

Reticulados y Álgebras de Boole

Héctor Gramaglia y Alejandro Tiraboschi

1 Relaciones

1.1 El concepto de relación

Según la Real Academia Española, el término relación remite a:

1. Exposición que se hace de un hecho.
2. Conexión, correspondencia de algo con otra cosa.
3. Conexión, correspondencia, trato, comunicación de alguien con otra persona.
4. Trato de carácter amoroso. U. m. en pl. Tienen relaciones desde hace tiempo
5. Lista de nombres o elementos de cualquier clase.
6. Informe que generalmente se hace por escrito, y se presenta ante una autoridad.
7. En el poema dramático, trozo largo que dice un personaje para contar o narrar algo.
8. Gram. Conexión o enlace entre dos términos de una misma oración.
9. Mat. Resultado de comparar dos cantidades expresadas en números.
10. En diversos bailes tradicionales, copla que se dicen los integrantes de las parejas.
11. Conocidos o amigos influyentes. Sin relaciones no se puede triunfar en esa profesión.

Probablemente esta cita no aporte mucho a las ideas que el lector tiene sobre lo que es una relación, pero en realidad aquí estamos interesados en la *determinación* que la matemática logra para sus propósitos de dicho concepto. El punto 9, referido a la matemática, nos da una pista: el resultado de comparar dos cantidades expresadas en números es un “sí” o un “no”, si es que la relación está perfectamente determinada. Por ejemplo, podemos determinar completamente la relación “es menor que”, siempre que logremos responder “sí” o “no” cada vez que se hace la pregunta ¿es x menor que y ?, cualesquiera sean los elementos x e y que se tomen.

Vemos entonces que una relación entre individuos del universo X e individuos del universo Y , determina un conjunto: el conjunto de todos los pares (ordenados) de individuos para los cuales la pregunta

¿está x relacionado con y ?

se contesta afirmativamente. Ese conjunto será nuestra determinación matemática del concepto de relación. Por ejemplo, si

C representa la relación “es la capital de”

P representa la relación “es subconjunto de”

entonces decimos que el par (El Cairo, Egipto) pertenece al conjunto determinado por la relación C , mientras que $(\{1, 2\}, \{1, 3, 4\})$ no pertenece al conjunto determinado por la relación P . Nótese que es importante el *orden* de los objetos en cuestión, ya que por un lado porque pueden pertenecer a universos distintos, y por otro lado porque al alterar el orden puede cambiar el valor de verdad de la proposición. Esto ocurre con el predicado P .

Las relaciones “denotan” conjuntos de pares ordenados de la misma manera que una proposición Q (que se refiere a individuos en un universo X) denota el conjunto formado por los individuos que la satisfacen:

$$Q \text{ denota } \{x \in X : Q(x)\}$$

Recurra aquí a cualquier noción provisoria que usted tenga del término proposición, inclusive no matemática.

Definición 1.1. Sean A y B conjuntos. Una relación entre A y B es un subconjunto del producto cartesiano $A \times B$.

Si R es una relación entre A y B decimos que x está relacionado con y (y lo denotamos $x \sim_R y$) si $(x, y) \in R$. Notaciones alternativas son $R(x, y)$, xRy o simplemente $x \sim y$. Si $A = B$ solemos decir que R es una relación sobre A .

Ejemplo 1.1. Sea $A = \{2, 3\}$ y $B = \{3, 4, 5, 6\}$, y consideremos la relación “divide”, que vincula elementos de A con elementos de b . Podemos definir R mediante:

$$R = \{(a, b) \mid a \in A, b \in B \text{ y } a \text{ divide a } b\}$$

Luego $R = \{(2, 4), (2, 6), (3, 3), (3, 6)\}$ y decimos que $2 \sim 4$, $2 \sim 6$, $3 \sim 3$ y $3 \sim 6$. También decimos que 2 no está relacionado con 5 y que 3 no está relacionado con 4 y escribimos $2 \not\sim 5$ y $3 \not\sim 4$.

Ejemplo 1.2. Sea $A = B = \mathbb{Z}$, $R = \{(x, y) \mid y = x^2\}$. R es un subconjunto de $\mathbb{Z} \times \mathbb{Z}$ y con una cantidad infinita de elementos:

$$-1 \sim 1 \quad 1 \sim 1$$

$$-2 \sim 4 \quad 2 \sim 4$$

$$-3 \sim 9 \quad 3 \sim 9$$

$$\vdots \quad \vdots$$

Tres tipos de relaciones son las más relevantes dentro de la matemática: las *funciones*, las *relaciones de orden* y las de *equivalencia*. Las funciones son relaciones entre dos conjuntos que pueden ser distintos y no se incluirán en este texto debido a que es usual verlas en profundidad en otras materias. Las relaciones de orden y de equivalencia son relaciones sobre un mismo conjunto y veremos su definición y algunas propiedades en este capítulo, concentrándonos sobre todo en las relaciones de orden.

Consideraremos de ahora en más relaciones sobre un mismo conjunto.

1.2 Propiedades de las relaciones

La forma natural de distinguir tipos de relaciones es considerar sus propiedades más relevantes. Cuando hablamos de *propiedades de las relaciones*, nos estamos refiriendo a aquellas características que no tengan que ver con un universo particular, sino que refieran a situaciones factibles de ser observadas (afirmadas o refutadas) en cualquier relación, independientemente del universo particular en donde cada una este definida. El uso de distintos tipos de relaciones en diversas áreas de la matemática ha arrojado variados tipos de propiedades, de las cuales vamos a mencionar las que son relevantes para nuestros objetivos.

Definición 1.2. Sea R una relación sobre un conjunto A . Decimos que R es

(a) *reflexiva* si y sólo si para todo a en A , $a \sim a$, en símbolos:

$$\forall a \ a \sim a;$$

(b) *simétrica* si y sólo si para todo $a, b \in A$, $a \sim b$ implica que $b \sim a$, en símbolos:

$$\forall a \ \forall b \ a \sim b \Rightarrow b \sim a;$$

(c) *antisimétrica* si y sólo si para todo $a, b \in A$ $a \sim b$ y $b \sim a$ implican que $a = b$, en símbolos:

$$\forall a \ \forall b \ (a \sim b) \wedge (b \sim a) \Rightarrow a = b;$$

(d) *transitiva* si y sólo si para todo a, b y c , $a \sim b$ y $b \sim c$ implican que $a \sim c$, en símbolos:

$$\forall a \ \forall b \ \forall c \ (a \sim b) \wedge (b \sim c) \Rightarrow a \sim c.$$

Antes de continuar, para poner en juego las propiedades definidas, sugerimos responder las siguientes cuestiones.

1. Para cada una de las siguientes relaciones responda si es válida cada una de las cuatro propiedades anteriores.

- (a) Sobre las ciudades de Argentina: la distancia de x a Buenos Aires es menor o igual que la distancia de y a Buenos Aires.
- (b) Sobre las ciudades de Argentina: la distancia de x a Buenos Aires es igual a la distancia de y a Buenos Aires.

2. Sea G un grafo dirigido con vértices V . Considere sobre V la relación

“existe un camino dirigido que lleva desde x hasta y ”.

Considere además las siguientes propiedades sobre los grafos:

- (a) G es **no dirigido** (si existe una arista de a a b , también existe una de b a a)
- (b) G es **completo**
- (c) G es **acíclico**

Determine cuales de estas propiedades son **suficientes**, y cuales **necesarias** para asegurar que:

- (a) La relación es **reflexiva**
- (b) La relación es **simétrica**
- (c) La relación es **antisimétrica**

- 3. Responda si la relación sobre $A = \mathbb{R}$ dada por $a \sim b$ si y sólo si $a \leq b$ es reflexiva, simétrica, antisimétrica y/o transitiva.
- 4. Responda si la relación sobre $A = \mathcal{P}(X)$ dada por $A \sim B$ si y sólo si $A \subseteq B$ es reflexiva, simétrica, antisimétrica y/o transitiva.

1.3 Relación “divide” y “congruente”

Estas dos relaciones serán ejemplos paradigmáticos de las categorías de relaciones que nos interesa estudiar. Analicemos ahora las propiedades que cada una de estas relaciones tiene.

Sea R la relación sobre \mathbb{N} dada por:

$a \sim b$ si y sólo si a divide a b .

- (1) Es reflexiva:

$a = a \cdot 1$, luego a divide a a para todo $a \in \mathbb{N}$;

(2) no es simétrica, pues

2 divide a 4 pero 4 no divide a 2;

(3) es antisimétrica, pues

si a divide a b entonces $b = a.m$ para algún $m \in \mathbb{Z}, m > 0$,

si b divide a a entonces $a = b.k$, para algún $k \in \mathbb{Z}, k > 0$,

por lo tanto $a = b.k = (a.m).k = a.(m.k)$, de donde se deduce que $m = k = 1$ y entonces $a = b$.

(4) es transitiva, pues

si a divide a b entonces $b = a.k$, para algún $k \in \mathbb{Z}$,

si b divide a c entonces $c = b.j$, para algún $j \in \mathbb{Z}$,

pero entonces $c = b.j = a(k.j)$, es decir que a divide a c .

Resumiendo, la relación “**divide**” es **reflexiva, antisimétrica y transitiva**.

Considere ahora $A = \mathbb{Z}$, y sea R la relación dada por

$a \sim b$ si y sólo si a y b tienen la misma paridad.

Observemos que si a y b son ambos pares o ambos impares entonces $a - b$ es par y que si tienen distinta paridad entonces $a - b$ es impar. Luego

$$R = \{(m, n) : 2|m - n\}$$

A esta relación se la conoce como “congruencia módulo 2”. De manera similar se puede definir la “congruencia módulo k ”, en la que dos números resultarán congruentes si al dividirlos por k tienen el mismo resto.

Vamos ahora a justificar las propiedades de la relación R .

(1) es reflexiva,

$m - m = 0$, y 0 es par;

(2) es simétrica

si $m - n$ es par, entonces $n - m = -(m - n)$ es par;

(3) no es antisimétrica

$2 \sim 4$ y $4 \sim 2$ pero $2 \neq 4$;

(4) es transitiva

si $m - n$ es par y $n - p$ es par entonces $m - p = (m - n) + (n - p)$ que es par.

Resumiendo, la relación “congruencia módulo 2” es **reflexiva, simétrica y transitiva**.

1.4 Relaciones de equivalencia

El ejemplo de la relación “congruencia” nos acerca a un tipo de relaciones muy relevante en matemática, que están presentes fuertemente en los desarrollos de las estructuras algebraicas y la topología.

Definición 1.3. Una relación \simeq sobre un conjunto A es de equivalencia si es reflexiva, simétrica y transitiva.

Sobre cualquier conjunto, la relación “igual” es trivialmente una relación de equivalencia. Además hemos justificado detalladamente que la relación “tienen la misma paridad” también lo es. De la misma manera se puede demostrar que la relación “congruencia módulo k ” es una relación de equivalencia.

Las tres propiedades que definen este tipo de relaciones permiten que emerja la noción de *clase de equivalencia* de un elemento x , refiriéndose ésta al conjunto de todos los elementos que están relacionados con x .

Definición 1.4. Sea \simeq una relación de equivalencia sobre un conjunto A y sea x un elemento de A . La clase de equivalencia de x se denota por $[x]$ y es el conjunto

$$[x] = \{y \mid y \in A \text{ e } y \simeq x\}.$$

Note que la simetría hace que la propiedad $y \simeq x$ pueda ser reemplazada por $x \simeq y$, obteniendo el mismo conjunto. Por ejemplo, en la relación “tienen la misma paridad”, los números pares están en la clase de equivalencia del 2, mientras que los impares están en la clase de equivalencia del 1.

Preguntas:

1. ¿Qué resulta la clase de x , entendida como el conjunto $[x] = \{y \mid y \in A \text{ e } y \sim x\}$, en la relación “divide”?
2. ¿Cuáles de las siguientes propiedades son ciertas en las clases de la relación “misma paridad”, y cuáles en las clases de la relación “divide”?
 - (a) $x \sim y \Rightarrow [x] = [y]$
 - (b) $[x] = [y] \Rightarrow x = y$

$$(c) x \in [x]$$

$$(d) x \not\sim y \Rightarrow [x] \cap [y] = \emptyset$$

La acción conjunta de la transitividad y la simetría provocan que las clases de equivalencia no se superpongan (son disjuntas), salvo que se trate de las clases de dos elementos relacionados (por ejemplo el 2 y el 10, en la relación anterior). En este caso las clases coinciden. El lector habrá podido observar este fenómeno analizando las propiedades (a) y (d) de arriba para la relación “misma paridad”.

Teorema 1.1. *Sea \simeq una relación de equivalencia en un conjunto A y sean x, y elementos de A . Entonces*

1. $[x] = [y]$ si y sólo si $x \simeq y$.
2. si $x \not\sim y$, entonces $[x]$ e $[y]$ son disjuntas.

Demostración. (1) Sean $[x]$ e $[y]$ dos clases de equivalencia, tales que $[x] = [y]$. Eso significa que

$$\{a \mid a \simeq x\} = \{a \mid a \simeq y\}.$$

Puesto que $x \simeq x$ eso significa que $x \in [x]$ y por lo tanto $x \in [y]$. Luego $x \simeq y$.

Recíprocamente, si $x \simeq y$ queremos ver que $[x] = [y]$. Probaremos entonces que $[y] \subseteq [x]$ y que $[x] \subseteq [y]$. Ahora bien, $a \in [x]$ si y sólo si $a \simeq x$. Como $x \simeq y$ por transitividad se sigue que $a \simeq y$ y por lo tanto $a \in [y]$.

Análogamente, $a \in [y]$ si y sólo si $a \simeq y$. Pero entonces $a \simeq y$ e $y \simeq x$ de donde se sigue que $a \simeq x$ y por lo tanto $a \in [x]$.

(2) Supongamos que $x \not\sim y$, y tomemos $a \in [x] \cap [y]$, para arribar a una contradicción. Como $a \in [x]$, entonces $a \simeq x$, y por simetría, $x \simeq a$. Por otro lado, como $a \in [y]$, entonces $a \simeq y$. Por transitividad $x \simeq y$, lo que es una contradicción. \square

De esta manera, las relaciones de equivalencia están ligadas a la noción de partición de un conjunto. Recordemos la definición:

Definición 1.5. *Una partición de un conjunto A es una familia de subconjuntos no vacíos de A que son disjuntos entre sí y cuya unión es todo A .*

Por ejemplo, las siguientes son particiones de $A = \{a, b, c\}$:

$$P_1 : \quad \{a\}, \{b\}, \{c\};$$

$$P_2 : \quad \{a\}, \{b, c\};$$

$$P_3 : \quad \{a, b, c\}.$$

Si \simeq es una relación de equivalencia sobre A , entonces podemos partir A de manera que cada parte agrupe a todos los elementos que son equivalentes entre sí.

Por ejemplo, considere $A = \{0, 1, 2, 3, 4, 5, 6\}$, y sea \simeq la relación dada por:

$$a \simeq b \text{ si y sólo si } 3 \text{ divide a } (a - b).$$

Podemos buscar las “partes” en las que se parte A comenzando a rastrear los equivalentes a 0, a saber, $0, 3, 6$. Luego, una parte de la partición está dada por $\{0, 3, 6\}$.

Para encontrar otra de las partes, buscamos los que son equivalentes a alguno de los elementos que no estén en la primera parte, por ejemplo 1. Podemos repetir este procedimiento hasta agotar el conjunto.

La relación \simeq conduce a la siguiente partición:

$$\{0, 3, 6\}, \quad \{1, 4\}, \quad \{2, 5\}.$$

Luego, el teorema anterior que describe las propiedades de las clases de equivalencia puede ser reformulado en términos de las particiones de la siguiente manera.

Teorema 1.2. *Sea \equiv una relación de equivalencia sobre un conjunto A no vacío. La familia de clases de equivalencia es una partición de A . Y recíprocamente, toda partición P de un conjunto A induce una relación de equivalencia definida como $a \simeq_P b$ si y sólo si existe $S \in P$ tal que $a \in S$ y $b \in S$.*

1.5 Relaciones de orden

La idea de “orden” (en un sentido quizá más laxo que el usual) queda capturada a través de 3 de las propiedades antes estudiadas:

Definición 1.6. *Un orden parcial R sobre un conjunto es una relación que es reflexiva, anti-simétrica y transitiva.*

Cuando R sea un orden parcial usaremos la notación $a \preceq b$ si $(a, b) \in R$.

Del trabajo previo ya disponemos de varios ejemplos de relaciones de orden:

1. La relación \leq sobre \mathbb{R} (o \mathbb{Z})
2. La relación “divide” (usamos el símbolo $|$), sobre \mathbb{N}
3. La relación \subseteq sobre $\mathcal{P}(A)$

1.5.1 Diagramas de Hasse

Las relaciones de orden sobre conjuntos finitos pueden ser visualizadas a través de dibujos llamados *diagramas de Hasse*. Se adoptó ese nombre en honor al matemático Helmut Hasse (1898-1979).

La idea del diagrama de Hasse (y de todos los diagramas en general) es eliminar información superflua y concentrarse en la información más relevante relativa al orden. Esta (para los conjuntos finitos) es convenientemente capturada por la noción de cubrimiento.

Definición 1.7. Sea A un conjunto finito parcialmente ordenado. Sean $a, b \in A$ elementos distintos. Decimos que b cubre a a si $a \preceq b$ y no existe c distinto de a y b tal que $a \preceq c$ y $c \preceq b$.

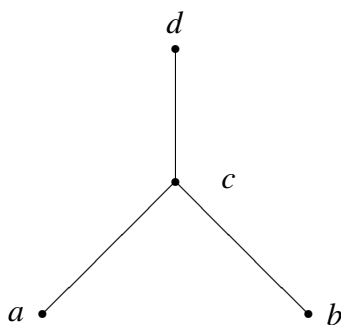
Por ejemplo, sea $X = \{1, 2, 3, 6, 12\}$, con la relación dada por la relación “divide”. Entonces 2 cubre a 1, pero no cubre a 3. Por otro lado, 6 cubre a 2 y 3, pero no cubre a 1 ni 12.

Un *diagrama de Hasse* para un conjunto parcialmente ordenado finito consiste de puntos en el plano llamados *vértices* que representan los elementos del conjunto y de arcos o segmentos ascendentes que unen dos vértices a y b si y sólo si b cubre a a .

