Facultad de Ciencias Exactas, Ingeniería y Agrimensura
Departamento de Matemática - Escuela de Ciencias Exactas y Naturales
COMPLEMENTOS DE MATEMÁTICA II
Licenciatura en Ciencias de la Computación - Año 2023
Docentes: Francisco Vittone - Mauro Lucci - Delfina Martin

Unidad 3: Retículos

1. Retículos.

En esta Unidad estudiaremos un tipo particular de conjuntos ordenados, denominados *retículos*. Estos conjuntos tienen particular interes puesto que definen una de las primeras estructuras algebraicas que estudiaremos y que son distintas de las que utilizamos habitualmente. En términos generales, una estructura algebraica es un conjunto que posee una o más operaciones (cerradas o *externas*) y que satisfacen una serie de propiedades.

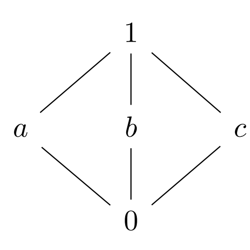
Definición **1.** *Un conjunto parcialmente ordenado $(L, \preceq)$ se denomina un* ***retículo*** *(también llamado* ***reticulado*** *o* ***lattice****) si para cada $x, y \in L$, el conjunto $\{x, y\}$ posee supremo e ínfimo (que denotamos $\sup\{x, y\}$ e $\inf\{x, y\}$ respectivamente).*

Ejemplos **1.**

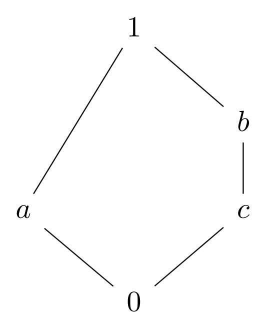
1. Si $(A, \preceq)$ es un conjunto totalmente ordenado, entonces $(A, \preceq)$ es trivialmente un retículo dado que el ínfimo y el supremo de $\{x, y\}$ son x o y y son además mínimo y máximo de $\{x, y\}$. En particular, cualquier subconjunto de $\mathbb{R}$ con las relaciones $\leq$ o $\geq$ es un retículo.

2. Por el principio de dualidad que presentamos en la Unidad 2, resulta inmediato que $(L, \preceq)$ es un retículo si y sólo si $(L, \succeq)$ es un retículo.

3. **Retículos M_3 y N_5.** Consideremos los posets M_3 y N_5 cuyos diagramas de Hasse son los siguientes:



M_3



N_5

Es fácil ver que ambos conjuntos son retículos, que resultarán muy importantes más adelante.

4. **Retículo producto** Consideremos dos retículos $(L, \preceq)$ y $(L', \preceq')$ y consideremos el poset producto $(L \times L', \preceq_{prod})$.

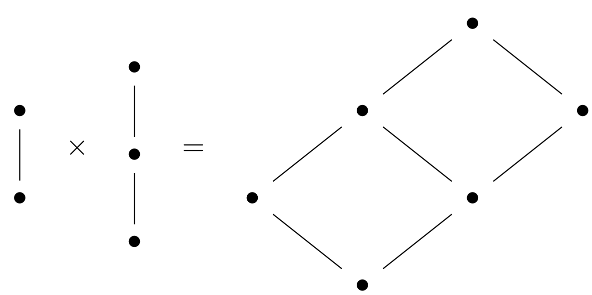
   Veamos que $(L \times L', \preceq_{prod})$ es un retículo. Sean (x, x') y (y, y') en $L \times L'$ y sean $a = \sup\{x, y\}$ $a' = \sup\{x', y'\}$. Entonces es claro que $(x, x') \preceq_{prod} (a, a')$ y $(y, y') \preceq_{prod} (a, a')$, con lo cual (a, a') es una cota superior de $\{(x, x'), (y, y')\}$. Si (c, c') es otra cota superior de $\{(x, x'), (y, y')\}$ entonces

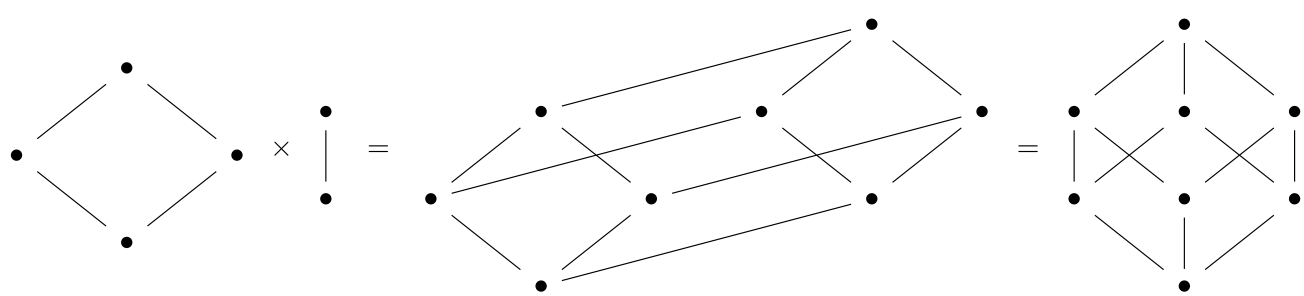
   $$(x, x') \preceq_{prod} (c, c') \implies x \preceq c, \ x' \preceq' c'.$$

   De manera análoga, $y \preceq c$ y $y' \preceq' c'$, con lo cual c es una cota superior de $\{x, y\}$ en L y c' es una cota superior de $\{x', y'\}$ en L'. Luego $a \preceq c$ y $a' \preceq c'$ y entonces $(a, a') \preceq_{prod} (c, c')$. Concluimos que (a, a') es el mínimo del conjunto de cotas superiores y entonces $(c, c') = \sup\{(x, x'), (y, y')\}$.

   Análogamente se muestra que si $b = \inf\{x, y\}$ y $b' = \inf\{x', y'\}$ entonces $(b, b') = \inf\{(x, x'), (y, y')\}$.

   Informalmente, podemos dibujar el diagrama de Hasse de un producto $L \times L'$ (o reconocer cuándo un determinado diagrama se corresponde con un producto) reemplazando cada punto del diagrama de L por una copia del diagrama de L', y conectando "puntos correspondientes", colocando siempre los puntos de modo que se respete el modo ascendente de construir un diagrama de Hasse (esto mismo aplica para el producto de dos posets cualesquiera, no necesariamente de retículos). En las figuras siguientes damos algunos ejemplos:





5. Sea $X \neq \emptyset$. Entonces $(\mathcal{P}(X), \subseteq)$ es un retículo. En efecto, sean $C, D \subseteq X$ y sea $I = C \cap D$. Entonces I es una cota inferior de $\{C, D\}$ (pues $I \subseteq C$ y $I \subseteq D$) y si $B \subset X$ es una cota inferior de $\{C, D\}$, entonces $B \subseteq C$ y $B \subseteq D$, con lo cual $B \subseteq C \cap D = I$. Luego $I = \inf\{C, D\}$. De manera similar se prueba que $U = C \cup D = \sup\{C, D\}$.

6. Consideremos el poset $(\mathbb{N}, \mid)$. Vimos en el ejemplo 19 de la Unidad 2 que todo subconjunto finito no vacío de $(\mathbb{N}, \mid)$ tiene un ínfimo y un supremo, el máximo común divisor y el mínimo común múltiplo de sus elementos respectivamente. Por lo tanto $(\mathbb{N}, \mid)$ es un retículo.

   Observemos que **no todo subconjunto de un retículo (con el orden restringido) es un retículo**. Por ejemplo si tomamos el subconjunto $P \subseteq \mathbb{N}$ de los números primos (aquellos que tienen exáctamente dos divisores positivos) entonces $(P, \mid)$ no es un retículo. Más aún ningún subconjunto $\{x, y\} \subseteq P$ con $x \neq y$ tiene ínfimo ni supremo.

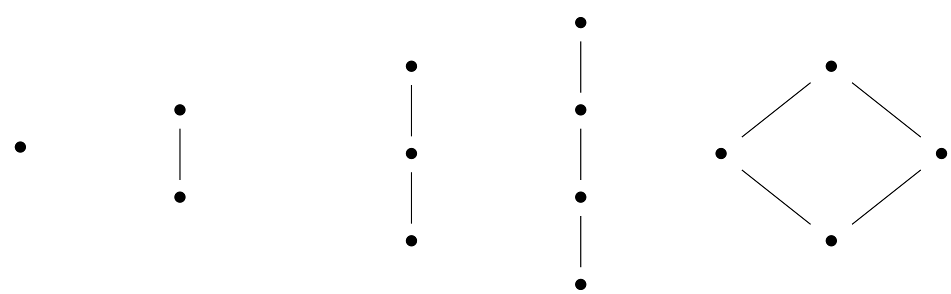
   Fijemos ahora $n \in \mathbb{N}$ y sea D_n el conjunto de divisores de n, esto es,

$$D_n = \{m \in \mathbb{N} : m \mid n\}.$$

   Observemos que si $m \in D_n$ y $k \in \mathbb{N}$ divide a m, entonces $k \mid n$. Luego $k \in D_n$. Por lo tanto si $m_1, m_2 \in D_n$, como $mcd(m_1, m_2)$ (donde mcd representa el máximo común divisor) divide a ambos, $mcd(m_1, m_2) \in D_n$ y por lo tanto existe (en D_n) el ínfimo $\inf\{m_1, m_2\} = mcd(m_1, m_2)$.

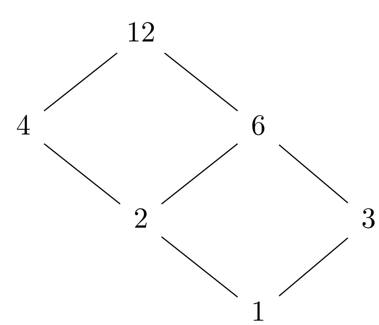
   Por otra parte, si $m_1, m_2 \in D_n$, entonces n es un múltiplo común de m_1 y m_2. Luego n es divisible por el mínimo común múltiplo de ambos (que denotamos $mcm(m_1, m_2)$). Es decir, $mcm(m_1, m_2) \in D_n$ y por lo tanto existe (en D_n) el supremo $\sup\{m_1, m_2\} = mcm(m_1, m_2)$. Concluimos que $(D_n, \mid)$ es un retículo.

