Semana 14: Álgebras de Boole

1. Retículas modulares y distributivas

Las retículas distributivas y modulares son aquellas que satisfacen las leyes distributiva y modular respectivamente. Antes de formularlas, observemos algunas propiedades.

Lema 14.1. *Para cualesquiera a, b y c elementos en una retícula se cumplen:*

1. $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$.
2. $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$.
3. $c \leq a$ *implica* $a \wedge (b \vee c) \geq (a \wedge b) \vee c$.
4. $a \leq c$ *implicas* $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.

La prueba del lema anterior, es relativamente sencilla y a aparecido ya como un ejercicio en la semana pasada.

Definición 14.1. Sea L una retícula. Entonces:

1. L se dice *distributiva* si cumple la siguiente ley distributiva: Para cualesquiera a, b y c en la retícula
$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$
2. L se dice *modular* si cumple la siguiente ley modular: Para cualesquiera a, b y c en la retícula, si $c \leq a$, entonces
$$a \wedge (b \vee c) = (a \wedge b) \vee c.$$

Es importante notar que, según el lema 14.1, cualquier retícula es «*casi*» distributiva y «*casi*» modular. Esto quiere decir que sólo una desigualdad basta para poder garantizar las leyes distributiva y modular enunciadas.

Lema 14.2. *Sea L una retícula. Entonces son equivalentes:*

1. *Para a, b y c en la retícula, se cumple* $a \wedge (b \vee c) = (a \wedge b) \vee (a \vee c)$.
2. *Para a, b y c en la retícula, se cumple* $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

Demostración. Supongamos que 1 se cumple. Entonces

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

Por lo que 1 implica 2. El hecho que 2 implique 1 resulta por dualidad. ■

El lema 14.2 nos aclara que la aparente necesidad de tener dos leyes distributivas, como naturalmente podríamos pensar, es una mera ilusión. Basta con que una de las operaciones de retícula distribuya sobre la otra para garantizar cualquiera de las dos versiones.

Teorema 14.3. *Cada retícula distributiva es modular.*

Demostración. Basta notar que si $a \geq c$, el lema de la conexión implica que $a \wedge c = c$ y por ser L distributiva,

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

Lo anterior muestra precisamente que la ley modular vale en toda retícula distributiva. ■

Ejemplo. Recordemos que la retícula de los naturales ordenados por divisibilidad, tiene como operaciones al mínimo común múltiplo y al máximo común divisor. En ese contexto, es fácil mostrar que $d_1 = (m, [n, l])$ divide a $d_2 = [(m, n), (m.n)]$. En este conjunto parcialmente ordenado, debemos entonces tener

$$m \vee (n \wedge l) \preceq (m \wedge n) \vee (m \wedge l).$$

Según el lema 14.1, lo anterior es suficiente para garantizar que la retícula resulta distributiva (y de acuerdo al teorema 14.3, también modular).

M_5 N_5

(a) Retícula no distributiva pero modular. (b) Retícula no distributiva y no modular.

Figura 1: Ejemplos de distributividad y modularidad.

Ejemplo. Considérese $(\mathbb{Z}, +)$ como un grupo conmutativo. Si tomamos $\mathrm{Sub}(\mathbb{Z})$ como el conjunto de todos los subgrupos de los enteros, ordenado por contención, podemos probar que ésta es una retícula y que sus operaciones están dadas por $H \vee K = \langle H \cup K \rangle$ y $H \wedge K = H \cap K$ donde $\langle H \cup K \rangle$ es el subgrupo generado por la unión. Además, usando la función esta retícula es isomorfa al dual de la retícula formada por los naturales ordenados por divisibilidad y en consecuencia debe ser también distributiva.

Mucho del estudio de una estructura algebraica consiste en realizar clasificaciones. Hemos introducido ya dos clasificaciones de retículas que son importantes tanto en la teoría como en ciertas aplicaciones y esto nos demanda introducir algunos métodos que nos permitan identificarlas. Pondremos un especial interés en aquellas identificaciones establecidas por las estabilidad de las retículas distributivas y modulares bajo subretículas, productos e imágenes de homomorfismos. Vamos a establecer esto último con precisión.

