Retículos. Parte 1.

Silvio Reggiani

Complementos de Matemática II (LCC)
Facultad de Ciencias Exactas, Ingeniería y Agrimensura
Universidad Nacional de Rosario

28 de septiembre de 2020

Retículos (lattices)

Hay dos definiciones equivalentes de **retículo** (también llamado **reticulado** o **lattice**). Esto tiene que ver con que hay en principio dos enfoques distintos para estudiar estos objetos.

Definición 1 (teoría del orden)

Un poset $(L, \leq)$ se dice un **retículo** si

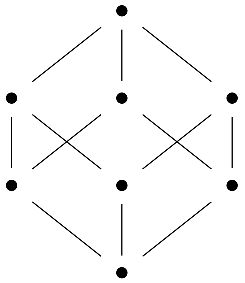
$$\forall a, b \in L, \text{ existen } \sup\{a, b\} \text{ e } \text{ínf}\{a, b\}.$$

Atención

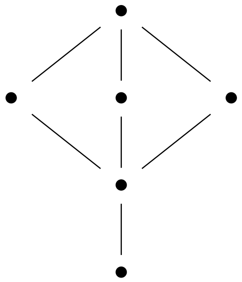
No necesariamente existen $\text{máx}\{a, b\}$ y $\text{mín}\{a, b\}$. De hecho, los casos más interesantes para estudiar son cuando no existen los máximos ni los mínimos.

Ejemplo

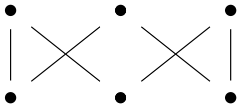
¿Son retículos los siguientes posets?



✓ ¿quién es?



✓



✗

Observación importante

Tomar supremo/ínfimo define dos operaciones (asociativas) en L

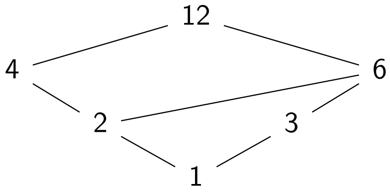
$$a \vee b := \sup\{a, b\}$$
$$a \wedge b := \inf\{a, b\}$$

- Esto convierte a un retículo en un objeto algebraico.
- La pregunta natural que surge es: ¿qué propiedades algebraicas caracterizan completamente a estas operaciones?

Ejemplo $D_n = \{x \in \mathbb{N} : x \mid n\}$

- $(D_n, \mid)$ es un retículo.
- $D_n \ni x \vee y = \mathrm{mcm}(x, y)$.
- $D_n \ni x \wedge y = \mathrm{mcd}(x, y)$.
- Ejercicio.

Subejemplo: D_{12}



Propiedades de las operaciones

Sean $(L, \leq)$ un retículo y $x, y, z, w \in L$. Entonces:

(a) $x \leq x \vee y$

(b) $x \wedge y \leq x$

(c) $x \leq y \iff x \vee y = y \iff x \wedge y = x$

(d) Asociatividad:
- $(x \vee y) \vee z = x \vee (y \vee z)$
- $(x \wedge y) \wedge z = x \wedge (y \wedge z)$

(e) Conmutatividad: $x \vee y = y \vee x$, $x \wedge y = y \wedge x$

(f) Idempotencia: $x \vee x = x = x \wedge x$

(g) Absorción: $x \vee (x \wedge y) = x = x \wedge (x \vee y)$

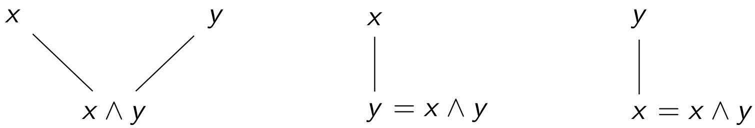
(h) Compatibilidad:

$$\left.\begin{array}{r} x \leq z \\ y \leq w \end{array}\right\} \Longrightarrow \begin{cases} x \vee y \leq z \vee w \\ x \wedge y \leq z \wedge w \end{cases}$$

Demostración.

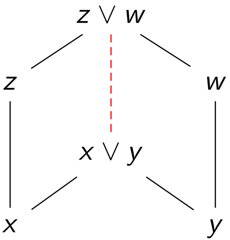
(1)-(f) Hacerlas como ejercicio.

(g) $x \wedge y \overset{(2)}{\leq} x \implies x \vee (x \wedge y) \overset{(c)}{=} x$ (el otro como ejercicio).



