Capítulo 2

Conjuntos ordenados. Retículos y álgebras de Boole.

2.1. Conjuntos ordenados.

En este capítulo vamos a estudiar el concepto de retículo. Hay dos caminos para llegar a esta estructura. Uno es mediante un conjunto con dos operaciones binarias que satisfacen una serie de axiomas. El otro es a partir del concepto de conjunto ordenado. Nosotros aquí hemos adoptado el segundo. Si enriquecemos la estructura de retículo con unos axiomas adicionales obtenemos lo que se conoce como *Álgebra de Boole*. Analizaremos su estructura, y llegaremos a que en el caso finito, las álgebras de Boole tiene una forma muy particular. Estudiaremos el álgebra de Boole de las funciones booleanas, y el teorema de estructura nos conducirá a las formas normales. Terminaremos viendo algunas aplicaciones de las álgebras de Boole al diseño de circuitos lógicos.

Definición 5. *Sea X un conjunto, y $\leq$ una relación binaria en X. Se dice que $\leq$ es una relación de orden si se verifican las siguientes propiedades.*

Reflexiva: $x \leq x$ para todo $x \in X$.

Antisimétrica: Si $x \leq y$ e $y \leq x$ entonces $x = y$.

Transitiva: Si $x \leq y$ e $y \leq z$ entonces $x \leq z$.

Si X es un conjunto en el que tenemos definida una relación de orden $\leq$, se dice que $(X, \leq)$ es un conjunto ordenado (o, si está claro cual es la relación $\leq$ se dice simplemente que X es un conjunto ordenado).

Si $\leq$ es una relación de orden en X que satisface la propiedad adicional de que dados $x, y \in X$ entonces $x \leq y$ ó $y \leq x$, se dice entonces que $\leq$ es una relación de orden total, y que $(X, \leq)$ (o X) es un conjunto totalmente ordenado (en ocasiones, para destacar que $(X, \leq)$ es una relación de orden, pero que no es total se dice que $\leq$ es una relación de orden parcial y que $(X, \leq)$ es un conjunto parcialmente ordenado).

Ejemplo 2.1.1.

1. *El conjunto de los números naturales, con el orden natural ($m \leq n$ si existe $k \in \mathbb{N}$ tal que $n = m+k$) es un conjunto totalmente ordenado. De la misma forma, también lo son $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$ y $(\mathbb{R}, \leq)$.*

2. *Dado un conjunto X, entonces $\mathcal{P}(X)$, con el orden dado por la inclusión es un conjunto ordenado. Si X tiene más de un elemento, este orden no es total, pues dados $x, y \in X$ distintos se tiene que $\{x\} \not\subseteq \{y\}$ y $\{y\} \not\subseteq \{x\}$.*

3. *En el conjunto de los números naturales, la relación de divisibilidad es una relación de orden que no es total. Esta relación viene dada por* $a|b$ *si existe* $c \in \mathbb{N}$ *tal que* $b = a \cdot c$ *(compara con la relación de orden natural). Sin embargo, en el conjunto de los números enteros esta relación no es de orden pues no es antisimétrica, ya que* $2|-2$, $-2|2$ *y sin embargo* $2 \neq -2$.

4. *Para cualquier número natural* n *consideramos el conjunto*

$$D(n) = \{m \in \mathbb{N} : m|n\}$$

Entonces $(D(n), |)$ *es un conjunto (parcialmente) ordenado.*

5. *Sea* $(X, \leq)$ *es un conjunto ordenado, e* Y *un subconjunto de* X*. Definimos en* Y *el orden* $x \preceq y$ *si* $x \leq y$ *(vistos como elementos de* X*). Entonces,* $(Y, \preceq)$ *es un conjunto ordenado. De ahora en adelante, el orden en* Y *lo denotaremos igual que en* X*.*

Un ejemplo de esto último podría ser el caso de los divisores de un número natural n*.*

Si $(X, \leq)$ *es un conjunto totalmente ordenado, entonces, para cualquier* $Y \subseteq X$ *se tiene que* $(Y, \leq)$ *es un conjunto totalmente ordenado.*

La definición de conjunto ordenado puede hacerse también a partir de la noción de *orden estricto*.

Definición 6. *Sea* X *un conjunto, y* $<$ *una relación binaria en* X*. Se dice que* $<$ *es un orden estricto si se verifican las siguientes propiedades:*

Antirreflexiva Para cualquier $x \in X$ *se tiene que* $x \not< x$.

Transitiva Si $x < y$ *e* $y < z$ *entonces* $x < z$.

Es fácil comprobar que si $\leq$ es una relación de orden en un conjunto X, entonces si definimos

$$x < y \text{ si } x \leq y \text{ y } x \neq y$$

se tiene que $<$ es una relación de orden estricto en X.

De la misma forma, si $<$ es una relación de orden estricto en X entonces la relación siguiente:

$$x \leq y \text{ si } x < y \text{ o } x = y$$

es una relación de orden en X.

Vemos entonces que los conceptos de *relación de orden* y *relación de orden estricto* son equivalentes, pues dada una relación de orden tenemos determinada una relación de orden estricto y viceversa. Además, los caminos para pasar de orden a orden estricto, y de orden estricto a orden, son uno el inverso del otro.

A continuación vamos a construir un grafo (dirigido) asociado a una relación de orden. Aún cuando los grafos serán estudiados con posterioridad, la representación de una relación de orden mediante este grafo ayuda a visualizar mejor el orden dado.

Definición 7. *El diagrama de Hasse de un conjunto ordenado* $(X, \leq)$ *es un grafo dirigido cuyos vértices son los elementos de* X*, y existe un lado de* x *a* y *si* $x < y$ *y no existe* z *tal que* $x < z < y$*.*

El diagrama de Hasse está definido para cualquier conjunto ordenado. Sin embargo, en general dicho diagrama no permite recuperar el orden. Por ejemplo, en el caso del conjunto $(\mathbb{R}, \leq)$, dado cualquier $x \in \mathbb{R}$ no existe ningún $y \in \mathbb{R}$ que esté conectado a x por algún lado.

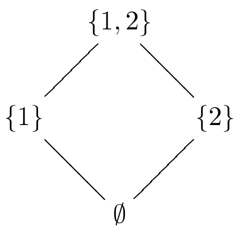
Sin embargo, si el conjunto X es finito, entonces dados $x, y \in X$ se tiene que $x \leq y$ si $x = y$ o existe algún camino que parta de x y termine en y.

Una forma habitual de representar el diagrama de Hasse es dibujar los lados como líneas ascendentes, lo que implica colocar los vértices de forma apropiada.

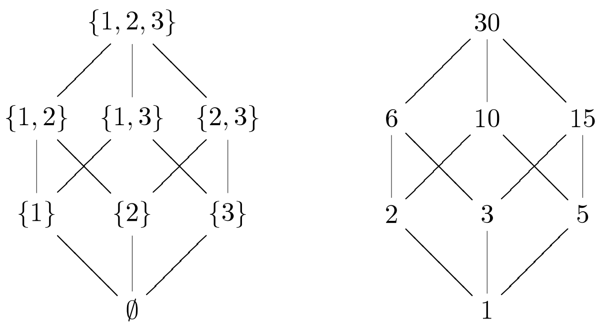
Ejemplo 2.1.2.