Teorema 14.4. *Cualquier subretícula de una retícula modular, es modular. De la misma forma, cualquier subretícula de una retícula distributiva es distributiva.*

Demostración. Sea $L = (A, \vee, \wedge)$ una retícula y sea $K \subseteq A$ una subretícula de L. Si a, b y c son elementos de K de forma que $a \geq c$, al ser K un subconjunto L y L ser modular, tenemos $a \wedge (b \vee c) = (a \wedge b) \vee c$. Ahora, como K es cerrado para las operaciones de la retícula lo anterior implica que K es modular. Supongamos ahora que L retícula es distributiva. Entonces, para elementos a, b y c en K, debemos tener $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ pues K es un subconjunto de L y L ser distributiva. Ahora, como K es cerrado para las operaciones de la retícula lo anterior implica que K es distributiva. ∎

Teorema 14.5. *Sean L y K retículas. Si L y K son distributivas, entonces $L \times K$ es distributiva. De igual forma, si son modulares, entonces $L \times K$ es modular.*

Demostración. Sean $\vee$, $\wedge$ y $\leq$ la disyunción, conjunción y el orden de L y sean también $\curlyvee$, $\curlywedge$ y $\preceq$ la disyunción, la conjunción y el orden de K. Supongamos además que $\sqcup$, $\sqcap$ y $\sqsubset$ son la disyunción, conjunción y el orden de la retícula $L \times K$. Si suponemos que L y K son modulares, y tomamos (a_1, a_2), (b_1, b_2) y (c_1, c_2) en $L \times K$ de forma que $(c_1, c_2) \sqsubset (a_1, a_2)$ entonces, por definición, $c_1 \leq a_1$ y $c_2 \preceq a_2$ por lo que

$$a_1 \wedge (b_1 \vee c_1) = (a_1 \wedge b_1) \vee c_1$$

y de igual forma

$$a_2 \curlywedge (b_2 \curlyvee c_2) = (a_2 \curlywedge b_2) \curlyvee c_2.$$

Lo anterior implica que

$$\begin{aligned}
(a_1, a_2) \sqcap ((b_1, b_2) \sqcup (c_1, c_3)) &= (a_1 \wedge (b_1 \vee c_1), a_2 \curlywedge (b_2 \curlyvee c_3)) \\
&= ((a_1 \wedge b_1) \vee c_1, (a_2 \curlywedge b_2) \curlyvee c_3) \\
&= ((a_1, a_2) \sqcap (b_1, b_2)) \sqcup (c_1, c_3).
\end{aligned}$$

La anterior igualdad, muestra que $L \times K$ es modular. El resultado para retículas distributivas se deja como ejercicio (14.1). ∎

Teorema 14.6. *Sean L y K retículas de forma que $K \hookrightarrow L$. Si L es distributiva, entonces K es distributiva. De igual forma, si L es modular entonces K es modular.*

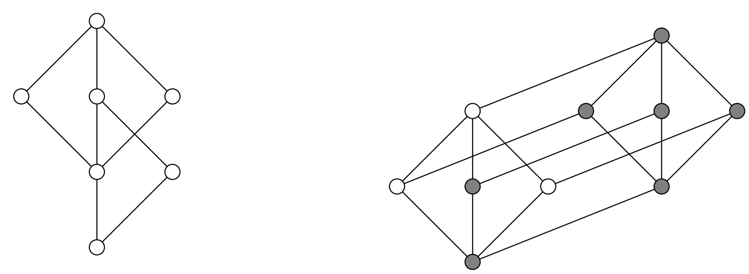
Demostración. Supongamos que f es la inmersión de retículas que sumerge K en L. En ese caso, debemos tener que $\mathrm{im}(f)$ es una subretícula de L y además las retículas $\mathrm{im}(f)$ y K son isomorfas. En ese caso, el resultado sigue del teorema 14.4. ■

El teorema 14.4 muestra que la modularidad y distributividad en retículas son estables bajo subretículas, el teorema 14.5 hace lo propio para productos y el teorema 14.6 lo hace para imágenes de homomorfismos. Resumimos estos tres resultados en la siguiente proposición.

Proposición 14.7. *Si una retícula L es isomorfa a una subretícula de un producto entre retículas distributivas, entonces L es distributiva. De igual forma, si las retículas son modulares, entonces L es modular.*

La proposición anterior constituye un método de encontrar retículas modulares o distributivas a través de extenderlas a una retícula que conozcamos es modular o distributiva.