(h)

- $x \leq z \leq z \vee w$
- $y \leq w \leq z \vee w$
- Luego $z \vee w$ es cota superior de $\{x, y\}$ y por ende $x \vee y \leq z \vee w$
- Hacer el otro caso como ejercicio $\square$



Definición alternativa de retículo

Definición 2 (álgebra)

Un **retículo** $(L, \vee, \wedge)$ consiste de un conjunto no vacío L junto con dos operaciones $\vee, \wedge$ que satisfacen las siguientes propiedades

Asociatividad $\forall x, y, z \in L, \begin{cases} x \vee (y \vee z) = (x \vee y) \vee z \\ x \wedge (y \wedge z) = (x \wedge y) \wedge z \end{cases}$

Conmutatividad $\forall x, y \in L, \begin{cases} x \vee y = y \vee x \\ x \wedge y = y \wedge x \end{cases}$

Idempotencia $\forall x \in L, \begin{cases} x \vee x = x \\ x \wedge x = x \end{cases}$

Absorción $\forall x, y \in L, \begin{cases} x \vee (x \wedge y) = x \\ x \wedge (x \vee y) = x \end{cases}$

Teorema

La Definición 1 es equivalente a la Definición 2. Más precisamente, si $(L, \vee, \wedge)$ es un retículo como en la Definición 2, entonces

$$x \leq y \overset{\cdot}{\iff} x \vee y = y$$

define un orden parcial en L tal que

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

Demostración.

Veamos que $\leq$ así definido es un orden parcial.

- Reflexividad: $x \leq x \iff x \vee x = x$ (idempotencia). ✓
- Antisimetría: supongamos $x \leq y$ e $y \leq x$.
  - $x \leq y \iff x \vee y = y$,
  - $y \leq x \iff y \vee x = x$.
  - Luego, $x = y \vee x = x \vee y = y$ (conmutatividad). ✓

Demostración (continuación).

- Transitividad: supongamos que $x \leq y$ e $y \leq z$.

$$\begin{aligned} x \vee z &= x \vee (y \vee z) && [y \leq z] \\ &= (x \vee y) \vee z && [\text{asociatividad}] \\ &= y \vee z && [x \leq y] \\ &= z && [y \leq z] \end{aligned}$$

$$\begin{array}{c} z \\ | \\ y \\ | \\ x \end{array}$$

Finalmente veamos que $x \vee y = \sup\{x, y\}$ y $x \wedge y = \text{ínf}\{x, y\}$.

- Claramente $x \vee y$ es cota superior de $\{x, y\}$.
- Sea z tal que $x \leq z$ e $y \leq z$. Entonces

$$(x \vee y) \vee z = x \vee (y \vee z) = x \vee z = z \implies x \vee y \leq z.$$

- Luego $x \vee z$ es la cota superior mínima de $\{x, y\}$, $x \vee y = \sup\{x, y\}$. $\square$

Ejercicio

Faltó probar que $x \wedge y = \text{ínf}\{x, y\}$. Probarlo usando un argumento similar al anterior. Ayuda: usar que $x \leq y \iff x \wedge y = x$. Para ver esto notemos que

- $x \leq y \implies x \vee y = y \overset{\text{absorción}}{\implies} x = x \wedge (x \vee y) = x \wedge y$,
- $x \wedge y = x \overset{\text{absorción}}{\implies} y = y \vee (x \wedge y) = y \vee x = x \vee y \implies x \leq y$.

Semirretículos

- Si "olvidamos" parte de la estructura, $(L, \vee)$ y $(L, \wedge)$ son ejemplos de **semirretículos**, es decir, L es un conjunto no vacío con una operación asociativa, conmutativa e idempotente.
- Recíprocamente si $(L, \leq)$ es un poset tal que $\forall x, y, \exists \sup\{x, y\}$, entonces esta operación induce en L una estructura de semirretículo (lo mismo se puede hacer cambiando sup por ínf).

