De la teoría del orden a la teoría de retículas

Matemáticas Discretas
Matemáticas Aplicadas y Computación 2016-I

1. Elementos de teoría del orden

Hasta ahora hemos discutido la estructura de un conjunto parcialmente ordenado, presentando sus definiciones elementales, su representación por diagramas, algunas caracterizaciones importantes. Sin embargo no hemos entregado en absoluto resultados, esto se debe a que no hemos desarrollado una teoría correspondiente al orden. Precisaremos ahora de introducir más conceptos y presentar algunos resultados simples pero profundos de la teoría del orden, esto con el objetivo de transitar de la definición de orden a la de retícula de una manera muy peculiar. Desde este punto nos sumergiremos en la teoría de retículas ahora ya desde el punto de vista algebraico sin abandonar los resultados y estrategias usadas en la teoría del orden, obteniendo así con un proceso constructivo la teoría que detonará en las algebras booleanas. Mucho de lo aquí expuesto se puede encontrar en [DP02].

1.1. Construcción y deconstrucción del orden

Definición 1.1 (dualidad)**.** Sea A un conjunto parcialmente ordenado. El conjunto dual del conjunto A, en símbolos A^{∂}, es el conjunto parcialmente ordenado que como conjunto base tiene de nueva cuenta a A y su orden está dado de la siguiente manera: $x \leq y$ en A^{∂} si y sólo si $y \leq x$ en A.

Bajo esta definición, podemos aceptar un hecho interesante de dualidad en la teoría del orden, a decir que cada enunciado Φ de conjuntos parcialmente ordenados tendrá *un enunciado dual*, Φ^{∂}, construido de la siguiente manera:

- Cada ocurrencia de $\leq$ en Φ será sustituida por $\geq$ en Φ^{∂}.
- Cada ocurrencia de $\geq$ en Φ será sustituida por $\leq$ en Φ^{∂}.

Principio de dualidad (para conjuntos parcialmente ordenados)**.** Si un enunciado Φ sobre conjuntos parcialmente ordenados es válido para todo conjunto parcialmente ordenado, entonces el enunciado dual de Φ es también válido para cualquier conjunto parcialmente ordenado.

Una vez que hallamos establecido algunos resultados y otras definiciones, tendremos la oportunidad de jugar con el principio de dualidad, por el momento debemos solamente aceptarlo (aunque desde el punto de vista lógico, del cual carecemos de experiencia, es un resultado inmediato).

Definición 1.2. Sea A un conjuntos parcialmente ordenado. Si un elemento $t \in A$ satisface para todo $a \in A$, $a \leq t$, entonces a t lo llamaremos *una cima* de A. De manera análoga, si un elemento $b \in A$ satisface para todo $a \in A$, $b \leq a$, entonces a b lo llamaremos *un fondo* de A.

Proposición 1.1. *Sea A un conjunto parcialmente ordenado. Si A tiene una cima, entonces la cima es única.*

Demostración. Supongamos que los elementos s y t son ambos cimas de A, entonces debemos tener que $t \leq s$ pues s es una cima de A; también debemos tener que $s \leq t$ pues t es una cima de A. Por anti-simetría del orden, $s = t$. $\square$

La proposición anterior contiene algunas definiciones que no se desarrollan, sin embargo no resultará difícil desarmarla para convencernos que la proposición dual es aquella que afirma la existencia de un fondo implica su unicidad. Con esto podemos tener la certeza que los fondos y las cimas son únicas, lo que nos faculta a denotarlos de manera única. En caso de un conjunto parcialmente ordenado tenga cima, a ésta la denotaremos por $\top$, mientras que si posee fondo, a éste lo denotaremos por $\perp$.

Ejemplo. Para el conjunto parcialmente ordenado $(\mathcal{P}(A), \subset)$, la cima será el elemento $\top = A$ mientras que el fondo será el elemento $\perp = \varnothing$.

Podemos encontrarnos con conjuntos parcialmente ordenados que no tiene un elemento que sea una cima del conjunto. Considérese a manera de ejemplo los conjuntos de las cadenas binarias o de las funciones. Esta situación puede ser remediada, añadiendo un elemento al conjunto A e imponiendo un nuevo orden a base del anterior.