1. *El diagrama de Hasse del conjunto* $(\mathbb{N}, \leq)$ *sería*

2. *Consideramos el conjunto ordenado* $(\mathcal{P}(\{1,2\}, \subseteq)$. *Entonces el diagrama de Hasse sería:*

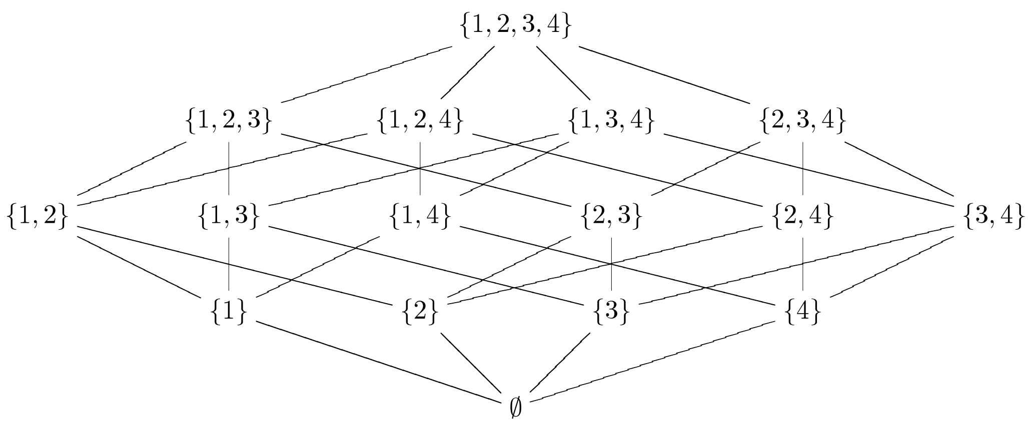


3. *Vamos a representar los diagramas de Hasse de los conjuntos ordenados* $\mathcal{P}(\{1,2,3\})$ *y* $D(30)$.



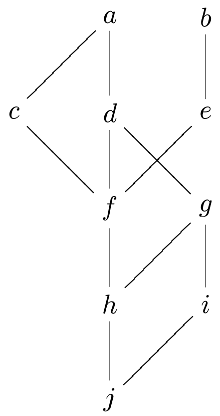
Observa como la estructura de conjunto ordenado es igual en ambos casos.

4. *Vamos a representar el diagrama de Hasse de* $\mathcal{P}(\{1,2,3,4\})$.



Prueba a dibujar el diagrama de Hasse de los divisores de 210 y compáralo con este último.

5. *Si tenemos un grafo dirigido que no contiene caminos cerrados, entonces podemos definir un orden en el conjunto de los vértices.* $x \leq y$ *si* $x = y$ *o existe un camino con inicio* x *y fin* y*. Si en el grafo no hay caminos entre dos vértices adyacentes, entonces el grafo es el diagrama de Hasse de un conjunto ordenado.*



tenemos definido un orden en el conjunto $X = \{a, b, c, d, e, f, g, h, i\}$*. Con este orden se tiene, por ejemplo que,*

$h \leq e$*, pues tenemos un camino* $h - f - e$ *que empieza en* h *y termina en* e*.*

$i \leq a$*, pues el camino* $i - g - d - a$ *empieza en* i *y termina en* a*.*

$i \not\leq e$*, pues ningún camino empieza en* i *y termina en* e*.*

Definición 8. *Sea* $(X, \leq)$ *un conjunto ordenado.*

1. *Un elemento* $x \in X$ *se dice que es maximal, si no existe* $y \in X$ *tal que* $x \leq y$ *y* $x \neq y$*.*

2. *Un elemento* $x \in X$ *se dice que es máximo, si para todo* $y \in X$ *se verifica que* $y \leq x$*.*

De la misma forma se puede definir lo que es un elemento minimal y lo que es un mínimo.

Ejemplo 2.1.3. *En el último conjunto ordenado del ejemplo anterior se tiene que* a *y* b *son elementos maximales, pues no hay ningún elemento que sea mayor que ellos. Sin embargo, el conjunto* X *no tiene máximo.*

El elemento j *es un elemento minimal, y además es mínimo.*

En el conjunto de los divisores de 30 (ver ejemplo anterior) tenemos que 10 *no es un elemento maximal, pues* $10 \leq 30$*. Sí se tiene que* 30 *es un elemento maximal, pues no hay ningún elemento que sea mayor que él. También se tiene que* 30 *es un máximo de ese conjunto.*

En el conjunto $(\mathbb{N}, \leq)$*, el cero es el mínimo y es el único elemento minimal. Este conjunto no tiene máximo ni elementos maximales.*

Si $(X, \leq)$ *es un conjunto ordenado finito, entonces* X *tiene al menos un elemento maximal y un elemento minimal.*

Nótese, que si un conjunto tiene máximo, entonces este es único. Además, en el caso de que tenga máximo, entonces tiene sólo un elemento maximal, que coincide con el máximo.

Idéntica observación vale para mínimo y elemento minimal.

Denotaremos por $\max(X)$ al máximo del conjunto X, en el caso de que exista, y por $\min(X)$ al mínimo.

En el ejemplo que hemos estudiado anteriormente no existe $\max(X)$, mientras que $\min(X) = j$.

Definición 9. *Sea* $(X, \leq)$ *un conjunto ordenado, e* Y *un subconjunto de* X*. Consideramos en* Y *el orden inducido de* X*.*

1. *Un elemento* $x \in X$ *se dice que es* cota superior *de* Y *si* $x \geq y$ *para todo* $y \in Y$*.*

2. *Un elemento $x \in X$ se dice que es* supremo *de Y si es el mínimo del conjunto de las cotas superiores de Y.*

De la misma forma se define lo que es una cota inferior y un ínfimo.

Ejemplo 2.1.4. *Si $X = \{a, b, c, d, e, f, g, h, i, j\}$ con el orden dado anteriormente, e $Y = \{c, d, f, g, h\}$ entonces:*

El conjunto de las cotas superiores de Y es $\{a\}$.

Puesto que este conjunto tiene mínimo, que es a, entonces a es el supremo de Y.

Los elementos c y d son elementos maximales de Y.

El conjunto de las cotas inferiores es $\{h, j\}$.

De éstas, h es el máximo, luego h es el ínfimo de Y.

h es además el único elemento minimal y el mínimo de Y.

Cuando un conjunto tiene supremo éste es único. Podemos entonces hablar de *el supremo de Y*, y lo representaremos mediante $\sup(Y)$.

De la misma forma, denotaremos por $\text{ínf}(Y)$ al ínfimo del conjunto Y cuando exista.

Cuando un conjunto tiene máximo, entonces también tiene supremo, y coincide con él. En el último ejemplo vemos como el recíproco no es cierto, pues Y tiene supremo pero no tiene máximo.

Cuando el supremo de un conjunto pertenezca al conjunto, entonces será también el máximo.