Ejemplo. No es difícil convencernos que los conjuntos linealmente ordenados son retículas modulares y así **2** es modular. En la figura 2a aparece una retícula, L, la cual es isomorfa a la subretícula indicada en gris en la figura 2b. De acuerdo a la proposición anterior, la retícula L debe ser modular, al poderse sumergir en el producto de las retículas modulares M_5 y **2**.



(a) La retícula L resulta modular al ser isomorfa a una subretícula de $M_5 \times \mathbf{2}$.

(b) $M_5 \times \mathbf{2}$.

Figura 2: Ejemplos de distributividad y modularidad.

El método expuesto en la proposición 14.7 es positivo en el sentido de ser capaz de encontrar cuales retículas son modulares o distributivas. Sin embargo, podemos también construir un método que nos permita encontrar cuáles retículas no son modulares o distributivas. Para conseguirlo basta usar el teorema 14.4 con contraposición para concluir la siguiente proposición.

Proposición 14.8. *Sean L y K son retículas de forma que $L \hookrightarrow K$. Si L no es distributiva, entonces K no es distributiva. De la misma forma, si L no es modular, entonces K no es modular.*

Para que la proposición tenga utilidad, debemos conocer retículas no distributivas y no modulares. En la figura 1 podemos encontrar estos ejemplos. En la práctica, para mostrar que una retícula no es distributiva será suficiente sumergir M_5 o N_5 como una subretícula. Por otro lado, si podemos sumergir N_5 como subretícula, habremos mostrado que ésta no es modular.

Ejemplo. Considerando los conjuntos que aparecen en la figura 3. Para el la retícula en la figura 3a, existe como una subretícula, un conjunto es isomorfo (como retícula) a M_5, con lo que podemos concluir que esta retícula no es distributiva. En la retícula de la figura 3b, aparece como subretícula un subconjunto que es isomorfo a N_5, con lo que podemos concluir que la retícula es no modular.

(a) Una copia de M_5 (en gris) como subretícula.

(b) Una copia de N_5 (en gris) aparece como subretícula.

Figura 3: Ejemplos de inmersiones de M_5 y N_5.

Habrá que tener cuidado usando estos resultados. Es necesario que la inmersión sea entre retículas. Esto quiere decir que debemos encontrar un subconjunto que sea una subretícula y que sea isomorfo como retícula a M_5 o N_5. Considérese, por ejemplo, la figura **??**. En ésta aparece de la retícula N_5 la cual se puede sumergir como conjunto parcialmente ordenado en $2^{[3]}$ y esto nos puede llevar a la conclusión errónea que N_5 es una retícula distributiva. El problema radica en que N_5 no está presente como subretícula en $2^{[3]}$ sólo como subconjunto y en esos casos, los resultados anteriores no son necesariamente ciertos.

2. Álgebras de Boole

En esta sección definiremos una estructura de mucha impostancia en diversas areas de la matemática. A pesar de que pudimos comenzar presentando su definición de manera inmediata, se gana mucho desarrollando paulatinamente los conceptos y la teoría asociados. De esta manera, puede parecer justificada la siguiente definición.

Definición 14.2. Sea L una retícula. Se dice que L es *un álgebra de Boole* si cumple con las siguientes propiedades:

- L es distributiva.
- L tiene elementos 0_L y 1_L.
- Para cada elemento a en la retícula, existe un único elemento $\neg a$, llamado *el negado de a*, que satisface las siguientes igualdades:
  - $a \vee \neg a = 1_L$.
  - $a \wedge \neg a = 0_L$.

Lo primero que hay notar de la definición es cómo se obtienen los negados de los elementos 0_L y 1_L. Sabemos que $0_L \leq 1_L$ lo cual indica que $0_L \vee 1_L = 1_L$ y al mismo tiempo $0_L \wedge 1_L = 0_L$. Como los negados son únicos, lo anterior nos permite concluir de inmediato que $\neg 0_L = 1_L$ y $\neg 1_L = 0_L$. La conmutatividad de ambas operaciones, permite observar que las identidades que definen al negado, garantizan también que $\neg(\neg a) = a$ para cualquier elemento del álgebra. Resumimos esto en el siguiente lema.