Definición 1.3. Sea A un conjunto parcialmente ordenado. El conjunto parcialmente ordenado llamado *el alzamiento de A*, estará definido por la pareja $A_\perp = A \cup \{*\}$, donde $* \notin A$, y el orden parcial en $A_\perp$ definido de la siguiente manera de la siguiente manera: tendremos $x \leq y$ en $A_\perp$ si y sólo si $x = *$ o $x \leq y$ en A.

Presentamos ahora un par de construcciones que nos servirán en lo inmediato para construir y dar conjuntos parcialmente ordenados a través de información mínima. El primero se trata de proveer un orden para un conjunto cualquier, para esto procedemos como sigue: si A es un conjunto, la relación de igualdad resulta en un orden. A esta relación se le conoce como el orden discreto. Denotemos $\bar{A}$ como el conjunto parcialmente ordenado con el orden discreto, entonces podríamos sencillamente tomar $\bar{A}_\perp$ para notar que cualquier conjunto es capaz de generar un conjunto parcialmente ordenado con fondo.

Podemos construir otro conjunto parcialmente ordenado a partir de un número natural cualquiera y obtener una cadena o conjunto totalmente ordenado a nuestra disposición. Sea n un número natural, denotamos por $\mathbf{n}$ al conjunto parcialmente ordenado $\{1, \ldots, n\}, \leq$ con orden dado por

$$1 < 2 < \ldots < n.$$

Estas dos construcciones nos permitirán establecer diversos resultados.

Definiremos ahora un concepto complementario al de máximo y mínimo. Sabemos al igual que las cimas y los fondos, que son únicos, sin embargo en un orden parcial podríamos encontrar elementos que son de alguna manera los "más grandes" comparativamente.

Definición 1.4. Sea A un conjunto parcialmente ordenado y sea $B \subset A$. Un elemento $b \in B$ se dice *maximal de* B si $b \leq x$ y $x \in B$ implica que $b = x$. De manera análoga, un elemento $b \in B$ se dice *minimal de* B si $b \geq x$ y $x \in B$ implica que $b = x$.

Quizá es importante mostrar la diferencia entre un elemento máximo y un maximal (lo cual por el principio de dualidad también ilustraría la diferencia entre mínimo y minimal).

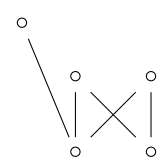

Figura 1: Un conjunto parcialmente ordenado con tres maximales.

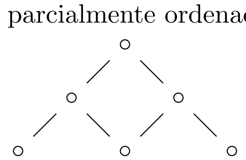

Figura 2: Un conjunto parcialmente ordenado con máximo.

1.2. Operaciones sobre conjuntos parcialmente ordenados

Al menos se pueden dos tipos diferentes de agregación entre dos conjuntos con un orden establecido. El primero resulta ser la unión disjunta y el segundo la suma directa.

Definición 1.5. Suponga que A y B son dos conjuntos parcialmente ordenados de forma que $A \cap B = \varnothing$. *La unión disjunta de* A *y* B[1] será el conjunto parcialmente ordenado $A \dot{\cup} B$ donde el orden siguiente se define como sigue: $x \leq y$ en

[1]Podemos pensar que pasaría en caso de que dos conjuntos no sean disjuntos. Ese caso no significa ningún problema, podemos tomar simplemente los conjuntos $A \times \{0\}$ y $B \times \{1\}$ notando que estos son disjuntos sin importar de que conjuntos A y B se trate, por lo que la definición no estaría restringida a un caso particular.

$A \cup B$ si y sólo si x y y son elementos de A y $x \leq y$ en A o x y y son elementos de B y $x \leq y$ en B.

Un diagrama para la unión disjunta de dos conjuntos parcialmente ordenados sería simplemente poner lado a lado de manera *disjunta* los diagramas de los conjuntos involucrados. Quizá por esto sería interesante no sumarlos de manera disjunta sino crear un orden que vincule los elementos que comparten.

Definición 1.6. Supongamos A y B son dos conjuntos parcialmente ordenados. La suma lineal de los conjuntos, $A \oplus B$, se define tomando la siguiente relación en $A \cup B$: $x \leq y$ en $A \oplus B$ si y sólo si:

- x y y son elementos de A y $x \leq y$ en A.
- x y y son elementos de B y $x \leq y$ en B.
- x es elemento de A y y es elemento de B.