Definición 10 (Buen orden)**.** *Sea $(X, \leq)$ un conjunto ordenado. Se dice que $\leq$ es un buen orden si todo subconjunto no vacío de X tiene mínimo. En tal caso, se dice que $(X, \leq)$ (o X) es un conjunto bien ordenado.*

Observación: Todo conjunto bien ordenado es un conjunto totalmente ordenado, pues dados dos elementos $x, y \in X$ el subconjunto $\{x, y\}$ tiene mínimo. Si $\text{mín}(\{x, y\}) = x$ entonces $x \leq y$, mientras que si $\text{mín}(\{x, y\}) = y$ entonces $y \leq x$.

El recíproco no es cierto. Busca un ejemplo.

Ejemplo 2.1.5. *El conjunto de los números naturales, con el orden usual, es un conjunto bien ordenado, como demostramos en el Teorema 1.1.1.*

Definición 11. *Sean $(X_1, \leq_1)$ y $(X_2, \leq_2)$ dos conjuntos ordenados.*

Se define el orden producto *en $X_1 \times X_2$ como sigue:*

$$(x_1, x_2) \leq_{prod} (y_1, y_2) \text{ si } x_1 \leq_1 y_1 \text{ y } x_2 \leq_2 y_2.$$

Se define el orden lexicográfico *en $X_1 \times X_2$ como sigue:*

$$(x_1, x_2) \leq_{lex} (y_1, y_2) \overset{def}{\Longleftrightarrow} \begin{cases} x_1 <_1 y_1 & \text{ó} \\ x_1 = y_1 \text{ y } x_2 \leq_2 y_2. \end{cases}$$

Claramente, si $(x_1, x_2) \leq_{prod} (y_1, y_2)$ entonces $(x_1, x_2) \leq_{lex} (y_1, y_2)$.

Proposición 2.1.1. *Si* $(X_1, \leq_1)$ *y* $(X_2, \leq_2)$ *son dos conjuntos ordenados, entonces* $(X_1 \times X_2, \leq_{prod})$ *y* $(X_1 \times X_2, \leq_{lex})$ *son conjuntos ordenados.*

Además, si $\leq_1$ *y* $\leq_2$ *son órdenes totales (resp. buenos órdenes) entonces* $\leq_{lex}$ *es un orden total (resp. buen orden).*

Demostración: La demostración de que el orden producto es una relación de orden es fácil, y se deja como ejercicio. Centrémonos pues en el orden lexicográfico.

Notemos en primer lugar que si $(x_1, x_2) \leq_{lex} (y_1, y_2)$ entonces $x_1 \leq_1 y_1$.

Veamos que la relación es de orden.

Reflexiva: Si $(x_1, x_2) \in X_1 \times X_2$ entonces $(x_1, x_2) \leq_{lex} (x_1, x_2)$, pues se da la segunda opción ($x_1 = x_1$ y $x_2 \leq x_2$).

Simétrica: Supongamos que $(x_1, x_2) \leq_{lex} (y_1, y_2)$ y $(y_1, y_2) \leq_{lex} (x_1, x_2)$. Entonces se tiene que $x_1 \leq_1 y_1$ e $y_1 \leq_1 x_1$, de donde $x_1 = y_1$. Deducimos entonces que $x_2 \leq_2 y_2$ e $y_2 \leq_2 x_2$, lo que implica que $x_2 = y_2$.

Transitiva: Supongamos ahora que $(x_1, x_2) \leq_{lex} (y_1, y_2)$ y $(y_1, y_2) \leq_{lex} (z_1, z_2)$. Pueden darse entonces tres opciones(no excluyentes):

- $x_1 <_1 y_1$, en cuyo caso $x_1 <_1 z_1$, luego $(x_1, x_2) \leq_{lex} (z_1, z_2)$.
- $y_1 <_1 z_1$, en cuyo caso $x_1 <_1 z_1$ y concluimos como en la opción anterior.
- $x_1 = y_1$ e $y_1 = z_1$. En tal caso, $x_2 \leq_2 y_2$ e $y_2 \leq_2 z_2$, de donde $x_1 = z_1$ y $x_2 \leq_2 z_2$, es decir, $(x_1, x_2) \leq_{lex} (z_1, z_2)$.

Supongamos ahora que $\leq_1$ y $\leq_2$ son órdenes totales. Sean $(x_1, x_2), (y_1, y_2) \in X_1 \times X_2$. Aquí pueden darse tres opciones (mutuamente excluyentes):

- $x_1 <_1 y_1$. En tal caso $(x_1, x_2) \leq_{lex} (y_1, y_2)$.
- $y_1 <_1 x_1$. En este caso $(y_1, y_2) \leq_{lex} (x_1, x_2)$.
- $x_1 = y_1$. Entonces dependiendo de que $x_2 \leq_2 y_2$ o $y_2 \leq_2 x_2$ se tendrá que $(x_1, x_2) \leq_{lex} (y_1, y_2)$ o que $(y_1, y_2) \leq_{lex} (x_1, x_2)$.

Por último, supongamos que $\leq_1$ y $\leq_2$ son buenos órdenes, y sea $Y \subseteq X_1 \times X_2$ un subconjunto no vacío.

Nos quedamos con el conjunto de todas las primeras coordenadas de los elementos de A, es decir, tomamos

$$Y_1 = \{x_1 \in X_1 : (x_1, x_2) \in A \text{ para algún } x_2 \in X_2\}.$$

Sea $a = \min(Y_1)$. Tomamos entonces $Y_2 = \{x_2 \in X_2 : (a, x_2) \in A\}$. Como $Y_2 \neq \emptyset$, tiene mínimo. Sea éste b. Entonces $(a, b) = \min(A)$. ■

Observación: Si tenemos n conjuntos ordenados $X_1, X_2, \ldots, X_n$, podemos definir recursivamente el orden producto y el orden lexicográfico en $X_1 \times X_2 \times \cdots \times X_n$.

Supuesto definido el orden producto $\leq_{prod}$ en $X_1 \times \cdots \times X_{n-1}$ se define en $X_1 \times \cdots \times X_n$:

$$(x_1, \ldots x_{n-1}, x_n) \leq_{prod} (y_1, \ldots, y_{n-1}, y_n) \ si \ (x_1, \ldots, x_{n-1}) \leq_{prod} (y_1, \ldots, y_{n-1}) \text{ y } x_n \leq y_n,$$

es decir, definimos el orden producto en $(X_1 \times \cdots \times X_{n-1}) \times X_n$.

Supuesto definido el orden lexicográfico $\leq_{lex}$ en $X_1 \times \cdots \times X_{n-1}$ se define en $X_1 \times \cdots \times X_n$:

$$(x_1, \ldots x_{n-1}, x_n) \leq_{lex} (y_1, \ldots, y_{n-1}, y_n) \overset{\text{def}}{\Longleftrightarrow} \begin{cases} (x_1, \ldots, x_{n-1}) <_{lex} (y_1, \ldots, y_{n-1}) & \text{ó} \\ (x_1, \ldots, x_{n-1}) = (y_1, \ldots, y_{n-1}) \ y \ x_n \leq y_n. \end{cases}$$

Sea el conjunto

$$\mathcal{A} = \{\ , a, b, c, d, e, f, g, h, i, j, l, l, m, n, \tilde{n}, o, p, q, r, s, t, u, v, w, x, y, z\},$$

es decir, las 27 letras del alfabeto junto con el espacio en blanco.