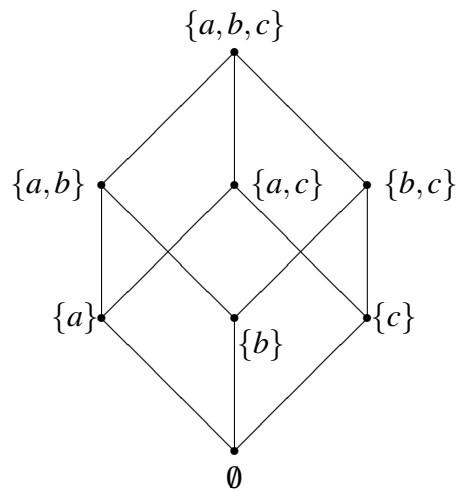
Por ejemplo, sea $P = \{a, b, c, d\}$, y sea \preceq la relación dada por el conjunto

$$\{(a, a), (b, b), (c, c), (d, d), (a, c), (a, d), (c, d), (b, c), (b, d)\}$$

Entonces el diagrama de Hasse correspondiente es:



Ejemplo 1.3. El diagrama de Hasse para $\mathcal{P}(\{a, b, c\})$ ordenado por inclusión es el siguiente.



1.6 Ejercicios

1. Determine si las siguientes relaciones sobre \mathbb{N} son reflexivas, simétricas, antisimétricas o transitivas:
 - (a) $(x, y) \in R$ sii $x^2 = y^2$
 - (b) $(x, y) \in R$ sii $x > y$
 - (c) $(x, y) \in R$ sii $x \geq y$
 - (d) $(x, y) \in R$ sii si el m.c.d. de x e y es 1
 - (e) $(x, y) \in R$ sii $n \neq m$

2. Sea \simeq la relación “congruencia módulo 5”, dada en \mathbb{Z} por $x \simeq y$ si y sólo si 5 divide a $x - y$. Verifique que es una relación de equivalencia.

3. Dé ejemplos de relaciones sobre $\{1, 2, 3, 4\}$ que cumplan las propiedades:
 - (a) Reflexiva, simétrica, no transitiva.
 - (b) Reflexiva, no simétrica, no transitiva.
 - (c) Reflexiva, antisimétrica, no transitiva.
 - (d) No reflexiva, simétrica, no antisimétrica, transitiva.
 - (e) No reflexiva, no simétrica, transitiva.

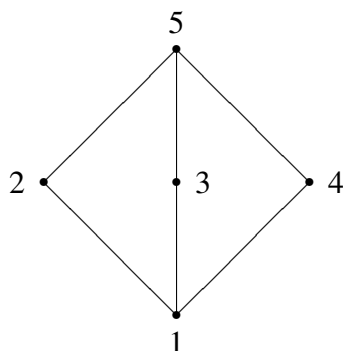
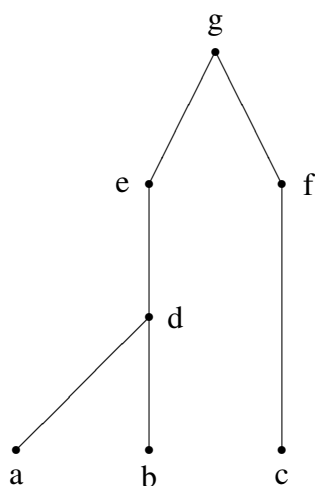
4. Determine si la relación dada es una relación de equivalencia sobre $\{1, 2, 3, 4, 5\}$. Si la relación es de equivalencia, indique las clases de equivalencia.

- (a) $\{(1,1), (2,2), (3,3), (4,4), (5,5), (1,3), (3,1)\}$
- (b) $\{(1,1), (2,2), (3,3), (4,4), (5,5), (1,3), (3,1), (3,4), (4,3)\}$
- (c) $\{(1,1), (2,2), (3,3), (4,4)\}$
- (d) $\{(1,1), (2,2), (3,3), (4,4), (5,5), (1,5), (5,1), (3,5), (5,3), (1,3), (3,1)\}$
- (e) $\{(x,y) \mid 1 \leq x \leq 5, 1 \leq y \leq 5\}$
- (f) $\{(x,y) \mid 4 \text{ divide a } x - y\}$
- (g) $\{(x,y) \mid 4 \text{ divide a } x + y\}$
- (h) $\{(x,y) \mid x \text{ divide a } 2 - y\}$

5. Liste los pares de la relación de equivalencia sobre $\{1, 2, 3, 4\}$ definida por la partición P dada. También señale, en cada caso, las clases de equivalencia $[1]$, $[2]$, $[3]$ y $[4]$.

- (a) $P = \{\{1,2\}, \{3,4\}\}$
- (b) $P = \{\{1\}, \{2\}, \{3\}, \{4\}\}$
- (c) $P = \{\{1,2,3,4\}\}$
- (d) $P = \{\{1\}, \{2,4\}, \{3\}\}$

6. Dados los siguientes diagramas de Hasse, liste todos los pares ordenados de la relación:



7. Dibuje los diagramas de Hasse para cada uno de los siguientes conjuntos con la relación de divisibilidad: $n \sim m$ si y sólo si n divide a m :

- (a) $\{1, 2, 3, 4, 6, 12\}$
- (b) $\{1, 2, 4, 5, 10, 20\}$
- (c) $\{1, 2, 4, 8, 16, 32\}$
- (d) $\{1, 2, 3, 5, 6, 10, 15, 30\}$

8. Sea A un conjunto de personas. ¿Bajo qué circunstancias la relación

$$x \preceq y \text{ si y sólo si } x \text{ es más joven o tiene la misma edad que } y$$

define un orden parcial sobre A ?

9. Dibuje el diagrama de Hasse para el conjunto de subconjuntos propios de $\{a, b, c, d\}$ ordenado por inclusión.

1.7 Problemas

1. Sea R la relación en $D_{60} = \{d \mid d \text{ divide a } 60\}$ dada por:

$$(a, b) \in R \Leftrightarrow 5 \text{ divide a } (a - b)$$

- (a) ¿Sirve la prueba dada en el ejercicio 2 para concluir que R es de equivalencia? ¿Cómo lo justificaría?
- (b) Hallar todas las clases de equivalencia.

2. Sea A el conjunto formado por todas las palabras del alfabeto $\{a, b, c\}$. Considere las palabras como secuencias finitas de símbolos del alfabeto. Por ejemplo $acaaab$, a y ε (la palabra vacía) son elementos de A .

- (a) Defina la relación \trianglelefteq , que representa el orden lexicográfico (o sea el del diccionario) sobre A
- (b) Pruebe \trianglelefteq es una relación de orden.

3. Sea A un conjunto de tres elementos, y sea R una relación de orden parcial sobre A . ¿Cuántos tipos diferentes de diagramas de Hasse de A son posibles? De esta manera sabemos cuántos ordenes parciales diferentes pueden ser definidos sobre un conjunto con tres elementos. Piense detenidamente cuando dos diagramas pueden ser considerados “iguales” y cuando diferentes. Por ejemplo, ¿importan las longitudes de los arcos?, o ¿importan las pendientes de los arcos?

4. Repita la consigna anterior para conjuntos de cuatro elementos. (Ayuda: hay 16.)

5. Sea $S = \{A \mid A \neq \emptyset \text{ and } A \subseteq \{a, b, c\}\}$. Sea R la relación en S dada por:

$$(A, B) \in R \Leftrightarrow (A = \{a\} \text{ y } a \notin B) \text{ o } A \subseteq B.$$

- (a) Probar que es una relación de orden.
- (b) Hacer el diagrama de Hasse correspondiente.

1.8 Operadores

Con las relaciones podemos operar de la misma manera que con las funciones. Una operación muy común en el manejo de funciones es la *composición* (denotada mediante \circ), y su definición puede ser extendida a las relaciones. En este contexto, esta operación hace referencia al resultado de “conectar” relaciones. Por ejemplo, si x es padre de y , e y es padre de z , entonces x es abuelo de z . Esto lo podemos decir escribiendo: *padre* \circ *padre* = *abuelo*. Vamos ahora a introducir formalmente ésta y otras operaciones que también serán de utilidad.

Definición 1.8. Sea R_1 una relación de A a B y sea R_2 una relación de B a C . La composición de R_2 con R_1 es la relación entre A y C dada por:

$$R_2 \circ R_1 = \{(a, c) \mid \text{existe algún } b \in B \text{ tal que } (a, b) \in R_1 \text{ y } (b, c) \in R_2\}$$

Definición 1.9. Δ_A denotará la relación sobre A definida mediante:

$$\Delta_A = \{(x, x) : x \in A\}.$$

A tal relación la llamaremos diagonal.

Definición 1.10. Sea R una relación entre A y B . Entonces la relación inversa, es una relación entre B y A que está dada por:

$$R^{-1} = \{(b, a) \mid b \in B, a \in A \text{ y } (a, b) \in R\}.$$

Ejemplo 1.4. Sean $A = \{1, 2, 3, 4, 5\}$, y las siguientes relaciones sobre A :

$$R = \{(a, b) \mid a > b\}$$

$$S = \{(a, b) \mid b - a = 3\}.$$

Describamos por extensión los conjuntos R^{-1} , S^{-1} y $S \circ R$.

Por definición $R^{-1} = \{(b, a) \mid (a, b) \in R\} = \{(b, a) \mid b < a\} = R$, luego

$$R^{-1} = \{(1, 2), (1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 4), (4, 5)\}.$$

Por otro lado $S^{-1} = \{(b, a) \mid (a, b) \in S\} = \{(b, a) \mid b - a = 3\}$, es decir

$$S^{-1} = \{(5, 2), (4, 1)\}.$$

Finalmente, $S \circ R = \{(a, c) \mid \text{existe algún } b \text{ tal que } (a, b) \in R \text{ y } (b, c) \in S\} = \{(a, c) \mid \text{existe algún } b \text{ tal que } a > b \text{ y } c - b = 3\}$. Comprobando elemento por elemento (buscando siempre un “pivot”, el elemento b), obtenemos

$$S \circ R = \{(2, 4), (3, 4), (3, 5), (4, 5), (5, 5)\}$$

Para los primeros 4 elementos se toma como pivot a 1, para los últimos 3 se toma como pivot a 2. \square

Con estas nuevas incorporaciones a nuestro lenguaje matemático podemos reescribir las propiedades estudiadas de una forma más sintética.

Propiedades de las relaciones

- (a) R es reflexiva si y sólo si $\Delta_A \subseteq R$.
- (b) R es simétrica si y sólo si $R \subseteq R^{-1}$.
- (c) R es antisimétrica si y sólo si $R \cap R^{-1} \subseteq \Delta_A$.
- (d) R es transitiva si y sólo si $R \circ R \subseteq R$.

1.8.1 Ejercicios

1. Sean R_1 y R_2 las relaciones dadas sobre $\{1, 2, 3, 4\}$ por:

$$R_1 = \{(1, 1), (1, 2), (3, 4), (4, 2)\}$$

$$R_2 = \{(1, 1), (2, 1), (3, 1), (4, 4), (2, 2)\}$$

Liste los elementos de $R_2 \circ R_1$ y de $R_1 \circ R_2$.

2. Pruebe que para cualquier relación R vale

$$R = R^{-1} \Leftrightarrow R \subseteq R^{-1} \Leftrightarrow R^{-1} \subseteq R.$$

3. Analice la validez de las siguientes afirmaciones, para una relación cualquiera R no vacía:

- (a) Si R no es simétrica entonces $R \cap R^{-1} \subseteq \Delta_A$.
- (b) $R \circ R^{-1} \subseteq \Delta_A$.
- (c) $\Delta_A \subseteq R \circ R^{-1}$.
- (d) Si R es simétrica entonces $R \circ R^{-1} \subseteq \Delta_A$.
- (e) Si R es simétrica y transitiva entonces $R \circ R^{-1} \subseteq R$.

4. Sea R una relación entre A y B (i.e., $R \subseteq A \times B$), sea S una relación entre B y C (i.e., $S \subseteq B \times C$), y sea T una relación entre C y D (i.e., $T \subseteq C \times D$). Muestre que $(T \circ S) \circ R = T \circ (S \circ R)$.

2 Conjuntos parcialmente ordenados

En este capítulo nos dedicamos a estudiar las relaciones de orden, y comenzaremos a preguntarnos sobre las distintas estructuras que el orden genera sobre el conjunto en el cual está definido. Este conjunto será llamado conjunto parcialmente ordenado.

Definición 2.1. Un par (P, \leq) donde P es un conjunto y \leq es un orden parcial sobre P se llama conjunto parcialmente ordenado.

Note que utilizamos para denotar una relación de orden parcial genérica el símbolo \leq , que hasta el momento estuvo reservado para el orden de los números reales. Nos vamos a permitir esta ambigüedad de notación, que resolveremos en cada caso observando el contexto. Pero el lector debe tener presente que de ahora en más el símbolo \leq no necesariamente hace referencia al orden de los números, ni siquiera hace referencia a un orden total.

Para referirnos a los conjuntos parcialmente ordenados utilizaremos en este apunte dos abreviaturas que son clásicas en la literatura: *posets* (por partially ordered sets), o *cpo's*, proveniente de la abreviatura en castellano.

Para terminar estos comentarios sobre la notación mencionamos que dado un orden parcial \leq sobre P podemos definir una nueva relación $<$ sobre P de la siguiente manera: $a < b$ si y sólo si $a \leq b$ y $a \neq b$. Esta convención también es compatible con el uso que se le da habitualmente al símbolo $<$ en los reales.

2.1 Maximales, minimales, máximos y mínimos

En un subconjunto de \mathbb{R} ordenado por la relación \leq (menor o igual), podemos tener un elemento mínimo y uno máximo, o sólo uno de ellos o quizás ninguno. No es ésta la única situación en la que no existen elementos extremos. Considere por ejemplo los diagramas del Problema 3 del capítulo anterior. Y algunos ejemplos más:

Ejemplo 2.1. 1. (\mathbb{Z}, \leq) no tiene ningún elemento máximo ni ninguno mínimo.

2. (\mathbb{N}, \leq) tiene un elemento mínimo: el 1, pero no tiene elemento máximo.

3. $[0, 1)$ tiene un elemento mínimo que es el 0 y pero no tiene máximo.

4. Tomemos X el subconjunto de $\mathcal{P}(\{a, b, c\})$ dado por

$$X = \{\{c\}, \{a, b\}, \{a, b, c\}\}$$

Es el caso de los diagramas mencionados, en los cuales podemos observar un máximo, pero no hay mínimo.

Para precisar todos estos conceptos daremos las siguientes definiciones:

Definición 2.2. Sea \leq un orden parcial sobre un conjunto P . El elemento máximo de P (si existe) es el elemento α en A que cumple que

$$a \leq \alpha, \quad \text{para todo } a \in P.$$

El elemento mínimo de P (si existe) es el elemento β en P que cumple que

$$\beta \leq a, \quad \text{para todo } a \in P.$$

Una notación usual consiste en utilizar el símbolo 1 para denotar el máximo del conjunto (en el caso de que exista), y 0 para el mínimo. Luego, interpretamos que cuando aparece en un contexto abstracto cualquiera de estos símbolos, entonces estamos asumiendo que el conjunto en cuestión posee máximo o mínimo, según corresponda.

En muchos ejemplos observamos que aunque no existe un elemento mínimo, encontramos elementos que no tienen ningún otro elemento menor (por ejemplo $\{a, b\}$ del ejemplo anterior). Este tipo de elementos se llamarán minimales, como lo establece la siguiente definición.

Definición 2.3. Sea P un conjunto parcialmente ordenado con orden parcial \leq . Un elemento $x \in P$ se dice maximal si para todo a en P , $x \leq a$ implica que $x = a$.

Un elemento $y \in P$ se dice minimal si para todo a en P , $a \leq y$ implica que $a = y$.

Ejemplo 2.2. Sea $P = \{2, 3, 4, 5, 6, 7, 8\}$ ordenado por divisibilidad, esto es $a \leq b$ si y sólo si a divide a b . En este caso tenemos

4 elementos minimales: 2, 3, 5, 7;

4 elementos maximales: 5, 6, 7, 8;

y no hay elemento mínimo ni elemento máximo.

Ejemplo 2.3. Sea $P = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{a, b, c\}\}$ con la relación de inclusión: \subseteq . Entonces

hay 3 elementos minimales: $\{a\}, \{b\}, \{c\}$;

hay 1 elemento maximal: $\{a, b, c\}$;

hay 1 elemento máximo: $\{a, b, c\}$;

y no hay elemento mínimo.

Observemos que un conjunto puede tener varios elementos maximales o varios elementos minimales. Sin embargo, si α es un elemento máximo de P entonces α es único, y si β es un elemento mínimo de P entonces β es también único. Esta propiedad se enuncia en el siguiente teorema. Trate de dar una prueba formal del mismo.

Teorema 2.1. Sea \leq un orden parcial sobre P .

1. Si P tiene un elemento máximo α entonces α es maximal y no existen otros elementos maximales.
2. Si P tiene un elemento mínimo β entonces β es minimal y no existen otros elementos minimales.

Existen órdenes en los que todo par de elementos está relacionado. Por ejemplo, en el caso de \leq en \mathbb{R} tenemos que para todo x, y en \mathbb{R} se cumple que o bien $x \leq y$ o bien que $y \leq x$. Tenemos un nombre para este tipo de conjuntos.

Definición 2.4. Un orden total sobre un conjunto P es un orden parcial \leq sobre P que satisface la ley de dicotomía:

$$\text{para todo } a, b \in P, \quad a \leq b \text{ o } b \leq a.$$

Algunos ejemplos de órdenes totales:

1. El orden \leq en \mathbb{R} y el orden \geq en \mathbb{R} .
2. El orden lexicográfico en un diccionario.
3. El orden “ a divide a b ” en el conjunto $A = \{2^k \mid k \in \mathbb{N}\}$.

Por supuesto esta es una categoría muy particular de orden, por ejemplo si tomamos la relación \leq sobre \mathbb{N} dada por: $a \sim b$ si y sólo si a divide a b entonces puede ocurrir que $a \not\leq b$ y que $b \not\leq a$, por ejemplo, 5 no divide a 8 y 8 no divide a 5.

Finalmente mencionamos un hecho que no desafía nuestra intuición, relativo a los órdenes finitos. Queda como ejercicio para el lector imaginar una justificación.