Podemos construir el diagrama de la suma de dos conjuntos parcialmente ordenados simplemente poniendo los diagramas del primero sobre el segundo (¡notemos que la suma no es conmutativa!) y uniendo cada elemento maximal del primero con cada elemento minimal del segundo.

Figura 3: Un par de conjuntos parcialmente ordenados y disjuntos.

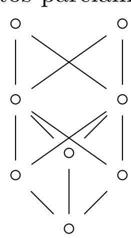

Figura 4: La suma lineal de los conjuntos A y B

El caso del alzamiento de un conjunto ¡resulta en un caso particular de la suma lineal! Para notar esto, tomemos el conjunto $\{*\}$ de forma tal que $* \notin A$. Podemos dotar a $\{*\}$ del orden discreto como hemos antes para considerarlo un conjunto parcialmente ordenado, en ese caso $A_{\perp} = \{*\} \oplus A$.

Estamos viendo que las operaciones de conjuntos resultan en las operaciones base para determinar nuevos conjuntos parcialmente ordenados.

De hecho, se puede definir la unión disjunta (desde el punto de vista de conjuntos) de A y B simplemente como el conjunto

$$A \dot{\cup} B = A \times \{0\} \cup B \times \{1\}.$$

Definición 1.7 (Orden cartesiano)**.** Sean A y B conjuntos parcialmente ordenados. El producto de A con B es el conjunto parcialmente ordenado que se define con la siguiente relación en $A \times B$: $(x, y) \leq (z, w)$ si y sólo si $x \leq z$ en A y $y \leq w$ en B. A este conjunto se le acostumbra denotar por $A \times B$ abusando de la notación y entendiendo que es un conjunto parcialmente ordenado.

Definición 1.8 (Orden lexicográfico)**.** Sean A y B conjuntos parcialmente ordenados. El producto de A con B es el conjunto parcialmente ordenado $A \otimes B$ se define tomando la siguiente relación en $A \times B$: $(x, y) \leq (z, w)$ si y sólo si $x < z$ en A o $x = y$ y $y \leq w$ en B.

Definición 1.9. Sea A un conjunto parcialmente ordenado y sea S un subconjunto de A. Se dice que:

- El conjunto S es *decreciente*, si $x \in S$ $y \in A$ y $y \leq x$ implica $y \in S$.
- El conjunto S es *creciente*, si $x \in S$ $y \in A$ y $x \leq y$ implica $y \in S$.

Vamos a intentar identificar conjuntos decrecientes dados, para esto propondremos un conjunto decreciente que nos permita obtener el más pequeño de ellos.

Definición 1.10. Sea A un conjuntos parcialmente ordenado y sea $S \subset A$. Definimos

$$\downarrow S = \{y \in A \mid \text{existe } x \in S \text{ tal que } y \leq x\}.$$

El conjunto $\uparrow S$ se define por dualidad. Además, si el subconjunto S es unitario, podemos tener un caso particular al cual denotaremos de la siguiente manera $\downarrow x = \downarrow \{x\}$. En otras palabras

$$\downarrow x = \{y \in A \mid y \leq x\}.$$

Introduzcamos ahora algo más de notación para dar la última construcción que presentaremos de conjuntos parcialmente ordenados. Denotemos por $\mathcal{O}(A)$ el conjunto de todos los subconjuntos decrecientes del conjunto parcialmente ordenado A, entonces la contención define un orden parcial en $\mathcal{O}(A)$. Como es costumbre abusaremos de la notación y diremos que $\mathcal{O}(A)$ es un conjunto parcialmente ordenado.

Proponemos ahora un lema que conecta las ideas de order y conjuntos decrecientes mostrando que son elementalmente lo mismo.

Lema 1.2. *Sea A un conjunto parcialmente ordenado. Entonces, son equivalentes:*

1. $x \leq y$.
2. $\downarrow x \subset \downarrow y$.
3. *Para cualquier conjunto decreciente S, si $y \in S$, entonces $x \in S$.*

Demostración. Probaremos primero que 1) implica 2). Supongamos entonces que $x \leq y$; continuemos tomando $s \in \downarrow x$, en ese caso $s \leq x$ y por transitividad del orden $s \leq y$, por lo tanto $s \in \downarrow y$. Entonces $\downarrow x \subset \downarrow y$.