Claramente, $\mathcal{A}$ tiene un orden total de todos conocido.

Supongamos que n es el número de letras de la palabra más larga de la lengua española. Entonces, cada palabra puede representarse como un elemento de $\mathcal{A}^n$ (poniendo tantos espacios al final como sea necesario).

Cuando ordenamos las palabras, tal y como vienen en un diccionario, nos fijamos en la primera letra, y es la que nos da el orden. Cuando ésta coincide, pasamos a la segunda, y es ésta entonces la que nos da el orden. De coincidir también, nos fijamos en la tercera, y así sucesivamente. Es decir, las palabras de la lengua están ordenadas siguiendo el orden lexicográfico.

Ejemplo 2.1.6.

Consideramos en $\mathbb{N}\times\mathbb{N}$ *los órdenes producto* ($\leq$) *y lexicográfico* $\leq_{lex}$ *deducidos a partir del orden usual en* $\mathbb{N}$. *Entonces:*

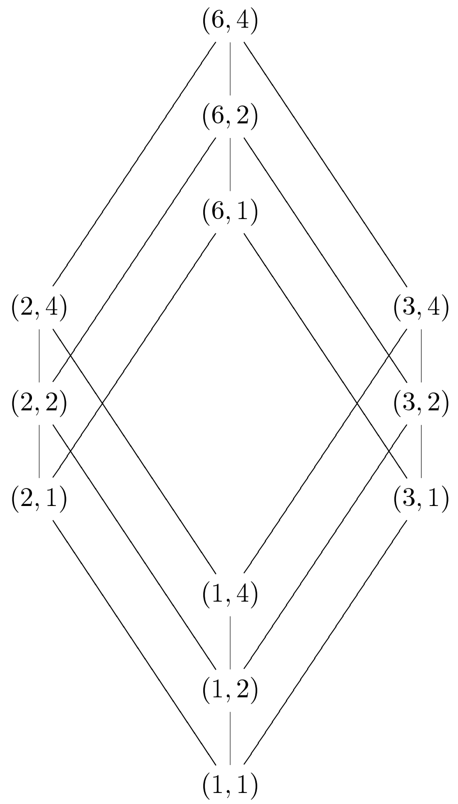
Los elementos $(0,n),(1,n-1),\ldots,(n-1,1),(n,0)$ *están ordenados según el orden lexicográfico, mientras que con el orden producto ninguna pareja de ellos es comparable.*

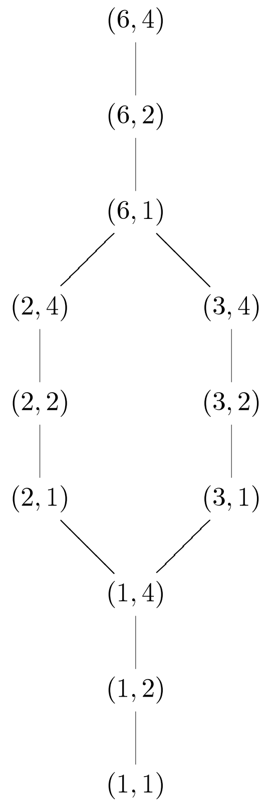
Se puede ver entonces que la propiedad de ser orden total o buen orden no se mantiene al tomar el orden producto.

Si $X=\{(0,n),(1,n-1),\ldots,(n-1,1),(n,0)\}$ *entonces:*

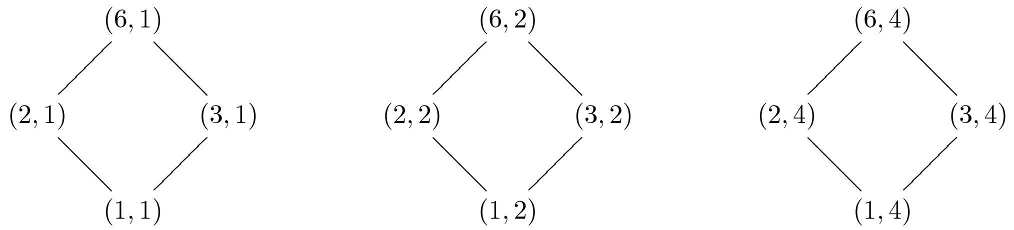
- *El conjunto de cotas inferiores con respecto al orden lexicográfico es* $\{(0,0),(0,1),\ldots,(0,n)\}$, *mientras que con respecto al orden producto tiene una única cota inferior, que es* $(0,0)$.
- *El ínfimo, respecto al orden lexicográfico es* $(0,n)$, *que es también el mínimo. Con respecto al orden producto es* $(0,0)$, *y no tiene mínimo.*
- *Con respecto al orden lexicográfico tiene un elemento minimal, que es* $(0,n)$ *y un elemento maximal, que es* $(n,0)$. *Con respecto al orden producto, todos los elementos son maximales y minimales.*

Sean ahora los conjuntos ordenados $(D(6),|)$ *y* $(D(4),|)$. *Entonces los diagramas de Hasse de* $D(6)\times D(4)$ *con el orden producto y el orden lexicográfico son respectivamente:*

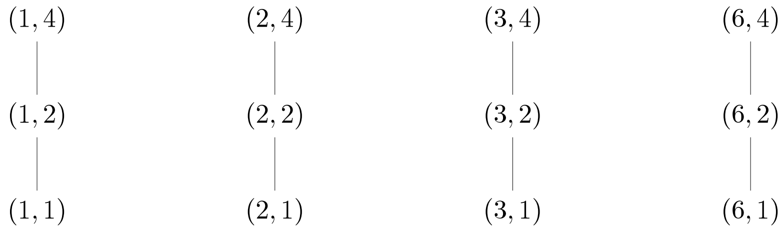




Nótese como el diagrama de Hasse de $D(6) \times D(4)$ con el orden producto consiste en "pegar" tres diagramas como el de $D(6)$