Ejemplos

- Si X es un conjunto, entonces $(\mathcal{P}(X), \subset)$ es un retículo, que visto algebraicamente es $(\mathcal{P}(X), \cup, \cap)$, en efecto

$$A \cup B = B \iff A \subset B.$$

- $(D_n, \mid\,) \leftrightsquigarrow (D_n, \mathrm{mcm}, \mathrm{mcd})$ es un retículo:

$$\forall x, y \in D_n, (\mathrm{mcm}(x, y) = y \iff x \mid y).$$

Morfismos de retículos

Definición (algebraica)

Sean $(L, \vee, \wedge), (L', \vee, \wedge)$ dos retículos. Una función $f : L \to L'$ se dice un

- **morfismo de retículos** si

$$\forall x, y \in L, \begin{cases} f(x \vee y) = f(x) \vee f(y) \\ f(x \wedge y) = f(x) \wedge f(y) \end{cases}$$

- **isomorfismo de retículos** si f es un morfismo de retículos biyectivo.

Definición (teoría del orden)

…(ya la dimos).

Equivalencia de las definiciones

Proposición

Sean

$$\begin{matrix} (L, \vee, \wedge) \leftrightsquigarrow (L, \leq) \\ (L', \vee, \wedge) \leftrightsquigarrow (L', \leq) \end{matrix} \qquad \textit{(posets asociados)}$$

dos retículos. Entonces $f : (L, \vee, \wedge) \to (L', \vee, \wedge)$ *es un isomorfismo de retículos* $\iff$ $f : (L, \leq) \to (L', \leq)$ *es un isomorfismo de orden.*

Corolario

Si $f : (L, \vee, \wedge) \to (L', \vee, \wedge)$ *es un isomorfismo de retículos, entonces* $f^{-1} : (L', \vee, \wedge) \to (L', \vee, \wedge)$ *también lo es.*

Atención

En la definición de isomorfismo de retículo (a diferencia de la definición de isomorfismo de orden) no pedimos que la inversa preserve las operaciones.

Demostración de la Proposición.

- Supongamos que $f : (L, \leq) \to (L', \leq)$ es un isomorfismo de orden. Entones f manda supremos en supremos e ínfimos en ínfimos. En particular,
  - $f(x \vee y) = f(\sup\{x, y\}) = \sup\{f(x), f(y)\} = f(x) \vee f(y)$,
  - $f(x \wedge y) = f(x) \wedge f(y)$ (ídem).
- Supongamos que $f : (L, \vee, \wedge) \to (L', \vee, \wedge)$ es un isomorfismo de retículos. Debemos probar que $x \leq y \iff f(x) \leq f(y)$. En efecto,

$$
\begin{aligned}
x \leq y &\iff x \vee y = y \\
&\iff f(x \vee y) = f(y) && [f \text{ biyectiva}] \\
&\iff f(x) \vee f(y) = f(y) && [f \text{ morf. de retículos}] \\
&\iff f(x) \leq f(y). && \square
\end{aligned}
$$

Dualidad

Si $(L, \leq) \leftrightsquigarrow (L, \vee, \wedge)$ es un retículo, el **retículo dual** es

$$(L, \geq) \leftrightsquigarrow (L, \wedge, \vee).$$

Antimorfismos

Una función $f : (L, \vee, \wedge) \to (L', \vee, \wedge)$ entre dos retículos es un **antimorfismo** si

$$\forall x, y \in L, \begin{cases} f(x \vee y) = f(x) \wedge f(y) \\ f(x \wedge y) = f(x) \vee f(y) \end{cases}$$

En otras palabras, f es un morfismo de retículos de $(L, \vee, \wedge)$ en el retículo dual de $(L', \vee, \wedge)$.

Ejemplo

La función complemento comp : $\mathcal{P}(X) \to \mathcal{P}(X)$ definida como $\text{comp}(A) = A^c = X - A$ es un antiisomorfismo de retículos:

- $(A \cup B)^c = A^c \cap B^c$.
- $(A \cap B)^c = A^c \cup B^c$.
- Claramente comp es biyectiva.

Ejemplo/Ejercicio

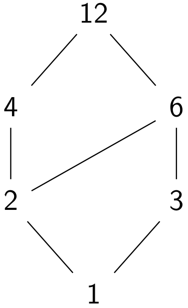
Una función $f : X \to Y$ induce las dos siguientes funciones entre sus respectivos conjuntos de partes:

- $F : \mathcal{P}(Y) \to \mathcal{P}(X)$, $F(B) = f^{-1}(B)$ (imagen inversa),
- $G : \mathcal{P}(X) \to \mathcal{P}(Y)$, $G(A) = f(A)$ (imagen directa).