Teorema 2.2. 1. Sea \leq un orden parcial en un conjunto finito no vacío P . Entonces P contiene al menos un elemento minimal y si existe sólo uno entonces es el mínimo.

2. Sea \leq un orden parcial en un conjunto finito no vacío P . Entonces P contiene al menos un elemento maximal y si existe sólo uno entonces es el máximo.

2.2 Supremos e ínfimos

Seguramente en el curso de Cálculo el lector se habrá encontrado con la noción de supremo (y su dual, ínfimo), que emerge en la recta real producto de su orden particular. Una propiedad característica de este orden es la existencia de subconjuntos acotados que no poseen último elemento, debido a que su supremo (que siempre existe) no pertenece al conjunto (por ejemplo el intervalo $[0, 1)$).

Los conceptos de supremo e ínfimo adquieren una relevancia especial en el estudio de las estructuras ordenadas debido a que es justamente a través de ellos como se revela su verdadera estructura. Vamos a continuación a definir formalmente estos conceptos, y luego veremos algunos ejemplos.

Definición 2.5. Sea (P, \leq) un poset y sea $S \subseteq P$.

- (a) Un elemento $a \in P$ se dice cota superior de S si para todo $b \in S$ ocurre que $b \leq a$.
- (b) Un elemento $a \in P$ se dice cota inferior de S si para todo $b \in S$ ocurre que $a \leq b$.
- (c) Un elemento $a \in P$ se dice supremo de S si a es una cota superior de S y para toda cota superior b de S se cumple que $a \leq b$.
- (d) Un elemento $a \in P$ se dice ínfimo de S si a es una cota inferior de S y para toda cota inferior b de S se cumple que $b \leq a$.

Ejemplo 2.4. Consideremos (\mathbb{R}, \leq) con la relación de orden usual. Entonces 4 y 5 son cotas superiores del subconjunto $[1, 2)$. Notemos que 2 es el supremo, que no pertenece al conjunto y 1 es el ínfimo, que sí pertenece al conjunto.

Antes de continuar, y para poner en juego los conceptos definidos, sugerimos responder las siguientes cuestiones:

1. Considerando (\mathbb{R}, \leq) como en el ejemplo anterior, responda cuáles de las siguientes condiciones son necesarias, y cuáles son suficientes para que el subconjunto $S \subseteq \mathbb{R}$ tenga supremo dentro de S .
 - (a) S es finito
 - (b) S es acotado superiormente
 - (c) S es un intervalo cerrado
 - (d) S es unión de intervalos
 - (e) S es unión de intervalos cerrados
2. Sea $P = \{a, b, c, d, e\}$. Construya diagramas de Hasse que representen posets formados por estos 4 elementos, y que satisfagan:
 - (a) El supremo de $\{a, b\}$ es c , y el ínfimo es d . Además el ínfimo de P es e .
 - (b) El supremo de $\{a, b\}$, el supremo de $\{a, c\}$ y el supremo de $\{b, c\}$ coinciden, y son todos el elemento d .
 - (c) P no tiene supremo ni ínfimo.
 - (d) El supremo de $\{a, b\}$ no existe puesto que $\{a, b\}$ no tienen cotas superiores.
 - (e) Aunque $\{a, b\}$ tiene cotas superiores, el supremo de $\{a, b\}$ no existe.

Dado (P, \leq) un poset, para referirnos al supremo e ínfimo de un subconjunto S utilizaremos en general la notación $\sup(S)$ e $\inf(S)$, respectivamente. En el caso de existir 0 y 1, tendremos que $0 = \inf(P)$ y $1 = \sup(P)$.

Ejemplo 2.5. Consideremos el poset $(\mathcal{P}(\mathbb{R}), \subseteq)$. Se debe tener presente que ahora los elementos de nuestro poset son conjuntos. Luego, cuando buscamos supremo o ínfimo de un conjunto $S \subseteq \mathcal{P}(\mathbb{R})$, estamos buscando el conjunto más chico que contenga a cada uno de los conjuntos que viven en S . Dado que manejamos tres categorías de objetos, conviene adoptar una convención sobre la notación y el estilo de letra utilizada:

1. los elementos de \mathbb{R} son denotados mediante a, x, \dots
2. los elementos de $\mathcal{P}(\mathbb{R})$ son denotados con A, B, \dots
3. los subconjuntos de $\mathcal{P}(\mathbb{R})$ son denotados mediante S, \mathcal{A}, \dots

Por ejemplo, sean A, B subconjuntos de \mathbb{R} (o sea elementos de $\mathcal{P}(\mathbb{R})$). El supremo del conjunto $S = \{A, B\}$ será $A \cup B$, por ser este el conjunto más chico que contiene a ambos, A y B . En general se tiene que dado $S \subseteq \mathcal{P}(\mathbb{R})$,

$$\sup S := \bigcup S = \{r \in \mathbb{R} \mid r \in A, \text{ para algún } A \in S\},$$

$$\inf S := \bigcap S = \{r \in \mathbb{R} \mid r \in A, \text{ para todo } A \in S\},$$

lo cual en particular nos dice que

$$\sup\{A, B\} = A \cup B, \quad \inf\{A, B\} = A \cap B$$

□

Por último vamos a estudiar en general que ocurre con $\sup(S)$ e $\inf(S)$ cuando $S = \emptyset$. Notemos que todo elemento de P es cota superior e inferior del conjunto \emptyset . De modo que

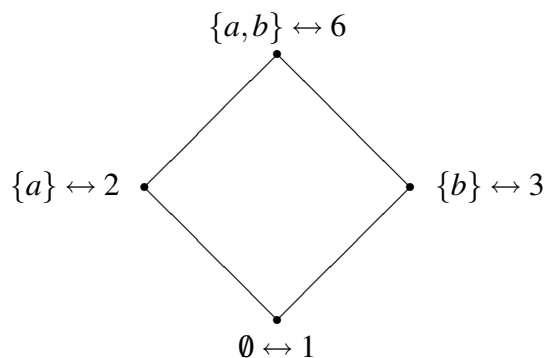
1. $\sup(\emptyset)$ existe si y sólo si P tiene menor elemento,
2. $\inf(\emptyset)$ existe si y sólo si P tiene mayor elemento.

2.3 Isomorfismos de posets

La noción de poset, como concepto abstracto, tiene por objetivo capturar los aspectos relevantes relativos al orden de una estructura, ignorando otros aspectos particulares que no se consideran relevantes. Por ejemplo, los conjuntos

$$\mathcal{P} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\} \quad P = \{1, 2, 3, 6\}$$

están formados por objetos de distinta naturaleza, pero cuando consideramos los posets (\mathcal{P}, \subseteq) y $(P, |)$ (es decir, P con la relación “divide”) comienza a haber ciertas similitudes. Podemos establecer una conexión entre los objetos de \mathcal{P} y los objetos de P de manera de hacer corresponder los roles que cada uno ocupa en sus respectivas estructuras ordenadas. Por ejemplo, a $\emptyset \in \mathcal{P}$ le corresponde $1 \in P$, debido a que ambos son los menores elementos. Dicho de otra manera: los posets poseen el mismo diagrama de Hasse. En la siguiente figura, el símbolo \leftrightarrow significa “se corresponde con”.



En matemática, la noción de isomorfismo trata de capturar la idea de que dos estructuras son indistinguibles cuando nos concentramos en ciertos aspectos relevantes, ignorando otros aspectos particulares. En este lenguaje diríamos que (\mathcal{P}, \subseteq) y $(P, |)$ son isomorfas.

Definición 2.6 (Isomorfismo de posets). Sean (P, \leq) , (Q, \leq') dos posets, y sea $f : P \rightarrow Q$ una función. Diremos que f es un isomorfismo si f es biyectiva y para todo $x, y \in P$, se cumple que $x \leq y$ si y sólo si $f(x) \leq' f(y)$. Si existe un isomorfismo entre (P, \leq) y (Q, \leq') diremos que estos posets son isomorfos y escribiremos $(P, \leq) \cong (Q, \leq')$.

Ejemplo 2.6. Sean $A = \{1, 2, 3, 4\}$ y $B = \{2, 4, 8, 16\}$, y consideremos los posets (A, \leq) con la relación de orden usual y $(B, |)$ donde $x|y$ significa que x divide a y . Luego la función $f : A \mapsto B$ dada por $f(n) = 2^n$ es un isomorfismo de posets.

El siguiente lema muestra que dos posets isomorfos tienen las mismas propiedades matemáticas, en lo que se refiere a las relaciones de orden.

Lema 2.3. Sean (P, \leq) y (Q, \leq') posets. Sea $f : P \rightarrow Q$ un isomorfismo.

- (a) Para cada $S \subseteq P$, se tiene que existe $\sup(S)$ si y sólo si existe $\sup(f(S))$ y en el caso de que existan tales elementos se tiene que $f(\sup(S)) = \sup(f(S))$.
- (b) Para cada $S \subseteq P$, se tiene que existe $\inf(S)$ si y sólo si existe $\inf(f(S))$ y en el caso de que existan tales elementos se tiene que $f(\inf(S)) = \inf(f(S))$.
- (c) P tiene 1 (resp. 0) si y sólo si Q tiene 1 (resp. 0) y en tal caso se tiene que $f(1) = 1$ y $f(0) = 0$.
- (d) Para cada $p \in P$, p es maximal (respectivamente minimal) si y sólo si $f(p)$ es maximal (respectivamente minimal).

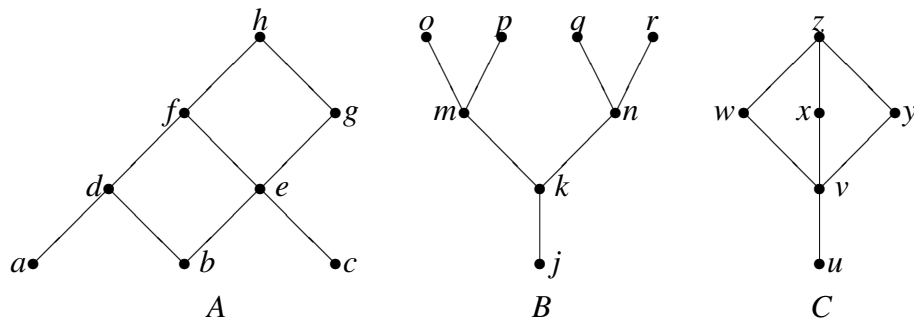
Demostración. Notemos que si f es un isomorfismo entonces su inversa f^{-1} también es un isomorfismo. Probemos el inciso (a). Si existe $a = \sup(S)$ entonces $x \leq a$ para todo $x \in S$. Luego $f(x) \leq' f(a)$ para todo $f(x) \in f(S)$. Esto dice que $f(a)$ es una cota superior de $f(S)$.

Veamos ahora que $f(a)$ es la menor cota superior. Supongamos que b es una cota superior de $f(S)$ y que $b \leq' f(a)$. Entonces $f^{-1}(b) \leq f^{-1}(f(a)) = a$. Si logramos ver que $f^{-1}(b)$ es cota superior de S entonces podremos concluir que $a = f^{-1}(b)$. Para esto notemos que si $x \in S$ entonces $f(x) \leq b$. Luego $x = f^{-1}(f(x)) \leq f^{-1}(b)$.

Las demás demostraciones son análogas y se dejan a cargo del lector. \square

2.4 Ejercicios

- La siguiente figura muestra los diagramas de Hasse de tres conjuntos parcialmente ordenados.



- ¿Cuáles son los elementos maximales y minimales de estos conjuntos?
- ¿Cuáles de estos conjuntos tienen mínimo, cuáles máximo?
- ¿Qué elementos cubren e ?
- Encuentre cada uno de los siguientes, si es que existe. En cada caso determine previamente el conjunto de cotas correspondiente.

$$\sup\{d, c\}, \quad \sup\{w, y, v\}, \quad \sup\{p, m\}, \quad \inf\{a, g\}, \quad \sup\{m, n\}, \quad \inf\{g, a, f\}$$

- Considere el conjunto parcialmente ordenado $(D_{90}, |)$

- Dibuje el diagrama de Hasse.
- Calcule $\sup\{6, 10\}$, $\inf\{6, 10\}$, $\sup\{30, 9\}$ y $\inf\{9, 30\}$.

- (c) ¿Cuál es el subconjunto más grande que encuentra dentro de D_{90} que constituya en sí mismo un orden total?
3. Considere el poset $(\mathbb{N}, |)$; recuerde que $m|n$ si m divide a n .
- (a) ¿Cuál es el elemento mínimo?
- (b) ¿Tiene \mathbb{N} un elemento máximo?
- (c) Describa $\sup\{n, m\}$ e $\inf\{n, m\}$, para cualquier m, n .
4. Determine cuales de los siguientes mapas de P a Q son isomorfismos. En caso de no serlo determine qué es lo que falla.
- (a) $P = Q = \mathbb{Z}$ (con el orden usual), $f(x) = x + 1$
- (b) $P = Q = \mathbb{Z}$ (con el orden usual), $f(x) = 2x$
- (c) $P = Q = \mathbb{Z}$ (con el orden usual), $f(x) = -x$
- (d) $P = Q = \mathcal{P}(\{a, b, c\})$ (con la inclusión). La función f está definida de la siguiente manera. Si a, b están ambos en A , o no están ninguno de los dos en A , entonces $f(A) = A$. En otro caso f quita de A al que está y pone al que no está. Por ejemplo, $f(\{a\}) = \{b\}$ $f(\{a, c\}) = \{b, c\}$.
- (e) $P = Q = \mathcal{P}(\{a, b, c\})$ (con la inclusión), y $f(A) = A^c$.

2.5 Problemas

1. En la noción de isomorfismo podemos observar que se recurre a un “si y sólo si” para capturar la idea de que el orden es el mismo en las dos estructuras. Considere esta definición alternativa de isomorfismo:

Sean (P, \leq) , (Q, \leq') dos posets, y sea $f : P \rightarrow Q$ una función. Diremos que f es un *isomorfismo* si f es biyectiva y para todo $x, y \in P$, se cumple que $x \leq y$ implica $f(x) \leq' f(y)$.

¿Es equivalente a la anterior? ¿Qué problemas tendría el adoptar esta definición?

2. Determine si es posible encontrar dentro del poset $(\mathcal{P}(\{a, b, c, d\}), \subseteq)$ un subconjunto que visto como poset sea isomorfo a D_{90}

3. La Tabla 1 fue llenada parcialmente. La misma da los valores de $\sup\{x, y\}$ para x e y en cierto poset (S, \preceq) . Por ejemplo $\sup\{b, c\} = d$.

- (a) Llene el resto de la tabla.
- (b) ¿Cuál es el mínimo y el máximo de S ?
- (c) Muestre que $f \preceq c \preceq d \preceq e$.
- (d) Dibuje el diagrama de Hasse asociado a (S, \preceq) .

sup	a	b	c	d	e	f
a		e	a	e	e	a
b			d	d	e	b
c				d	e	c
d					e	d
e						e
f						

Tabla 1:

- 4. Supongamos que un poset tiene la siguiente propiedad: para todo $a, b \in P$ se tiene que $\sup\{a, b\}$ existe. ¿Podemos concluir que $\sup(S)$ existe para cualquier S finito, $S \neq \emptyset$?
- 5. Supongamos que un poset tiene la siguiente propiedad: para todo subconjunto finito S de P se tiene que $\sup(S)$ existe. ¿Podemos concluir que $\sup(S)$ existe para cualquier S ?
- 6. Supongamos que un poset tiene la siguiente propiedad: para todo subconjunto S de P se tiene que $\sup(S)$ existe (en particular existe $\sup(P)$ y $\sup(\emptyset)$). ¿Podemos concluir que $\inf(S)$ existe para cualquier S ?
- 7. En un poset, un subconjunto D se dice *decreciente* si cada vez que un elemento está en D , también están los más chicos. En símbolos: si $d \in D$ y $c \leq d$, entonces $c \in D$. Sea f de P en Q una función. Probar que son equivalentes:
 - (a) f preserva el orden, o sea, $x \leq y$ implica $f(x) \leq' f(y)$.
 - (b) si D es un subconjunto decreciente de Q , entonces $f^{-1}(D)$ es decreciente en P .

8. Determine cuántos isomorfismos hay de $(\mathcal{P}(\{a, b, c\}), \subseteq)$ en sí mismo.

3 Reticulados y Álgebras

Los conjuntos parcialmente ordenados constituyen un marco abstracto apropiado para modelar una enorme cantidad de fenómenos, resultando así una herramienta teórica de mucha utilidad, sobre todo a la hora de establecer las bases fundacionales de las Ciencias de la Computación. Por ejemplo, permiten introducir la noción de *dominio*, pilar del desarrollo de la semántica denotacional de los lenguajes de programación. Por otro lado, los conjuntos parcialmente ordenados son la puerta de entrada a las estructuras que permiten la algebrización de la lógica, constituyéndose así en un concepto central en los desarrollos de la Lógica Matemática, la Teoría de Pruebas, la Teoría de Modelos y el Álgebra Universal.

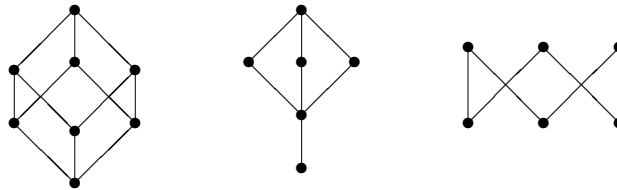
En este capítulo vamos a introducir dos estructuras fundamentales para la lógica: los Reticulados y las Álgebras de Boole. Estudiaremos sus propiedades fundamentales y sus distintas formas de presentación.

3.1 Reticulados como posets (o posets reticulados)

Los reticulados son una estructura matemática que posee distintas formas de presentación. Introducimos por primera vez esta noción a través del concepto de poset.