Supongamos ahora que $\downarrow x \subset \downarrow y$. Tomemos entonces S como un conjunto decreciente con $y \in S$. Como $\downarrow y$ es el menor conjunto decreciente que contiene al conjunto y y $y \subset S$, debemos tener que $\downarrow y \subset S$. En ese caso, debemos igualmente tener que $\downarrow x \subset S$ por ser un subconjunto del conjunto decreciente de y.

Supongamos ahora que para cualquier conjunto S decreciente si $y \in S$ entonces $x \in S$. En particular esto debe ser cierto para el conjunto $\downarrow y$ y como $y \in \downarrow y$, entonces $x \in \downarrow y$ y por definición debemos tener que $x \leq y$ como se quería. Con esto, todos los enunciados son equivalentes. $\square$

Terminamos esta sección, y nuestra discusión general de la teoría del orden, mostrando uno de los conceptos básicos en cualquier teoría matemática para nuestra teoría: funciones entre conjuntos parcialmente ordenados.

Definición 1.11. Sean A y B conjuntos parcialmente ordenados. Una función $\phi\colon A \to B$ se dice:

- *Monótona*, si $x \leq y$ implica que $\phi(x) \leq \phi(y)$.
- *Inmersión de orden*, cuando $x \leq y$ si y sólo si $\phi(x) \leq \phi(y)$.
- *Isomorfismo de orden*, cuando ϕ es biyectiva y una inmersión de orden.

Cuando para conjuntos parcialmente ordenados A y B exista entre ellos un isomorfismo, diremos que son *isomorfos*. Este hecho lo denotaremos por

$$A \cong B.$$

Si existiera una inmersión entre los conjuntos parcialmente ordenados, escribiremos este hecho por

$$A \hookrightarrow B.$$

Tenemos varios ejemplos en abstracto de estas funciones, por ejemplo es de notarse que la composición de funciones monótonas es de nueva cuenta monótona. También, si tenemos el caso que $A \hookrightarrow B$ a través de la función ϕ, entonces $\mathrm{im}(\phi) \cong A$ (esto último justifica el uso del terminó inmersión), para probar esto es determinante notar que ϕ debe ser inyectivo pues $\phi(x) = \phi(y)$ sucede si y sólo si $\phi(x) \leq \phi(y)$ y $\phi(y) \leq \phi(x)$ lo que también sucede si y sólo si $x \leq y$ y $y \leq x$ que la vez tenemos si y sólo si $x = y$, por lo que debemos tener una función inyectiva. De hecho las inyecciones que preservan alguna estructura son muchas veces llamadas inmersiones (como en el caso de la geometría diferencial).

Con el simple objeto de ilustrar el concepto anterior, podemos jugar un poco con el concepto usando el hecho que un conjunto parcialmente ordenado puede ser *inmerso* en $\mathcal{O}(A)$, esto a través de la función

$$x \mapsto \downarrow x.$$

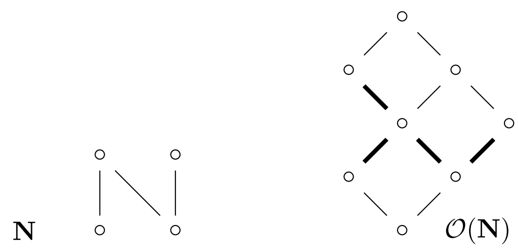

Figura 5: Un ejemplo del conjunto parcialmente ordenado $\mathcal{O}$.

Esta última afirmación es interesante de ilustrar, nótese que el conjunto $\mathbf{N}$ aparece en $\mathcal{O}(\mathbf{N})$ ilustrado bajo las lineas más oscuras en la figura 5.