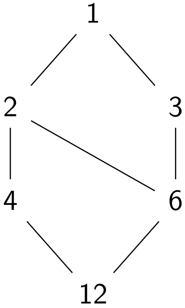
Probar que F siempre es un morfismo de retículos, pero G es un morfismo de retículo si y sólo si f es inyectiva (en cuyo caso puede interpretarse también como una imagen inversa).

Ejemplo

D_{12} :



D_{12}^{*} (dual) :



- id : $D_{12} \to D_{12}^{*}$ es antiisomorfismo.
- $\exists f : D_{12} \to D_{12}^{*}$ isomorfismo: $\begin{cases} f(1) = 12 & f(12) = 1 \\ f(2) = 6 & f(3) = 4 \\ f(4) = 3 & f(6) = 2 \end{cases}$

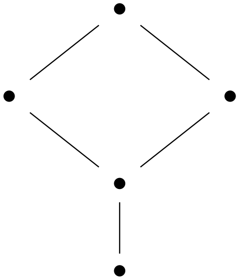
Ejemplo anterior generalizado

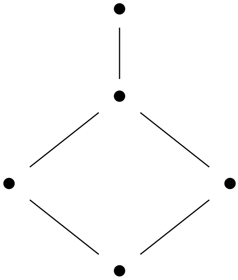
- $D_n \simeq D_n^*$ (isomorfismo de retículos).
- Más precisamente, $f : D_n \to D_n^*$ definida por $f(x) = \frac{n}{x}$ es un isomorfismo (ejercicio). Hay que probar:

$$\forall x, y \in D_n, \begin{cases} \dfrac{n}{\mathrm{mcm}(x,y)} = \mathrm{mcd}\left(\dfrac{n}{x}, \dfrac{n}{y}\right) \\ \dfrac{n}{\mathrm{mcd}(x,y)} = \mathrm{mcm}\left(\dfrac{n}{x}, \dfrac{n}{y}\right) \end{cases}$$

Observación

- Siempre vale que L es antiisomorfo a L^* (la identidad es un antiisomorfismo).
- No siempre es cierto que L sea isomorfo a L^*.





(Distinto diagrama de Hasse.)

Retículos acotados y complementados

Definición

Un **retículo acotado** es una estructura de la forma

$$(\underbrace{L, \vee, \wedge}_{\text{retículo}}, \underbrace{0}_{\text{mínimo}}, \underbrace{1}_{\text{máximo}}).$$

Es decir,

- $\forall x \in L, 0 \vee x = x$,
- $\forall x \in L, x \vee 1 = 1$.

Ejemplos

- $(D_n, \mathrm{mcm}, \mathrm{mcd}, 1, n)$ es un retículo acotado.
- $(\mathbb{N}, \mathrm{mcm}, \mathrm{mcd})$ no admite una estructura de retículo acotado (no tiene máximo).
- $(\mathcal{P}(X), \cup, \cap, \varnothing, X)$ es un retículo acotado.

Definición

Sea $(L, \vee, \wedge, 0, 1)$ un retículo acotado. Decimos que $a \in L$ es **complementado** por $b \in L$ (o que b es un **complemento** de a) si

$$a \vee b = 1, \qquad\qquad a \wedge b = 0.$$

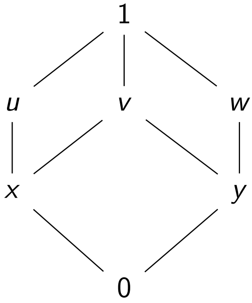
Ejemplo paradigmático

Consideremos el retículo acotado $(\mathcal{P}(X), \cup, \cap, \varnothing, X)$. Entonces

$$\forall A \in \mathcal{P}(X), \begin{cases} A \cup A^c = X \\ A \cap A^c = \varnothing \end{cases}$$

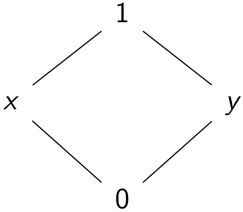
Por lo tanto, A^c es un complemento (el único en este caso) de A, de acuerdo a nuestra nueva definición.

Más ejemplos



- comps(v) $= \varnothing$
- comps(w) $= \{x, u\}$

- comps(x) $= \varnothing$
- comps(0) $= \{1\}$
- comps(1) $= \{0\}$



Todo elto. tiene un complemento.

