

Retículos. Parte 2.

Silvio Reggiani

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

5 de octubre de 2020

Álgebras de Boole

Definición

Un **álgebra de Boole** es un retículo acotado, distributivo con complementos:

$$(B, \vee, \wedge, 0, 1, ()^c).$$

(Recordar que la distributividad implica que la función $()^c$ es única.)

Las álgebras de Boole son importantes porque:

- ▶ capturan la estructura fundamental de la lógica clásica:
 $\vee = \text{OR}$, $\wedge = \text{AND}$, $0 = \perp$, $1 = \top$, $()^c = \text{NOT}$;
- ▶ modelan la teoría de conjuntos (en la cual se basa toda la matemática).

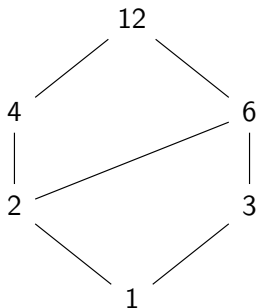
Ejemplo

$(\mathcal{P}(X), \cup, \cap, \emptyset, X, ()^c)$ es un álgebra de Boole.

Ejemplo

$(D_n, \text{mcm}, \text{mcd}, 1, n)$ admite una estructura de álgebra de Boole
 $\iff n = p_1 \cdot p_2 \cdots p_s$ es producto de primos distintos.

Subejemplo D_{12}



No es álgebra de Boole pues 2 no tiene complementos.

Subejemplo

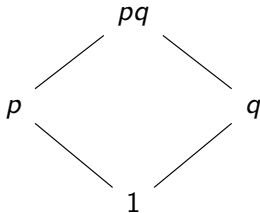
Si n es tal que $p^2 \mid n$ (con p primo) entonces p no tiene complementos en D_n . Por lo tanto D_n no es álgebra de Boole si n no es producto de primos distintos (faltaría probar la otra implicación). En efecto,

$$\text{mcm}(p, x) = n \implies p \mid x \implies p \mid \text{mcd}(p, x) \neq 1.$$

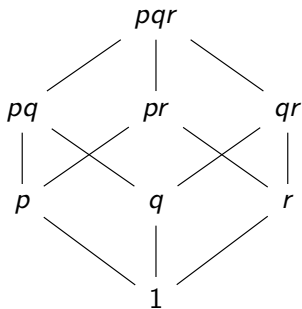
Ejemplo $D_p \simeq \mathcal{P}(\{p\})$



Ejemplo $D_{pq} \simeq \mathcal{P}(\{p, q\})$



Ejemplo $D_{pqr} \simeq \mathcal{P}(\{p, q, r\})$



Caso general

- ▶ D_n con $n = p_1 \cdot p_2 \cdots p_s$ (primos distintos).
- ▶ $x \in D_n \iff x = p_{i_1} \cdots p_{i_k}$ para algún subconjunto $\{i_1, \dots, i_k\} \subset \{1, \dots, s\}$.
- ▶ $\frac{n}{x} = \prod_{j \notin \{i_1, \dots, i_k\}} p_j$ y por lo tanto
- ▶ $\text{mcm}\left(x, \frac{n}{x}\right) = n$ y $\text{mcd}\left(x, \frac{n}{x}\right) = 1$.
- ▶ Es decir, $\frac{n}{x}$ es el complemento de x .

Ejercicio

La función $f : D_n \rightarrow \mathcal{P}(\{p_1, \dots, p_s\})$ definida como

$$f(x) = \{p_{i_1}, \dots, p_{i_k}\}$$

es un isomorfismo de retículos.

Morfismos de álgebras de Boole

- ▶ Los **(iso)morfismos de álgebras de Boole** pueden definirse abstractamente como las funciones (biyectivas)

$$f : (B, \vee, \wedge, 0, 1, ()^c) \rightarrow (B', \vee, \wedge, 0, 1, ()^c)$$

tales que $\forall x, y \in B$,

- ▶ $f(x \vee y) = f(x) \vee f(y)$,
 - ▶ $f(x \wedge y) = f(x) \wedge f(y)$,
 - ▶ $f(0) = 0$,
 - ▶ $f(1) = 1$,
 - ▶ $f(x^c) = f(x)^c$.
- ▶ Ya vimos que las dos primeras condiciones implican las otras tres. Es decir, los isomorfismos de álgebras de Boole no son otra cosa que los isomorfismos de retículos.