   Para los primeros 11 números naturales, los diagramas de Hasse de $(D_n, \mid)$ tienen alguna de las siguientes formas:

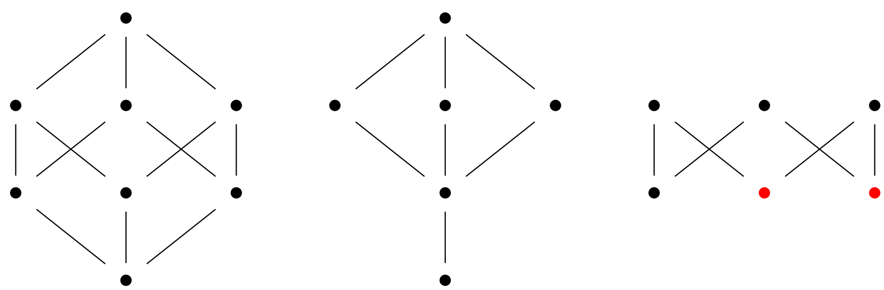


$n = 1$ $\quad n = 2, 3, 5, 7, 11$ $\quad n = 4, 9$ $\quad n = 8$ $\quad n = 6, 10$

   Observemos que el segundo diagrama (de izquierda a derecha) representa $(D_p, \mid)$ para cualquier número primo p. El diagrama de Hasse para D_{12} es



7. De los siguientes diagramas de Hasse, los dos primeros corresponden a retículos (ejercicio, ¿Qué posets representan?).



El tercero no corresponde a un retículo, pues por ejemplo el conjunto formado por los elementos cuyos nodos están en rojo no tiene ni supremo ni ínfimo.

Ejercicio **1.** *¿Cómo son los diagramas de Hasse de $(D_{p^2}, |)$, $(D_{p^3}, |)$, y más generalmente $(D_{p^k}, |)$, $k \in \mathbb{N}$, para un número primo $p \in \mathbb{N}$?*

La existencia de supremo e ínfimo para los conjuntos de dos elementos permite definir dos **operaciones binarias** en un retículo $(L, \preceq)$ (trataremos este tema formalmente en la próxima Unidad). Es decir, si para cada $x, y \in L$ ponemos

$$x \vee y = \sup\{x, y\}, \quad x \wedge y = \text{ínf}\{x, y\}$$

quedan bien definidas dos funciones

$$\vee : L \times L \to L, \quad \wedge : L \times L \to L.$$

$x \vee y$ suele llamarse **join** de x e y y $x \wedge y$ suele llamarse **meet** de x e y.

Teorema **1.** *Sea $(L, \preceq)$ un retículo. Entonces para cada $x, y, z \in L$ se verifica:*

1. $x \preceq x \vee y$.

2. $x \wedge y \preceq x$.

3. $x \preceq y \iff x = x \wedge y \iff y = x \vee y$.

4. *$\vee$ y $\wedge$ son asociativas, esto es,*

$$(x \vee y) \vee z = x \vee (y \vee z) \quad (x \wedge y) \wedge z = x \wedge (y \wedge z).$$

5. *$\vee$ y $\wedge$ son conmutativas, esto es,*

$$x \vee y = y \vee x, \quad x \wedge y = y \wedge x.$$

6. *Cada elemento es idempotente, esto es, $x \vee x = x$ y $x \wedge x = x$.*

7. $x \vee (x \wedge y) = x = x \wedge (x \vee y)$ *(propiedad de absorción).*

8. $\vee$ *y* $\wedge$ *son compatibles con el orden* $\preceq$*, esto es,*

$$\left.\begin{array}{l} x \preceq y \\ x' \preceq y' \end{array}\right\} \Longrightarrow x \vee x' \preceq y \vee y', \qquad \left.\begin{array}{l} x \preceq y \\ x' \preceq y' \end{array}\right\} \Longrightarrow x \wedge x' \preceq y \wedge y'$$

Demostración. La prueba de los items 1, 2, 3, 5 y 6 son inmediatas y las dejamos como ejercicio.

Probemos 4. Sean $x, y, z \in L$ y consideremos

$$a = x \wedge y = \operatorname{ínf}\{x, y\}, \quad a' = y \wedge z = \operatorname{ínf}\{y, z\}.$$

Sean $b = \operatorname{ínf}\{a, z\}$. Debemos probar que $b = \operatorname{ínf}\{x, a'\}$.

Veamos primero que b es una cota inferior de $\{x, a'\}$. Como $b \preceq a$ y $a \preceq x$, resulta

$$b \preceq x. \tag{1}$$

Con el mismo argumento, $b \preceq y$ y por definición de b, $b \preceq z$. Luego

$$b \preceq \operatorname{ínf}\{y, z\} = a'. \tag{2}$$

De (1) y (2), b resulta una cota inferior de $\{x, a'\}$.

Veamos ahora que para cualquier cota inferior c de $\{x, a'\}$, $c \preceq b$.

En efecto, si c es cota inferior de $\{x, a'\}$ entonces $c \preceq x$ y $c \preceq a' = \operatorname{ínf}\{y, z\}$. De esto último obtenemos que $c \preceq y$ y $c \preceq z$. Tenemos entonces que

$$c \preceq x, \ c \preceq y, \ c \preceq z.$$

En particular, c es una cota inferior de $\{x, y\}$ y por lo tanto $c \preceq a = \operatorname{ínf}\{x, y\}$. Luego c es una cota inferior de $\{a, z\}$ y por lo tanto $c \preceq b$ como queríamos probar.

La prueba de la asociatividad de $\vee$ es análoga y la dejamos como ejercicio.

Probemos 6. Por el item 2, $x \wedge y \preceq x$. Luego por el item 3, $x = (x \wedge y) \vee x = x \vee (x \wedge y)$, donde la última igualdad vale por la conmutatividad de $\vee$ (item 5). La otra propiedad de absorción es análoga y la dejamos como ejercicio.

Probemos finalmente la compatibilidad de estas operaciones con el orden $\preceq$ (item 8). Supongamos que $x \preceq y$ y $x' \preceq y'$. Sea $a = y \vee y'$. Entonces $y \preceq a$ y $y' \preceq a$, con lo cual $x \preceq a$ y $x' \preceq a$. Luego a es una cota superior de $\{x, x'\}$ y entonces $\sup\{x, x'\} \preceq a$. Es decir $x \vee x' \preceq y \vee y'$. La compatibilidad de $\wedge$ con $\preceq$ es análoga y la dejamos como ejercicio. $\square$

Las operaciones $\wedge$ y $\vee$ caracterizan completamente los retículos, en el sentido que cualquier conjunto con dos operaciones que satisfagan los item 4 a 7 admite un orden para el cual es un retículo:

Teorema **2.** *Sea* L *un conjunto no vacío con dos operaciones,* $\tilde{\vee} : L \times L \to L$ *y* $\tilde{\wedge} : L \times L \to L$ *tales que:*

1. $\tilde{\vee}$ y $\tilde{\wedge}$ son asociativas: para cada $x, y, z \in L$,

$$(x \,\tilde{\vee}\, y) \,\tilde{\vee}\, z = x \,\tilde{\vee}\, (y \,\tilde{\vee}\, z) \quad (x \,\tilde{\wedge}\, y) \,\tilde{\wedge}\, z = x \,\tilde{\wedge}\, (y \,\tilde{\wedge}\, z).$$

2. $\tilde{\vee}$ y $\tilde{\wedge}$ son conmutativas: para cada $x, y \in L$,

$$x \,\tilde{\vee}\, y = y \,\tilde{\vee}\, x, \quad x \,\tilde{\wedge}\, y = y \,\tilde{\wedge}\, x.$$

3. Cada elemento es idempotente, esto es, $x \,\tilde{\vee}\, x = x$ y $x \,\tilde{\wedge}\, x = x$ para cada $x \in L$.

4. Valen las propiedades de absorción: para cada $x, y \in L$,

$$x \,\tilde{\vee}\, (x \,\tilde{\wedge}\, y) = x = x \,\tilde{\wedge}\, (x \,\tilde{\vee}\, y)$$

Entonces la relación $\preceq$ en L definida por

$$x \preceq y \iff x \tilde{\vee} y = y$$

es un orden parcial en L tal que $(L, \preceq)$ es un retículo para el cual $\wedge = \tilde{\wedge}$ y $\vee = \tilde{\vee}$.

Demostración. Comencemos probando que $\preceq$ es una relación de orden en L.

Sea $x \in L$. Como x es idempotente para $\tilde{\vee}$, resulta $x = x \,\tilde{\vee}\, x$ y por lo tanto $x \preceq x$. Luego $\preceq$ es reflexiva.

Sean $x, y \in L$ tales que $x \preceq y$ y $y \preceq x$. Entonces $x \,\tilde{\vee}\, y = y$ y $y \,\tilde{\vee}\, x = x$. Como $\tilde{\vee}$ es conmutativa, resulta $x \,\tilde{\vee}\, y = y \,\tilde{\vee}\, x$ y por lo tanto $x = y$. Luego $\preceq$ es antisimétrica.

Veamos finalmente que $\preceq$ es transitiva. Sean $x, y, z \in L$ tales que $x \preceq y$ y $y \preceq z$. Entonces $x \,\tilde{\vee}\, y = y$ y $y \,\tilde{\vee}\, z = z$. Por lo tanto, como $\tilde{\vee}$ es asociativa tendremos

$$x \,\tilde{\vee}\, z = x \,\tilde{\vee}\, (y \,\tilde{\vee}\, z) = (x \,\tilde{\vee}\, y) \,\tilde{\vee}\, z = y \,\tilde{\vee}\, z = z \implies x \preceq z.$$

Veamos ahora que $(L, \preceq)$ es un retículo para el cual $\tilde{\vee} = \vee$ y $\tilde{\wedge} = \wedge$. Tomemos $x, y \in L$ qualesquiera. Debemos probar que existen $\inf\{x, y\} = x \,\tilde{\wedge}\, y$ y $\sup\{x, y\} = x \,\tilde{\vee}\, y$.

Sea $w = x \,\tilde{\vee}\, y$. Entonces tendremos que

$$x \,\tilde{\vee}\, w = x \,\tilde{\vee}\, (x \,\tilde{\vee}\, y) = (x \,\tilde{\vee}\, x) \,\tilde{\vee}\, y = x \,\tilde{\vee}\, y = w \implies x \preceq w$$

y de manera análoga $y \preceq w$. Luego w es una cota superior de $\{x, y\}$.