Definición 3.1 (Poset reticulado). *Diremos que un poset (L, \leq) es un poset reticulado si para todo $a, b \in L$, existen $\sup(\{a, b\})$ e $\inf(\{a, b\})$.*

Ejemplo 3.1. *De los tres órdenes siguientes, los dos primeros son posets reticulados y el tercero no.*

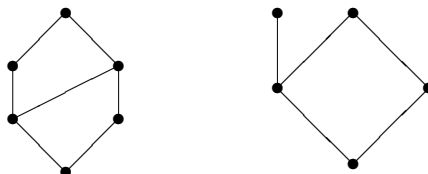


Dado que un poset reticulado garantiza la existencia de ínfimos y supremos de pares de elementos, podemos introducir dos operaciones binarias definidas en todo poset reticulado (para todo par de elementos) representando las operaciones de “tomar el supremo del par” y “tomar el ínfimo del par”. Utilizaremos la notación:

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

Antes de continuar, y como una manera de fijar los conceptos, sugerimos responder lo siguiente:

1. Determine cómo y cuándo están definidas las operaciones \bigwedge , \bigvee en los siguientes posets. Considere todos los pares de elementos posibles.
 - (a) $(\mathbb{N}, |)$ (aquí $x|y$ si y solo si x divide a y)
 - (b) $(\{1, 2, 3, 4, 6, 12\}, |)$
 - (c) $(\{1, 2, 3, 4, 6\}, |)$
2. ¿Cuáles de los anteriores posets son posets reticulados?
3. Relacione los siguientes diagramas de Hasse con los anteriores posets.



Ejemplo 3.2. Sea $n \in \mathbb{N}$, entonces definimos $D_n = \{k \in \mathbb{N} : k|n\}$. Es decir D_n es el conjunto de divisores de n . Probemos que $(D_n, |)$ es un reticulado (observar que el conjunto de 1b. es D_{12}).

Demostración. Sean x, y elementos de D_n , entonces $\text{mcm}(x, y)$ es también elemento de D_n , pues como n es múltiplo de x e y y $\text{mcm}(x, y)$ es el mínimo común múltiplo entre x e y , se deduce que $\text{mcm}(x, y)|n$. Como en 1a. es fácil ver entonces que $x \bigvee y = \text{mcm}(x, y)$. En forma análoga se ve que $x \bigwedge y = \text{mcd}(x, y)$.

□

Dado que tenemos definidas dos operaciones binarias sobre todos los posets reticulados, podemos comenzar a indagar qué leyes (propiedades) estas satisfacen. Por ley entendemos una expresión que vincula mediante los conectivos lógicos usuales ciertas ecuaciones (o inecuaciones). Cada una de éstas relacionan dos términos que denotan elementos del poset. Cuando decimos que un poset reticulado satisface una ley o propiedad, estamos afirmando que para toda posible elección de elementos, la propiedad se satisface. Para chequear esto debemos comprobar la propiedad para toda posible forma de reemplazar las variables no cuantificadas por elementos del poset reticulado.

Para comprobar si este punto ha quedado claro, sugerimos completar la siguiente actividad: para cada propiedad de la lista siguiente, dé diagramas de Hasse representando reticulados que la satisfagan, y que no la satisfagan, en el caso de existir.

1. $(x \otimes y = y) \vee (x \otimes y = x)$
2. $x \otimes y = y$
3. $\exists x \, x \otimes y = x$

El siguiente lema nos muestra una serie de propiedades básicas que son válidas en todos los reticulados.

Lema 3.1. *Dado un reticulado (L, \leq) , y elementos $x, y, z, w \in L$, se cumplen las siguientes propiedades:*

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

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

(c) $x \leq y \iff x \vee y = y \iff x \otimes y = x$,

(d) *leyes de idempotencia:*

$$x \vee x = x \otimes x = x$$

(e) *leyes conmutativas:*

$$x \vee y = y \vee x, \quad x \otimes y = y \otimes x$$

(f) *leyes de absorción:*

$$x \vee (x \otimes y) = x, \quad x \otimes (x \vee y) = x$$

(g) *ley de compatibilidad*

$$x \leq z \text{ e } y \leq w \text{ implican } x \vee y \leq z \vee w, \quad x \otimes y \leq z \otimes w$$

(h) *desigualdades distributivas*

$$x \vee (y \otimes z) \leq (x \vee y) \otimes (x \vee z) \quad (x \otimes y) \vee (x \otimes z) \leq x \otimes (y \vee z)$$

(i) *leyes asociativas:*

$$(x \vee y) \vee z = x \vee (y \vee z), \quad (x \otimes y) \otimes z = x \otimes (y \otimes z)$$

Demostración. Las pruebas de los incisos (a) hasta (f) son dejados al lector. Veamos (g). Puesto que

$$x \leq z \leq z \vee w, \quad y \leq w \leq z \vee w,$$

tenemos que $z \vee w$ es cota superior de $\{x, y\}$ lo cual dice que $x \vee y \leq z \vee w$. La demostración para la otra desigualdad es análoga.

(h) Veamos la segunda desigualdad. La primera queda para el lector. Puesto que $(x \wedge y) \leq x$, $(x \wedge z) \leq x$, $(x \wedge y) \leq y \vee z$ y $(x \wedge z) \leq y \vee z$, tenemos que

$$(x \wedge y) \leq x \wedge (y \vee z) \quad \text{y} \quad (x \wedge z) \leq x \wedge (y \vee z),$$

por lo cual $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$.

(i) Notemos que por (i), $x \vee (y \vee z)$ es cota superior del conjunto $\{x \vee y, z\}$, lo cual dice que $(x \vee y) \vee z \leq x \vee (y \vee z)$. Análogamente se puede probar que $x \vee (y \vee z) \leq (x \vee y) \vee z$. \square

Dado que la distribución de paréntesis en una expresión del tipo

$$(\dots(x_1 \vee x_2) \vee \dots) \vee x_n,$$

es irrelevante (ya que \vee es asociativa), en general suprimiremos los paréntesis.

3.2 Reticulados como estructuras algebraicas (o simplemente reticulados)

Los reticulados poseen una propiedad notable: pueden ser presentados (o definidos) de dos manera muy diferentes, que sorprendentemente resultan equivalentes. La primera es la que vimos anteriormente: un reticulado es presentado como un poset con la propiedad de poseer supremo e ínfimo de todo par de elementos. La siguiente definición describe a los reticulados como un tipo de estructura algebraica. Por estructura algebraica entendemos un conjunto no vacío dotado de algunas operaciones.

Definición 3.2 (Reticulado). *Una estructura del tipo $\langle L, \vee, \wedge \rangle$, donde L es un conjunto no vacío cualquiera y \vee e \wedge son dos operaciones binarias sobre L será llamada un reticulado, si se satisfacen las siguientes identidades:*

R1 leyes de idempotencia:

$$x \vee x = x \wedge x = x,$$

R2 leyes conmutativas:

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

R3 leyes asociativas:

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

R4 leyes de absorción:

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

Notemos que no toda estructura del tipo $\langle L, \vee, \wedge \rangle$ es un reticulado. Por ejemplo la estructura $\langle \mathbb{R}, +, \cdot \rangle$ donde $+$ y \cdot son las operaciones de suma y producto usuales de \mathbb{R} , no es un reticulado ya que no cumple, por ejemplo, la primera de las identidades.

Está claro desde el lema 3.1 que un poset reticulado (L, \leq) puede “mutar” para convertirse en un reticulado (como estructura algebraica): la estructura $\langle L, \vee, \wedge \rangle$ satisface las propiedades R1, R2, R3 y R4, en tanto definamos $x \wedge y = \inf\{x, y\}$, y $x \vee y = \sup\{x, y\}$.

El siguiente teorema muestra que podemos realizar la mutación a la inversa: toda estructura del tipo $\langle L, \vee, \wedge \rangle$ que cumpla las propiedades R1, R2, R3 y R4, determina un único poset reticulado (L, \leq) en donde las nociones de supremo e ínfimos están dadas por las operaciones \wedge y \vee .

Teorema 3.2. *Sea $\langle L, \vee, \wedge \rangle$ un reticulado (como estructura algebraica). La relación binaria definida por:*

$$x \leq y \text{ si y sólo si } x \vee y = y$$

es un orden parcial sobre L para el cual se cumple:

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

Demostración. Dejamos como ejercicio para el lector probar que \leq es reflexiva y antisimétrica. Veamos que \leq es transitiva. Supongamos que $x \leq y$ y $y \leq z$. Entonces $x \vee z = x \vee (y \vee z) = (x \vee y) \vee z = y \vee z = z$, por lo cual $x \leq z$. Veamos ahora que $x \vee y = \sup\{x, y\}$. Es claro que $x \vee y$ es una cota superior del conjunto $\{x, y\}$. Supongamos $x, y \leq z$. Entonces

$$(x \vee y) \vee z = (x \vee y) \vee (z \vee z) = (x \vee z) \vee (y \vee z) = z \vee z = z,$$

por lo que $x \vee y$ es la menor cota superior.

Para probar $x \wedge y = \inf(\{x, y\})$, probaremos que

$$x \leq y \text{ si y sólo si } x \wedge y = x,$$

lo cual le permitirá al lector aplicar un razonamiento similar al usado en el caso de la operación \vee . Supongamos que $x \vee y = y$. Entonces $x \wedge y = x \wedge (x \vee y) = x$. Recíprocamente si $x \wedge y = x$, entonces $x \vee y = (x \wedge y) \vee y = y$.

□

El teorema anterior asegura que las dos definiciones de reticulado dadas anteriormente (como poset o como estructura del tipo $\langle L, \bigvee, \bigwedge \rangle$) son equivalentes. Por esto, en lo que sigue muchas veces utilizaremos la hipótesis “ L es un reticulado” sin especificar si se trata de un poset o una estructura algebraica. Una vez asumido que L es un reticulado, por lo anterior podremos disponer tanto del orden, como de las operaciones \bigvee e \bigwedge .

Ejemplo 3.3. (a) Si X es un conjunto arbitrario, entonces $\langle \mathcal{P}(X), \cup, \cap \rangle$ es un reticulado. La relación binaria inducida por \cup y \cap es precisamente la inclusión, pues $A = A \cup B$ si y sólo si $B \subseteq A$.

(b) Si $n \in \mathbb{N}$ entonces $\langle D_n, \text{mcm}, \text{mcd} \rangle$ es un reticulado. La relación binaria inducida es la de divisibilidad, pues $\text{mcm}(x, y) = y$ si y sólo si x divide a y .

3.3 Isomorfismos de reticulados

Dados dos reticulados, por tener estos una estructura de posets, podemos analizar si son isomorfos o no. Pero las estructuras algebraicas poseen su propia definición de isomorfismo: dos estructuras del mismo tipo son isomorfas si existe entre ellas un biyección que preserve las operaciones de las mismas. En nuestro caso, esta definición se formaliza de la siguiente manera:

Definición 3.3 (Isomorfismo de reticulados (vistos como estructuras algebraicas)). Sean $\langle L, \bigvee, \bigwedge \rangle$ y $\langle L', \bigvee', \bigwedge' \rangle$ reticulados. Una función $F : L \rightarrow L'$ se dice un isomorfismo de reticulados si F es biyectiva y para todo $x, y \in L$ se cumple que

$$F(x \bigvee y) = F(x) \bigvee' F(y) \quad F(x \bigwedge y) = F(x) \bigwedge' F(y).$$

Escribiremos $\langle L, \bigvee, \bigwedge \rangle \cong \langle L', \bigvee', \bigwedge' \rangle$ cuando exista un isomorfismo de L en L' .

Dado que hemos dado dos presentaciones diferentes para el mismo concepto de reticulado, debemos además probar que si dos reticulados son isomorfos vistos como posets, son también isomorfos vistos como estructuras algebraicas.

Lema 3.3. Sean $\langle L, \bigvee, \bigwedge \rangle$ y $\langle L', \bigvee', \bigwedge' \rangle$ reticulados y sean (L, \leq) y (L', \leq') los posets asociados. Entonces una función $F : L \rightarrow L'$ es un isomorfismo entre las estructuras $\langle L, \bigvee, \bigwedge \rangle$ y $\langle L', \bigvee', \bigwedge' \rangle$ si y sólo si lo es entre los posets (L, \leq) y (L', \leq') .

Demostración. Sea $F : L \rightarrow L'$ un isomorfismo de reticulados (vistos como estructuras algebraicas). Veamos que $x \leq y \Leftrightarrow F(x) \leq' F(y)$. Recordemos que $x \leq y$ si y sólo si $x \bigvee y = y$. Luego

$$x \leq y \Leftrightarrow F(x \bigvee y) = F(y) \Leftrightarrow F(x) \bigvee' F(y) = F(y) \Leftrightarrow F(x) \leq' F(y).$$

La recíproca se deduce del Lema 2.3.

□

3.4 Reticulados acotados y complementados

En esta sección vamos a incorporar los conceptos necesarios para aproximarnos a un tipo especial de reticulado: el álgebra de Boole.

Definición 3.4 (Reticulado acotado). *Una estructura del tipo $\langle L, \bigvee, \bigwedge, 0, 1 \rangle$ donde L es un conjunto no vacío, \bigvee e \bigwedge son operaciones binarias sobre L y $0, 1 \in L$, se dice un reticulado acotado si $\langle L, \bigvee, \bigwedge \rangle$ es un reticulado y además para cada $x, y \in L$,*

$$0 \bigvee x = x, \quad x \bigvee 1 = 1.$$

Notemos que si (P, \leq) es un reticulado con máximo 1 y mínimo 0, entonces $\langle P, \sup, \inf, 0, 1 \rangle$ es un reticulado acotado. Además en virtud del Teorema 3.2 todo reticulado acotado se obtiene de esta forma.

Ejemplo 3.4. (a) $\langle D_n, \text{mcm}, \text{mcd}, 1, n \rangle$ es un reticulado acotado.

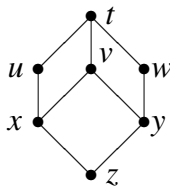
(b) $\langle \mathbb{N}, \text{mcm}, \text{mcd} \rangle$ no tiene estructura de reticulado acotado pues no tiene máximo.

(c) Si X es un conjunto finito, entonces $\langle \mathcal{P}(X), \cup, \cap, \emptyset, X \rangle$ es un reticulado acotado.

Definición 3.5 (Complemento). *Sea $\langle L, \bigvee, \bigwedge, 0, 1 \rangle$ un reticulado acotado. Dado $a \in L$, diremos que a es complementado cuando exista un elemento $b \in L$ llamado complemento de a tal que:*

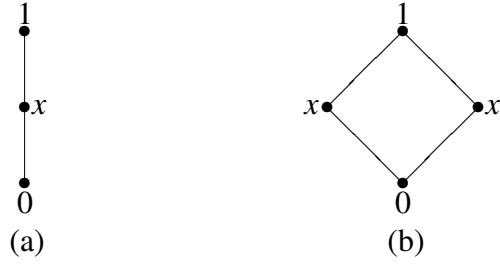
$$a \bigvee b = 1, \quad a \bigwedge b = 0.$$

Notemos que un elemento puede no tener complementos, o tener varios complementos. Por ejemplo en el reticulado S dado por el diagrama



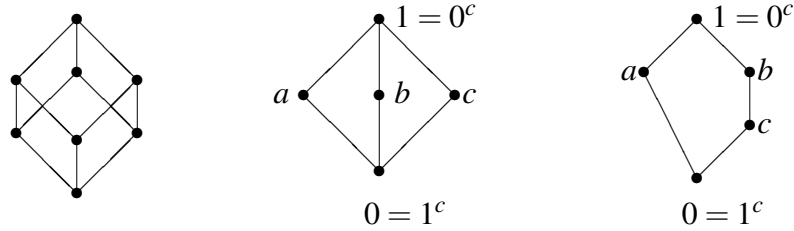
vemos que v no tiene complementos, mientras que w tiene a u y x como complementos.

Las cadenas, como por ejemplo la de la figura (a), son ejemplos de reticulados en los cuales el 0 y el 1 son los únicos elementos complementados. El reticulado de la figura (b) es un reticulado en el cual todo elemento tiene complemento



Definición 3.6 (Reticulado complementado). *Un reticulado complementado será un estructura del tipo Sea $\langle L, \odot, \oslash, 0, 1, ^c \rangle$ tal que $\langle L, \odot, \oslash, 0, 1 \rangle$ un reticulado acotado y para todo $a \in L$ se tiene que a^c es un complemento de a .*

Por ejemplo, en los siguientes reticulados podemos definir x^c para cada x , de manera de convertirlos en reticulados complementados:



Es un ejercicio útil comprobar que en el primer reticulado existe una única forma de definir x^c , para cualquier elemento x del reticulado. No ocurre lo mismo en los demás reticulados, en los cuales tenemos distintas manera de definir x^c para aquellos elementos x que poseen más de un complemento. Por ejemplo, en el reticulado del medio podemos definir $a^c = b^c = c$, $c^c = a$, pero también podríamos definir $a^c = c^c = b$, $b^c = a$, y esto no agota todas las posibilidades. Un fenómeno parecido ocurre en el último reticulado, debido a que a posee dos complementos.

3.5 Reticulados distributivos

El último ejemplo de la sección anterior nos muestra que la operación complemento (cuando existe) no está determinada por la estructura de poset (o sea por el orden), ya que existe un poset en el cuál podemos definir la operación complemento de distintas maneras.

Este fenómeno se revierte mediante la noción de reticulado distributivo, que nos acercará al concepto de álgebra de Boole. Vamos a introducir este concepto, y veremos que en los reticulados distributivos no pueden existir dos complementos de un mismo elemento. Luego encontraremos una caracterización sencilla de los reticulados distributivos.

Primero vamos a probar el siguiente lema.

Lema 3.4. Sea $\langle L, \vee, \wedge \rangle$ un reticulado; entonces son equivalentes:

1. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$, cualesquiera sean $x, y, z \in L$,
2. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$, cualesquiera sean $x, y, z \in L$.

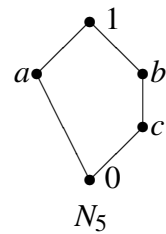
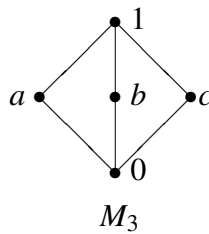
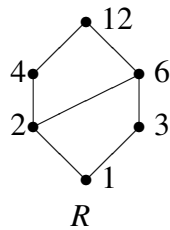
Demostración. Veamos que (1) \Rightarrow (2).