Existen algunos ejemplos de isomorfismos de algunas construcciones que ya hemos visto. Por ejemplo si $\mathbf{n}$ es la cadena con n elementos, $\mathcal{O}(A) = \{\downarrow x \mid x \in A\} \cup \{\varnothing\}$. Esto quiere decir que $\mathcal{O}(A)$ es una cadena con $n+1$ elementos. En otras palabras

$$\mathcal{O}(A) \cong \mathbf{n} + \mathbf{1}.$$

De igual forma no es difícil ver que la construcción del alzamiento de un conjunto resulta simplemente sumar linealmente la cadena de tamaño 1 con el conjunto parcialmente ordenado en cuestión. Esto es

$$A_{\perp} \cong 1 \oplus A.$$

Por último, y a manera de curiosidad, proponemos un resultado interesante de dualidad acerca del conjunto $\mathcal{O}(A)$, este se puede formular de manera muy sencilla como

$$\mathcal{O}(A)^{\partial} \cong \mathcal{O}(A^{\partial}).$$

Ejercicios

Ejercicio 1.1. Sea A un conjunto parcialmente ordenado con order $\leq$. Demuestra que la relación $<$ asociada a $\leq$ satisface

1. Para todo x, $x < x$ es falso.
2. Si $x < y$ y $y < z$, entonces $x < z$.

Supongamos ahora una relación con las dos propiedades anteriores y asociemos la relación $\leq$ definida por $x \leq y$ si y sólo si $x < y$ o $x = y$. Prueba que esta última es un orden parcial. Esto quiere decir que cualquier orden parcial proviene de una relación $<$ que satisface 1) y 2) (a una relación de este tipo se le llama orden estricto).

Ejercicio 1.2. Comprueba que la suma lineal de dos conjuntos parcialmente ordenados resulta en un conjunto parcialmente ordenado.

Ejercicio 1.3. Comprueba que el producto de dos conjuntos parcialmente ordenados resulta en un conjunto parcialmente ordenado.

Ejercicio 1.4. Sean A y B conjuntos parcialmente ordenados. Demuestra que $(a_1, b_1) \ll (a_2, b_2)$ si y sólo si

- $a_1 = a_2$ y $b_1 \ll b_2$ en B o
- $b_1 = b_2$ y $a_1 \ll a_2$.

Ejercicio 1.5. Sean A y B conjuntos parcialmente ordenados. Demuestra que si a es un elemento maximal de A y b es un elemento minimal de B, entoncs $a \ll b$ en $A \oplus B$.

Ejercicio 1.6. Sean A y B conjuntos parcialmente ordenados. Demuestra que si $a \in A$, $b \in B$ y $a \ll b$ en $A \oplus B$, entonces a es un maximal de A y b es un minimal de B.

Ejercicio 1.7. Demuestra que

$$P \oplus (Q \oplus R) \cong (P \oplus Q) \oplus R.$$

Ejercicio 1.8. Demuestra que

$$A_\perp \cong \mathbf{1} \oplus A$$

Ejercicio 1.9. Demuestre que $\downarrow S$ es el conjunto decreciente mśa pequeño que contiene a S, i.e., si T es un conjunto decreciente tal que $S \subset T$, entonces $\downarrow S \subset T$.

Ejercicio 1.10. Verifica que $\mathcal{O}(A)$ para un conjunto parcialmente ordenado A es en verdad un conjunto parcialmente ordenado bajo la inclusión.

Ejercicio 1.11. Sean $f\colon A \to B$ y $g\colon B \to C$ funciones monótonas. Demuestra que $g \circ f$ es tambin monótona.

Ejercicio 1.12. Sea $\phi\colon A \hookrightarrow B$ una inmersión de orden. Demuestra que

$$\mathrm{ran}(\phi) \cong A.$$

Ejercicio 1.13. Demuestre que para un conjuntos parcialmente ordenado A,

$$\mathcal{O}(A)^\partial \cong \mathcal{O}(A^\partial).$$

2. Un teorema estructural

2.1. Pequeña excursión a la teoría de grafos

Existe una increíble forma de relacionar los conjuntos parcialmente ordenados con la teoría de gráficas. Para conseguir, nos expondremos un poco a dicha teoría definiendo lo que es una gráfica, sus homomorfismos y algunas de sus definiciones. En dicha teoría la visualización juega un rol importante en su desarrollo. Si podemos formular como es que un conjunto parcialmente ordenado es un gráfica, todos los resultados que ésta nos presenta estarán justificados matemáticamente. Comencemos entonces con la definición de de gráfica.

Definición 2.1. Sean V un conjunto cualquiera y E una relación en V. A la pareja (G, E) se le llama *gráfica dirigida*.