Sea ahora z una cota superior cualquiera de $\{x, y\}$. Entonces $x \preceq z$ y $y \preceq z$, de donde $x \,\tilde{\vee}\, z = z$ y $y \,\tilde{\vee}\, z = z$. Luego

$$w \,\tilde{\vee}\, z = (x \,\tilde{\vee}\, y) \,\tilde{\vee}\, z = x \,\tilde{\vee}\, (y \,\tilde{\vee}\, z) = x \,\tilde{\vee}\, z = z \Rightarrow w \preceq z.$$

Concluimos que $w = x \,\tilde{\vee}\, y$ es un mínimo en el conjunto de cotas superiores de $\{x, y\}$ y por lo tanto $x \,\tilde{\vee}\, y = \sup\{x, y\}$.

Observemos que la relación $\preceq$ verifica que

$$x \preceq y \iff x \,\tilde{\wedge}\, y = x.$$

En efecto, si $x \preceq y$ entonces $x \tilde{\vee} y = y$ y por lo tanto, de las propiedades de absorción resulta

$$x \tilde{\wedge} y = x \tilde{\wedge} (x \tilde{\vee} y) = x.$$

Recíprocamente, si $x \tilde{\wedge} y = x$, entonces $x \tilde{\vee} y = (x \tilde{\wedge} y) \tilde{\vee} y = y \tilde{\vee} (y \tilde{\wedge} x) = y$, y por lo tanto $x \preceq y$.

Ahora la prueba de que $\inf\{x, y\} = x \tilde{\wedge} y$ es análoga a la prueba de que $\sup\{x, y\} = x \tilde{\vee} y$ y la dejamos como ejercicio. $\square$

El Teorema 2 nos permite dar una definición equivalente de un retículo a partir de un conjunto con dos operaciones que verifiquen las propiedades de asociatividad, conmutatividad, idempotencia de todos sus elementos y absorción. Nos referiremos frecuentemene a esta construcciómo como la **definición algebraica** del retículo, y la denotaremos $(L, \vee, \wedge)$.

Ejemplos **2.**

1. Sea X un conjunto no vacío y sea $L = \mathcal{P}(X)$. Entonces es fácil ver que las operaciones de unión $\tilde{\vee} = \cup$ e intersección $\tilde{\wedge} = \cap$ verifican las hipótesis del Teorema 2. Luego $(\mathcal{P}(X), \cup, \cap)$ es un retículo definido algebraicamente, tal que el orden $\preceq$ está dado por

$$C \preceq D \iff C \cup D = D \iff C \subseteq D$$

es decir, la relación de contención, como vimos en el item 5 de los Ejemplos 1.

2. Las operaciones $\tilde{\vee} = mcm$ y $\tilde{\wedge} = mcd$ en $\mathbb{N}$ (es decir tomar mínimo común múltiplo y máximo común divisor de dos números) verifican trivialmente las hipótesis del Teorema 2. Por lo tanto $(\mathbb{N}, mcm, mcd)$ es un retículo definido algebraicamente, tal que el orden $\preceq$ está dado por

$$x \preceq y \quad \Leftrightarrow \quad mcm(x, y) = y \quad \Leftrightarrow \quad y \text{ es múltiplo de } x \;\Leftrightarrow\; x \mid y$$

es decir, la relación $\preceq$ es "divide a", como vimos en el item 6 de los Ejemplos 1.

3. Consideremos dos retículos $(L, \vee, \wedge)$ y $(L', \tilde{\vee}, \tilde{\wedge})$ definidos algebraicamente. En $L \times L'$ consideremos las funciones $\vee_{prod}$ y $\wedge_{prod}$ de la siguiente manera:

$$(x, x') \vee_{prod} (y, y') = (x \vee x', y \tilde{\vee} y'), \quad (x, x') \wedge_{prod} (y, y') = (x \wedge x', y \tilde{\wedge} y').$$

Entonces $\vee_{prod}$ y $\wedge_{prod}$ verifican las hipótesis del Teorema 2 y se corresponden a un retículo cuyo orden es el orden producto $\preceq_{prod}$ dado en el item 4 de los Ejemplos 1.

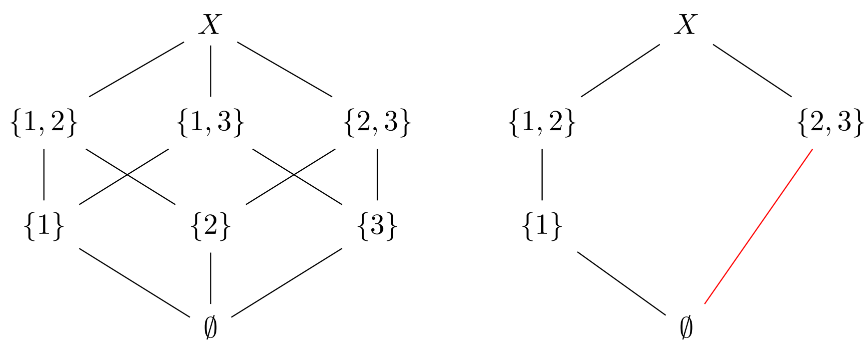
4. Si $(L, \vee, \wedge)$ es un retículo definido algebraicamente, entonces $(L, \wedge, \vee)$ también lo es. Si $\preceq$ es el orden asociado a $(L, \vee, \wedge)$, entonces el orden asociado a $(L, \wedge, \vee)$ es el orden inverso $\succeq$.

Definición **2.** *Si $(L, \preceq)$ es un retículo, entonces $(L, \succeq)$ se denomina **retículo dual** de $(L, \preceq)$. Cuando la relación se da por conocida y denotamos al retículo directamente por L, su dual suele denotarse por L^*. Además, si $\wedge^*$ y $\vee^*$ son las operaciones asociadas a L^* es inmediato que $\wedge^* = \vee$ y $\vee^* = \wedge$. Si $(L, \vee, \wedge)$ es un retículo definido algebraicamente a partir de las operaciones $\vee$ y $\wedge$ (o sea como en el Teorema 2), entonces su dual es el retículo definido algebraicamente por $(L, \wedge, \vee)$.*

2. Subretículos

Si $(A, \preceq)$ es un poset, entonces $(A, \preceq_{|A})$ es un poset. Sin embargo, vimos en el item 6 de los Ejemplos 1 que esto es falso si reemplazamos "poset" por "retículo". Es decir, un subconjunto de un retículo con el orden restringido no necesariamente es un retículo. Incluso si esto ocurre, podría suceder que las operaciones $\vee$ y $\wedge$ no se restrinjan adeacuadamente a L':

Ejemplo **3.** Consideremos $X = \{1,2,3\}$ y el retículo $L = (\mathcal{P}(X), \subseteq)$. Sea $L' = \{\emptyset, \{1\}, \{1,2\}, \{2,3\}, X\}$. Entonces $(L', \subseteq_{|L'})$ es un retículo:



Observemos que en L, $\vee = \cup$ y $\wedge = \cap$, pero en L', $\{1,2\} \wedge' \{2,3\} = \emptyset \neq \{1,2\} \wedge \{2,3\}$. Esto último se debe a que $\{1,2\} \cap \{2,3\} \notin L'$, es decir, $\wedge$ no es una operación *cerrada* en L'.

Esta última observación motiva la siguiente definición:

Definición **3.** *Sea $(L, \preceq) = (L, \vee, \wedge)$ un retículo. Un subconjunto $L' \subseteq L$ es un **subretículo** de L si para cada $x, y \in L'$, $x \vee y \in L'$ y $x \wedge y \in L'$, es decir, $(L', \vee', \wedge')$ es un retículo definido algebraicamente, donde $\vee' = \vee_{|L' \times L'}$, $\wedge' = \wedge_{|L' \times L'}$.*

Observación **1.** *A partir de la definición anterior, es fácil ver que si $(L, \preceq) = (L, \vee, \wedge)$ es un retículo y L' es un subretículo de L, entonces $L' = (L', \preceq_{L'})$ es un retículo cuyas operaciones $\vee'$ y $\wedge'$ son las restricciones a L' de las operaciones de L.*

Como hemos visto en el Ejemplo 3 la recíproca es falsa. Es decir, si L' es un subconjunto de L tal que $(L', \preceq_{|L'})$ es un retículo, entonces $(L', \preceq_{|L'})$ no necesariamente es un subretículo de L.

Ejemplos **4.**

1. Continuando con el ejemplo 3, $L' = \{\emptyset, \{2\}, \{1,3\}, X\}$ es un subretículo de $L = (\mathcal{P}(X), \subseteq)$. El conjunto $L'' = \{\emptyset, \{1\}, \{3\}, X\}$ con la relación de contención es un retículo, pero no es un subretículo de $(\mathcal{P}(X), \subseteq)$.

2. Toda cadena L' contenida en un retículo $(L, \preceq)$ es un subretículo de $(L, \preceq)$ (dejamos los detalles como ejercicio).

3. Los retículos $(D_n, |)$ son subretículos de $(\mathbb{N}, |)$ para cada $n \in \mathbb{N}$, puesto que en ambos casos $\vee = mcm$ y $\wedge = mcd$.

Ejercicio **2.** *Probar que si L y S son retículos y L' y S' son subretículos de L y S respectivamente, entonces $L' \times S'$ es un subretículo de $(L \times S, \preceq_{prod})$.*

3. Morfismos de retículos

Recordemos que una función $f : (L, \preceq) \to (L', \preceq')$ es un morfismo de orden si se verifica que para cada $x, y \in L$,

$$x \preceq y \implies f(x) \preceq' f(y)$$

y que f es un isomorfismo entre L y L' si f es un morfismo de orden biyectivo tal que su inversa es un morfismo de orden, o equivalentemente, si f es sobreyectiva y para cada $x, y \in L$

$$x \preceq y \iff f(x) \preceq' f(y).$$

f es un **anti-isomorfismo** si es un isomorfismo de $(L, \preceq)$ en $(L', \succeq)$.

Recordemos además que un morfismo de orden biyectivo no es necesariamente un isomorfismo de orden.