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

La demostración de que (2) \Rightarrow (1) es similar. □

Definición 3.7 (Reticulado Distributivo). *Un reticulado se llamará distributivo cuando cumpla alguna de las propiedades del Lema 3.4.*

Ejemplo 3.5. *En los siguientes reticulados, el primero es distributivo, y los restantes no lo son. Los dos últimos tendrán una importancia relevante en el estudio de los reticulados distributivos, por eso serán llamados M_3 y N_5 , respectivamente.*



Demostración. Notemos que el reticulado R es el correspondiente a $(D_{12}, |)$. Haremos el caso D_n en general en el Ejemplo 3.8. El reticulado M_3 no es distributivo, pues, por ejemplo,

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

en tanto que

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

El reticulado N_5 tampoco es distributivo. Queda como ejercicio para el lector encontrar tres elementos que no satisfagan las ecuaciones requeridas. □

Como mencionamos al principio, la distributividad tiene una consecuencia importante sobre los complementos:

Lema 3.5. Si $\langle L, \vee, \wedge, 0, 1 \rangle$ es un reticulado acotado y distributivo, entonces todo elemento tiene a lo sumo un complemento.

Demostración. Supongamos $x \in L$ tiene complementos y, z . Luego

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

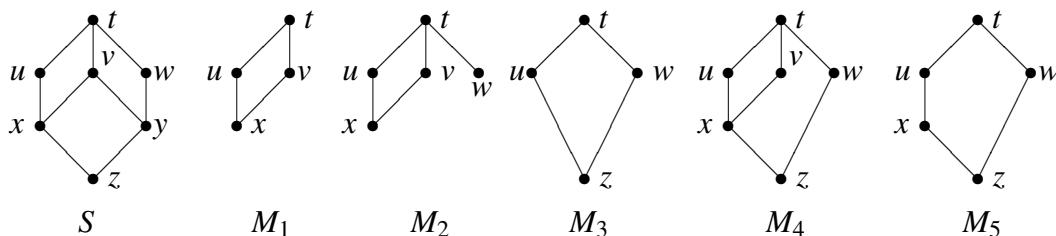
por lo cual $y \leq z$. En forma análoga se puede mostrar que $z \leq y$ y por lo tanto $z = y$. \square

Existe una caracterización muy sencilla de los reticulados distributivos que consiste en observar la forma que tienen sus subreticulados de 5 elementos. Para formular esta caracterización vamos primero a precisar algunos conceptos.

Definición 3.8 (Subreticulado). Sea $\langle L, \vee, \wedge \rangle$ un reticulado. Un subconjunto $M \subseteq L$ será llamado subestructura o subreticulado de $\langle L, \vee, \wedge \rangle$ si

- (a) $M \neq \emptyset$,
- (b) para todo $x, y \in M$, se tiene que $x \vee y, x \wedge y \in M$.

Ejemplo 3.6. Consideremos el reticulado $\langle S, \vee, \wedge \rangle$ de la siguiente figura.



La figura también muestra los diagramas de Hasse de cinco subconjuntos parcialmente ordenados de (S, \leq) . El subconjunto M_1 es un subreticulado ya que $a \vee b \in M_1$, para todo $a, b \in M_1$. El subconjunto M_2 no es un subreticulado pues, en particular, no es un reticulado. El subconjunto M_3 es un subreticulado. El subconjunto M_4 es por si mismo un reticulado, pero como $v \wedge w = y$ e $y \notin M_4$, entonces no es un subreticulado. Por último el conjunto M_5 es también un subreticulado.

El siguiente teorema resulta muy útil cuando se desea determinar si un reticulado es distributivo. Sólo daremos el enunciado y remitimos al libro de Davey and Priestley, *Introduction to lattices and order*, Teorema 6.10 para quien desee conocer una demostración del mismo.

Teorema 3.6. *Un reticulado es distributivo si y sólo si no contiene subreticulados isomorfos a M_3 y N_5 del Ejemplo 3.5.*

Ejemplo 3.7. 1. *El reticulado $\mathcal{P}(A)$ de los subconjuntos de un conjunto A es distributivo como ya fue probado anteriormente.*

2. *Cualquier orden total da un reticulado distributivo. Se puede ver usando el Teorema 3.6 o directamente de la siguiente forma: claramente $x \odot y = \max\{x, y\}$ y $x \oslash y = \min\{x, y\}$, entonces una de las leyes distributivas dice*

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

Para verificar esto, primero supondremos que $y \leq z$, entonces $\min\{y, z\} = y$ y $\max\{x, y\} \leq \max\{y, z\}$, luego el lado izquierdo y derecho de la ecuación queda igual a $\max\{x, y\}$. El caso $y \geq z$ tiene una verificación similar.

Ejemplo 3.8. *Veamos que D_n es distributivo y para ello usemos el Teorema 3.6. Supongamos que tenemos en D_n un subreticulado de la forma de la figura M_3 del Ejemplo 3.5, luego $\text{mcd}(a, b) = \text{mcd}(b, c) = \text{mcd}(c, a) = 0^{M_3}$. Supongamos que $0^{M_3} = k \in D_n$. Tenemos entonces que $a = k.a'$, $b = k.b'$ y $c = k.c''$, y además a', b', c' son coprimos entre sí, pues sino algún máximo común divisor sería más grande. Ahora bien, por el diagrama tenemos también que*

$$\text{mcm}(a, b) = \text{mcm}(b, c) = \text{mcm}(c, a) = 1^{M_3} \quad (I),$$

pero por lo anterior $\text{mcm}(a, b) = k.a'.b'$ y $\text{mcm}(a, c) = k.a'.c'$ que son claramente diferentes (pues al ser coprimos b' y c' no son iguales). Esto contradice (I).

Supongamos ahora que tenemos en D_n un subreticulado de la forma de la figura N_5 del Ejemplo 3.5, luego $\text{mcd}(a, b) = \text{mcd}(a, c) = 0^{N_5}$. Como antes, llamemos $k = 0^{M_3}$. Tenemos que $a = k.a'$, $b = k.b'$, $c = k.c'$, y además a' es coprimo con b' y c' . Por otro lado $\text{mcm}(a, b) = \text{mcm}(a, c) = 1^{N_5}$, y por las fórmulas anteriores tenemos que $\text{mcm}(a, b) = k.a'.b'$ y $\text{mcm}(a, c) = k.a'.c'$, de lo cual concluimos que $b' = c'$, que implica que $b = k.b' = k.c' = c$, absurdo.

Es decir, suponiendo que D_n tiene un subreticulado de la forma M o N del Ejemplo 3.5 llegamos a un absurdo. Entonces el Teorema 3.6 implica que D_n es distributivo.

3.6 Álgebras de Boole

Cuando dotamos a un reticulado con la operación complemento, incluimos su máximo y mínimo como operaciones (de aridad 0), y pedimos distributividad para evitar los problemas antes mencionados, estamos en presencia de un álgebra de Boole, estructura fundamental de la lógica, y modelo abstracto de la teoría de conjuntos.

Definición 3.9 (Álgebra de Boole). Una estructura del tipo $\langle B, \odot, \oslash, ^c, 0, 1 \rangle$, donde B es un conjunto no vacío, \odot e \oslash son operaciones binarias sobre B , c es una operación unaria sobre B y $0, 1 \in B$, será llamada un álgebra de Boole si $\langle B, \odot, \oslash, 0, 1 \rangle$ es un reticulado acotado y distributivo y además para cada $x \in B$,

$$x \odot x^c = 1, \quad x \oslash x^c = 0 \quad \text{Ley de Complementación.}$$

Ejemplo 3.9. Sea X un conjunto finito. Entonces $\langle \mathcal{P}(X), \cup, \cap, ^c, \emptyset, X \rangle$ es un álgebra de Boole, donde $A^c = X - A$ para cada $A \subseteq X$.

El ejemplo anterior tiene una importancia fundamental, puesto que el álgebra de Boole se introduce para modelar abstractamente el álgebra de conjuntos. A tal punto este modelado resulta acertado, que veremos más adelante que toda álgebra de Boole finita es esencialmente un álgebra de conjuntos.

Ejemplo 3.10. Veamos que D_n tiene estructura de álgebra de Boole si y sólo si n es producto de factores primos distintos (i.e., $n = p_1 \dots p_k$, con $p_i \neq p_j$ si $i \neq j$).

Demostración. Ya hemos visto que para todo n , $\langle D_n, \text{mcm}, \text{mcd}, 1, n \rangle$ es un reticulado acotado distributivo. Veamos en qué casos todo elemento de D_n tiene complementos. Supongamos que n es producto de factores primos distintos. Sea x en D_n , es decir $x|n$, luego $n = x.k$, como n es producto de factores primos distintos, es claro que x y k son coprimos, luego $\text{mcd}(x, k) = 1$ y $\text{mcm}(x, k) = n$, es decir que $x \oslash k = 0$ y $x \odot k = 1$. Luego x tiene complemento. Notemos que $x^c = n/x$.

Supongamos ahora que n no es producto de factores primos distintos, luego $n = p^2.r$ para algún p primo. Veamos que p no tiene complemento. Si lo tuviera existiría y tal que $\text{mcd}(p, y) = 1$ y $\text{mcm}(p, y) = n$, ahora bien, la primera igualdad implica que p e y son coprimos y por lo tanto $p.y = \text{mcm}(p, y)$, es decir que $p.y = n$, luego $y = p.r$ (pues $n = p^2.r$). Pero entonces $\text{mcd}(p, y) = \text{mcd}(p, p.r) = p$ y llegamos a una contradicción. \square

Leyes fundamentales que el lector seguramente recordará del álgebra de conjuntos se reproducen en el álgebra de Boole.

Teorema 3.7. Sea $\langle B, \odot, \oslash, ^c, 0, 1 \rangle$ un álgebra de Boole, entonces se cumplen las **leyes De Morgan**:

$$(x \odot y)^c = x^c \oslash y^c \quad (x \oslash y)^c = x^c \odot y^c$$

para todo x e y en B .

Demostración. Probando que $(x \odot y) \oslash (x^c \oslash y^c) = 0$ y $(x \odot y) \odot (x^c \oslash y^c) = 1$, se deduce de la unicidad del complemento que $x^c \oslash y^c = (x \odot y)^c$. Probemos primero que $(x \odot y) \oslash (x^c \oslash y^c) = 0$:

$$\begin{aligned}
(x \vee y) \wedge (x^c \wedge y^c) &= (x^c \wedge y^c) \wedge (x \vee y) && \text{Ley Conmutativa} \\
&= ((x^c \wedge y^c) \wedge x) \vee ((x^c \wedge y^c) \wedge y) && \text{Ley Distributiva} \\
&= (x \wedge (x^c \wedge y^c)) \vee ((x^c \wedge y^c) \wedge y) && \text{Ley Conmutativa} \\
&= ((x \wedge x^c) \wedge y^c) \vee (x^c \wedge (y^c \wedge y)) && \text{Ley Asociativa} \\
&= ((x \wedge x^c) \wedge y^c) \vee (x^c \wedge (y \wedge y^c)) && \text{Ley Conmutativa} \\
&= (0 \wedge y^c) \vee (x^c \wedge 0) && \text{Ley de Complementación} \\
&= (y^c \wedge 0) \vee (x^c \wedge 0) && \text{Ley Conmutativa} \\
&= 0 \vee 0 && \text{Ley de Absorción} \\
&= 0 && \text{Ley de Idempotencia.}
\end{aligned}$$

Ahora probemos que $(x \vee y) \vee (x^c \wedge y^c) = 1$:

$$\begin{aligned}
(x \vee y) \vee (x^c \wedge y^c) &= ((x \vee y) \vee x^c) \wedge ((x \vee y) \vee y^c) && \text{Ley Distributiva} \\
&= ((y \vee x) \vee x^c) \wedge ((x \vee y) \vee y^c) && \text{Ley Conmutativa} \\
&= (y \vee (x \vee x^c)) \wedge (x \vee (y \vee y^c)) && \text{Ley Asociativa} \\
&= (y \vee 1) \wedge (x \vee 1) && \text{Ley de Complementación} \\
&= 1 \wedge 1 && \text{Ley de Absorción} \\
&= 1 && \text{Ley de Idempotencia.}
\end{aligned}$$

□

Definición 3.10 (Isomorfismo de Álgebras de Boole). Si $\langle B, \vee, \wedge, ^c, 0, 1 \rangle$ y $\langle B', \vee', \wedge', ^{c'}, 0', 1' \rangle$ son álgebras de Boole, entonces una función $F : B \rightarrow B'$ será llamada un isomorfismo si F es biyectiva $F(0) = 0'$, $F(1) = 1'$ y para todo $x, y \in B$ se cumple que

$$F(x \vee y) = F(x) \vee' F(y), \quad F(x \wedge y) = F(x) \wedge' F(y), \quad F(x^c) = F(x)^{c'}.$$

La propiedad de distributividad juega un rol fundamental para determinar la estructura de un álgebra de Boole, como lo muestra el siguiente resultado. El mismo no puede ser probado sin la hipótesis de la distributividad, como lo muestra el problema 1.

Teorema 3.8. Sean $\langle B, \vee, \wedge, ^c, 0, 1 \rangle$ y $\langle B', \vee', \wedge', ^{c'}, 0', 1' \rangle$ álgebras de Boole, y sea $F : B \rightarrow B'$. Entonces F es un isomorfismo de álgebras de Boole si y sólo si es un isomorfismo de posets.

Demostración. Ya hemos probado que F es un isomorfismo de reticulados acotados si y sólo si es un isomorfismo de poset. Resta ver que si F es un isomorfismo de posets entonces $F(x^c) =$

$(F(x))^{c'}$, para todo $x \in B$. Note que, si vemos que $F(x^c)$ es un complemento de $F(x)$ en B' , entonces por la unicidad del complemento tendremos que $F(x^c) = (F(x))^{c'}$. Que $F(x^c)$ es un complemento de $F(x)$ sale inmediatamente del hecho que F preserva las operaciones \bigwedge y \bigvee . \square

3.7 Ejercicios

1. Considere el reticulado L_2 de la Fig. 1.b.

- Encuentre $v \bigvee x$, $s \bigvee v$ y $u \bigvee v$.
- ¿Es L_2 un reticulado con complementos?
- Encuentre un elemento con dos complementos.
- ¿Es L_2 un reticulado distributivo?

2. Considere el reticulado L_1 de la Fig. 1.a.

- Para los elementos $1, b, c$, muestre todas las formas posibles de escribirlo como supremo. Por ejemplo, una manera sería $1 = d \bigvee c$.
- Dé los complementos, si es que existen, de los siguientes elementos: $a, b, d, 0$.
- ¿Es L_1 un reticulado con complementos?
- ¿Es L_1 un reticulado distributivo?

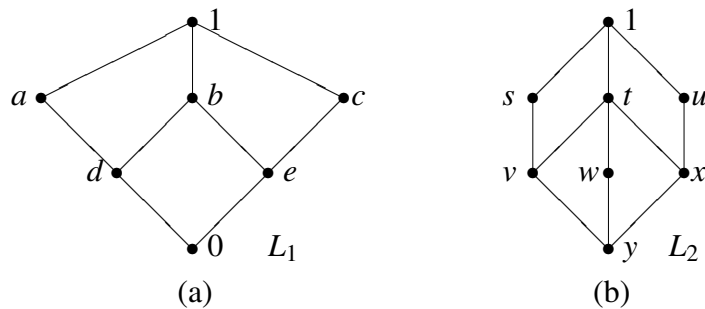


Figura 1:

3. De un ejemplo de un poset finito **no** reticulado P con la siguiente propiedad: para todo $S \subseteq P$, los conjuntos $\{x : x \text{ es cota superior de } S\}$ y $\{x : x \text{ es cota inferior de } S\}$ son ambos no vacíos.

4. (a) Dibuje el diagrama de Hasse para el reticulado $(D_{24}, |)$.
 (b) ¿Es D_{24} un reticulado con complementos?
 (c) ¿Es D_{24} un reticulado distributivo?
 (d) ¿Es D_{24} un álgebra de Boole?
5. (a) Muestre que las figuras 2.b y 2.c son diagramas de Hasse de reticulados distributivos.
 (b) ¿Es Fig. 2.b un reticulado con complementos?
 (c) ¿Es Fig. 2.c un reticulado con complementos?
6. (a) Muestre que la Fig. 2.a es el diagrama de Hasse para $(D_{36}, |)$.
 (b) ¿Es D_{36} un reticulado distributivo?
 (c) ¿Es D_{36} un reticulado con complementos?

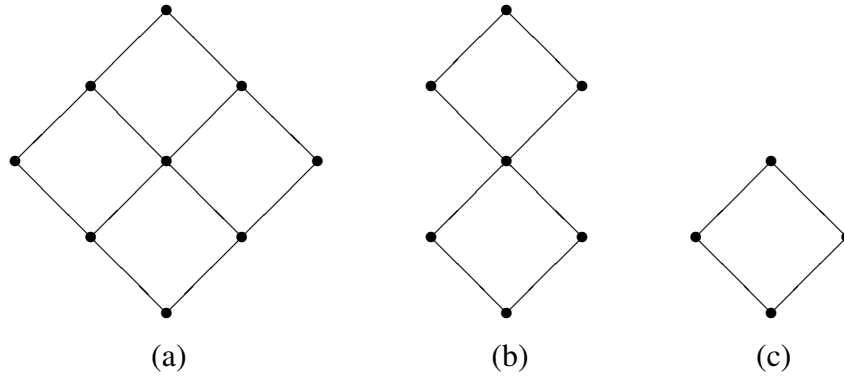


Figura 2:

7. Sea (S, \preceq) un reticulado. Demuestre que si $x \preceq y$, entonces $x \vee (z \wedge y) \preceq (x \vee z) \wedge y$ para toda z en S .
8. Considere los diagramas de la Fig. 3.
 - (a) Determine cuáles son reticulados distributivos.
 - (b) Determine cuáles son álgebras de Boole. Determine en cada caso los subreticulados que son álgebras de Boole (no considere el álgebra de Boole trivial $\{0, 1\}$).