Ejercicio

- 0 y 1 son complementos uno del otro.
- En una cadena, 0 y 1 son los únicos elementos que tienen complementos.

Retículo complementado

Es un retículo

$$(\underbrace{L, \vee, \wedge, 0, 1}_{\text{retículo acotado}}, (\ )^c)$$

En donde $(\ )^c : L \to L$ es una función $a \mapsto a^c$ que asigna al elemento a un complemento a^c.

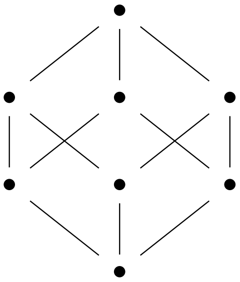
Observación

En general no hay una única forma de definir la función complemento (si es que existe).

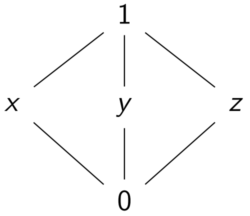
Ejemplo paradigmático

$(\mathcal{P}(X), \cup, \cap, \varnothing, X, (\ )^c)$.

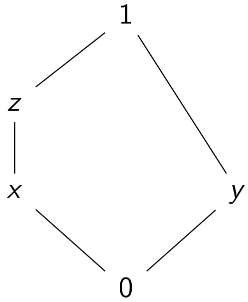
Ejemplos



$\exists!(\ )^c$ ¿por qué?



- $0^c = 1$, $1^c = 0$
- $x^c = y$ ó $x^c = z$
- $y^c = x$ ó $x^c = z$
- $z^c = x$ ó $x^c = y$
- 8 posibles $(\ )^c$



- $0^c = 1$, $1^c = 0$
- $x^c = y$
- $y^c = x$ ó $y^c = z$
- $z^c = y$
- 2 posibles $(\ )^c$

Retículos distributivos

Lema

Sea $(L, \vee, \wedge)$ *un retículo. Son equivalentes:*

1. $\forall x, y, z \in L$, $\boxed{x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)}$,
2. $\forall x, y, z \in L$, $\boxed{x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)}$.

Demostración.

$1 \implies 2$:

$$\begin{aligned}
(x \vee y) \wedge (x \vee z) &= ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) && \text{[por 1]} \\
&= x \vee (z \wedge (x \vee y)) && \text{[conmut., abs.]} \\
&= x \vee ((z \wedge x) \vee (z \wedge y)) && \text{[por 1]} \\
&= (x \vee (z \wedge x)) \vee (z \wedge y) && \text{[asoc.]} \\
&= x \vee (y \wedge z) && \text{[conmut., abs.]}
\end{aligned}$$

$2 \implies 1$: Ejercicio (se puede hacer en un renglón). $\square$

Definición

Un **retículo distributivo** es un retículo que satisface alguna de las condiciones equivalentes del lema anterior.

Ejemplo

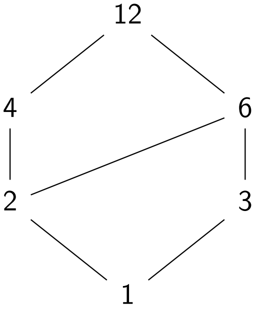
$(\mathcal{P}(X), \cup, \cap)$ es un retículo distributivo:

- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

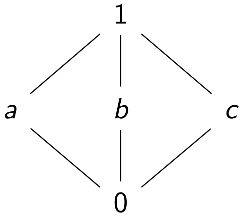
Ejemplo

¿Son distributivos los siguientes retículos?

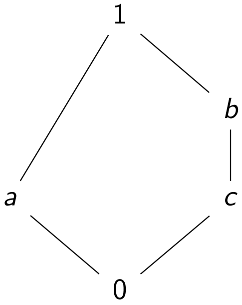
D_{12}



M_3



N_5



Solución

- D_{12}: sí es distributivo. Habría que probar que $\forall x, y, z \in D_{12}$,

$$\mathrm{mcd}(x, \mathrm{mcm}(y, z)) = \mathrm{mcm}(\mathrm{mcd}(x, y), \mathrm{mcd}(x, z)),$$

  lo cual veremos más adelante.
- M_3 (el *diamante*): no es distributivo, por ejemplo

$$\begin{aligned} a \wedge (b \vee c) &= a \\ (a \wedge b) \vee (a \wedge c) &= 0 \end{aligned}$$

- N_5 (el *pentágono*): no es distributivo. (Ejercicio: usar un razonamiento análogo al que usamos para M_3.)