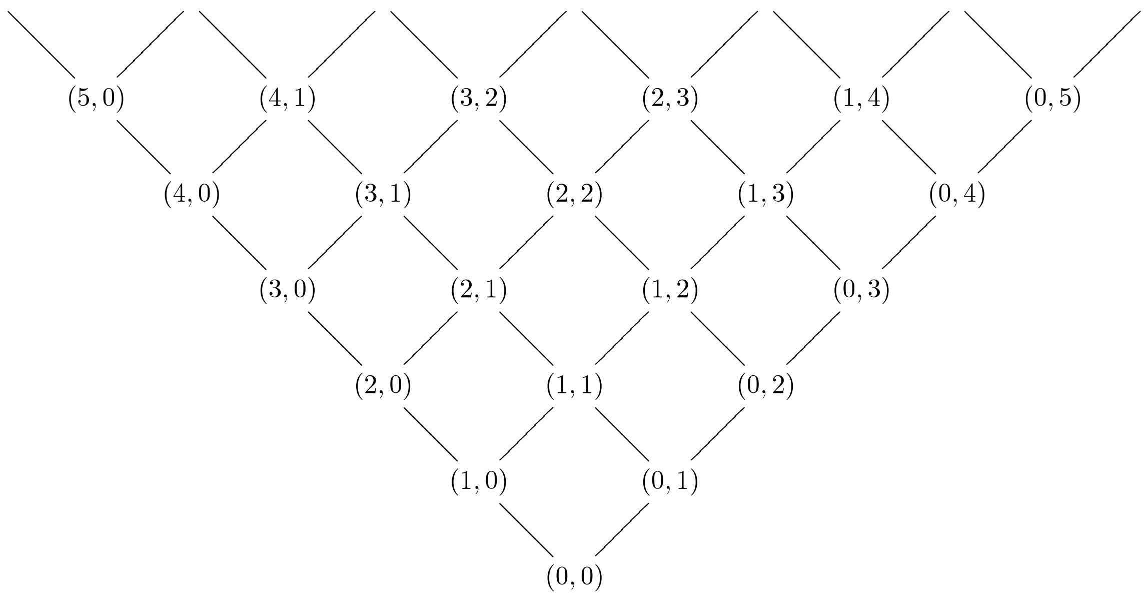


y cuatro diagramas como el de $D(4)$



mientras que el diagrama de Hasse de $D(6) \times D(4)$ con el orden lexicográfico tiene la "misma forma" que el de $D(6)$, salvo que en cada vértice tenemos un diagrama de $D(4)$.

El diagrama de Hasse de $(\mathbb{N}^2, \leq_{prod})$ sería como sigue:



2.2. Retículos.

Definición 12. *Un retículo es un conjunto ordenado, $(L, \leq)$ en el que cualquier conjunto finito tiene supremo e ínfimo.*

Si $(L, \leq)$ es un retículo y $x, y \in L$, denotaremos por $x \vee y$ al supremo del conjunto $\{x, y\}$ y por $x \wedge y$ al ínfimo del conjunto $\{x, y\}$.

Nótese que $x \vee y$ está definido por la propiedad:

$$x \leq x \vee y; \; y \leq x \vee y \qquad (x \leq z \text{ e } y \leq z) \Longrightarrow x \vee y \leq z$$

La primera parte dice que $x \vee y$ es una cota superior del conjunto $\{x, y\}$, mientras que la segunda dice que es la menor de las cotas superiores.

Proposición 2.2.1. *Si $(L, \leq)$ es un retículo, las operaciones $\vee$ y $\wedge$ satisfacen las siguienes propiedades:*

$$\begin{array}{rl}
\textit{Conmutativa} & \left\{\begin{array}{l} x \vee y = y \vee x \\ x \wedge y = y \wedge x. \end{array}\right. \\
\textit{Asociativa} & \left\{\begin{array}{l} x \vee (y \vee z) = (x \vee y) \vee z \\ x \wedge (y \wedge z) = (x \wedge y) \wedge z. \end{array}\right. \\
\textit{Absorción} & \left\{\begin{array}{l} x \vee (x \wedge y) = x \\ x \wedge (x \vee y) = x. \end{array}\right. \\
\textit{Idempotencia} & \left\{\begin{array}{l} x \vee x = x \\ x \wedge x = x. \end{array}\right.
\end{array}$$

Demostración: La demostración de la propiedad conmutativa, así como la de idempotencia es inmediata. Para demostrar la propiedad asociativa basta comprobar que tanto $x\vee(y\vee z)$ como $(x\vee y)\vee z$ representa el supremo del conjunto $\{x, y, z\}$, y lo mismo para el ínfimo. Veamos que $\sup(\{x, y, z\}) = x \vee (y \vee z)$.

Es claro que $x \leq x \vee (y \vee z)$, $y \leq x \vee (y \vee z)$ y $z \leq x \vee (y \vee z)$. Por otra parte,

$$\left.\begin{array}{l} x \leq u \\ \left.\begin{array}{l} y \leq u \\ z \leq u \end{array}\right\} \Longrightarrow y \vee z \leq u \end{array}\right\} \Longrightarrow x \vee (y \vee z) \leq u.$$

Por tanto, $x \vee (y \vee z)$ es el supremo del conjunto $\{x, y, z\}$.

En cuanto a la absorción, la primera se deduce fácilmente del hecho de que $x \wedge y \leq x$ y la segunda de que $x \leq x \vee y$. ■

Ejemplo 2.2.1.

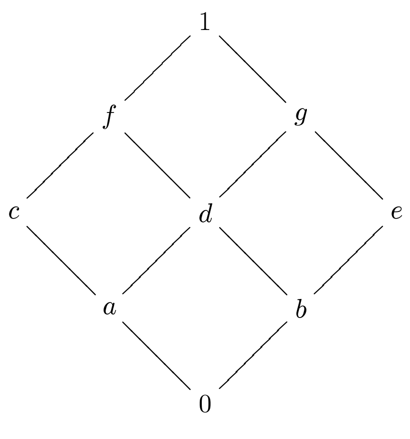
1. *Si X es un conjunto totalmente ordenado, entonces X es un retículo. Dados $x, y \in X$ se tiene que $x \vee y =$ máx$(\{x, y\})$ mientras que $x \wedge y =$ mín$(\{x, y\})$.*

2. *El conjunto ordenado $(\mathbb{N}, |)$ es un retículo. En este caso se tiene que $x\vee y = mcm(x, y)$ mientras que $x\wedge y = mcd(x, y)$. De la misma forma, si $n \in \mathbb{N}$ entonces $D(n)$, con el orden dado por la divisibilidad es un retículo. Supremo e ínfimo vienen dado por el mínimo común múltiplo y el máximo común divisor respectivamente.*

3. *Si X es un conjunto, entonces $\mathcal{P}(X)$ es un retículo. En este caso supremo e ínfimo vienen dados por la unión y la intersección respectivamente; es decir, $A \vee B = A \cup B$ y $A \wedge B = A \cap B$.*

4. *Si V es un K-espacio vectorial, el conjunto de los subespacios vectoriales de V es un retículo, con el orden dado por la inclusión. Aquí, dado dos subespacios vectoriales V_1 y V_2 se tiene que $V_1 \vee V_2 = V_1 + V_2$ mientras que $V_1 \wedge V_2 = V_1 \cap V_2$.*

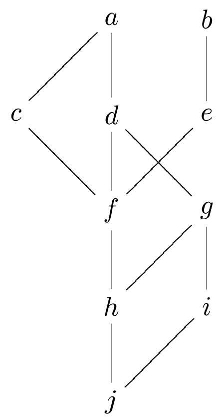
5. *El conjunto ordenado cuyo diagrama de Hasse es*



es un retículo.

Se tiene, por ejemplo: $c \vee d = f$, $c \wedge d = a$, $b \vee c = f$, $b \wedge c = 0$, $c \vee e = 1$, $c \wedge e = 0$.