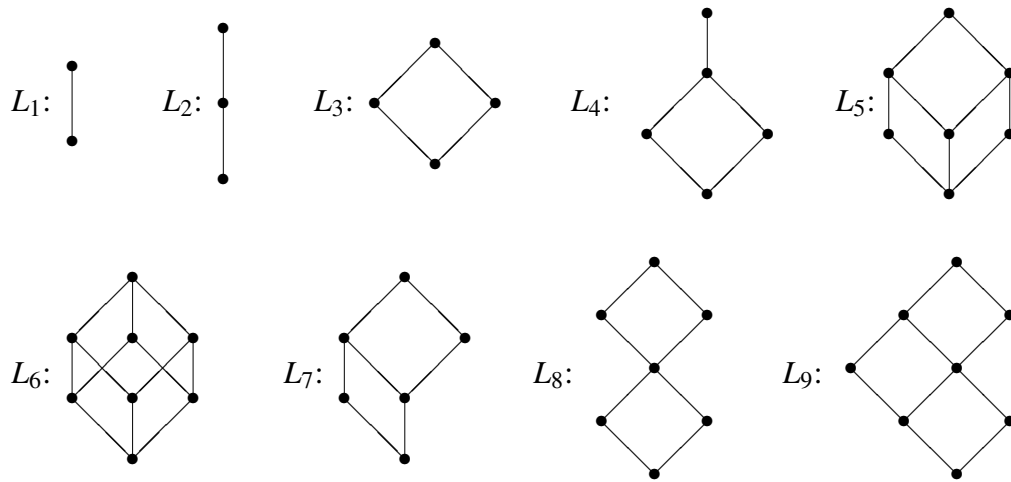


Figura 3:

- (c) Encuentre para L_i con $i = 1, 2, 3, 7, 8$ un álgebra de Boole B_i tal que L_i sea subreticulado de B_i .
9. Sea S un reticulado distributivo. Demuestre que si x e y en S satisfacen $x \vee a = y \vee a$ y $x \wedge a = y \wedge a$ para alguna a en S , entonces $x = y$.
10. Sea B un álgebra de Boole y \preceq el orden asociado a B . Demuestre que
- (a) si $x \preceq y$ entonces $y^c \preceq x^c$;
 - (b) si $y \wedge z = 0$ entonces $y \preceq z^c$;
 - (c) si $x \preceq y$ e $y \wedge z = 0$ entonces $z \preceq x^c$.
11. Sea L un reticulado. Pruebe o refute cada una de las siguientes desigualdades:
1. $x \vee (y \wedge z) \leq (x \vee y \vee z) \wedge (x \vee y)$
 2. $x \vee (y \wedge z) \leq (x \vee y) \wedge (y \vee z)$
 3. $x \wedge (y \vee z) \leq (x \wedge y) \vee (x \wedge z)$
 4. $a \geq c \Rightarrow a \wedge (b \vee c) \geq (a \wedge b) \vee c$

$$5. (a \otimes b) \otimes (a \otimes c) \otimes (b \otimes c) \leq (a \otimes b) \otimes (a \otimes c) \otimes (b \otimes c)$$

$$6. (a \otimes b) \otimes (a \otimes c) \otimes (b \otimes c) \geq (a \otimes b) \otimes (a \otimes c) \otimes (b \otimes c)$$

12. Sea C un orden total (o sea una cadena). Pruebe la identidad

$$x \otimes (y \otimes z) = (x \otimes y) \otimes (x \otimes z),$$

que demuestra la distributividad de C .

3.8 Problemas

- Recordamos que pudimos concluir que $f : L \rightarrow L'$ es un isomorfismo de reticulados si y sólo si es un isomorfismo de posets (Lema 2.3). Lamentablemente, este resultado no puede ser extendido a la estructura de reticulado complementado. Supongamos se define *isomorfismo* de reticulados complementados como un isomorfismo f de reticulados que satisface las ecuaciones

$$f(0) = 0' \quad f(1) = 1' \quad f(x^c) = (f(x))^{c'}.$$

Encuentre dos reticulados complementados, y un iso de posets f entre ellos que no sea iso de reticulados complementados.

- Una mapa $f : L_0 \rightarrow L_1$ se dice un homomorfismo de reticulados si satisface las ecuaciones

$$f(x \otimes y) = f(x) \otimes f(y) \quad f(x \otimes y) = f(x) \otimes f(y).$$

De las siguientes propiedades, que son válidas si f es un isomorfismo, diga cuáles son válidas si f es un homomorfismo.

- f preserva orden,
- si L_0 es distributivo entonces L_1 también lo es,
- si x es complementado entonces $f(x)$ también lo es,
- $f(L_0)$ es subreticulado de L_1 ,
- si L_0 tiene una copia de M_3 entonces L_1 también,

3. Para los puntos 1,...,5 del ejercicio anterior, determinar en que casos los falsos se vuelven verdaderos:
- f inyectiva,
 - f sobre,
 - f biyectiva.

4. Sean L, M dos poset. Considere el conjunto $L \times M$ con la relación \preceq definida:

$$(x_1, y_1) \preceq (x_2, y_2) \text{ si } x_1 \leq_L x_2 \text{ y } y_1 \leq_M y_2.$$

- i. Dé los diagramas de Hasse de :

- $\mathbf{2} \times \mathbf{3}$ (aquí \mathbf{n} denota la cadena de n elementos).
- $\mathcal{P}(\{a, b\}) \times \mathbf{4}$.

- ii. Pruebe que si L, M son reticulados entonces $L \times M$ es un reticulado. Dé explícitamente las operaciones

$$(x_1, y_1) \bigwedge (x_2, y_2)$$

$$(x_1, y_1) \bigvee (x_2, y_2)$$

- iii. Pruebe que si L, M (vistos como estructuras algebraicas) son distributivos, entonces $L \times M$ también lo es.

- iv. Utilizando como guía lo hecho en ii defina el producto $B_0 \times B_1$ de las álgebras de Boole B_0 y B_1 .

5. Sea L un reticulado. Pruebe que L es distributivo si y sólo si para todo $a \in L$, el mapa

$$f_a(x) = (x \bigwedge a, x \bigvee a)$$

definido en L , con imagen en $[a] \times [a]$, es un homomorfismo inyectivo.

6. En un reticulado distributivo $(L, \bigwedge, \bigvee, 0)$ el pseudocomplemento de x es el máximo elemento z (si existe) que satisface $x \bigwedge z = 0$. Pruebe que en las álgebras de Boole el pseudocomplemento es exactamente el complemento.
7. Pruebe que si B es un álgebra de Boole finita entonces B es isomorfa a $\mathbf{2}^n$ para algún $n \geq 1$. (Aquí $\mathbf{2}^n$ denota al álgebra de Boole $\mathbf{2} \times \dots \times \mathbf{2}$).

4 Teoremas de representación

El primer objetivo de este capítulo será demostrar que toda álgebra de Boole finita es isomorfa al álgebra de subconjuntos de un conjunto finito (o sea $\mathcal{P}(X)$). Luego llegaremos a un resultado análogo para los reticulados distributivos finitos. En este caso ya no podremos hablar del álgebra de todos los subconjuntos de un conjunto finito (puesto que no todo reticulado distributivo finito es complementado), pero podremos establecer un resultado similar quedándonos con un subreticulado de tal álgebra de conjuntos.

4.1 Álgebras de Boole finitas

Procedamos ahora con la construcción de un conjunto X asociado a un álgebra de Boole finita B , tal que $\mathcal{P}(X)$ resulte isomorfo a B . El conjunto X que necesitamos estará formado por elementos de B . Una particularidad que tendrá este conjunto es que a partir de él podemos generar todos los elementos del álgebra a través de la operación supremo (o sea para todo $x \in B$ existe $S \subseteq B$ tal que $x = \sup S$). Es un buen ejercicio buscar en los diagramas de las álgebras de Boole de 4 y 8 elementos que subconjuntos tiene esta particularidad, y cuál de todos es el más chico.

Definición 4.1 (Átomo). *Sea B un álgebra de Boole. Un elemento $a \in B$ será llamado átomo si a cubre a 0. Mediante $At(B)$ denotamos el conjunto de todos los átomos de B .*

El siguiente lema muestra que $At(B)$ es el conjunto que buscábamos.

Lema 4.1. *Sea B un álgebra de Boole finita. Entonces todo elemento de B se escribe de manera única como supremo de átomos. O sea: para todo $x \in B$ se tiene:*

1. $x = \sup\{a \in At(B) : a \leq x\}$,
2. si $A \subseteq At(B)$ y $x = \sup A$, entonces $A = \{a \in At(B) : a \leq x\}$.

Vamos a proceder ahora con la prueba de este lema. Para esto necesitamos los siguientes resultados. El primero se prueba fácilmente.

Lema 4.2. *Sea B un álgebra de Boole finita. Para todo $x \in B$ distinto de 0 existe $a \in At(B)$ tal que $a \leq x$.*

Lema 4.3. *Sea B un álgebra de Boole finita, y sean $x, y \in B$ tales que $x \not\leq y$. Entonces existe $a \in At(B)$ tal que $a \leq x$ y $a \not\leq y$.*

Demostración. Veamos que $x \wedge y^c \neq 0$. Si $x \wedge y^c = 0$, entonces $y \vee (x \wedge y^c) = y \vee 0$, o sea $y \vee x = y$, lo que contradice la hipótesis del lema. Luego $x \wedge y^c \neq 0$. Por el lema anterior existe $a \in At(B)$ tal que $a \leq x \wedge y^c$. Claramente $a \leq x$, veamos que $a \not\leq y$. Si $a \leq y$, como $a \leq x \wedge y^c$ tendríamos $a \leq x \wedge y^c \wedge y = 0$, lo que es absurdo puesto que a es un átomo. Luego $a \not\leq y$. \square

Demostración. (del Lema 4.1)

Sea $A_x = \{a \in At(B) : a \leq x\}$, y sea $y = \sup\{a \in At(B) : a \leq x\} = \sup A_x$.

1. Como x es cota superior de A_x , entonces claramente $y \leq x$. Supongamos ahora que $x \not\leq y$. Por el lema 4.3, existe $a \in At(B)$ tal que $a \leq x$ y $a \not\leq y$. Pero esto es absurdo, pues $a \leq x$ implica $a \in A_x$, lo que indica que $a \leq y$. Concluimos que $x \leq y$, y por lo tanto $x = y$.
2. Que $A \subseteq A_x$ es inmediato: $a \in A$ implica $a \leq x$, lo que indica que $a \in A_x$. Veamos que $A_x \subseteq A$. Sea $b \in A_x$, y supongamos que $A = \{a_1, \dots, a_n\}$. Como $x = a_1 \vee \dots \vee a_n$ y B es distributiva, tenemos que

$$b = b \wedge x = (b \wedge a_1) \vee \dots \vee (b \wedge a_n)$$

Como b es un átomo (y por lo tanto cubre al 0), tenemos que para todo $i = 1, \dots, n$, el elemento $b \wedge a_i$ debe ser 0 o b , y además no puede ser que $b \wedge a_i = 0$ para todo i (sino b sería 0). Luego existe i tal que $b \wedge a_i = b$, lo que indica que $b = a_i$, puesto que ambos son átomos. Luego $b \in A$.

□

Ahora si estamos en condiciones de probar lo que era nuestro objetivo.

Teorema 4.4. Sea $\langle B, \vee, \wedge, ^c, 0, 1 \rangle$ un álgebra de Boole finita, y sea $X = At(B)$. La función

$$\begin{aligned} F : B &\longrightarrow \mathcal{P}(X) \\ x &\longrightarrow \{a \in X : a \leq x\} \end{aligned}$$

es un isomorfismo entre $\langle B, \vee, \wedge, ^c, 0, 1 \rangle$ y $\langle \mathcal{P}(X), \cup, \cap, ^c, \emptyset, X \rangle$.

Demostración. Sea $A_x = \{a \in At(B) : a \leq x\}$. Vemos primero que el mapa definido mediante $F(x) = A_x$ es una biyección entre B y $\mathcal{P}(At(B))$.

F es **uno-a-uno** porque $A_x = A_y$ implica $\sup A_x = \sup A_y$, lo que nos permite concluir desde el lema 4.1 (inciso 1) que $x = y$, dado que $x = \sup A_x$ y $y = \sup A_y$.

Vemos que F es **sobre**. Sea $A \subseteq At(B)$. Definamos $x = \sup A$, y verifiquemos que $F(x) = A$. Por el lema 4.1 (inciso 2) tenemos que $A = A_x$, lo que indica que $F(x) = A$.

Veamos ahora que F es un isomorfismo. Hemos probado en el capítulo anterior que F es isomorfismo de álgebras de Boole si y sólo si es isomorfismo de posets. Luego, resta verificar:

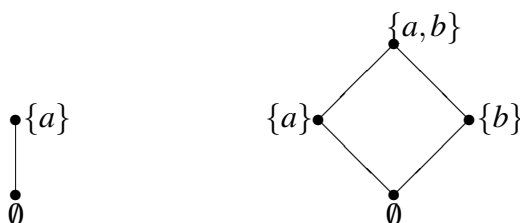
$$x \leq y \Leftrightarrow A_x \subseteq A_y,$$

o sea,

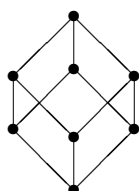
$$\sup A_x \leq \sup A_y \Leftrightarrow A_x \subseteq A_y.$$

La implicación (\Leftarrow) no presenta dificultades, y se deja como ejercicio para el lector. Supongamos $\sup A_x \leq \sup A_y$, y tomemos $a \in A_x$. Entonces $a \leq x = \sup A_x \leq \sup A_y = y$. Luego $a \in A_y$. □

Desde el Teorema anterior, concluimos que las dos álgebras de Boole no triviales más chicas son $\mathcal{P}(\{a\})$ y $\mathcal{P}(\{a,b\})$, cuyos diagramas son



Luego, le siguen en orden creciente $\mathcal{P}(X)$, con $|X| = 3, 4, \dots$. El caso $|X| = 3$ tiene aún un diagrama fácil de dibujar:



Por último, el Teorema anterior nos permite responder la siguiente pregunta: Para qué números naturales n existe un álgebra de Boole B tal que $|B| = n$? La respuesta es: para todo número de la forma 2^k , con $k = 0, 1, \dots$

Antes de pasar al estudio de los reticulados distributivos, es natural preguntarse si el Teorema anterior puede extenderse a las álgebras de Boole infinitas. Lamentablemente, la respuesta es negativa, como lo demuestra el siguiente resultado.

Lema 4.5. *Existe un álgebra de Boole infinita que no es isomorfa $\mathcal{P}(X)$, para ningún X .*

Demostración. Un subconjunto de números naturales se dice *cofinito* si su complemento es finito. Definamos

$$\mathcal{B} = \{X \subseteq \mathbf{N} : X \text{ es finito o cofinito}\}.$$

Note que las operaciones \cup, \cap y c están bien definidas sobre \mathcal{B} puesto que

$$X \in \mathcal{B}, Y \in \mathcal{B} \Rightarrow (X \cup Y) \in \mathcal{B},$$

$$X \in \mathcal{B}, Y \in \mathcal{B} \Rightarrow (X \cap Y) \in \mathcal{B},$$

$$X \in \mathcal{B} \Rightarrow X^c \in \mathcal{B}.$$

Luego, la estructura $\langle \mathcal{B}, \cup, \cap, \emptyset, \mathbf{N}, ^c \rangle$ es claramente un álgebra de Boole.

Veamos que no puede ser isomorfa a $\mathcal{P}(X)$, para ningún X . Para esto veremos que es imposible encontrar una función biyectiva entre \mathcal{B} y $\mathcal{P}(X)$, cualquiera sea el X . Si X es finito, entonces $\mathcal{P}(X)$ es finito, por lo tanto es imposible encontrar tal biyección puesto que \mathcal{B} es infinito.

El caso X infinito requiere un poco más de trabajo. Primero notemos que el conjunto \mathcal{B} es infinito y numerable (o sea que puede ponerse en correspondencia biyectiva con los números naturales). En efecto, es sabido que $\{X \subseteq \mathbf{N} : X \text{ es finito}\}$ es numerable, y el mapa $X \rightarrow X^c$ es una biyección entre $\{X \subseteq \mathbf{N} : X \text{ es finito}\}$ y $\{X \subseteq \mathbf{N} : X \text{ es cofinito}\}$. Luego \mathcal{B} resulta numerable puesto que es unión de dos conjuntos numerables.

Por otro lado, es sabido que si X es un conjunto infinito, entonces $\mathcal{P}(X)$ es un conjunto infinito no numerable, luego no puede ponerse de ninguna manera en correspondencia con \mathcal{B} , que es numerable. \square

4.2 Reticulados distributivos finitos

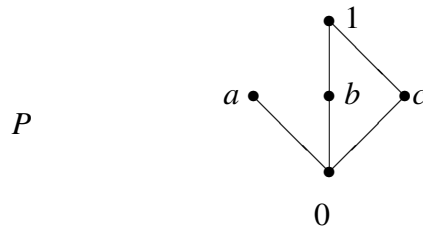
Anteriormente mencionamos que un reticulado distributivo finito no necesariamente será de la forma $\mathcal{P}(X)$, puesto que no todos son complementados. Vamos a introducir ahora un álgebra (incompleta) de conjuntos, que jugará para los reticulados distributivos finitos el mismo rol que jugaba $\mathcal{P}(X)$ para las álgebras de Boole.

Dado un poset (P, \leq) , diremos que un subconjunto $D \subseteq P$ es *decreciente* si para todo $x, z \in P$ se tiene que:

$$x \in D \text{ y } z \leq x \implies z \in D.$$

O sea, un conjunto decreciente satisface que si un elemento se encuentra en el conjunto, entonces todos los elementos menores también están.

Por ejemplo, considere el poset P de abajo. El conjunto $\{0, a\}$ es decreciente, pero el conjunto $\{0, b, 1\}$ no lo es, porque 1 está en el conjunto y c no.



Denotaremos mediante $\mathcal{D}(P)$ a la familia de todos los subconjuntos decrecientes de P :

$$\mathcal{D}(P) = \{D \subseteq P : D \text{ es decreciente}\}.$$

Notemos que \emptyset y P son decrecientes. Además la unión e intersección de subconjuntos decrecientes es decreciente.

Las observaciones anteriores nos dicen que dado un poset finito (P, \leq) , tenemos asociado naturalmente el reticulado acotado

$$\langle \mathcal{D}(P), \cup, \cap, \emptyset, P \rangle.$$

Además tal reticulado es distributivo, puesto que en el álgebra de conjuntos se satisfacen las leyes distributivas.

Tenemos entonces un reticulado formado por conjuntos que jugará para los reticulados distributivos finitos el rol que jugaba $\mathcal{P}(X)$ para las álgebras de Boole.

Qué elementos desempeñarán el rol de los átomos?

Definición 4.2. Sea $\langle L, \vee, \wedge, 0, 1 \rangle$ un reticulado acotado. Un elemento $x \in L$ será llamado \vee -irreducible si

1. $x \neq 0$,
2. si $x = y \vee z$, entonces $x = y$ o $x = z$, para todo $y, z \in L$.