¿Por qué falla la distributividad?

Parece haber problemas cuando hay más de una forma de elegir el complemento de un elemento dado.

Lema

Si $(L, \vee, \wedge, 0, 1)$ *es un retículo acotado y distributivo, entonces todo elemento tiene a lo sumo un complemento.*

Demostración.

Supongamos que $x \in L$ tiene dos complementos $y, z \in L$. Es decir,

$$\begin{aligned} x \wedge y &= x \wedge z = 0, \\ x \vee y &= x \vee z = 1. \end{aligned}$$

Luego

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

Ídem $z \leq y$ y por lo tanto $y = z$. □

Subrretículos

Los subrretículos de un retículo dado $(L, \vee, \wedge)$ son los subconjuntos de L que "heredan" la estructura reticular en el sentido que la inclusión sea un morfismo de retículos. Esto es más fuerte que pedir que restringiendo el orden obtengamos un retículo. Una definición un poco más precisa es la siguiente.

Definición

Sea $(L, \vee, \wedge)$ un retículo. Un subconjunto $M \subset L$ es un subrretículo de L si

- $M \neq \varnothing$,
- $\forall x, y \in M$, $(x \vee y, x \wedge y \in M)$

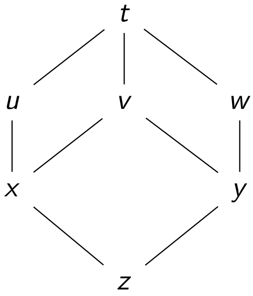
O sea, M es un subconjunto no vacío, el cual es cerrado por las operaciones de L (en particular, M resulta un retículo).

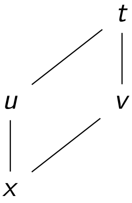
Ejercicio

La inclusión $i : M \hookrightarrow L$ es un morfismo de retículos.

Ejemplo

Consideremos el siguiente retículo $(S, \vee, \wedge)$

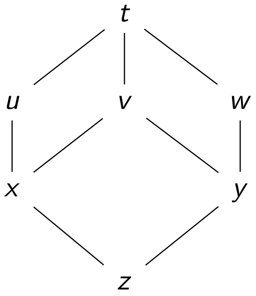


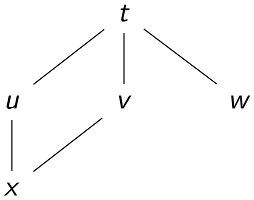


subrretículo (M_1)

Ejemplo

Consideremos el siguiente retículo $(S, \vee, \wedge)$

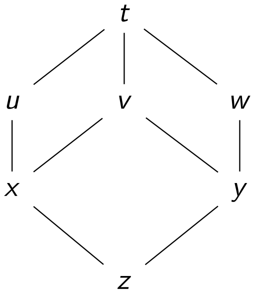


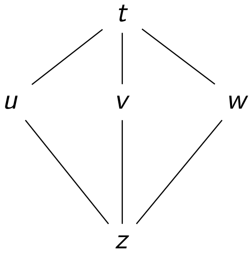


no es retículo (M_2)

Ejemplo

Consideremos el siguiente retículo $(S, \vee, \wedge)$

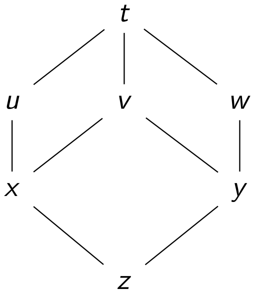


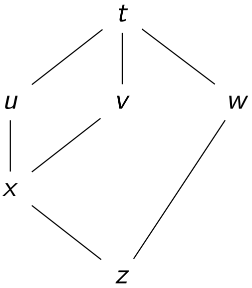


es retículo (M_3) pero NO es subrretículo

Ejemplo

Consideremos el siguiente retículo $(S, \vee, \wedge)$

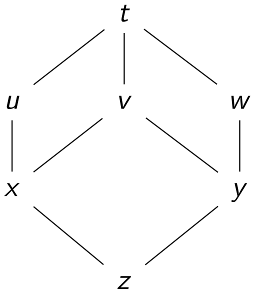


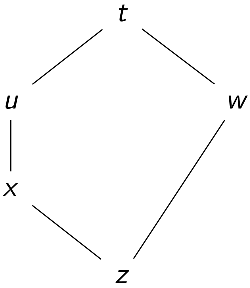


es retículo (M_4) pero NO es subrretículo

Ejemplo

Consideremos el siguiente retículo $(S, \vee, \wedge)$





subrretículo (N_5)