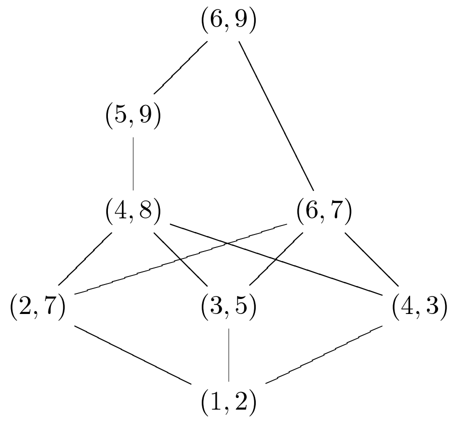
6. *El conjunto ordenado cuyo diagrama de Hasse es*



no es un retículo, pues por ejemplo, no existe el supremo del conjunto $\{a, e\}$*. Sin embargo, el conjunto* $\{f, i\}$ *sí tiene supremo (*d*) e ínfimo (*j*).*

7. *Dado el conjunto* $A = \{(1,2);\ (4,3);\ (3,5);\ (2,7);\ (4,8);\ (6,9);\ (6,7); (5,9)\} \subseteq \mathbb{N}^2$*, consideramos en* A *el orden inducido del orden producto en* $\mathbb{N}^2$*.*

El diagrama de Hasse de A *sería:*



Este conjunto no es un retículo. Por ejemplo, tomamos $x = (2,7)$ *e* $y = (3,5)$*. El conjunto de las cotas superiores de* x *e* y *es* $\{(4,8);\ (6,7);\ (5,9);\ (6,9)\}$*. Y ese conjunto no tiene mínimo. Por tanto, no existe la menor de las cotas superiores, luego no existe el supremo de* x *e* y*.*

Nótese que si $(L, \leq)$ es un retículo, entonces dados $x, y \in L$ se verifica que $x \leq y$ si, y sólo si, $x \vee y = y$, o si queremos, $x \leq y$ si, y sólo si, $x \wedge y = x$. Es decir, podemos recuperar el orden dentro del retículo a partir del conocimiento de las operaciones supremo o ínfimo.

La siguiente proposición nos da condiciones suficientes para que dos operaciones definidas en un conjunto puedan ser el supremo y el ínfimo de alguna relación de orden en ese conjunto.

Proposición 2.2.2. *Sea* L *un conjunto en el que tenemos definidas dos operaciones* $\vee$ *y* $\wedge$ *que satisfacen las propiedades conmutativa, asociativa, idempotencia y de absorción. Supongamos que en* L *definimos la relación*

$$x \leq y \quad \text{si } x \vee y = y.$$

Entonces, $(L, \leq)$ *es un retículo donde las operaciones supremo e ínfimo vienen dadas por* $\vee$ *y* $\wedge$ *respectivamente.*

Demostración:

1. Veamos en primer lugar que $(L, \leq)$ es un conjunto ordenado. Para esto, comprobemos que la relación $\leq$ es reflexiva, antisimétrica y transitiva.

   Reflexiva. Puesto que $x \vee x = x$ se tiene que $x \leq x$ para cualquier $x \in L$.

   Antisimétrica. Supongamos que $x \leq y$ e $y \leq x$. Esto implica que $x \vee y = y$ y que $y \vee x = x$. Puesto que $\vee$ es conmutativa deducimos que $x = y (= x \vee y)$.

   Transitiva. Supongamos ahora que $x \leq y$ y que $y \leq z$, es decir, $x \vee y = y$ e $y \vee z = z$. Entonces:
$$x \vee z = x \vee (y \vee z) = (x \vee y) \vee z = y \vee z = z$$
   luego $x \leq z$.

2. Comprobemos ahora que dados $x, y \in L$ se verifica que $\sup(\{x, y\}) = x \vee y$.

   Puesto que $x \vee (x \vee y) = (x \vee x) \vee y = x \vee y$ se tiene que $x \leq x \vee y$. De la misma forma se comprueba que $y \leq x \vee y$.

   Si $x \leq u$ e $y \leq u$ (es decir, $x \vee u = u$ e $y \vee u = u$). Entonces:
$$(x \vee y) \vee u = x \vee (y \vee u) = x \vee u = u,$$
   de donde se deduce que $x \vee y \leq u$.

3. Por último, veamos que $\text{ínf}(\{x, y\}) = x \wedge y$.

   $(x \wedge y) \vee x = x \vee (x \wedge y) = x$ luego $x \wedge y \leq x$.

   De la misma forma se comprueba que $x \wedge y \leq y$.

   Si $u \leq x$ y $u \leq y$ (es decir, $u \vee x = x$ y $u \vee y = y$) se tiene que:
$$u \wedge x = u \wedge (u \vee x) = u \qquad u \wedge y = u \wedge (u \vee y) = u,$$
$$u \wedge (x \wedge y) = (u \wedge x) \wedge y = u \wedge y = u,$$
$$u \vee (x \wedge y) = (u \wedge (x \wedge y)) \vee (x \wedge y) = (x \wedge y) \vee ((x \wedge y) \wedge u) = x \wedge y,$$
   luego $u \leq x \wedge y$.

■

Nótese que se tiene que $x \vee y = y$ si, y sólo si, $x \wedge y = x$, luego podría haberse hecho la demostración definiendo la relación
$$x \leq y \quad \text{si } x \wedge y = x.$$

Nótese también que la propiedad de idempotencia se puede deducir a partir de la de absorción, pues
$$x \vee x = x \vee [x \wedge (x \vee x)] = x,$$
luego podemos demostrar la proposición anterior partiendo de que las operaciones $\vee$ y $\wedge$ satisfacen las propiedades asociativa, conmutativa y de absorción.

Esta proposición permite definir un retículo, bien dando la relación de orden, bien dando las operaciones $\vee$ y $\wedge$.

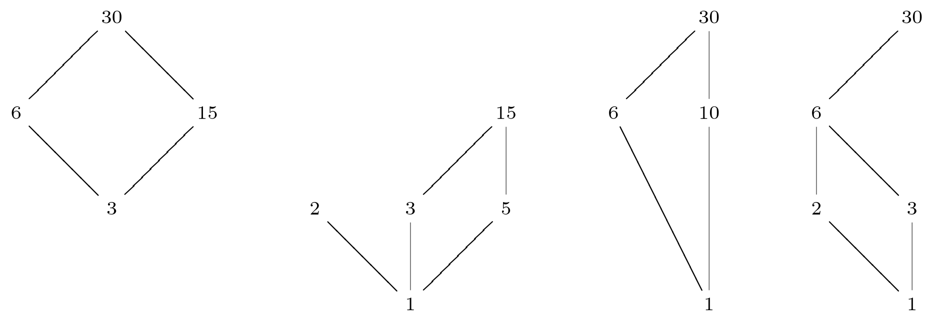
Si $(L, \leq)$ es un retículo y L tiene máximo, denotaremos a éste por 1, mientras que si tiene mínimo lo denotaremos por 0. Se tiene entonces, $x \vee 1 = 1$, $x \wedge 1 = x$, $x \vee 0 = x$ y $x \wedge 0 = 0$.