Ejercicio*

Si (B, \leq) es un álgebra de Boole finita, entonces

$$(B, \leq) \simeq (\mathcal{P}(X), \subset)$$

para algún conjunto finito X . ¿Quién debería ser el conjunto X ?

Corolario

Si $(B, \vee, \wedge, 0, 1, ()^c)$ es un álgebra de Boole finita, entonces $|B| = 2^n$ para algún $n \in \mathbb{N}_0$.

Contraejemplo

El resultado anterior deja de valer si B tiene infinitos. Por ejemplo, si $(B, \vee, \wedge, 0, 1, ()^c)$ es un álgebra de Boole numerable, entonces $B \not\cong \mathcal{P}(X)$ para todo conjunto X . En efecto, B no puede estar en biyección con $\mathcal{P}(X)$ pues

- ▶ si X es finito, entonces $\mathcal{P}(X)$ es finito de cardinal $2^{|X|}$ y
- ▶ si X es numerable (no puede ser más grande), entonces $|\mathcal{P}(X)| = |\mathcal{P}(\mathbb{N})| = |\mathbb{R}| > |\mathbb{N}| = |B|$ (¿por qué?).

Ejemplo concreto (ejercicio)

- ▶ $\mathcal{P}(\mathbb{N})_{\text{fin}} := \{A \subset \mathbb{N} : |A| < \infty\}$ (subconjuntos finitos de \mathbb{N}),
- ▶ $\mathcal{P}(\mathbb{N})_{\text{cofin}} := \{A \subset \mathbb{N} : |A^c| < \infty\}$, (subconjuntos de \mathbb{N} con complemento finito),
- ▶ $B := \mathcal{P}(\mathbb{N})_{\text{fin}} \cup \mathcal{P}(\mathbb{N})_{\text{cofin}}$,
- ▶ B es numerable,
- ▶ $(B, \cup, \cap, \emptyset, \mathbb{N}, ()^c)$ es un álgebra de Boole (más aún, es una *subálgebra* de Boole de $\mathcal{P}(\mathbb{N})$).

Leyes de De Morgan

Proposición

Si $(B, \vee, \wedge, 0, 1, ()^c)$ es un álgebra de Boole entonces para todos $x, y \in B$ se cumplen:

► $(x \vee y)^c = x^c \wedge y^c;$

► $(x \wedge y)^c = x^c \vee y^c.$

En otras palabras: la función complemento es un antiisomorfismo de álgebras de Boole.

Demostración.

Para el primer ítem debemos chequear que

► $(x \vee y) \wedge (x^c \wedge y^c) = 0$

► $(x \vee y) \vee (x^c \wedge y^c) = 1$

y para el segundo debemos chequear que

► $(x \wedge y) \wedge (x^c \vee y^c) = 0$

► $(x \wedge y) \vee (x^c \vee y^c) = 1.$

Demostración (cont.)

$$\begin{aligned}(x \vee y) \wedge (x^c \wedge y^c) &= [(x \vee y) \wedge x^c] \wedge y^c \\&= [(x \wedge x^c) \vee (y \wedge x^c)] \wedge y^c \\&= [0 \vee (y \wedge x^c)] \wedge y^c \\&= (y \wedge x^c) \wedge y^c = (y \wedge y^c) \wedge x^c \\&= 0 \wedge x^c = 0\end{aligned}$$

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

Ejercicio: completar las otras dos igualdades (se puede hacer bien fácil por dualidad, teniendo en cuenta una sutileza). □

Idea de la demostración del teorema M_3-N_5

Retículos modulares

Un retículo (L, \vee, \wedge) se dice **modular** si

$$\forall x, y, z \in L, [x \geq z \implies x \wedge (y \vee z) = (x \wedge y) \vee z].$$

Observar que **distributivo** \implies **modular**.

Ejemplo

- ▶ $L = \{\text{subespacios vectoriales de } \mathbb{R}^n\}$,
- ▶ (L, \subset) es retículo, **pero no es subretículo de $\mathcal{P}(\mathbb{R}^n)$** (pues la unión de subespacios no necesariamente es un subespacio),
- ▶ $V \wedge W = V \cap W$,
- ▶ $V \vee W = V + W := \langle V \cup W \rangle$ (subespacio generado).
- ▶ L es modular. En efecto, debemos probar que

$$U \supset W \implies U \cap (V + W) = (U \cap V) + W.$$

Ejemplo (cont.)