Los ejemplos anteriores no fueron tomados al azar:

Teorema (M_3-N_5 Theorem)

Un retículo es distributivo $\iff$ *no contiene subrretículos isomorfos a* M_3 *o* N_5*.*

Aplicación 1

Un orden total es un retículo distributivo. Es inmediato del teorema (pues ni M_3 ni N_5 tienen órdenes totales). Pero también podemos probarlo directamente: notar que en este caso

- $x \vee y = \max\{x, y\}$,
- $x \wedge y = \min\{x, y\}$.

Luego, hay que probar (ejercicio) que $\forall x, y, z$,

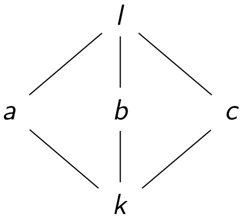
$$\max\{x, \min\{y, z\}\} = \min\{\max\{x, y\}, \max\{x, z\}\}$$
$$\min\{x, \max\{y, z\}\} = \max\{\min\{x, y\}, \min\{x, z\}\}$$

(Basta con probar una sola de estas dos igualdades)

Aplicación 2

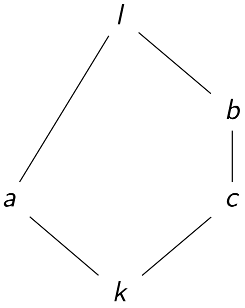
$(D_n, \mid)$ es un retículo distributivo. Usando el teorema tenemos que descartar dos casos.

- D_n no tiene un subrretículo isomorfo a M_3



- $\mathrm{mcd}(a, b) = \mathrm{mcd}(a, c) = \mathrm{mcd}(b, c) = k$
- $a = ka'$, $b = kb'$, $c = kc'$ en donde a', b', c' son coprimos dos a dos
- $\mathrm{mcm}(a, b) = \mathrm{mcm}(a, c) = \mathrm{mcm}(b, c) = l$
- $\mathrm{mcm}(a, b) = ka'b' = l$
- $\mathrm{mcm}(a, c) = ka'c' = l$
- Luego, $b' = c' \implies b = c$. Absurdo.

- D_n no tiene un subrretículo isomorfo a N_5



- $\text{mcd}(a,b) = \text{mcd}(a,c) = k$, $c \mid b$
- $a = ka'$, $b = kb'$, $c = kc'$
- a', b' coprimos, $c' \mid b'$
- $\text{mcm}(a,b) = ka'b' = l$
- $\text{mcm}(a,c) = ka'c' = l$
- Luego $b' = c' \implies b = c$. Absurdo.

Ejemplo

También se puede ver que D_n es distributivo sin usar el teorema M_3-N_5. Veamos que mcd se distribuye sobre mcm (la otra queda como ejercicio). Es decir, hay que ver que

$$\mathrm{mcd}(a, \mathrm{mcm}(b, c)) = \mathrm{mcm}(\mathrm{mcd}(a, b), \mathrm{mcd}(a, c)) \qquad (1)$$

Usamos el teorema fundamental de la aritmética

$$\begin{array}{ll}
n = p_1^{N_1} \cdots p_s^{N_s} & \text{descomp. en primos } \neq \\
a = p_1^{A_1} \cdots p_s^{A_s} & A_i, B_i, C_i \leq N_i \\
b = p_1^{B_1} \cdots p_s^{B_s} & \mathrm{mcd}(a, b) = \prod p_i^{\text{mín}(A_i, B_i)} \\
c = p_1^{C_1} \cdots p_s^{C_s} & \mathrm{mcm}(a, b) = \prod p_i^{\text{máx}(A_i, B_i)}
\end{array}$$

Luego, (1) es equivalente a la distributividad en $(\mathbb{N}_0, \leq)$:

$$\text{mín}(A_i, \text{máx}(B_i, C_i)) = \text{máx}(\text{mín}(A_i, B_i), \text{mín}(A_i, C_i)).$$