Notemos que la condición (2) es equivalente a la siguiente condición, la cual es mas fácil de chequear en los diagramas de Hasse:

(2') si $y < x$ y $z < x$, entonces $y \vee z < x$, para todo $y, z \in L$.

En el caso en que L es finito, nótese que 2' es equivalente a

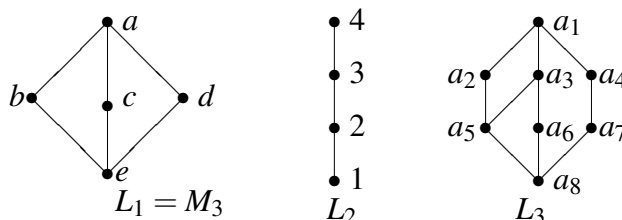
(2'') existe un z tal que $z < x$ y $z = \sup\{y \mid y < x\}$.

De la condición (2'') podemos concluir fácilmente que todo átomo de $\langle L, \vee, \wedge, 0, 1 \rangle$ es un elemento \vee -irreducible.

Si $\langle L, \vee, \wedge, 0, 1 \rangle$ es un reticulado acotado, denotaremos

$$Irr(L) = \{i \in L : i \text{ es } \vee\text{-irreducible}\}.$$

Por ejemplo, considere los siguientes reticulados.



Los conjuntos de átomos e irreducibles son dados a continuación.

$$\begin{aligned} At(L_1) &= \{b, c, d\} & Irr(L_1) &= \{b, c, d\}, \\ At(L_2) &= \{2\} & Irr(L_2) &= \{2, 3, 4\}, \\ At(L_3) &= \{a_5, a_6, a_7\}, & Irr(L_3) &= \{a_2, a_4, a_5, a_6, a_7\}. \end{aligned}$$

Si X es un conjunto finito, entonces ya hemos mencionado que los subconjuntos que contienen un solo elemento son los átomos de $\mathcal{P}(X)$. Es un buen ejercicio comprobar en algunos casos ($|X| = 2, 4, 8$) que estos además son los únicos elementos irreducibles de $\mathcal{P}(X)$. La noción de \bigvee -irreducible se reduce a la noción de átomo, en el caso de las álgebras de Boole. Esto establece el siguiente Lema.

Lema 4.6. *Sea $\langle B, \bigvee, \bigwedge, ^c, 0, 1 \rangle$ un álgebra de Boole. Un elemento $x \in B$ es \bigvee -irreducible si y sólo si x es un átomo.*

Demostración. Como ya se observó anteriormente todo átomo es \bigvee -irreducible. Supongamos ahora que $x \in Irr(B)$ y sea $y \in B$ tal que $0 \leq y < x$. Veremos que $y = 0$. Tenemos

$$x = x \bigwedge 1 = x \bigwedge (y \bigvee y^c) = y \bigvee (x \bigwedge y^c)$$

En consecuencia $x \leq x \bigwedge y^c$, lo cual implica que $x = x \bigwedge y^c$, es decir $x \leq y^c$. Pero entonces tenemos que $y \leq x^c$, lo cual nos dice que $y = 0$, ya que $y < x$. □

Nuestro próximo objetivo es demostrar que todo reticulado distributivo finito es isomorfo al reticulado de los decrecientes de un poset P . Seguiremos exactamente los pasos que efectuamos para el caso de las álgebras de Boole. En particular, el candidato a ser el poset (P, \leq) asociado al reticulado L es $(Irr(L), \leq)$, donde \leq es el orden heredado de L .

Vamos ahora a probar una serie de lemas que nos permitirán estructurar para los reticulados una demostración similar a la desarrollada para el caso de las álgebras de Boole.

Lema 4.7. *Sea $\langle L, \bigvee, \bigwedge, 0, 1 \rangle$ un reticulado acotado distributivo y sea $x \in Irr(L)$. Si $x_1, \dots, x_n \in L$ y $x \leq x_1 \bigvee x_2 \bigvee \dots \bigvee x_n$, entonces $x \leq x_i$, para algún $i = 1, \dots, n$.*

Demostración. Haremos la prueba haciendo inducción en n . Si $n = 1$ el resultado es obvio. Probemos para $n = 2$. Entonces si $x \leq x_1 \bigvee x_2$ tenemos que

$$\begin{aligned} x &= x \bigwedge (x_1 \bigvee x_2) && (\text{pues } x \leq x_1 \bigvee x_2) \\ &= (x \bigwedge x_1) \bigvee (x \bigwedge x_2) && (\text{pues } L \text{ es distributivo}). \end{aligned}$$

Dado que x es irreducible debe ser $x = x \wedge x_1$ o $x = x \wedge x_2$, luego $x \leq x_1$ o $x \leq x_2$.

Supongamos ahora que si $x \leq x_1 \vee x_2 \vee \dots \vee x_k$, entonces $x \leq x_i$, para algún $i = 1, \dots, k$. Veamos que lo mismo ocurre si $n = k + 1$. Por lo visto en el caso $n = 2$ podemos ver que si $x \leq (x_1 \vee x_2 \vee \dots \vee x_k) \vee x_{k+1}$ entonces $x \leq (x_1 \vee x_2 \vee \dots \vee x_k)$ o $x \leq x_{k+1}$. Aplicando la hipótesis inductiva concluimos que $x \leq x_i$ para algún i , $1 \leq i \leq k$ o $x \leq x_{k+1}$; luego $x \leq x_i$ para algún i , $1 \leq i \leq x_{k+1}$. □

Lema 4.8. Sea L un reticulado finito, y sean $x, y \in L$ tales que $x \not\leq y$. Entonces existe $i \in \text{Irr}(L)$ tal que $i \leq x$ e $i \not\leq y$.

Demostración. Sea $I = \{z \in L : i \leq x \text{ e } i \not\leq y\}$. Claramente I no es el conjunto \emptyset , puesto que x es un elemento de I . Entonces como L es finito, I posee un elemento minimal, llamémoslo i . Para concluir la prueba, sólo tenemos que ver que $i \in \text{Irr}(L)$. Sean u, v tales que $i = u \vee v$, sin pérdida de generalidad, supongamos que $i \neq u$. Veamos que $i = v$.

Claramente $v \leq x$. Veamos primero que $v \not\leq y$. Supongamos por un momento que $v \leq y$. Entonces $u \not\leq y$, porque de lo contrario tendríamos $i = u \vee v \leq y$, lo que es una contradicción. Pero entonces $u \in I$, lo que es un absurdo, puesto que i es minimal de I .

Entonces tenemos que $v \not\leq y$, lo que indica que $v \in I$. Como i es minimal, concluimos que $v = i$. □

Lema 4.9. Sea L un reticulado distributivo finito. Entonces para todo $x \in L$ se tiene:

1. $x = \sup\{i \in \text{Irr}(L) : i \leq x\}$,
2. si $D \subseteq \text{Irr}(L)$ es decreciente, y $x = \sup D$, entonces $D = \{i \in \text{Irr}(L) : i \leq x\}$.

Demostración. Sea $D_x = \{i \in \text{Irr}(L) : i \leq x\}$, y sea $y = \sup\{i \in \text{Irr}(L) : i \leq x\}$.

1. Se repite exactamente el argumento desarrollado para las álgebras de Boole.
2. El argumento es muy similar al desarrollado para el caso de la álgebras de Boole. De todas maneras la haremos en detalle.

Que $D \subseteq D_x$ es inmediato: $i \in D$ implica $i \leq x$, lo que indica que $i \in D_x$. Veamos que $D_x \subseteq D$. Sea $j \in D_x$, y supongamos que $D = \{i_1, \dots, i_n\}$. Como $x = i_1 \vee \dots \vee i_n$ y L es distributiva, tenemos que

$$j = j \wedge x = (j \wedge i_1) \vee \dots \vee (j \wedge i_n)$$

Como $j \in \text{Irr}(L)$, tenemos que existe k tal que $j \wedge i_k = j$, lo que indica que $j \leq i_k$. Como D es decreciente tenemos que $j \in D$.

□

Después de esta maratón de lemas estamos en condiciones de probar nuestro (mejor dicho, de Birkhoff) teorema de representación para reticulados distributivos finitos.

Teorema 4.10 (Teorema de representación de Birkhoff). *Sea $\langle L, \vee, \wedge, 0, 1 \rangle$ un reticulado acotado distributivo finito, y sea $P = \text{Irr}(L)$. Entonces la función*

$$\begin{aligned} F : L &\longrightarrow \mathcal{D}(P) \\ x &\longrightarrow \{y \in P : y \leq x\} \end{aligned}$$

es un isomorfismo entre $\langle L, \vee, \wedge, 0, 1 \rangle$ y $\langle \mathcal{D}(P), \cup, \cap, \emptyset, P \rangle$.

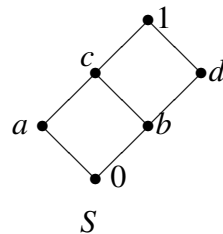
Demostración. Sea $D_x = \{i \in \text{Irr}(L) : i \leq x\}$. Para ver que el mapa definido mediante $F(x) = D_x$ es una biyección entre L y $\mathcal{D}(\text{Irr}(L))$, repetimos exactamente el argumento hecho para el caso de las álgebras de Boole, pero usando en este caso el Lema 4.9.

Veamos ahora que F es un isomorfismo. Hemos probado en el capítulo anterior que F es isomorfismo de reticulados distributivos acotados si y sólo si es isomorfismo de posets. Luego, resta verificar:

$$x \leq y \Leftrightarrow D_x \subseteq D_y,$$

Aquí nuevamente repetimos el argumento hecho para el caso de las álgebras de Boole. □

Por ejemplo, consideremos el siguiente reticulado S .



Aquí $\text{Irr}(S) = \{a, b, d\}$. La familia de subconjuntos decrecientes de $\text{Irr}(S)$ es

$$\mathcal{D}(\text{Irr}(S)) = \{\emptyset, \{a\}, \{b\}, \{b, d\}, \{a, b\}, \{a, b, d\}\}.$$

La correspondencia F dada por el Teorema 4.10 es:

$$\begin{array}{ll} 0 \rightarrow \emptyset & a \rightarrow \{a\} \\ b \rightarrow \{b\} & d \rightarrow \{b, d\} \\ c \rightarrow \{a, b\} & 1 \rightarrow \{a, b, d\} \end{array}$$

Finalmente, consideremos el reticulado $L = D_{36}$. Entonces $Irr(L) = \{2, 3, 4, 9\}$. La familia de subconjuntos decrecientes de $Irr(L)$ es:

$$\mathcal{D}(Irr(L)) = \{\emptyset, \{2\}, \{2, 4\}, \{3\}, \{3, 9\}, \{2, 3\}, \{2, 4, 3\}, \{2, 3, 9\}, \{2, 3, 4, 9\}\}.$$

La correspondencia entre L y $\mathcal{D}(Irr(L))$ está dada por

$$F(n) = \{k \in Irr(L) \mid k \text{ divide a } n\},$$

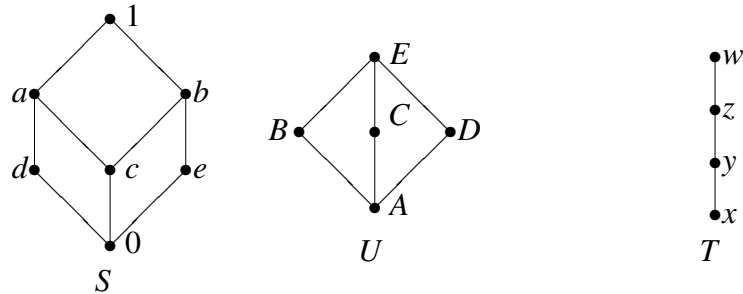
por ejemplo, $f(18) = \{2, 3, 9\}$.

Finalmente, los teoremas probados en las secciones anteriores nos permiten probar fácilmente la siguiente caracterización de las álgebras de Boole finitas:

Corolario 4.11. Si $\langle L, \bigvee, \bigwedge, 0, 1 \rangle$ es un reticulado acotado distributivo finito, entonces $\langle L, \bigvee, \bigwedge, 0, 1 \rangle$ es álgebra de Boole si y sólo si $Irr(L) = At(L)$.

4.3 Ejercicios

1. Considere los reticulados S , T y U de la siguiente figura:



- (a) Calcule el conjunto de átomos de cada reticulado.
 - (b) Calcule el conjunto de irreducibles de cada reticulado.
 - (c) ¿Tiene alguno de esos reticulados elementos irreducibles que no sean átomos?
2. (a) Encuentre los átomos de $(D_{12}, |)$.
 - (b) Muestre que los elementos 2 y 6 en D_{12} no tiene complementos.
 - (c) Encuentre los elementos irreducibles de D_{12} .
 - (d) Escriba el elemento máximo de D_{12} como supremos de elementos irreducibles.

3. (a) Encuentre los átomos de $(D_{36}, |)$.
 (b) Encuentre los elementos irreducibles de D_{36} .
 (c) Escriba al elemento máximo de D_{36} como unión de elementos irreducibles.
4. Considere los diagramas de la Fig. 4.

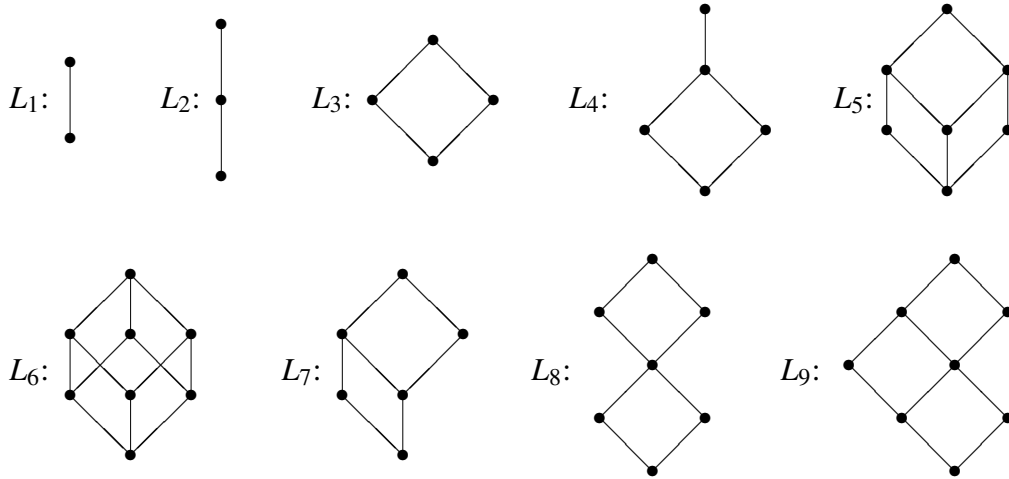


Figura 4:

- (a) Halle en cada caso $At(L)$.
 (b) Halle en cada caso $Irr(L)$.
 (c) Dibuje en cada caso el diagrama de Hasse de $\mathcal{P}(At(L))$.
 (d) Dibuje en cada caso el diagrama de Hasse de $\mathcal{D}(Irr(L))$.
 (e) Determine cuáles son álgebras de Boole.
5. Para cada uno de los reticulados de la Fig. 4, determine cuales satisfacen las hipótesis del Teorema 4.4. En tal caso dar explícitamente el mapa F .
6. Para cada uno de los reticulados de la Fig. 4, determine cuales satisfacen las hipótesis del Teorema 4.10. En tal caso dar explícitamente el mapa F . Qué propiedades tiene?
7. Para cada uno de los reticulados de la Fig. 4, utilice el Teorema 4.10 para determinar si el reticulado es distributivo o no.

4.4 Problemas

8. Encuentre todos los reticulados distributivos con exactamente 3 join irreducibles.
9. Encuentre todos los reticulados distributivos con exactamente 4 join irreducibles y un sólo átomo (que está contado entre los 4 join irred.).
10. Efectúe un rastreo en la prueba del Teorema de Birkhoff para comprobar que en la ausencia de la propiedad de distributividad, aún se puede probar que el mapa F es inyectivo. Utilice este hecho para demostrar que la siguiente propiedad es válida para todos los reticulados finitos:

L **no** es distributivo si y sólo si $|L| < |\mathcal{D}(\text{Irr}(L))|$.

11. Supongamos que n es producto de primos distintos p_1, p_2, \dots, p_k , ¿cuáles son los elementos irreducibles de D_n ?
12. Encuentre un homomorfismo f de D_{90} en $\mathbf{2}$ que separe el 10 del 9, o sea que $f(10) \neq f(9)$.
13. En ejercicios anteriores hemos definido el producto de reticulados. Pruebe lo siguiente:
 - (a) Si $i \in \text{Irr}(L)$ entonces $(i, 0_G) \in \text{Irr}(L \times G)$
 - (b) Si $j \in \text{Irr}(G)$ entonces $(0_L, j) \in \text{Irr}(L \times G)$
 - (c) Si $(x, y) \in \text{Irr}(L \times G)$, entonces ocurre una de las dos siguientes posibilidades:
 - i. $x = 0_L$ e $y \in \text{Irr}(G)$
 - ii. $y = 0_G$ y $x \in \text{Irr}(L)$.
14. Queremos abordar en este problema la siguiente cuestión, formulada para reticulados distributivos finitos L y G .
 Supongamos que $L \times G = \mathcal{D}(P)$, para cierto poset P . ¿Qué relación tiene P con $\text{Irr}(L)$ e $\text{Irr}(G)$?
 - (a) Estudie varios ejemplos (puede experimentar con $\mathbf{2} \times \mathbf{3}$, $\mathbf{3} \times \mathbf{3}$ y $\mathbf{2} \times \mathcal{P}(\{a, b\})$ por ejemplo).
 - (b) Formule una conjetura.
 - (c) Trate luego de obtener una prueba formal de la conjetura.

5 Filtros primos

En esta sección vamos a estudiar noción de *filtro primo*, que tiene fundamental importancia en la teoría de reticulados distributivos. Los conceptos y resultados vertidos en esta sección serán utilizados en Lógica.

Vamos a dar ahora las definiciones más importantes de esta sección. En esta sección L será siempre un reticulado distributivo. Un subconjunto no vacío $F \subseteq L$ se dice *filtro* si es *creciente* y *cerrado para el \otimes* , o sea:

- (1) $x \in F$, $x \leq y$ implica $y \in F$,
- (2) $x \in F$, $y \in F$ implican $x \otimes y \in F$.

