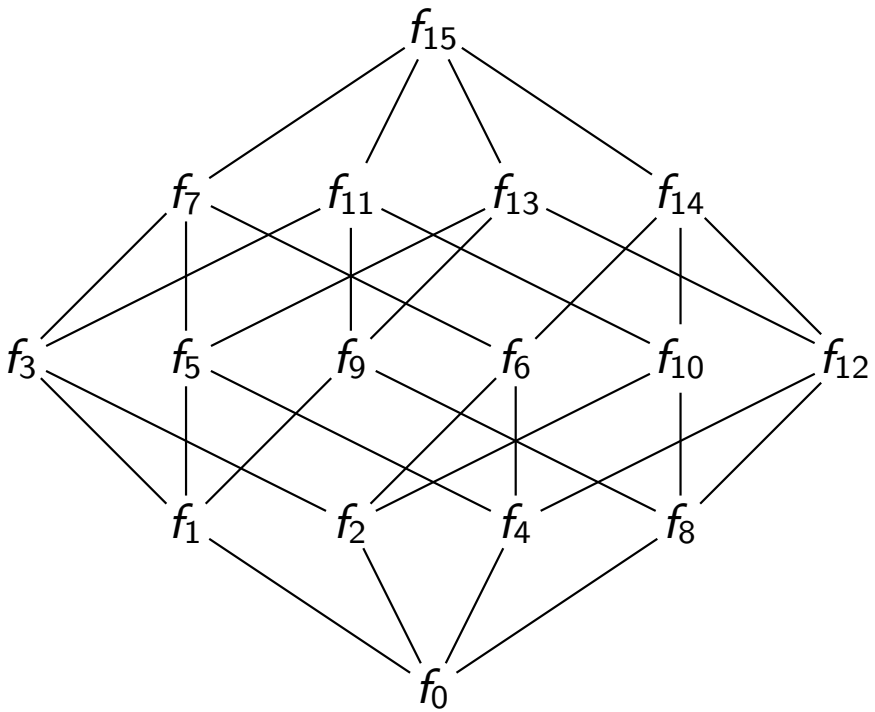
Ejemplo

- Una función booleana de 3 variables es una función $f(x, y, z)$ tal que vale 0 ó 1 para cada una de las 2^3 elecciones de x, y, z.
- Podemos pensar las variables como interruptores en una de las dos posiciones posibles. Como hay 8 formas de poner los interruptores y cada posición lleva a alguna de las dos salidas, dependiendo de la función, hay $2^{2^3} = 256$ funciones booleanas de 3 variables.
- En general, $|\mathcal{F}_n| = 2^{2^n}$.

El álgebra de Boole $\mathcal{F}_2$

$$\mathcal{F}_2 = \{f_j : \mathbb{B}^2 \to \mathbb{B},\ j : 0, ..., 15\}$$

x	y	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1



Expresiones booleanas

Definición

Una **expresión booleana** *sobre un álgebra de Boole* $(\mathcal{A}, +, \cdot, -, 0_{\mathcal{A}}, 1_{\mathcal{A}})$ *se define inductivamente de la siguiente manera:*

[B] *Cualquier elemento de* $\mathcal{A}$ *y cualquier símbolo de variable* $x_1, x_2, \ldots, x_n$ *son expresiones booleanas.*

[R] *Si* E_1 *y* E_2 *son expresiones booleanas, entonces* $E_1 + E_2$, $(E_1 \cdot E_2)$ *y* $\overline{E_1}$ *son también expresiones booleanas.*

- ✓ Las expresiones booleanas representan cálculos con elementos no específicos de una cierta álgebra de Boole $\mathcal{A}$.
- ✓ Se pueden manipular usando las propiedades de las operaciones definidas en el álgebra de Boole correspondiente.

Expresiones booleanas

Definición

Se dice que dos expresiones booleanas son **equivalentes** *si toman los mismos valores para las mismas asignaciones a las variables.*

Ejemplo

Las expresiones booleanas $E_1(x) = \overline{x} \vee 5$ y $E_2(x) = (\overline{5 \vee x}) \vee \overline{6}$ definidas en $(D_{30}, \vee, \wedge, -)$ son equivalentes, ya que

	1	2	3	5	6	10	15	30
$E_1(x)$	30	15	10	30	5	15	10	5
$E_2(x)$	30	15	10	30	5	15	10	5

Expresiones booleanas / Funciones booleanas

➢ En general, dada un álgebra de Boole $(\mathcal{A}, +, \cdot, -, 0_{\mathcal{A}}, 1_{\mathcal{A}})$, **no toda función** de $\mathcal{A}^n$ en $\mathcal{A}$ equivale a una expresión booleana sobre $\mathcal{A}$, aunque ...

Teorema

Toda función $f : \mathbb{B}^n \to \mathbb{B}$ se puede especificar mediante una expresión booleana.

Ejemplo

La función $f : \mathbb{B}^3 \to \mathbb{B}$ dada en la tabla se corresponde con las expresiones lógicas que la siguen:

$f(0,0,0) = 1$	$f(1,0,0) = 0$
$f(0,0,1) = 0$	$f(1,0,1) = 0$
$f(0,1,0) = 1$	$f(1,1,0) = 0$
$f(0,1,1) = 0$	$f(1,1,1) = 1$

$$(x_1 + x_2 + \overline{x}_3) \cdot (x_1 + \overline{x}_2 + \overline{x}_3) \cdot (\overline{x}_1 + x_2 + x_3) \cdot (\overline{x}_1 + x_2 + \overline{x}_3) \cdot (\overline{x}_1 + \overline{x}_2 + x_3)$$

$$(\overline{x}_1 \cdot \overline{x}_2 \cdot \overline{x}_3) + (\overline{x}_1 \cdot x_2 \cdot \overline{x}_3) + (x_1 \cdot x_2 \cdot x_3)$$

Expresiones booleanas / Funciones booleanas

Definiciones

- Las expresiones booleanas que constan de una única variable o su complemento se llaman **literales**.
- Un **minitérmino** es de la forma $y_1 \cdot y_2 \cdot \ldots \cdot y_n$, donde usamos y_j para denotar x_j o bien $\overline{x}_j$.
- Un **maxitérmino** es de la forma $y_1 + y_2 + \cdots + y_n$, donde usamos y_j para denotar x_j o bien $\overline{x}_j$.
- Una expresión booleana está en:
  - **forma normal disyuntiva** si es una suma de minitérminos.
  - **forma normal conjuntiva** si es un producto de maxitérminos.