Un retículo finito siempre tiene máximo y mínimo. Si el retículo es infinito, puede tenerlo o no. Así, por ejemplo, $(\mathbb{N}, \leq)$ tiene mínimo pero no tiene máximo; $(\mathbb{Z}, \leq)$ no tiene ni mínimo ni máximo. El retículo $(\mathbb{N}, |)$ es infinito y tiene máximo y mínimo. En este caso, el máximo es 0 mientras que el mínimo es 1.

Definición 13. *Sea $(L, \leq)$ un retículo, y $L' \subseteq L$ un subconjunto de L. Entonces L' es un subrretículo si para cualesquiera $x, y \in L'$ se verifica que $x \vee y \in L'$ y $x \wedge y \in L'$.*

Ejemplo 2.2.2. *Consideramos el retículo $D(30)$.*

Sean $L_1 = \{3, 6, 15, 30\}$, $L_2 = \{1, 2, 3, 5, 15\}$, $L_3 = \{1, 6, 10, 30\}$ y $L_4 = \{1, 2, 3, 6, 30\}$. Sus diagramas de Hasse son:



L_1 L_2 L_3 L_4

Entonces L_1 y L_4 son subrretículos de $D(30)$, mientras que L_2 y L_3 no lo son. L_2 no es subrretículo porque el supremo de 2 y 3 es 6, que no pertenece a L_2. L_3 no es subrretículo porque el ínfimo de 6 y 10 vale 2, que no pertenece a L_3. Nótese que L_3, con el orden que hereda de $D(30)$, es un retículo, pero no es subrretículo de L_3.

Definición 14. *Sea L un retículo. Se dice que L es distributivo si para cualesquiera $x, y, z \in L$ se verifica que*

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

En general, si L es un retículo se tiene que $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$.

$$\left.\begin{array}{l} \left.\begin{array}{l} x \leq x \vee y \\ x \leq x \vee z \end{array}\right\} \Longrightarrow x \leq (x \vee y) \wedge (x \vee z) \\ \\ \left.\begin{array}{l} y \wedge z \leq x \vee y \\ y \wedge z \leq x \vee z \end{array}\right\} \Longrightarrow y \wedge z \leq (x \vee y) \wedge (x \vee z) \end{array}\right\} \Longrightarrow x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z),$$

y de la misma forma se tiene que $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$. Por tanto, se tiene que un retículo es distributivo si $(x \vee y) \wedge (x \vee z) \leq x \vee (y \wedge z)$ y $(x \wedge (y \vee z) \leq x \wedge y) \vee (x \wedge z)$.

Por otra parte, si $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ para cualesquiera $x, y, z \in L$ se tiene que

$$\begin{array}{rcll} (x \wedge y) \vee (x \wedge z) & = & [(x \wedge y) \vee x] \wedge [(x \wedge y) \vee z] & \text{propiedad distributiva} \\ & = & [x \vee (x \wedge y)] \wedge [z \vee (x \wedge y)] & \text{pues } \vee \text{ es conmutativa} \\ & = & [(x \vee x) \wedge (x \vee y)] \wedge [(z \vee x) \wedge (z \vee y)] & \text{propiedad distributiva} \\ & = & (x \vee x) \wedge (x \vee y) \wedge (x \vee z) \wedge (y \vee z) & \text{propiedad asociativa y conmutativa} \\ & = & [x \wedge (x \vee y) \wedge (x \vee z)] \wedge (y \vee z) & \text{idempotencia y propiedad asociativa} \\ & = & x \wedge (y \vee z) & \text{Absorción} \end{array}$$

mientras que si $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ para cualesquiera $x, y, z \in L$ entonces se verifica que $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ también para cualesquiera $x, y, z \in L$.

Es decir, basta con que se dé una de las dos posibles propiedades distributivas para que se dé la otra.

Ejemplo 2.2.3.

1. *Si L es un conjunto totalmente ordenado, entonces L es un retículo distributivo. Basta comprobar que para cualesquiera $x, y, z \in L$ se verifica que*

$$\text{máx}\{x, \text{mín}\{y, z\}\} = \text{mín}\{\text{máx}\{x, y\}, \text{máx}\{x, z\}\},$$

   lo cual puede hacerse fácilmente comprobando que se da la igualdad en cualquiera de los seis casos siguientes:

$$x \leq y \leq z; \quad x \leq z \leq y; \quad y \leq x \leq z; \quad y \leq z \leq x; \quad z \leq x \leq y; \quad z \leq y \leq x,$$

   y puesto que en la igualdad el papel que juegan y y z es el mismo, bastaría con comprobarlo en los casos

$$x \leq y \leq z; \qquad y \leq x \leq z; \qquad y \leq z \leq x.$$

2. *El retículo $(\mathbb{N}, |)$ es un retículo distributivo. Basta ver que en este caso, el cálculo del supremo y el ínfimo se reduce al cálculo del máximo y el mínimo de los exponentes, y entonces reducirse al caso anterior.*

   Por el mismo motivo, para cada número natural $n \in \mathbb{N}$ el retículo $D(n)$ es distributivo.

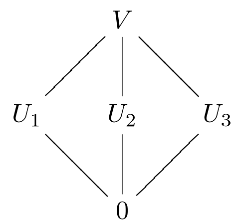
3. *Si X es un conjunto, entonces $(\mathcal{P}(X), \subseteq)$ es un retículo distributivo, pues la unión y la intersección de conjuntos son distributivas la una con respecto de la otra.*

4. *Si V es un K-espacio de dimensión mayor que 1, entonces el retículo de los subespacios vectoriales de V es un retículo que no es distributivo.*

   Como ejemplo, sea $K = \mathbb{Z}_2$ y $V = \mathbb{Z}_2^2$. Entonces V tiene 5 subespacios vectoriales que son:

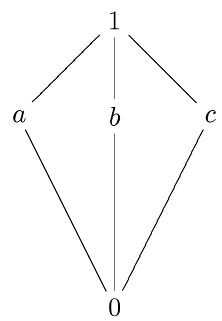
$$V; \quad U_1 = \{(0,0), (1,0)\}; \quad U_2 = \{(0,0), (0,1)\}; \quad U_3 = \{(0,0), (1,1)\}; \quad 0.$$

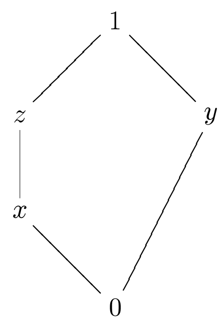
   y se tiene que $U_2 \cap U_3 = 0$, luego $U_1 + (U_2 \cap U_3) = U_1$, mientras que $(U_1 + U_2) \cap (U_1 + U_3) = V \cap V = V$. El diagrama de Hasse de este retículo es:



   En general, si V es un K-espacio de dimensión mayor o igual que 2, y u, v son dos vectores linealmente independientes, consideramos $U_1 = L\{u\}$, $U_2 = L\{v\}$ y $U_3 = L\{u + v\}$ y se verifica que $U_1 + (U_2 \cap U_3) = U_1$, mientras que $(U_1 + U_2) \cap (U_1 + U_3) = L\{u, v\}$.