Un filtro P se dice *propio* si está contenido estrictamente en L (o sea, si visto como conjunto es distinto de L). Un filtro propio P se dice *primo* si cada vez que $x \vee y \in P$ se tiene que $x \in P$ o $y \in P$. Por último un filtro F se dice *maximal* si no existe otro filtro propio Q (distinto de F) que lo contenga. Esto es lo mismo que decir que F es un elemento maximal del poset formado por todos los filtros propios.

Vamos a dar ahora algunos ejemplos.

- (1) Si C es una cadena, o sea un orden total, entonces para cada $x \in C$ se tiene que

$$[x) = \{z \in C : z \geq x\}$$

es un filtro, y $[x)$ será primo siempre que x no sea el menor elemento de C .

- (2) Consideremos el reticulado distributivo $(\mathcal{P}(X), \cap, \cup)$. Entonces para cada $Z \subseteq X$ se tiene que

$$F = \{Y \subseteq X : Z \subseteq Y\},$$

o sea, la familia de todos los conjuntos que contienen a Z es un filtro de $\mathcal{P}(X)$. Tal filtro será propio cuando $Z \neq \emptyset$, y será primo si y sólo si Z tiene un sólo elemento. En efecto, si Z tiene más de un elemento entonces es factible escribir $Z = Z_1 \cup Z_2$, con $Z_1 \neq Z \neq Z_2$, con lo que se demuestra que F no es primo. Por otro lado, si $Z = \{x\}$ y $Y \in F$ entonces $Y = Y_1 \cup Y_2$ implica $x \in Y_1$ o $x \in Y_2$, lo que indica que $Y_1 \in F$ o $Y_2 \in F$.

Por otro lado es fácil ver que si Z tiene un elemento entonces F es maximal.

- (3) Si L es cualquier reticulado distributivo entonces $F = L$ es un filtro que no es propio, y por lo tanto no es primo. Por otro lado, si $a \in L$ entonces

$$[a) = \{x \in L : x \geq a\}$$

es un filtro, llamado *principal*. Tenemos que $[a]$ es propio salvo que a sea el mínimo elemento de L . Note además que si L es finito entonces todo filtro F es principal. En efecto, si $F = \{x_1, \dots, x_n\}$ entonces

$$F = [x_1 \bigwedge \dots \bigwedge x_n].$$

Lema 5.1. *Sea L un reticulado distributivo. $[a]$ es un filtro primo si y sólo si a es join-irreducible. En consecuencia si L es finito entonces todo filtro primo es de la forma $[a]$, con $a \in \text{Irr}(L)$.*

Demostración. Supongamos que $[a]$ es primo, y sea $x, y \in L$ tales que $x \vee y = a$. Entonces $x \vee y \in [a]$, y por lo tanto $x \in [a]$ o $y \in [a]$. Como tanto x como y son menores o iguales a a se tiene que $x = a$ o $y = a$. Luego hemos probado que a es join-irreducible.

Supongamos ahora que a es join-irreducible. Sea $x, y \in L$ tales que $x \vee y \in [a]$. Entonces $a \leq x \vee y$, o sea

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

Luego como a es join-irreducible se tiene $a = x \wedge a$ o $a = y \wedge a$, o sea $x \in [a]$ o $y \in [a]$. Note que en esta parte de la prueba es fundamental la propiedad de distributividad. \square

La prueba del siguiente lema se deja como ejercicio.

Lema 5.2. *Sea L un reticulado distributivo. $[a]$ es un filtro maximal si y sólo si a es átomo. En consecuencia si L es finito entonces todo filtro maximal es de la forma $[a]$, con $a \in \text{At}(L)$.*

Corolario 5.3. *Sea B un álgebra de Boole finita entonces todo filtro primo es un filtro maximal de la forma $[a]$, con $a \in \text{At}(B)$.*

De este corolario se desprende el ejemplo (2) en donde se describen los filtros primos de $\mathcal{P}(X)$. Veremos más adelante que en las álgebras de Boole los filtros primos y los maximales coinciden. Esto no pasa en los reticulados distributivos en general. Obsérvese el ejemplo (1) de las cadenas. Allí todo elemento $x \in C$ distinto de 0 origina un filtro primo $[x]$ que será maximal sólo cuando x sea un átomo. Pero en todo reticulado distributivo vale el siguiente resultado.:

Lema 5.4. *Sea L un reticulado distributivo y sea F un filtro maximal de L . Entonces F es primo.*

Demostración. Supongamos que F es maximal y que x, y son elementos de L tales que $x \notin F$ y $x \vee y \in F$. Veamos que $y \in F$. Sea

$$Q = \{z \in L : z \geq y \wedge f \text{ para algún } f \in F\}$$

Veamos que Q es un filtro. Dejamos al lector el verificar que Q es creciente. Sea $z, w \in Q$, veamos que $z \otimes w \in Q$. Sabemos que existen $p, q \in F$ tales que $z \geq y \otimes p$ y $w \geq y \otimes q$. Luego

$$z \otimes w \geq (y \otimes p) \otimes (y \otimes q) = y \otimes (p \otimes q).$$

Como F es un filtro se tiene que $p \otimes q \in F$. Luego $z \otimes w \in Q$. Concluimos entonces que Q es un filtro. Como F es maximal tenemos que $Q = F$ o $Q = L$. Si $Q = F$ entonces tenemos que $y \in Q = F$, que es lo que queríamos demostrar. Veamos que la posibilidad $Q = L$ no puede ser. Si fuera $Q = L$ entonces $0 \in Q$ lo que dice que existe $f \in F$ tal que $0 = y \otimes f$. Luego

$$x = x \otimes (y \otimes f) = (x \otimes y) \otimes (y \otimes f).$$

Como $x \otimes y \in F$ y $y \otimes f \in F$ tenemos que $(x \otimes y) \otimes (y \otimes f) = x \in F$, lo que es una contradicción. \square

Lema 5.5. Sea B un álgebra de Boole, y sea P un filtro propio de B . Entonces son equivalentes:

- i. P es primo.
- ii. P es maximal.
- iii. Para todo $x \in B$ se tiene $x \in P$ o $x' \in P$.

Demostración. Supongamos i. Sea Q tal que $P \subset Q$ y Q es un filtro. Veamos que $Q = B$. Tomemos $a \in Q - P$. Como $a \otimes a' = 1 \in P$ y $a \notin P$, se tiene que $a' \in P \subset Q$. Luego $a, a' \in Q$ y por lo tanto $0 = a \otimes a' \in Q$. Como Q es un filtro se tiene que $Q = B$. Luego hemos demostrado ii.

Supongamos ii. Sea $a \notin P, a \neq 0$. Definamos

$$Q = \{x \in L : x \geq a \otimes p \text{ para algún } p \in P\}.$$

Al igual que en la prueba del Lema 5.4, Q es un filtro.

Q no puede ser propio, pues sino $P = Q$ (porque P es maximal) y tendríamos entonces $a \in P$, que es una contradicción. Luego $Q = B$. Como $0 \in Q$ deducimos que existe $p \in P$ tal que $0 \geq a \otimes p$, o sea $0 = a \otimes p$. Entonces

$$a' = a' \otimes (a \otimes p) = (a' \otimes a) \otimes (a' \otimes p) = a' \otimes p.$$

Esto dice que $a' \geq p \in P$, por lo tanto $a' \in P$. Luego hemos probado iii.

Supongamos por último iii. Sean $x, y \in L$ tales que $x \otimes y \in P$. Supongamos además que $x \notin P$. Entonces $x' \in P$, y también

$$x' \otimes (x \otimes y) = (x' \otimes x) \otimes (x' \otimes y) = x' \otimes y \in P.$$

Como $y \geq x' \otimes y \in P$ se tiene que $y \in P$. Luego hemos demostrado que para todo par $x, y \in L$ tales que $x \otimes y \in P$, se tiene $x \in P$ o $y \in P$. Esto concluye la demostración de i. \square

El siguiente teorema es una herramienta fundamental de la Teoría de Reticulados Distributivos, y se usará en las pruebas de completitud lógica.

Teorema 5.6 (del Filtro Primo). *Si Γ, Φ son subconjuntos del reticulado distributivo L , y para todo $x_1, \dots, x_n \in \Gamma, y_1, \dots, y_m \in \Phi$ se tiene*

$$x_1 \otimes \dots \otimes x_n \not\leq y_1 \otimes \dots \otimes y_m,$$

entonces existe un filtro primo P tal que $\Gamma \subseteq P$ y $P \cap \Phi = \emptyset$.

En particular, en el caso $\Gamma = \{x\}, \Phi = \{y\}$ obtenemos el resultado: "si $x \not\leq y$ entonces existe un filtro primo P tal que $x \in P$ y $y \notin P$."

Note que por el Lema 5.1, para el caso finito este hecho se traduce en el resultado siguiente, ya probado:

"si $y \not\leq x$ entonces existe un join irreducible j tal que $j \leq y$ y $j \not\leq x$."

De hecho la noción de filtro primo reemplaza a la noción de join irreducible en el caso infinito en el cual estos elementos no son suficientemente expresivos.

Por último estudiaremos la relación entre filtros primos y homomorfismos. Sean L, R dos reticulados. Un *homomorfismo de reticulados* es un mapa $f : L \rightarrow R$ tal que:

$$\begin{aligned} f(x \otimes y) &= f(x) \otimes f(y) \\ f(x \vee y) &= f(x) \vee f(y) \end{aligned}$$

para todo $x \in L$.

Denotaremos mediante $\mathbf{2}$ al reticulado formado por los elementos 0 y 1, satisfaciendo $0 < 1$. Existe una estrecha relación entre los filtros primos de un reticulado distributivo y los homomorfismos sobre el reticulado $\mathbf{2}$.

Lema 5.7. *Sea L un reticulado distributivo. Si $f : L \rightarrow \mathbf{2}$ es un homomorfismo entonces*

$$f^{-1}(1) = \{x \in L : f(x) = 1\}$$

es un filtro primo. Además, si P es un filtro primo de L entonces el mapa definido

$$f(x) = \begin{cases} 1 & x \in P \\ 0 & x \notin P \end{cases}$$

es un homomorfismo.

5.1 Ejercicios

1. Encuentre todos los filtros del reticulado D_{90} . Luego determine cuales son primos.
2. Encuentre todos los filtros primos de 3×4 .
3. Sea F un filtro en el reticulado distributivo L y sea $x \in L$ tal que $x \notin F$. Pruebe que

$$G = \{a \in L : a \geq x \bigwedge f \text{ para algún } f \in F\}$$

es un filtro, y además G es el filtro más chico que contiene a F y a x (o sea, si H es un filtro que contiene a $F \cup \{x\}$ entonces H contiene a G).

4. Sea L un reticulado distributivo, y supongamos que x, y son dos elementos tales que y cubre a x . Pruebe que

$$P = \{z \in L : (z \bigvee x) \bigwedge y = y\}$$

es un filtro primo. Determine tal filtro primo en el reticulado $\mathcal{P}(\{a, b, c\})$ con $x = \{a\}$, $y = \{a, c\}$.

5. Mostrar con un contraejemplo que el Lema 5.1 no vale para reticulados no distributivos.

6 Reticulados completos y operadores clausura

En esta sección L será un reticulado cualquiera, no necesariamente distributivo como en las secciones anteriores. Diremos que L es *completo* si todo subconjunto S (aún los infinitos) poseen supremo e ínfimo. Generalizando la notación de reticulados, utilizaremos $\bigvee S$ y $\bigwedge S$ para denotar al supremo y al ínfimo de S , respectivamente. El objetivo principal de esta sección es encontrar una representación de los reticulados completos como "álgebras de conjuntos", de manera similar a lo hecho para las álgebras de Boole y los reticulados distributivos finitos. Dado que no son necesariamente distributivos, no podremos representar ambas operaciones \bigvee, \bigwedge como \cup, \cap simultáneamente.

Note que todo reticulado completo L posee necesariamente un menor elemento $0 = \bigwedge L$, y un mayor elemento, $1 = \bigvee L$. Por otro lado todo reticulado finito es completo.

Lema 6.1. Sea P un poset. Son equivalentes:

- P es un reticulado completo.
- Existe $\bigwedge S$ para todo subconjunto S de P .
- P tiene mayor elemento 1 y existe $\bigwedge S$ para todo subconjunto no vacío S de P .

Demostración. La equivalencia entre *ii* y *iii* sale observando que $\bigwedge \emptyset$ es siempre el mayor elemento del poset.

La implicación $i \Rightarrow ii$ es trivial.

Supongamos *ii*. Sea $S \subseteq P$. Sea

$$S_1 = \{x \in P : x \text{ es cota superior de } S\}.$$

Definamos $a = \bigwedge S_1$, vamos a demostrar que a es el supremo de S . Si $S = \emptyset$ entonces $S_1 = P$, y por lo tanto $\bigwedge S_1 = 0 = \bigvee \emptyset$. Supongamos ahora que $S \neq \emptyset$, y sea $z \in S$. Entonces para todo $x \in S_1$ se tiene $z \leq x$, lo que indica que $z \leq \bigwedge S_1 = a$. Luego hemos demostrado que a es cota superior de S . Por definición de S_1 se tiene que a es la menor de las cotas superiores. \square

Lema 6.2. Sea L un reticulado completo. Entonces para todo $S, T \subseteq L$ se tiene:

$$\begin{aligned}\bigvee(S \cup T) &= (\bigvee S) \bigvee \left(\bigvee T\right) \\ \bigwedge(S \cup T) &= (\bigwedge S) \bigwedge \left(\bigwedge T\right).\end{aligned}$$

La prueba del lema se deja como ejercicio.

Para la representación de los reticulados completos como “álgebras de conjuntos” necesitamos el siguiente concepto.

Definición 6.1. Sea X cualquier conjunto. Una función $C : \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ se dice un operador clausura sobre X si para todo $A, B \subseteq X$ se cumple:

1. $A \subseteq C(A)$,
2. $A \subseteq B \Rightarrow C(A) \subseteq C(B)$,
3. $C(C(A)) = C(A)$.

Sea C un operador clausura sobre X . Diremos que un subconjunto A de X es *cerrado* si $C(A) = A$. Note que el conjunto total X es cerrado, por la propiedad 1. Una propiedad importante de los operadores clausura es que la intersección de cerrados es cerrada. No ocurre necesariamente lo mismo con la unión.

Lema 6.3. La intersección de una familia arbitraria de cerrados es también un cerrado. En símbolos, si $\{A_i\}_{i \in I}$ es una familia de subconjuntos cerrados de X , y

$$B = \bigcap_{i \in I} A_i,$$

entonces $C(B) = B$.

Demostración. Por la condición 1, basta ver que $C(B) \subseteq B$. Para cada $i \in I$ se tiene que $B \subseteq A_i$, y por la condición 2 tenemos

$$C(B) \subseteq C(A_i) = A_i.$$

Luego

$$C(B) \subseteq \bigcap_{i \in I} A_i = B. \quad \square$$

\square

Notemos que un caso particular contemplado en el Lema es el caso $I = \emptyset$. En tal caso $B = X$ que por la condición 1 es claramente un cerrado.

Asociado a un operador clausura tenemos siempre un reticulado completo. En efecto, sea C un operador clausura sobre X y sea Γ_C el conjunto de los subconjuntos cerrados de X . Consideremos la estructura de poset de Γ_C dada por la relación \subseteq .

Vamos a dar ahora algunos ejemplos.

1. Sea P un poset, y sea C el operador sobre P definido

$$C(X) = \{z \in P : z \geq x, \text{ para algún } x \in X\}.$$

Es fácil verificar que C es un operador clausura. Los cerrados del operador clausura son los subconjuntos crecientes de P . Este operador clausura satisface claramente que la unión de cerrados es cerrado.

2. Sea L un reticulado y sea C el operador clausura en L definido de la siguiente manera: para cada subconjunto X del reticulado, $C(X)$ es el subreticulado más chico que contiene a X . Entonces C es un operador clausura, y los cerrados del operador C son exactamente los subreticulados de L . Claramente este operador no satisface que la unión de cerrados es cerrado

Corolario 6.4. (Del Lema 6.1) Γ_C es un reticulado completo.

Demostración. Dado que la intersección de una familia arbitraria de miembros de Γ_C está en Γ_C , tenemos que el ínfimo de S existe para todo $S \subseteq \Gamma_C$. Por el Lema 6.1 tenemos que Γ_C es un reticulado completo, y la operación \bigwedge coincide con el operador \cap . \square

Si nos fijamos en la prueba del Lema 6.1 podremos determinar inmediatamente como está definida la operación \bigvee en Γ_C . En efecto, sea $S = \{A_i\}_{i \in I}$ una familia de cerrados. Entonces

$$\bigvee S = \bigcap S_1,$$

donde

$$S_1 = \{B \in \Gamma_C : A_i \subseteq B \text{ para todo } i \in I\}.$$

Claramente $A_i \subseteq \bigcap S_1$, lo que implica

$$\bigcup_{i \in I} A_i \subseteq \bigcap S_1.$$

Como $\cap S_1$ es cerrado tenemos

$$C(\cup_{i \in I} A_i) \subseteq \cap S_1.$$

Por otro lado, $C(\cup_{i \in I} A_i)$ es cerrado y es cota superior de S , lo que indica que

$$\cap S_1 \subseteq C(\cup_{i \in I} A_i),$$

pues $\cap S_1$ es el supremo de S . Concluimos que para toda familia de cerrados $\{A_i\}_{i \in I}$ se tiene:

$$\bigvee \{A_i\}_{i \in I} = C(\cup_{i \in I} A_i).$$

Hemos probado entonces el siguiente corolario:

Corolario 6.5. *Sea X un conjunto y sea C un operador clausura sobre X . Definamos para $S \subseteq \Gamma_C$:*

$$\bigvee S = C(\cup S).$$

Entonces $(\Gamma_C, \cap, \bigvee)$ es un reticulado completo.

6.1 Ejercicios

1. Sea P un poset, y sea C el operador sobre P definido

$$C(X) = \{z \in P : z \geq x, \text{ para algún } x \in X\}.$$

Pruebe que C es un operador clausura y que los cerrados de C son exactamente los subconjuntos crecientes.

2. Sea L un reticulado y sea C el operador clausura en L definido de la siguiente manera: para cada subconjunto X del reticulado, $C(X)$ es el subreticulado más chico que contiene a X . Pruebe que C es un operador clausura, y los cerrados del operador C son exactamente los subreticulados de L .