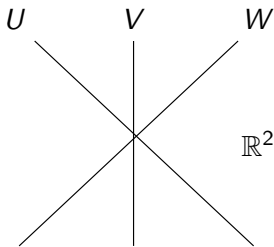
- ▶ $x \in U \cap (V + W) \implies x = v + w \in U$ con $v \in V, w \in W$.
- ▶ Luego $v = x - w \in U$ pues $W \subset U \implies v \in U \cap V$
- ▶ y por ende $x \in (U \cap V) + W$.

Recíprocamente,

- ▶ $x = u + w$ con $u \in U \cap V \subset V, w \in W \implies x \in U$.
- ▶ Luego $x \in U \cap (V + W)$.

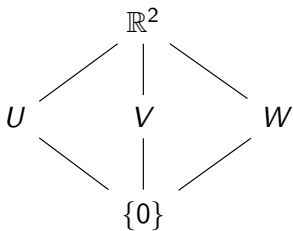
Observación

- ▶ L no es distributivo.
- ▶ $U \cap (V + W) = U \cap \mathbb{R}^2 = U$,
- ▶ $(U \cap V) + (U \cap W) = \{0\}$.



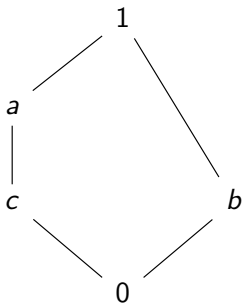
Ejemplo

M_3 es modular (no es distributivo):
ídem ejemplo anterior.



Ejemplo

- ▶ N_5 no es distributivo ni modular.
- ▶ $a \geq c$,
- ▶ $a \wedge (b \vee c) = a \wedge 1 = a$,
- ▶ $(a \wedge b) \vee c = 0 \vee c = c$.



Retículos libres

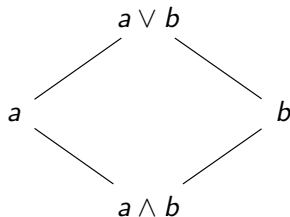
- ▶ Partimos de una cantidad prefijada de elementos (podrían ser infinitos):

$$X = \{x, y, z, \dots\}.$$

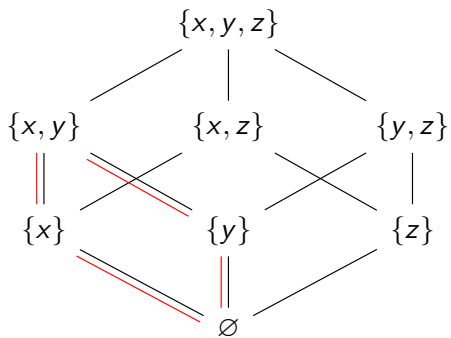
- ▶ Definimos las operaciones $x \wedge y$, $x \wedge z$, $y \vee z$, $x \wedge (y \vee z)$, etc. sin restricciones (de manera libre), agregando tantos elementos como sean necesarios, **salvo por las restricciones que impone la estructura, por ejemplo**
- ▶ $x \wedge x = x \vee x = x \vee (x \wedge z) = x$, etc.
- ▶ Formamos el **retículo libre** $F(X)$ (siempre existe).
- ▶ $F(X)$ tiene la siguiente **propiedad universal**: para todo retículo L tal que $X \subset L$ “monótonamente incluido” existe un único morfismo de retículos $\varphi : F(X) \rightarrow L$ tal que $\varphi(x) = x$ para todo $x \in X$.

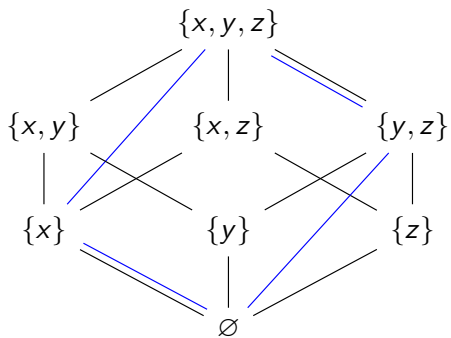
Ejemplo

- $F(\{a, b\}) \simeq \mathcal{P}(\{a, b\})$.