Por otra parte, un morfismo de orden entre dos retículos no necesariamente preserva la estructura de retículo. Consideremos por ejemplo $Id : (\mathbb{N}, |) \to (\mathbb{N}, \leq)$. Entonces no es cierto que $Id(\sup\{x, y\}_{(\mathbb{N}, |)}) = \sup\{Id(x), Id(y)\}_{(\mathbb{N}, \leq)}$. En efecto, basta tomar $x = 2$, $y = 3$ y tendremos que $\sup\{2, 3\}_{(\mathbb{N}, |)} = 6$ y $\sup\{2, 3\}_{(\mathbb{N}, \leq)} = 3 \neq Id(6)$.

Esto motiva la siguiente definición:

Definición **4.** *Sean $(L, \preceq)$ y $(L', \preceq')$ dos retículos. Una función $f : L \to L'$ es un **morfismo de retículos** si f es un morfismo de orden tal que para cada $x, y \in L$,*

$$f(\sup\{x, y\}_L) = \sup\{f(x), f(y)\}_{L'}, \quad f(\inf\{x, y\}_L) = \inf\{f(x), f(y)\}_{L'}$$

o equivalentemente, si $\vee$, $\wedge$ y $\tilde{\vee}$, $\tilde{\wedge}$ son las operaciones asociadas a los ordenes en L y L',

$$f(x \vee y) = f(x) \,\tilde{\vee}\, f(y), \quad f(x \wedge y) = f(x) \,\tilde{\wedge}\, f(y).$$

*f es un **isomorfismo de retículos** si f es un isomorfismo de orden tal que f y f^{-1} son morfismos de retículos.*

*f es un **antisomorfismo de retículos** de L en L' si f es un isomorfismo de retículos de $(L, \preceq)$ en $(L', \succeq)$.*

Cuando los retículos están definidos a partir de sus operaciones características, podemos caracterizar los morfismos de la siguiente manera:

Lema **3.** *Sean $(L, \preceq) = (L, \vee, \wedge)$ y $(L', \preceq') = (L', \tilde{\vee}, \tilde{\wedge})$ dos retículos (definidos como posets o algebraicamente) y sea $f : L \to L'$. Entonces:*

1. *f es un morfismo de retículos si y sólo si para cada $x, y \in L$ se verifican*

$$f(x \vee y) = f(x) \,\tilde{\vee}\, f(y), \quad f(x \wedge y) = f(x) \,\tilde{\wedge}\, f(y). \tag{3}$$

2. *f es un isomorfismo de retículos si y sólo si f es un morfismo de retículos biyectivo.*

Demostración. Para probar 1 sólo debemos ver que una función $f : L \to L'$ que verifique (3) es un morfismo de orden. Sean $x, y \in L$ tales que $x \preceq y$. Entonces $x \vee y = y$ y por (3) $f(x) \tilde{\vee} f(y) = f(y)$. Luego $f(x) \preceq' f(y)$.

Para probar 2, debemos ver que todo morfismo de retículos biyectivo es un isomorfismo de retículos, y para ello solo nos queda probar que f^{-1} es un morfismo de retículos. Sean entonces $v, w \in L'$ y sean $x = f^{-}(v)$, $y = f^{-1}(w)$. Entonces

$$f(x \vee y) = f(x) \tilde{\vee} f(y) = v \tilde{\vee} w \implies x \vee y = f^{-1}(v \tilde{\vee} w).$$

Por lo tanto tendremos $f^1(v \tilde{\vee} w) = x \vee y = f^{-1}(v) \vee f^{-1}(w)$ como queríamos probar. La demostración de que $f^1(v \tilde{\wedge} w) = f^{-1}(v) \wedge f^{-1}(w)$ es análoga. □

Corolario **4.** *Sean L, L' y L'' tres retículos y $f : L \to L'$, $g : L' \to L''$ isomorfismos de retículos. Entonces:*

1. *$f^{-1} : L' \to L$ es un isomorfismo de retículos.*

2. *$g \circ f : L \to L''$ es un isomorfismo de retículos.*

Corolario **5.** *Sea Ret el conjunto de todos los retículos. Entonces la relación $\sim$ en Ret definida por $L \sim L'$ si L y L' son retículos isomorfos es una relación de equivalencia.*

Ejercicio **3.** *Probar los Corolarios 4 y 5*

Ejemplos **5.**

1. Es inmediato de la definición que para cualquier retículo $(L, \preceq)$, la identidad $Id : L \to L$ es un isomorfismo de retículos entre L y L y un anti-isomorfismo de retículos entre L y su retículo dual L^*.

2. Si L' es un subretículo de un retículo L, es inmediato verificar que la inclusión $i : L' \to L$, dada por $i(x) = x$ es un morfismo de retículos. En efecto, las operaciones en L' son las restricciones de las operaciones de L, luego

$$i(x \vee' y) = x \vee y = i(x) \vee i(y), \quad i(x \wedge' y) = x \wedge i = i(x) \wedge i(y).$$

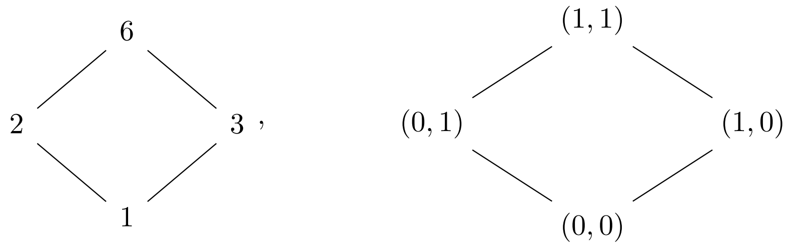
Consideremos ahora el subconjunto $L' = \{\emptyset, \{1\}, \{3\}, X\}$ de $L = \mathcal{P}(\{1, 2, 3\})$. Entonces $L' \subset L$ y $(L', \subseteq)$ y $(L, \subseteq)$ son retículos. Vimos en los Ejemplos 4 que L' no es un subretículo de L. Tiene sentido de todos modos considerar la función inclusión $i : L \to L'$, $i(x) = x$. En este caso,

$$i(\{1\} \vee' \{3\}) = i(X) = X \neq i(\{1\}) \vee i(\{3\}) = \{1, 3\}.$$

Dejamos como ejercicio probar que si L' es un subconjunto de un retículo $(L, \preceq)$ tal que $(L', \preceq_{|L'})$ es un retículo, entonces $(L', \preceq_{|L'})$ es un subretículo de $(L, \preceq)$ si y solo si $i : L' \to L$, $i(x) = x$, es un morfismo de retículos.

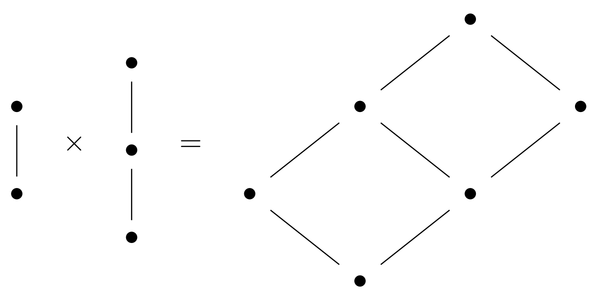
3. Vimos en la Unidad 2 que todos los conjuntos finitos totalmente ordenados son isomorfos. Es fácil ver que como $x \vee y$ y $x \wedge y$ son x o y, dependiendo de si $x \preceq y$ o $y \preceq x$, cualquier isomorfismo de orden entre dos conjuntos totalmente ordenados finitos es un isomorfismo de retículos. En particular, todo retículo totalmente ordenado finito L es isomorfo (y anti-isomorfo) a su dual L^*.

4. Consideremos el retículo $L = (D_6, \mid)$ y el retículo $L' = (\{0,1\} \times \{0,1\}, \leq_{prod})$, donde en $\{0,1\}$ tomamos el orden usual. Entonces L y L' son isomorfos. En efecto basta observar que ambos diagramas de Hasse son iguales, lo único que cambia es la etiqueta de los vértices:



Por lo tanto la función $f : L \to L'$ tal que $f(1) = (0,0)$, $f(2) = (0,1)$, $f(3) = (1,0)$ y $f(6) = (1,1)$ es un isomorfismo de retículos. Más aún, es fácil ver que ambos retículos son isomorfos a sus retículos duales, pues nuevamente el diagrama de Hasse que se obtiene es el mismo.

5. Consideremos los siguientes diagramas de Hasse introducidos en el item 4 de los Ejemplos 1:



El primer diagrama corresponde a cualquier conjunto totalmente ordenado de dos elementos, por ejemplo $(\{0,1\}, \leq)$ o $(D_p, \mid)$ con $p \in \mathbb{N}$ primo. El segundo corresponde a cualquier conjunto totalmente ordenado de tres elementos, por ejemplo $(\{0,1,2\}, \leq)$ o $(D_{p^2}, \mid)$, para $p \in \mathbb{N}$ primo. Todos los retículos que se representan con el primer diagrama son isomorfos entre sí, como lo son todos los retículos que se representan mediante el segundo diagrama. Veremos más adelante que entonces sus productos también son isomorfos entre sí.

Por el momento, elijamos $(D_2, \mid)$ y $(D_4, \mid)$ cuyos diagramas de Hasse son el primero y el segundo respectivamente. Entonces el tercer diagrama corresponde a $(D_2 \times D_4, \preceq_{prod})$, donde, $D_2 \times D_4 = \{(1,1),(1,2),(1,4),(2,1),(2,2),(2,4),(4,1),(4,2),(4,4)\}$ (dejamos como ejercicio colocar las etiquetas en los vértices correspondientes a estos elementos). Por otra parte, el tercer diagrama es el diagrama de Hasse de $(D_{12}, \mid)$. Luego $D_2 \times D_4$ y D_{12} deben ser isomorfos. Para encontrar explícitamente el isomorfismo, basta etiquetar los vértices del diagrama con los elementos de uno y otro conjunto. La función que manda un elemento del primer conjunto en el elemento del segundo conjunto que etiqueta el mismo vértice será un isomorfismo de retículos. Dejamos los detalles para este ejemplo puntual como ejercicio.