Lema 14.9. *En un álgebra de Boole, se satisfacen*

- $\neg 0_L = 1_L$.
- $\neg 1_L = 0_L$.
- $\neg(\neg a) = a$.

Bajo la óptica adecuada, el lema anterior parece describir algunas propiedades conocidas de la lógica proposicional. No es una coincidencia. Las álgebras de Boole sirven con un modelo adecuado para describir este tipo de sistemas lógicos. De hecho, las operaciones asociadas a la retícula base satisfacen las conocidas leyes de DeMorgan. La prueba de este hecho se deja como ejercicio (14.4).

Lema 14.10 (Leyes de De Morgan). *Para elementos a y b en un álgebra de Boole se cumplen:*

- $\neg(a \vee b) = (\neg a) \wedge (\neg b)$.
- $\neg(a \wedge b) = (\neg a) \vee (\neg b)$.

Lema 14.11. *Para elementos a y b en un álgebra de Boole, son equivalentes:*

- $a \leq b$.
- $(\neg a) \vee b = 1_L$.
- $a \wedge (\neg b) = 0_L$.

Demostración. Observemos primero que 2 y 3 son equivalentes según los lemas anteriores. Para mostrar que de 1 sigue 2, debemos recordar que $a \leq b$ si y sólo si $a \wedge b = a$ y en ese caso, el lema anterior implica $\neg a = (\neg a) \vee (\neg b)$. Ahora tenemos

$$\begin{aligned}
(\neg a) \vee b &= [(\neg a) \vee (\neg b)] \vee b \\
&= (\neg a) \vee [(\neg b) \vee b] \\
&= (\neg a) \vee 1_L \\
&= 1_B.
\end{aligned}$$

Con esta igualdad probamos que 1 implica 2. Supongamos ahora el enunciado en 2, i.e., $(\neg a) \vee b = 1_L$. Entonces,

$$\begin{aligned}
a \wedge b &= 0_l \vee (a \wedge b) \\
&= [a \wedge (\neg a)] \vee (a \wedge b) \\
&= a \wedge [(\neg a) \vee b] \\
&= a \wedge 1_L \\
&= a.
\end{aligned}$$

Esta igualdad implica por definición que $a \leq b$, luego 2 implica 1. ∎

Ejemplo. Sabemos que la retícula 2^A es distributiva. Además de tener $0_{2^A} = \varnothing$ y $1_{2^A} = A$. No es difícil verficar que tomando $\neg S = A \backslash S$ cumple con el apartado de existencia y unicidad que se pide para la negación. De esta forma, podemos concluir que 2^A es un álgebra de Boole. Veremos más adelante que éste es el ejemplo arquetípico de álgebra de Boole y es costumbre denominarlo *el álgebra del conjunto potencia de A*.

Como en el caso de retículas, debemos notar que la negación en las álgebras booleanas es capaz de definir una operación, además de tener elementos 0_L y 1_L que funcionan como constantes. En algunas ocasiones, es necesario dejar explícita la estructura y cuando esto sea necesario expresaremos un álgebra de Boole como $L = (A, 0_L, 1_L, \neg, \vee, \wedge)$, lo cual establece sin ambigüedad la estructura operativa de la retícula.

Definición 14.3. Sea B un álgebra de Boole. Un subconjunto M del conjunto base se dice *una subálgebra de Boole de B*, si cumple las siguientes propiedades:

- M es una subretícula de B.
- $0_B \in M$ y $1_B \in M$.
- Para cada $a \in M$, se tiene $\neg a \in M$.

En otras palabras, una subálgebra es un subconjunto que respeta las operaciones asociadas al álgebra. Esto nos permite observar sin mucho problema que cualquier subálgebra de Boole es por cuenta propia un álgebra.

Definición 14.4. Sean $L = (A, 0_L, 1_L, \neg, \vee, \wedge)$ y $K = (B, 0_K, 1_K, \sim, \curlyvee, \curlywedge)$ álgebras de Boole. Una función $f\colon A \to B$ se dice *un homomorfismo de Boole* si cumple las siguientes propiedades:

- f es un homomorfismo entre retículas.
- $f(0_L) = 0_K$ y $f(1_L) = 1_K$.
- $f(\neg a) = \sim f(a)$.