Por supuesto, esta definición no refleja nada en absoluto. Sin embargo, se acostumbra interpretar la conjunto V como los *nodos* o *vertices* de la gráfica y al conjunto E como los *arcos* o *aristas* de la gráfica. En ese sentido, tenemos un conjunto de puntos y un conjunto de lineas entre ellos que presentar dirección (una relación es un conjunto de parejas ordenadas). En ese sentido es sencillo presentar un concepto de gráfica a través de una ilustración.

Por supuesto, este tipo de ejemplos nos dejan ver algunas definiciones que pueden resultar atractivas en el marco de nuestra teoría.

Definición 2.2. Sea (V, E) una gráfica dirigida. Definimos

- A un elemento (a, a) de E lo llamamos *bucle*.
- A un conjunto finito $x_0, \ldots, x_n$ de vertices se llama una *caminata*, si $(x_{i-1}, x_i) \in E$ para cada $1 \leq i \leq n$.
- A una caminata con vertices $x_0, \ldots, x_n$ se le llama un *camino* si $x_i \neq x_{i+1}$.
- A un camino con vertices $x_0, \ldots, x_n$ se le llama *ciclo*, si $x_0 = x_n$.

De igual forma, las características de la relación que forman los arcos de una gráfica, sugiera su estructura gráfica. Por ejemplo, si E es una relación simétrica la gráfica resulta simétrica, si es reflexiva, todos los nodos contienen bucles. De hecho la relación que la forma es la que determina su comportamiento en su totalidad. Veremos en la siguiente sección una manera de manipularla de manera computacional.

Ahora definiremos un análogo a concepto de homomorfismos en la teoría orden, en la teoría de gráficos. Como pasa con el orden, dichos homomorfismos tendrán que preservar la estructura de la que estamos hablando.

Definición 2.3. Sean $G = (V, E)$ y $H = (W, F)$ gráficas dirigidas. Una función entre las gráficas $f \colon G \to H$, es una función $f \colon V \to W$ de forma que $(u, v) \in E$ entonces $(f(u), f(v)) \in F$.

Sólo por ilustración podemos mostrar un hecho destacable de los homomorfismo entre gráficas: Estos preservan caminos y ciclos. Podemos de hecho formular de hecho una proposición más fuerte. Consideremos P_k como la gráfica constituida por el conjunto de vértices $\{0, \ldots, k\}$ con aristas $\{(i-1, i) \mid 1 \leq i \leq k\}$. De igual forma consideraremos la gráfica C_k dada por el mismo conjunto de vértices pero con aristas $\{(i-1, i) \mid 1 \leq i \leq k\} \cup \{(k, 0)\}$.

Proposición 2.1. *Sea $G = (V, E)$ una gráfica. Una función $f \colon P_k \to V$ es un homomorfismo entre P_k y G si y sólo si la secuencia $f(0), \ldots, f(k)$ es una caminata en G.*

Demostración. Basta notar que $0, \ldots, k$ es un camino en P_k y como para todo $1 \leq i \leq k$, tenemos que $(i-1, i)$ es una arista de P_k. Si f fuer una homomorfismo, entonces $(f(i-1), f(i))$ sería una arista en G, o en otras palabras, la secuencia $f(0), \ldots, f(k)$ sería una caminata en G. Ahora si f no fuera un homomorfismo, existiría al menos una pareja $(i-1, i)$ para la cual f fallaría en preservar la arista correspondiente en G, en otras palabras $(f(i-1), f(i)) \notin E$, si este fuera el caso la secuencia$f(0), \ldots, f(k)$ no sería un camino en G. Por contraposición, esto termina la prueba. $\square$

La demostración de la siguiente proposición es prácticamente la misma que la anterior y podemos fácilmente convencernos que ésta es cierta.

Proposición 2.2. *Sea $G = (V, E)$ una gráfica. Una función $f\colon C_k \to V$ es un homomorfismo entre P_k y G si y sólo si la secuencia $f(0), \ldots, f(k)$ es un ciclo en G.*

De alguna forma estas proposiciones exhiben la naturaleza del homomorfismo entre gráficas. Podemos dar un paso para desarmar el concepto.

Definición 2.4. Sea $G = (V, E)$ una gráfica. Decimos que (W, F) es una subgráfica de G si $W \subset V$ y $F \subset E \cap (W \times W)$.

La imagen de un homomorfismo entre las gráficas G y H debe resultar en una subgráfica de H. Esta idea en realidad nos abre la posibilidad de entender más la clase de estructura que podemos introducir en una gráfica a través de los homomorfismos.