Generalizando este último ejemplo, tenemos:

Teorema **6.** *Si $f : L \to L'$ y $g : S \to S'$ son morfismos de retículos, entonces $f \times g : L \times S \to L' \times S'$ definido por $(f \times g)(x, y) = (f(x), g(y))$ es un morfismo de retículos. Si f y g son isomorfismos, entonces $f \times g$ es un isomorfismo.*

Ejercicio **4.** *Demostrar el Teorema 6.*

Definición **5.** *Un retículo L se dice **auto-dual** si L y L^* son isomorfos.*

Ejemplo **6.** El caso de D_6 del ejemplo anterior no es un caso aislado. De hecho, todos los retículos $(D_n, |)$ son autoduales. Si $m \in \mathbb{N}$, consideremos la función $c_m : \mathbb{N} \to \mathbb{N}$ tal que $c_m(k)$ es el cociente de la división de k por m (esto es, $k = c_m(k)m + r_m(k)$, donde $r_m(k)$ es el resto de dividir k por m). Observemos que dados $k, m \in \mathbb{N}$, tendremos que

$$m \mid k \iff k = c_m(k)m.$$

Si ahora tomamos $m \in D_n$, entonces $n = c_m(n)m$. Por lo tanto, $c_m(n)$ también es un divisor de n y

$$c_{c_m(n)}(n) = m.$$

Es decir, $c_m(n) \in D_n$ para cada $m \in D_n$ y podemos considerar entonces la función

$$f : D_n \to D_n, \quad f(m) = c_m(n)$$

(si nos permitimos trabajar con las operaciones de $\mathbb{Q}$, $f(m)$ no es más que n/m). Observemos que

$$f \circ f(m) = f(f(m)) = f(c_m(n)) = c_{c_m(n)}(n) = m.$$

O sea $f \circ f = Id$, y entonces f es biyectiva. Por lo tanto, para ver que f es un isomorfismo de retículos solo falta probar que f es un morfismo de retículos.

Observemos primero que la función f verifica que

$$m \mid k \implies f(k) \mid f(m). \tag{4}$$

En efecto, si $m \mid k$, entonces $k = c_m(k)m$ y como a su vez $k \mid n$, tendremos:

$$n = c_k(n)k = c_k(n)c_m(k)m \implies c_m(n) = c_k(n)c_m(k) \Rightarrow f(m) = f(k)c_m(k)$$

de donde se obtiene (4).

Sean $x, y \in D_n$ y sean $a = mcm(x, y) = x \vee y$, $b = mcd(x, y) = x \wedge y$. Veamos primero que $f(x \vee y) = f(x) \vee^* f(y)$, o lo que es lo mismo, como $\vee^* = \wedge = mcd$, que

$$f(a) = mcd\,(f(x), f(y))\,.$$

Como $a = mcm(x, y)$, entonces $x \mid a$, $y \mid a$ y a divide a cualquier otro múltiplo común de x e y. Luego de (4) tenemos que $f(a) \mid f(x)$ y $f(a) \mid f(y)$, o sea, $f(a)$ es un divisor común de $f(x)$ y $f(y)$. Luego solo nos resta ver que cualquier otro divisor de $f(x)$ y $f(y)$ divide a $f(a)$. Sea entonces d tal que $d \mid f(x)$ y $d \mid f(y)$. Como $f \circ f = Id$, aplicando (4) tendremos que

$$f(f(x)) \mid f(d),\ f(f(y)) \mid f(d) \implies x \mid f(d),\ y \mid f(d).$$

Luego $f(d)$ es un múltiplo común de x e y y por lo tanto $a \mid f(d)$. Aplicando nuevamente (4) y el hecho que $f \circ f = Id$ resultará

$$d = f(f(d)) \mid f(a)$$

como queríamos probar.

La prueba de que $f(b) = mcm(f(x), f(y))$ es análoga y la dejamos como ejercicio.

Ejemplo **7.** Recordemos que $(\mathbb{N}, \leq)$ no es isomorfo a $(\mathbb{N}, \geq)$ y por lo tanto no es auto-dual. Sin embargo $(\mathbb{R}, \leq)$ sí lo es. En efecto, consideremos la función $f : \mathbb{R} \to \mathbb{R}$, $f(x) = -x$. Tenemos que

$$x \leq y \iff -y \leq -x \iff f(x) \geq f(y)$$

de donde $f : (\mathbb{R}, \leq) \to (\mathbb{R}, \geq)$ es un isomorfismo de orden. Como $\mathbb{R}$ es totalmente ordenado, dados $x, y \in \mathbb{R}$ tendremos $x \leq y$ o $y \leq x$. En el primer caso, $x \vee y = y$, y como $-y \leq -x$,

$$f(x \vee y) = f(y) = -y = (-x) \wedge (-y) = f(x) \vee^* f(y).$$

De manera análoga se prueba que $f(x \wedge y) = f(x) \wedge^* f(y)$ y el caso en que $y \leq x$. Por lo tanto f es un isomorfismo de retículos.

Finalizamos esta sección con un resultado que establece como obtener subretículos de un retículo dado a partir de un morfismo de retículos. Dejamos la prueba como ejercicio:

Teorema **7.** *Sean L y S dos retículos y sea $f : L \to S$ un morfismo de retículos. Entonces:*

1. *Si L' es un subretículo de L, entonces $f(L')$ es un subretículo de S.*
2. *Si S' es un subretículo de S entonces $f^{-1}(S')$ es un subretículo de L.*

Ejercicio **5.** *Probar el Teorema 7.*

4. Retículos acotados y complementados

Definición **6.** *Un retículo $(L, \preceq) = (L, \vee, \wedge)$ se dice **acotado** si como conjunto ordenado tiene máximo y mínimo. El máximo de L suele denotarse por $\top$ o por 1 (y suele denorminarse **top**) y el mínimo de L por $\perp$ o 0 (y suele denominarse **bottom**). Denotaremos $(L, \preceq, 1, 0) = (L, \vee, \wedge, 1, 0)$ o $(L, \preceq, \top, \perp) = (L, \vee, \wedge, \top, \perp)$ a un retículo acotado con máximo 1 o $\top$ y mínimo 0 o $\perp$.*

Usualmente suelen reservarse los símbolos $\top$ y $\perp$ cuando tratamos con el orden de L y 1 y 0 cuando tratamos con su estructura algebraica, pero estos símbolos son intercambiables, y muchas veces es útil utilizar los primeros incluso cuando lidiamos con las operaciones $\vee$ y $\wedge$ para evitar confundir los elementos 1 y 0 (definidos en abstracto) con los números 1 y 0 que podrían estar presentes en el conjunto L sin ser su máximo o su mínimo.

En términos generales, tendremos que $(L, \preceq)$ es un retículo acotado si existen $\top, \perp \in L$ tales que

$$\perp \preceq x, \quad x \preceq \top, \ \ \forall x \in L$$

En términos de las operaciones $\vee$ y $\wedge$, $(L, \vee, \wedge)$ es un retículo acotado si existen $0, 1 \in L$ tales que

$$0 \wedge x = 0, \ \ x \vee 1 = 1, \ \ \forall x \in L$$

Ejemplos **8.**

1. Si $X \neq \emptyset$, $(\mathcal{P}(X), \subseteq) = (\mathcal{P}(X), \cup, \cap)$ es un retículo acotado con $1 = \top = X$ y $0 = \perp = \emptyset$.
2. Para cada $n \in \mathbb{N}$, $(D_n, \mid)$ es un retículo acotado con $1 = \top = n$, $0 = \perp = 1$ (en este caso, por ejemplo, es preferible usar las notaciones $\top$ y $\perp$, pues 1 adquiere dos significados distintos). Observemos que $(\mathbb{N}, \mid)$ no es un retículo acotado. Como $x \mid 0$ para cualquier $x \in \mathbb{N}$, muchas veces suele usarse la convención de que $0 \mid 0$. En este caso, el retículo $(\mathbb{N}_0, \mid)$ sí resulta acotado, siendo $\top = 0$.
3. Por el principio de dualidad resulta claro que L es un retículo acotado si y sólo si L^* es un retículo acotado, y valen $\top = \perp^*$, $\perp = \top^*$, o sea, $0^* = 1$ y $1^* = 0$.

Definición **7.** *Sea L un retículo acotado. Dado $a \in L$, un elemento $b \in L$ se denomina un* ***complemento*** *de a, o se dice que a está* ***complementado por*** *b, si*

$$a \vee b = \top, \quad a \wedge b = \perp.$$

Denotamos por $\operatorname{comp}(a) = \{b \in L : b \text{ es un complemento de } a\}$

Un retículo acotado se dice un ***retículo complementado*** *si existe una función*

$$(\cdot)^c : L \to L, \quad a \mapsto a^c$$

tal que para cada $a \in L$, a^c es un complemento de a.

Observación **2.** *Resulta claro (apelando al Axioma de elección) que un retículo es complementado si y sólo si todo elemento admite al menos un complemento, esto es, $\operatorname{comp}(a) \neq \emptyset$ para cada $a \in L$.*

En este caso, el complemento de a no necesariamente es único, y por lo tanto pueden existir distintas funciones $(\cdot)^c$ que hagan de L un retículo complementado.

Observación **3.** *Es inmediato de la conmutatividad de $\vee$ y $\wedge$ que para cada $a \in L$, b es un complemento de a si y sólo si a es un complemento de b.*

Además es claro que $\top$ y $\perp$ (o 1 y 0) son complementos uno del otro.

Teorema **8.** *Sean L y S retículos y $f : L \to S$ un isomorfismo de retículos. Entonces:*

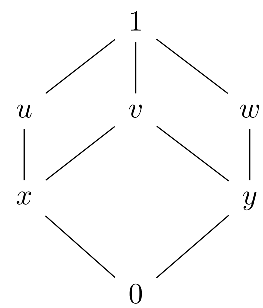
1. L es un retículo acotado si y sólo si S es un retículo acotado.