- $\{a, b\}$ se puede incluir monótonamente en $\mathcal{P}(\{x, y, z\})$ de varias formas distintas por ejemplo en $\{\{x\}, \{y\}\}$ o en $\{\{x\}, \{y, z\}\}$.
- Esto nos da distintas copias de $F(\{a, b\})$ dentro de $\mathcal{P}(\{x, y, z\})$ (como subrretículos).





Observación

- ▶ $\mathcal{P}(\{x, y, z\})$ no es un retículo libre.
- ▶ Más adelante veremos una justificación precisa mostrando explícitamente quién es el retículo libre en tres elementos.
- ▶ Idea intuitiva: $\mathcal{P}(\{x, y, z\})$ es un álgebra de Boole y propiedades como la distributividad imponen fuertes restricciones a las operaciones \vee, \wedge , que no están presentes en un retículo libre.
- ▶ Notar sin embargo (ejemplo anterior) que $\mathcal{P}(\{x, y\})$ sí es un retículo libre (al comenzar con tan pocos elementos, propiedades como la distributividad y la existencia de complementos deben valer forzosamente).

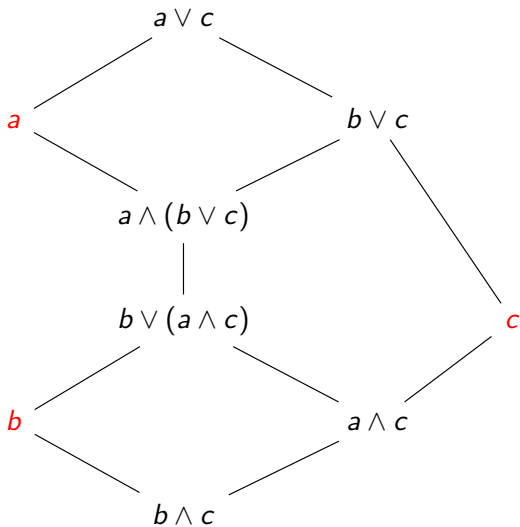
Retículos libres con restricciones

Es posible formar retículos libres en un conjunto X imponiendo ciertas relaciones entre elementos de X o ciertas propiedades sobre el retículo a construir (por ejemplo que sea distributivo, modular, etc.).

Ejemplo/Ejercicio

El retículo libre en $\{a, b, c\}$ sujeto a la restricción $b < a$ es:

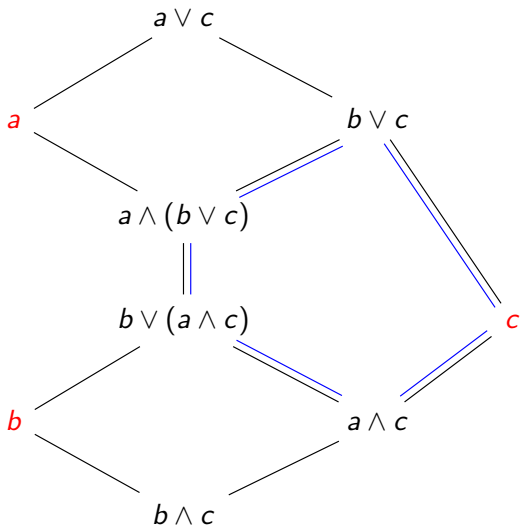
$$F_{b < a}(3)$$



Ejemplo/Ejercicio

El retículo libre en $\{a, b, c\}$ sujeto a la restricción $b < a$ es:

$$F_{b < a}(3)$$



Teorema

El retículo distributivo libre generado por $\{x, y, z\}$ tiene 18 elementos.

Teorema (Dedekind ~ 1900)

El retículo libre generado por $\{x, y, z\}$ tiene 28 elementos.

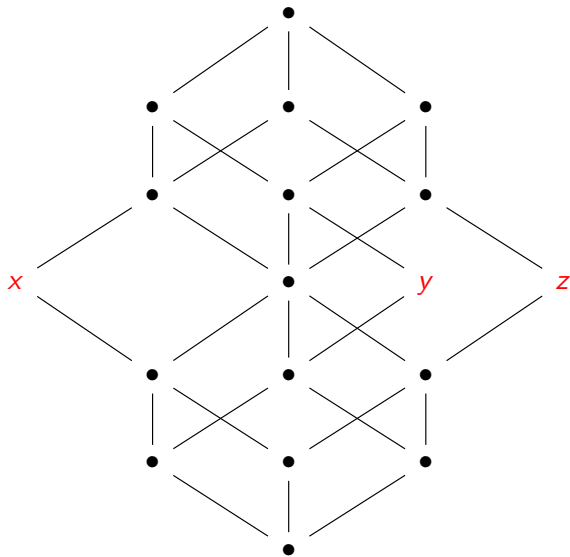
Corolario

$\mathcal{P}(\{x, y, z\})$ no es un retículo libre.