5. *Consideramos los siguientes retículos:*





   denominados respectivamente diamante *y* pentágono. *En el ejemplo anterior hemos visto que el diamente no es distributivo. En cuanto al pentágono, se tiene que*

$$x \vee (y \wedge z) = x \vee 0 = x, \qquad (x \vee y) \wedge (x \vee z) = 1 \wedge z = z.$$

luego tampoco es distributivo.

En general, se tiene que un retículo es distributivo si no contiene como subrretículos ni al pentágono ni al diamante. En el apartado anterior hemos visto como el retículo de subespacios vectoriales de un espacio vectorial tiene al diamante como subrretículo.

Proposición 2.2.3. *Sea L un retículo distributivo, y sen $x, y, z \in L$ tales que $x \vee y = x \vee z$ y $x \wedge y = x \wedge z$. Entonces $y = z$.*

Demostración: Se tiene que

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

■

Ejemplo 2.2.4. *En el diamante se tiene que $a \vee b = a \vee c = 1$, y $a \wedge b = a \wedge c = 0$, y sin embargo, $b \neq c$.*
En el pentágono, $y \vee x = y \vee z = 1$ e $y \wedge x = y \wedge z = 0$, y sin embargo, $x \neq z$.

Definición 15. *Sea L un retículo que tiene máximo y mínimo (a los que denotaremos por 1 y 0 respectivamente), y $x \in L$. Se dice que $y \in L$ es un complemento de x si $x \vee y = 1$ y $x \wedge y = 0$.*
Un reticulo en el que todo elemento tiene complemento se dice complementado.

Obviamente, si y es un complemento de x entonces x es un complemento de y.
Por otra parte, si L es un retículo distributivo y x un elemento de L que tiene complemento, entonces el complemento es único (ver Proposicion 2.2.3).
Si L es un retículo distributivo y x es un elemento que tiene complemento, denotaremos por x' o $\overline{x}$ al único complemento de x.

Ejemplo 2.2.5.

1. *Si L tiene máximo (1) y mínimo (0), entonces 0 es un complemento de 1.*
2. *El retículo $(\mathcal{P}(X), \subseteq)$ es un retículo complementado. Dado $A \in \mathcal{P}(X)$ se verifica que $A \cup (X \setminus A) = X$ y $A \cap (X \setminus A) = \emptyset$. Por ser un retículo distributivo, el complemento de cada elemento es único.*
3. *El pentágono y el diamente son retículos complementados. Vemos sin embargo, que los complementos de algunos elementos no son únicos.*

   Así, en el diamante, tanto b como c son complementos de a; tanto a como c son complementos de b y tanto a como b son complementos de c.

   En el pentágono, tanto x como z son complementos de y. Sin embargo, x tiene un único complemento, que es y, al igual que z.
4. *Si L es un conjunto totalmente ordenado con más de dos elementos, entonces es un retículo distributivo, pero no es complementado.*
5. *Si V es un K-espacio vectorial de dimensión finita (esto último no es necesario) entonces el retículo de los subespacios vectoriales de V es un retículo complementado.*

   Para ver esto, tomamos U un subespacio vectorial de V. Supongamos que $\mathcal{B}_U = \{u_1, \ldots, u_m\}$ es una base de U. Esta base puede ser ampliada hasta una base de V. Si dicha base ampliada es $\mathcal{B} = \{u_1, \ldots, u_m, u_{m+1}, \ldots, u_n\}$ entonces el subespacio generado por $\{u_{m+1}, \ldots, u_n\}$ es un complemento de U.

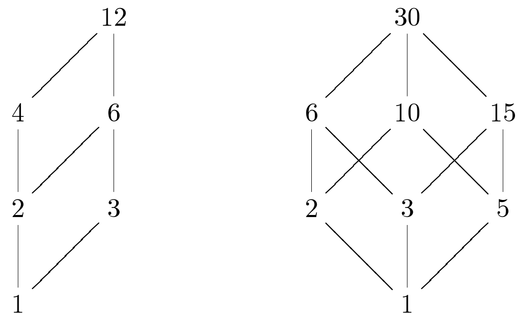
   Puesto que en general hay muchas formas de completar una base de V a partir de una base de U, el subespacio U puede tener muchos complementos.

   Así, si tomamos $U = \mathbb{R}^2$ y $U = L[(1,0)]$ (es decir, el eje OX) entonces cualquier recta que pase por el origen distinta del eje OX es un complemento de U.

6. *Dado un número natural $D(n)$, el retículo $D(n)$ no tiene por qué ser un retículo complementado. Por ejemplo, $D(4)$ no es complementado (es un conjunto totalmente ordenado con 3 elementos), mientras que $D(6)$ sí lo es.*

   Se pide, determinar qué elementos de $D(n)$ tienen complemento, y a partir de ahí, determinar para qué valores de n es $D(n)$ un retículo complementado.

   Así, por ejemplo, en $D(12)$ tienen complemento $1, 3, 4, 12$ mientras que no tienen $2, 6$. En $D(30)$ todos los elementos tienen complemento.



$D(12)$ $D(30)$

Proposición 2.2.4. *Sean $(L_1, \leq)$ y $(L_2, \leq)$ dos conjuntos ordenados. Consideramos en $L_1 \times L_2$ el orden producto. Entonces:*

- *Si L_1 y L_2 son retículos, también lo es $L_1 \times L_2$. Las operaciones supremo e ínfimo en $L_1 \times L_2$ vienen dadas por*

$$(x_1, x_2) \vee (y_1, y_2) = (x_1 \vee y_1, x_2 \vee y_2) \qquad (x_1, x_2) \wedge (y_1, y_2) = (x_1 \wedge y_1, x_2 \wedge y_2)$$

- *Si L_1 y L_2 son retículos distributivos, también lo es $L_1 \times L_2$.*
- *Si L_1 y L_2 son retículos complementados, también lo es $L_1 \times L_2$.*

2.3. Álgebras de Boole

2.3.1. Generalidades sobre álgebras de Boole

Definición 16. *Un* álgebra de Boole *es un retículo distributivo y complementado.*

Ejemplo 2.3.1.

1. *Dado un conjunto X, el conjunto $\mathcal{P}(X)$, con el orden dado por la inclusión es un álgebra de Boole.*
2. *$D(6)$, o $D(30)$ son álgebras de Boole. No es álgebra de Boole $D(4)$ o $D(12)$.*

Al igual que los retículos se pueden definir sin mencionar el orden, sino únicamente las operaciones supremo e ínfimo, con las respectivas propiedades, un álgebra de Boole puede definirse también a partir de las operaciones $\vee$ y $\wedge$.

Definición 17 (Segunda definición de álgebra de Boole)**.** *Sea B un conjunto. Supongamos que en B tenemos definidas dos operaciones, $\vee$ y $\wedge$ tales que:*

1. $x \vee (y \vee z) = (x \vee y) \vee z, \qquad x \wedge (y \wedge z) = (x \wedge y) \wedge z.$
2. $x \vee y = y \vee x, \qquad x \wedge y = y \wedge z.$