2. Para cada $x \in L$, $\mathrm{comp}(f(x)) = f(\mathrm{comp}(x))$.

3. L es un retículo complementado si y sólo si S es un retículo complementado.

Ejercicio **6.** *Probar el Teorema 8*

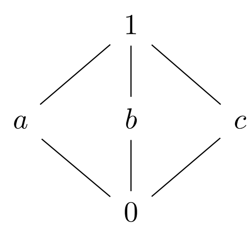
Ejemplos **9.** 1. Consideremos $L = \{0, x, y, u, v, w, 1\}$ con el orden $\preceq$ cuyo diagrama de Hasse es



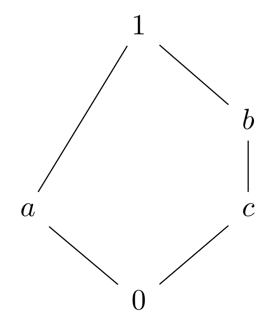
Es fácil ver que $(L, \preceq)$ es un retículo y con mínimo 0 y máximo 1. Tenemos además

$$\mathrm{comp}(x) = \{w\}, \quad \mathrm{comp}(y) = \{u\}, \quad \mathrm{comp}(u) = \{y, w\}, \quad \mathrm{comp}(v) = \emptyset, \quad \mathrm{comp}(w) = \{x, u\}$$

2. Los retículos M_3 y N_5 introducidos en el item 3 de los Ejemplos 1, cuyos diagramas de Hasse son



M_3



N_5

son ambos acotados. Observemos que en M_3 tenemos

$$\mathrm{comp}(0) = \{1\}, \quad \mathrm{comp}(1) = \{0\}, \quad \mathrm{comp}(a) = \{b, c\}, \quad \mathrm{comp}(b) = \{a, c\}, \quad \mathrm{comp}(c) = \{a, b\}$$

y en M_5

$$\mathrm{comp}(0) = \{1\}, \quad \mathrm{comp}(1) = \{0\}, \quad \mathrm{comp}(a) = \{b, c\}, \quad \mathrm{comp}(b) = \{a\}, \quad \mathrm{comp}(c) = \{a\}.$$

Por lo tanto M_3 y N_5 son retículos complementados.

3. Sea $X \neq \emptyset$. El retículo acotado $(\mathcal{P}(X), \cup, \cap, X, \emptyset)$ es complementado. En efecto, dado $B \in \mathcal{P}(X)$, $B^c = X - B$ verifica $B \cup B^c = X (= 1)$ y $B \cap B^c = \emptyset (= 0)$.

Observemos que existen muchos subconjuntos de X que verifican estas dos condiciones por separado, pero B^c es el único que las satisface simultáneamente. La función $(\cdot)^c$ que a cada subconjunto de X le asocia su complemento es en este caso la única que hace de $(\mathcal{P}(X), \subseteq)$ un retículo complementado.

4. Si L es un retículo acotado totalmente ordenado, los únicos elementos que admiten un complemento son 0 y 1. En efecto, si existe $x \in L$ tal que $x \neq 0, 1$, cualquier elemento $y \in L$ verifica $x \preceq y$ o $y \preceq x$. En el primer caso, resultará $x \wedge y = x \neq 0$ y en el segundo $x \vee y = x \neq 1$.

5. Consideremos el retículo acotado $(D_n, mcm, mcd, n, 1)$ para $n \in \mathbb{N}$ fijo. Si $n = p$ es un número primo, D_p es trivialmente un conjunto complementado, dado que $\top = p$ y $\bot = 1$ son los únicos elementos de D_p y se complementan mutuamente. Si $n = p^k$ para p primo y $k \in \mathbb{N},\ k \geq 2$, entonces D_{p^k} no es complementado, dado que es un conjunto totalmente ordenado con al menos tres elementos.

   Analicemos ahora qué ocurre para el resto de los D_n. Por el Teorema Fundamental de la Aritmética podemos descomponer a n en factores primos. Supongamos que

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

   es una descomposición en factores primos de n. Si x es un divisor de n, en su descomposición en factores primos podrán aparecer sólo los primos p_i elevados a un exponente menor o iual a n_i. Supongamos que existe al menos un exponente, digamos $n_{i_0} \geq 2$ y sea $x = p_1 p_2 \cdots p_k \neq n$. Observemos que como x ya tiene en su descomposición todos los factores primos posibles que conforman los elementos de D_n, no existe ningún $y \neq 1$ tal que $mcd(x, y) = 1$ (pues si $y \neq 1$ es divisor de n, debe compartir al menos un factor primo con x). Es decir, el único elemento y tal que $x \wedge y = 1$ es $y = 1$. Pero en este caso, $x \vee y = x \neq n$, con lo cual x no tiene ningún complemento en D_n. Concluimos que D_n no es un retículo complementado.

   Luego el único caso que nos queda analizar es aquel en que $n = p_1 p_2 \cdots p_k$ donde los primos p_i son todos distintos. En este caso es fácil ver que todo elemento $x \in D_n$ es el producto de algunos de estos primos, y un complemento de x es el producto de los primos que no aparecen en la descomposición de x. Formalmente, si ponemos $I = \{1, 2, \ldots, n\}$ y

$$x = \prod_{j \in J} p_j$$

   para algún $J \subseteq I$, entonces $y = \displaystyle\prod_{j \in I - J} p_j$ es un complemento de x En efecto, x e y son coprimos, puesto que no tienen factores primos en común. Luego $mcd(x, y) = 1$ y $mcm(x, y) = xy = n$.

   Veremos en los ejercicios que en este caso, $(D_n, |)$ es isomorfo a $(\mathcal{P}(X), \subseteq)$, donde $X = \{p_1, \ldots, p_k\}$.

Ejercicio **7.** *Analizar si las propiedades de ser acotado y/o complementado se heredan a subretículos y a productos de retículos. Esto es, sean L un retículo y L' un subretículo de L.*

1. *Si L es acotado, ¿es L' necesariamente acotado?*

2. *Si L es complementado ¿es L' complementado?*

3. *Si tanto L como S son retículos acotados, ¿es acotado $(L \times S, \preceq_{prod})$?*

4. *Si tanto L como S son retículos complementados, ¿es complementado $(L \times S, \preceq_{prod})$?*

5. Retículos distributivos

Definición **8.** *Sea $(L, \preceq) = (L, \vee, \wedge)$ un retículo. Decimos que L es un **retículo distributivo** si para cada $x, y, z \in L$ se verifican:*

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \tag{5}$$

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \tag{6}$$

Ejemplos **10.**

1. Si $X \neq \emptyset$, $(\mathcal{P}(X), \cup, \cap)$ es un retículo distributivo, pues las operaciones $\cup$ y $\cap$ verifican las propiedades (5) y (6).

2. Si $(L, \vee, \wedge)$ es un retículo distributivo, es inmediato que su dual $L^* = (L, \wedge, \vee)$ es un retículo distributivo.

3. La propiedad de ser distributivo es hereditaria, esto es, si L' es un subretículo de un retículo distributivo, entonces L' es un retículo distributivo. Esto es inmediato dado que las operaciones de L' no son más que las operaciones $\vee$ y $\wedge$ de L restringidas a L'.

Ejercicio **8.** *Probar que si L y S son retículos distributivos, entonces $(L \times S, \preceq_{prod})$ es un retículo distributivo.*

Teorema **9.** *Sean L y S retículos y sea $f : L \to S$ un isomorfismo de retículos. Entonces L es un retículo distributivo si y sólo si S es un retículo distributivo.*

Ejercicio **9.** *Probar el Teorema 9.*

Ejemplo **11.** Consideremos el retículo $(D_n, |)$ para $n = p_1 p_2 \cdots p_k$ con $p_1, \ldots, p_k \in \mathbb{N}$ números primos. Entonces si $X = \{p_1, \ldots, p_k\}$, $(D_n, |)$ es un retículo isomorfo a $(\mathcal{P}(X), \subseteq)$. Como este último es distributivo, resulta que $(D_n, |)$ es distributivo. Dejamos como ejercicio probar que en realidad todos los retículos $(D_n, |)$ son distributivos. Observemos que para ello hay que probar que dados $x, y, z \in D_n$,

$$mcm(x, mcd(y, z)) = mcd(mcm(x, y), mcm(x, z))$$

$$mcd(x, mcm(y, z)) = mcm(mcd(x, y), mcd(x, z)).$$

Resulta evidente que esta prueba es más complicada que apelar al isomorfismo anterior, pero hasta el momento no hemos visto que D_n sea isomorfo a ningún retículo distributivo para un n genérico. Veremos más adelante un criterio general que nos permitirá dar una prueba relativamente simple para todos los casos.

Veremos en el siguiente resultado que para probar que un retículo es distributivo, basta considerar sólo una de las propiedades (5) o (6) dado que son equivalentes:

Teorema **10.** *Si un retículo L satisface una de las propiedades (5) o (6) entonces satisface la otra, y por lo tanto es distributivo.*

Demostración. Supongamos primero que L satisface la ecuación (6) y veamos que entonces debe satisfacer (5). En efecto,

$$\begin{aligned}
(x \vee y) \wedge (x \vee z) &= ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) && \text{[por (6)]}\\
&= x \vee (z \wedge (x \vee y)) && \text{[conmutatividad, absorción]}\\
&= x \vee ((z \wedge x) \vee (z \wedge y)) && \text{[por (6)]}\\
&= (x \vee (z \wedge x)) \vee (z \wedge y) && \text{[asociatividad]}\\
&= x \vee (y \wedge z) && \text{[conmutatividad, absorción]}
\end{aligned}$$

Observemos que en el dual L^* las ecuaciones (5) y (6) se intercambian. Luego, como el dual de un retículo distributivo es distributivo, la prueba anterior aplicada a L^* prueba que (5) implica (6). $\square$

Ejemplo **12.** Todo conjunto totalmente ordenado es un retículo distributivo. En efecto, si $(L, \preceq)$ es totalmente ordenado,

$$x \wedge y = \max\{x, y\} = \begin{cases} x \text{ si } y \preceq x \\ y \text{ si } x \preceq y \end{cases}, \qquad x \vee y = \min\{x, y\} = \begin{cases} x \text{ si } x \preceq y \\ y \text{ si } y \preceq x \end{cases}$$

Para ver que L es un retículo distributivo, por el Teorema 10 basta probar que se verifica la ecuación (5), que en este caso es

$$\max\{x, \min\{y, z\}\} = \min\{\max\{x, y\}, \max\{x, z\}\}$$

Si $x, y, z \in L$, son comparables dos a dos así que necesariamente debe verificarse $x \preceq y \preceq z$ o alguna de sus permutaciones. Supondremos que valen estas relaciones y dejamos las otras como ejercicio (hay que analizar 9 casos). Tenemos entonces:

$$\max\{x, \min\{y, z\}\} = \max\{x, y\} = y, \quad \min\{\max\{x, y\}, \max\{x, z\}\} = \min\{y, z\} = y$$

como queríamos probar.