Diremos también que f es *inmersión de Boole* si f es inyectiva y *un isomorfismo de Boole* si f es biyectiva. Si existe una inmersión de Boole entre las álgebras L y K, diremos que *L se puede sumergir en K como álgebras de Boole* y escribiremos $L \hookrightarrow K$ cuando no exista ambigüedad. De la misma manera, si existe un isomorfismo entre L y K diremos que *L y K son álgebras de Boole isomorfas* y escribiremos $L \cong K$ cuando no exista abigüedad.

El concepto de homomorfismo de Boole, expande la definición del homomorfismo de retículas agregando la estructura asociada a un álgebra de Boole. No debe sorprender que en realidad ya hemos visto varios casos aunque no se han mencionado como tal.

Ejemplo. Hemos mostrado ya que las retículas $\mathbf{2}^n$ y $2^{[n]}$ son isomorfas. Basta notar que $\mathbf{2}^n$ tiene como constantes

$$0_{\mathbf{2}^n} = (1, 1, \ldots, 1) \quad \text{y} \quad 1_{\mathbf{2}^n} = (2, 2, \ldots, 2),$$

y como negación

$$\neg(a_1, a_2, \cdots, a_n) = (\neg a_1, \neg a_2, \cdots, \neg a_n).$$

Bajo esta estructura, es posible convencernos que la misma función que consigue mostrar a las retículas son isomorfas es suficiente también para mostrar que son isomorfas como álgebras de Boole.

Ejercicios

Ejercicio 14.1. Sean L y K retículas. Si L y K son distributivas, demuestra que $L \times K$ es distributiva.

Ejercicio 14.2. Sea L un álgebra de Boole. Demuestra que si $a \vee b = 1_L$ y $a \wedge b = 0_L$, entonces $b = \neg a$.

Ejercicio 14.3. Muestra que si en un álgebra de Boole $0_L = 1_L$ entonces L es la retícula trivial.

Ejercicio 14.4. Sea L un álgebra de Boole. Demuestra las siguiente igualdades

- $\neg(a \vee b) = \neg a \wedge \neg b$
- $\neg(a \wedge b) = \neg a \vee \neg b$.

Ejercicio 14.5. Si B y C son álgebras de Boole, demuestra que $B \times C$ es también un álgebra de Boole.

Ejercicio 14.6. Una anillo $(R, +\cdot)$ se dice *de Boole*, si para cada elemento en éste, $x^2 = x$.

1. Demuestra que en un anillo de Boole, $1_R + 1_R = 0_R$. Sugerencia: Considera $(1+1)^2$.
2. Demuestra que R es conmutativo. Sugerencia: Considera $(x+y)^2$.
3. En un anillo de Boole R se definen las operaciones $x \wedge y = x \cdot y$, $x \vee y = x + y + x \cdot y$ y $\neg x = 1_R + x$. Demuestra que con estas operaciones R es un álgebra de Boole.
4. Para un álgebra de Boole B se definen las operaciones $a \cdot b = a \wedge b$ y $a + b = (\neg a \wedge b) \vee (a \wedge \neg b)$. Demuestra que con estas operaciones B es un anillo de Boole.

Ejercicio 14.7. Demuestra que la asociación $b \mapsto \neg b$ es un isomorfismo entre B y su dual. Sugerencia: Recuerda que en el fondo B es un conjunto parcialmente ordenado.

Para entregar: Ejercicio 14.1

Referencias

[DP02] Davey, Brian A. y Priestley, Hilary A.: *Introduction to lattices and order*. Cambridge University Press, 2002.

[Gri97] Grimaldi, Ralph P.: *Matemáticas discreta y combinatoria*. Addison Wesley Iberoamericana, 3ª edición, 1997.

[Gó07] Gómez Laveaga, Carmen: *Introducción a la teoría intuitiva de conjuntos*. Las Prensas de Ciencias, 2007.

Considerar notas el texto precedente es producto de la imaginación febril de autor. El único propósito al que sirven es dar una interpretación personal de algunos textos que han sido usados para preparar el curso de «Matemáticas discretas» impartido en la carrera de Matemáticas Aplicadas y Computación de la FES Acatlán. Es muy probable que el presente texto esté lleno de errores gramaticales, imprecisiones técnicas y sea sujeto a cambios constantes.