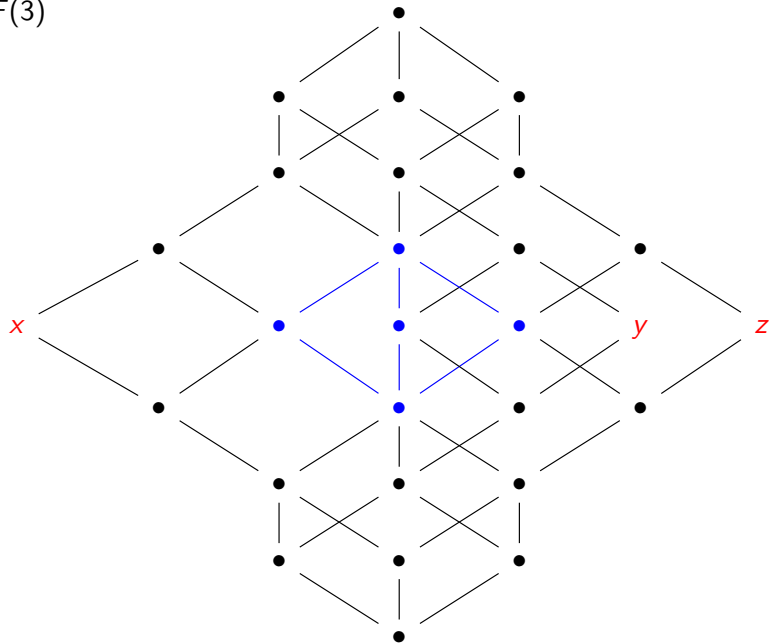
Teorema

El retículo libre en $\{x, y, z, t\}$ tiene infinitos elementos.

$$F_{\text{dist}}(3)$$



$F(3)$



Cocientes

- ▶ $\varphi : L \rightarrow K$ morfismo de retículos.
- ▶ $\ker \varphi$ relación de equivalencia en L :

$$a \sim b \iff \varphi(a) = \varphi(b).$$

- ▶ $L / \ker \varphi$ es un retículo isomorfo a $\text{im } \varphi$ (teorema de isomorfismo).

Teorema

Sea L un retículo. Entonces

1. *L es modular \iff no tiene subretículos isomorfos a N_5 .*
2. *Si L es modular entonces, L es distributivo \iff no tiene subretículos isomorfos a M_3 .*

Demostración

Lema (Ejercicio)

Un subretículo de un retículo modular (resp. distributivo) es modular (resp. distributivo).

Prueba de 1.

- ▶ Sean $a, b, c, \in L$ tales que $a > b$ y $a \wedge (b \vee c) \neq (a \vee b) \wedge c$.
- ▶ $\exists \varphi : F_{b < a}(3) \rightarrow L$ morfismo de retículos (inclusión).
- ▶ $N_5 \subset F_{b < a}(3)$ induce un morfismo de retículos $\varphi| : N_5 \rightarrow L$.
- ▶ $\text{im}(\varphi|) = N_5 / \ker(\varphi|) = N_5$.
- ▶ Ejercicio: N_5 no tiene cocientes, es decir $\ker(\varphi|) = \Delta$ es la relación de igualdad.

Prueba de 2.

- ▶ Si L es modular y no distributivo entonces existen $x, y, z \in L$ tales que $x \wedge (y \vee z) \neq (x \wedge y) \vee (x \wedge z)$.
- ▶ $\exists \varphi : F(3) \rightarrow L$ morfismo de retículos.
- ▶ $M_3 \subset F$ induce un morfismo $\varphi| : M_3 \rightarrow L$.
- ▶ $\text{im}(\varphi|) = M_3 / \ker(\varphi|) = M_3$.
- ▶ Ejercicio: M_3 no tiene cocientes.