En particular, los conjuntos numéricos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ con la relación $\leq$ son retículos distributivos y los retículos $(D_n, \mid)$ con $n = p^k$, p primo, $k \in \mathbb{N}$, son distributivos.

Ejemplo **13. Los retículos M_3 y N_5.** Los retículos M_3 y N_5 (ver item 3 de los Ejemplos 1) no son distributivos.

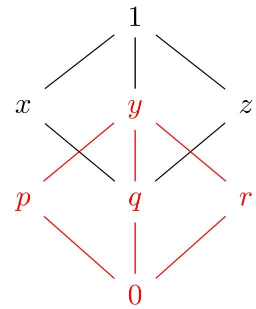
En M_3 tenemos por ejemplo

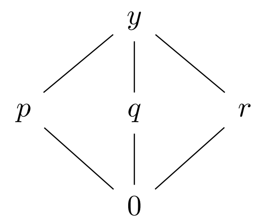
$$a \wedge (b \vee c) = a \wedge 1 = a, \quad (a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0$$

y en N_5,

$$b \wedge (a \vee c) = b \wedge 1 = b, \quad (b \wedge a) \vee (b \wedge c) = 0 \vee c = c.$$

Ejemplo **14.** Consideremos el retículo $L = \{0, p, q, r, x, y, z, 1\}$ cuyo diagrama de Hasse es el siguiente (dejamos como ejercicio verificar que se trata efectivamente de un retículo):



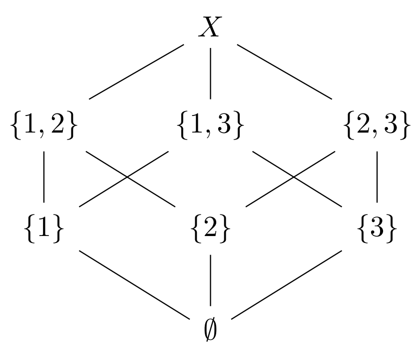


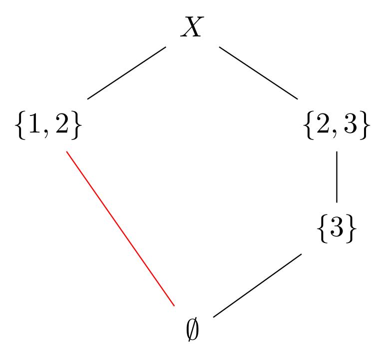
Es fácil verificar que $L' = \{0, p, q, r, y\}$ es un subretículo de L, claramente isomorfo a M_3. Entonces, por el Teorema 9, L' no es distributivo. Como la distributividad es una propiedad hereditaria en un retículo (todo subretículo de un retículo distributivo es distributivo) concluimos que L no puede ser distributivo.

Por esta misma razón, cualquier retículo que contenga un subretículo isomorfo a M_3 o N_5 no será distributivo. La recíproca de esta proposición también es válida y constituye un resultado muy importante cuya prueba escapa a nuestros objetivos:

Teorema **11** (Teorema M_3-N_5)**.** *Un retículo es distributivo si y sólo si no contiene subretículos isomorfos a M_3 o a N_5.*

Ejemplo **15.** Consideremos $X = \{1, 2, 3\}$ y el retículo $L = (\mathcal{P}(X), \subseteq)$. Sea $L' = \{\emptyset, \{3\}, \{1, 2\}, \{2, 3\}, X\}$.





L es un retículo distributivo, y L' es un retículo isomorfo a M_5. ¿Por qué este ejemplo no contradice al Teorema $M_3 - N_5$? Simplemente porque L' NO es un subretículo de L.

Ejemplos **16.** Aplicaremos el Teorema $M_3 - N_5$ para probar que los conjuntos totalmente ordenados y $(\mathbb{N}, |\,)$ (y en consecuencia todos los retículos $(D_n, |\,)$) son distributivos.

1. Si L es totalmente ordenado y L' es un subretículo de L, entonces L' es totalmente ordenado. Como ni M_3 ni N_5 son totalmente ordenados, no pueden ser isomorfos a L'.

2. Supongamos que $(\mathbb{N}\ |\,)$ tiene un subretículo isomorfo a M_3. Deberán existir entonces $a, b, c, u, v \in \mathbb{N}$ tales

que si $L' = \{a, b, c, u, v\}$, el diagrama de Hasse de $(L', |\,)$ es

$$\begin{tikzcd}[arrows=dash]
 & v & \\
a \arrow[ur] & b \arrow[u] & c \arrow[ul] \\
 & u \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

En este caso tendremos que

$$mcd(a, b) = mcd(a, c) = mcd(b, c) = u, \quad mcm(a, b) = mcm(a, c) = mcm(b, c) = v$$

Por lo tanto, existirán $k_1, k_2, k_3 \in \mathbb{N}$ tales que

$$a = k_1 u, \; b = k_2 u, \; c = k_3 u.$$

Por otra parte, es fácil ver a partir del Corolario 21 de la Unidad 2, que

$$ab = mcm(a, b)mcd(a, b)$$

Luego

$$k_1 k_2 u^2 = uv \implies v = k_1 k_2 u.$$

De manera análoga, tendremos que $v = k_1 k_3 u$, $v = k_2 k_3 u$. Pero entonces

$$k_1 k_2 u = k_1 k_3 u \implies k_2 = k_3 \implies b = c$$

lo cual es absurdo. Concluimos que $(\mathbb{N}, |\,)$ no puede tener ningún subretículo isomorfo a M_3. De manera similar (lo dejamos como ejercicio), $(\mathbb{N}, |\,)$ no puede tener ningún subretículo isomorfo a N_5, y por lo tanto $(\mathbb{N}, |\,)$ es distributivo.

Como cada $(D_n, |\,)$ es un subretículo de $(\mathbb{N}, |\,)$, todos estos retículos resultan distributivos.

Teorema **12.** *Sea L un retículo distributivo y acotado. Entonces todo elemento de L tiene a lo sumo un elemento complementario.*

Demostración. Sea $x \in L$ y supongamos que x tiene dos elementos complementarios y, y'. Esto es, existen $y, y' \in L$ tales que

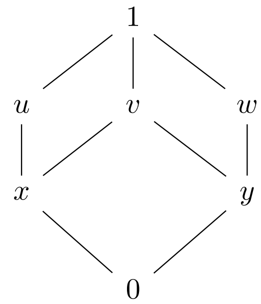
$$x \vee y = x \vee y' = 1, \quad x \wedge y = x \wedge y' = 0.$$

Además, para cada $z \in L$ se verifican $z \vee 1 = 1$, $z \wedge 1 = z$, $z \wedge 0 = 0$, $z \vee 0 = z$. Luego, como L es distributivo,

$$\begin{aligned} y &= y \wedge 1 = y \wedge (x \vee y') = (y \wedge x) \vee (y \wedge y') \\ &= 0 \vee (y \wedge y') = y \wedge y' \end{aligned}$$

de donde $y \preceq y'$. Con el mismo argumento, $y' = y' \wedge y$ y por lo tanto $y' \preceq y$. Luego $y = y'$. $\square$

Ejemplo **17.** Consideremos $L = \{0, x, y, u, v, w, 1\}$ con el orden $\preceq$ cuyo diagrama de Hasse es



(ver el item 1 de los Ejemplos 9). Como $\mathrm{comp}(u) = \{y, w\}$, por el Teorema 12, L no puede ser distributivo.

Finalizamos esta sección introduciendo una condición más relajada de la distributividad en un retículo:

Definición **9.** *Un retículo* $(L, \preceq) = (L, \vee, \wedge)$ *se dice* ***modular*** *si para cada* $a, b, c \in X$ *se verifica:*

$$a \preceq c \implies a \vee (b \wedge c) = (a \vee b) \wedge c. \tag{7}$$

Observación **4.** *Observemos que por la propiedad de absorción, la condición* (7) *se verifica trivialmente si* $a = c$. *Luego para probar modularidad, bastará demostrar que vale* (7) *cuando* $a \prec c$.

Es fácil ver (lo probaremos en la práctica) que todo subretículo de un retículo modular es modular, y que si $f : L \to L'$ *es un isomorfismo de retículos, entonces* L *es modular si y sólo si* L' *es modular.*

Lema **13.** *Todo retículo distributivo es modular.*

Demostración. Sean $a, b, c \in X$ tales que $a \preceq c$. Como X es distributivo,

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

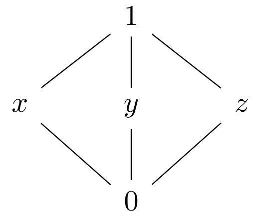
Pero como $a \preceq c$, $a \vee c = c$, con lo cual

$$a \vee (b \wedge c) = (a \vee b) \wedge c$$

como queríamos ver. □

Veremos en el siguiente ejemplo que la recíproca del Lema 13 es falsa:

Ejemplo **18.** Consideremos el retículo M_3,



Supongamos que $c = 1$. Para cualquier $m \in M_3$, $m \wedge c = m$, luego se verifica trivialmente la condición

$$a \vee (b \wedge c) = a \vee b = (a \vee b) \wedge c$$

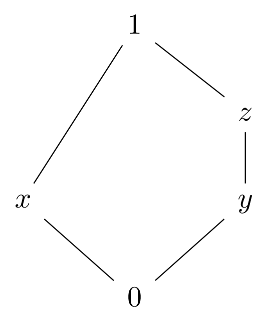
De manera análoga, si $a = 0$, para cualquier $m \in M_3$ $a \vee m = m$, con lo cual

$$(a \vee b) \wedge c = b \wedge c = a \vee (b \wedge c)$$

Si ahora elegimos $a, c \in M_3$ tales que $a \prec c$, tendremos necesariamente que $c = 1$ o $a = 0$. Luego M_3 es modular.

Sin embargo, hemos visto que M_3 no es distributivo.

Ejemplo **19.** Consideremos ahora el retículo N_5:



En este caso, tomando $a = y$, $c = z$ tenemos que $a \prec c$ y si tomamos $b = x$ tendremos que

$$(a \vee b) \wedge c = (y \vee x) \wedge z = 1 \wedge z = z, \quad a \vee (b \wedge c) = y \vee (x \wedge z) = y \vee 0 = y \neq z$$

luego N_5 no es modular (ni distributivo).

Tenemos para retículos modulares un resultado similar al Teorema 11, que no demostraremos. Observemos sin embargo que como todo subretítulo de un retículo modular es modular (ejercicio) si L es un retículo que tiene un subretículo isomorfo a M_3 entonces L no puede ser modular (y por lo tanto tampoco puede ser distributivo, aunque esto ya lo sabíamos).

Teorema **14.** *Un retículo L es modular si y sólo si no contiene ningún subretículo isomorfo a M_3.*

6. Álgebras de Boole

Las álgebras de Boole representan retículos que tienen todas las propiedades que estudiamos en esta Unidad:

Definición **10.** *Un retículo B se denomina* ***un álgebra de Boole*** *si es acotado, complementado y distributivo.*

Observación **5.** *Por el Teorema 12, todo elemento de un álgebra de Boole tiene un único complemento, y por lo tanto hay una única función complemento $(\cdot)^c : B \to B$ bien definida.*

Ejemplos **20.** A partir de los ejemplos que analizamos a lo largo de esta sección resultan inmediatos:

1. Si $X \neq \emptyset$, $(\mathcal{P}(X), \subseteq)$ es un álebra de Boole (con mínimo $0 = \emptyset$, máximo $1 = X$ y $(\cdot)^c$ la función que a cada $A \subset X$ le asigna su complemento).

2. $(D_n, |)$ es un retículo acotado y distributivo, pero vimos en el item 1 de los Ejemplos 9 que D_n es complementado si y sólo si $n = p_1 \cdots p_k$ es el producto de k números primos distintos. Por lo tanto sólo en este caso $(D_n, |)$ será un álgebra de Boole, que como retículo es isomorfo $(\mathcal{P}(X), \subseteq)$, con $X = \{p_1, \cdots, p_n\}$.

3. Si L es un conjunto totalmente ordenado, L es un retículo acotado y distributivo, pero no es complementado a menos que $L = \{0, 1\}$. En este caso es inmediato verificar que L es (isomorfo a) $(D_p, |)$ con p primo, que a su vez es (isomorfo a) $(\mathcal{P}(\{1\}), \subseteq)$.

Como las álgebras de Boole tienen más estructura que un simple retículo, necesitamos dar una definición más adecuada de un morfismo de álgebras de Boole, es decir, no solo necesitamos que se preserve su estructura de retículo, sino que deben preservarse las otras propiedades que la definen:

Definición **11.** *Sean $(B, \cup, \cap, 1, 0)$ y $(B', \cup, \cap, 1', 0')$ dos álgebras de Boole. Una función $f : B \to B'$ es un* ***morfismo de álgebras de Boole*** *si f es un morfismo de retículos tal que $f(0) = 0'$, $f(1) = 1'$, y $f(x^c) = x^c$ para cada $x \in B$.*

f es un ***isomorfismo*** *de álgebras de Boole si tanto f como f^{-1} son morfismos de álgebras de Boole.*

Es interesante notar que un isomorfismo de retículos ya verifica las propiedades de ser morfismo de álgebras de Boole, y por lo tanto isomorfismo de retículo e isomorfismo de álgebras de Boole son la misma cosa. Más precisamente:

Teorema **15.** *Sean B y B' retículos isomorfos. Entonces B es un álgebra de Boole si y sólo si B' es un álgebra de Boole, y cualquier isomorfismo de retículos $f : B \to B'$ mapea el máximo de B en el máximo de B', el mínimo de B en el mínimo de B' y el complemento x^c de cualquier elemento $x \in B$ en el complemento $f(x)^c$ de $f(x) \in B'$. Es decir, f es un isomorfismo de álgebras de Boole si y sólo si f es un isomorfismo de retículos.*

Ejercicio **10.** *Probar el Teorema 15.*

En el siguiente resultado reunimos las propiedades básicas de un álgebra de Boole:

Teorema **16.** *Sea B un álgebra de Boole con mínimo 0, máximo 1 y función complemento $(\cdot)^c$. Entonces:*

1. *$0^c = 1$ y $1^c = 0$;*

2. *para cada $x \in B$, $(x^c)^c = x$;*

3. *valen las* ***leyes de De Morgan****, esto es, para cada $x, y, z \in B$,*

$$(x \vee y)^c = x^c \wedge y^c \tag{8}$$

$$(x \wedge y)^c = x^c \vee y^c. \tag{9}$$

Demostración. La propiedad 1 es trivial, y es común a todos los retículos acotados. Para probar 2, observemos que x verifica $x \vee x^c = 1$ y $x \wedge x^c = 0$, y por la conmutatividad de $\vee$ y $\wedge$, resulta $x^c \vee x = 1$ y $x^c \wedge x = 0$. Luego, por definición de complemento, x es el complemento de x^c, es decir, $(x^c)^c = x$.

Veamos ahora que vale 3. Probemos sólo (8)

Para ver que el complemento de $x \vee y$ es $x^c \wedge y^c$, debemos probar que $(x \vee y) \vee (x^c \wedge y^c) = 1$ y que $(x \vee y) \wedge (x^c \wedge y^c) = 0$. Ahora:

$$\begin{aligned}
(x \vee y) \vee (x^c \wedge y^c) &= ((x \vee y) \vee x^c) \wedge ((x \vee y) \vee y^c) && \text{[por ser } B \text{ distributivo]} \\
&= ((x^c \vee x) \vee y) \vee (x \vee (y \vee y^c)) && \text{[conmutatividad, asociatividad de } \vee\text{]} \\
&= (1 \vee y) \vee (x \vee 1) && \text{[definición de complemento]} \\
&= 1 \vee 1 = 1
\end{aligned}$$

La prueba de que $(x \vee y) \wedge (x^c \wedge y^c) = 0$ es análoga y se deja como ejercicio, así como la prueba de 9. $\square$

Las propiedades de las álgebras de Boole del Teorema 16 son análogas a las propiedades de las operaciones unión, intersección y complemento de la teoría de conjuntos. Más aún, todos los ejemplos que vimos de álgebras de Boole son isomorfos a algún $(\mathcal{P}(X), \subseteq)$ para un X adecuado. Cabe preguntarse si todas las álgebras de Boole son de este tipo.

La respuesta es afirmativa (aunque no lo probaremos en este curso) si $(L, \preceq)$ es un álgebra de Boole finita. Es falsa en el caso que el cardinal de L sea infinito, como veremos en el próximo ejemplo:

Ejemplo **21.** Consideremos los conjuntos

$$\mathcal{P}_f(\mathbb{N}) = \{A \subset \mathbb{N} : \#A < \infty\}, \quad \mathcal{P}_{cof}(\mathbb{N}) = \{A \subset \mathbb{N} : \#A^c < \infty\}.$$

$\mathcal{P}_f(\mathbb{N})$ es el conjunto de partes finitas de $\mathbb{N}$ y $\mathcal{P}_{cof}(\mathbb{N})$ es el conjunto de partes *cofinitas* de $\mathbb{N}$, es decir, de aquellos subconjuntos tal que su complemento es finito.

Sea $B = \mathcal{P}_f(\mathbb{N}) \cup \mathcal{P}_{cof}(\mathbb{N})$. Entonces $B \subsetneq \mathcal{P}(\mathbb{N})$ (pues por ejemplo si A es el conjunto de números pares, $A \notin \mathcal{P}_f(\mathbb{N})$ y $A \notin \mathcal{P}_{cof}(\mathbb{N})$). Veamos que $(B, \cup, \cap, X, \emptyset)$ es un álgebra de Boole.

Comencemos probando que $(B, \cup, \cap)$ es un subretículo de $(\mathcal{P}(\mathbb{N}), \cup, \cap)$. En efecto, si $C, D \in \mathcal{P}_f(\mathbb{N})$, entonces $C \cup D$ y $C \cap D$ son finitos y por lo tanto están en $\mathcal{P}_f(\mathbb{N}) \subset B$. Si $C, D \in \mathcal{P}_{cof}(\mathbb{N})$, entonces $C^c \cap D^c$ Y $C^c \cup D^c$ son finitos, y entonces (por las Leyes de De Morgan) $C \cup D \in \mathcal{P}_{cof}(\mathbb{N})$, $C \cap D \in \mathcal{P}_{cof}(\mathbb{N})$. Finalmente, es fácil ver que si $C \in \mathcal{P}_f(\mathbb{N})$ y $D \in P_{cof}(\mathbb{N})$, entonces

$$C \cup D = D \cup C \in \mathcal{P}_{cof}(\mathbb{N}), \quad C \cap D = D \cap C \in \mathcal{P}_f(\mathbb{N})$$

En cualquier caso, tenemos que si $C, D \in B$, entonces $C \cup D \in B$ y $C \cap D \in B$ como queríamos ver.

Recordemos que un subretículo de un retículo acotado no necesariamente es acotado, y lo mismo ocurre con un subretículo de un retículo complementado. En este caso, $\emptyset \in \mathcal{P}_f(\mathbb{N})$ y $X \in \mathcal{P}_{cof}(\mathbb{N})$, con lo cual B resulta acotado. Además, es fácil ver tomando casos como antes, que si $D \in B$, entonces $D^c \in B$.

Concluimos que B es un retículo acotado y complementado, que además es distributivo por ser un subretículo de un retículo distributivo. Luego B es un álgebra de Boole.

Para ver que B no puede ser isomorfa a $(\mathcal{P}(X), \subseteq)$ para ningún conjunto X, basta analizar su cardinal. En efecto, es un hecho bien conocido (aunque difícil de probar) que $\mathcal{P}_f(\mathbb{N})$ y $\mathcal{P}_{cof}(\mathbb{N})$ son conjuntos infinitos numerables, es decir, su cardinal es $\aleph_0$. Pero no existe ningún conjunto X tal que el cardinal de $\mathcal{P}(X)$ sea $\aleph_0$, pues si X es finito, entonces $\#\mathcal{P}(X) = 2^{\#X} \in \mathbb{N}$ y si X es infinito, debe ser al menos infinito numerable, es decir, su cardinal debe ser al menos $\aleph_0$, y como es bien sabido, el cardinal de $\mathcal{P}(X)$ será al menos $\aleph_1$.