Definición 2.5. Sean G y H gráficas y sea f un homomorfismo de G a H. Decimos que

- f es una inmersión si f es inyectiva.
- f es un isomorfismo si f es biyectiva y su inversa es también un homomorfismo entre gráficas.

En particular diremos que dos gráficas son isomorfas si y sólo si existe un isomorfismo entre ellas. A esto lo denotaremos por

$$G \cong H.$$

Mientras si existe una inmersión de G a H, entonces escribiremos

$$G \hookrightarrow H.$$

Con un poco de astucia habremos de notar que todo lo mencionado anteriormente pero en un formato distinto y no por eso deja de sentirse como repetición. De hecho f será un isomorfismo cuando (x, y) es una arista de G si y sólo si $(f(x), f(y))$ es una arista de H.

2.2. Un teorema de isomorfismo

Es hora de presentar el teorema al que esta sección está dedicado, en él, y aunque parecería que nos alejamos a cada paso, intentaremos probar que toda nuestra intuición visual respecto a la teoría de gráficas es lo suficiente acertada cuando de conjuntos finitos se trata[2]

Probaremos primero algunos de lemas que caracterizan a la relación de cobertura, propondremos después el teorema principal que hemos estado persiguiendo.

Lema 2.3. *Sea A un conjunto finito parcialmente ordenado. Entonces, si $x < y$, entonces existe un elemento $x' \leq y$ tal que $x \ll x'$.*

Demostración. Probaremos por inducción sobre el número de elementos del conjunto $C(x, y) = \{z \mid x < z < y\}$. Si C no tiene elementos, entonces tenemos que $x \ll y$ por lo que el resultado es válido. Supongamos ahora el resultado válido para k, en otras palabras para cualesquiera dos elementos x y y, si el conjunto $C(x, y)$ tiene a lo más k elementos entonces existe $x' \leq y$ y $x \ll x'$. Supongamos entonces que $C(x, y)$ tiene $k+1$ elementos y tomemos $z \in C(x, y)$ entonces el conjunto $C(x, z)$ tiene menos de $k+1$ o en otras palabras tiene a lo más k elementos, entonces por hipótesis de inducción existe un elemento $x' \leq z$ tal que $x \ll x'$, con lo que el resultado es válido para cualquier natural. De esto sigue el resultado del lema. □

Lema 2.4. *Sea A un conjunto finito parcialmente ordenado. Entonces $x < y$ si y sólo si existen $x = x_0, \ldots, x_n = y$ tal que $x_{i-1} \ll x_i$ para todo $1 \leq i \leq n$.*

Demostración. Como $x < y$, por el lema anterior entonces existe $x_1 \leq y$ tal que $x \ll x_1$. Si $x_1 = y$, entonces hemos terminado, si es falso, entonces $x_1 < y$. Podemos continuar con este proceso y como el conjunto es finito, encontraremos al final un elemento x_n tal que $x = x_0 \ll x_1 \ll x_2 \ll \cdots \ll x_n = y$. Lo que prueba el lema. □

Lema 2.5. *Sean A y B conjuntos finitos parcialmente ordenados y sea $\phi\colon A \to B$ una función monótona. Entonces son equivalentes:*

1. *ϕ es un isomorfismo.*
2. *$x < y$ en A si y sólo si $\phi(x) < \phi(y)$ en B.*
3. *$x \ll y$ en A si y sólo si $\phi(x) \ll \phi(y)$ en B.*

Demostración. Si ϕ es un isomorfismo, $x < y$ implicará que $\phi(x) \leq \phi(y)$, sin embargo ϕ es una biyección y por definición $x < y$ si $x \neq y$ por lo que $\phi(x) \neq \phi(y)$ por lo que $\phi(x) < \phi(y)$. Esto prueba que 1) implica 2). Por analogía al argumento anterior, 2) implica también 1).

[2]Esta de más decirlo, pero habría que desarrollar mucho más la teoría de gráficas para poder afirmar tan tremendo enunciado, pero existe confianza que el día en que se comprenda mejor no esta lejos.

Supongamos ahora 2) y tomemos $x \ll y$ en A. Como en particular $x < y$, debemos tener que $\phi(x) < \phi(y)$; ahora si $\phi(x) < w < \phi(y)$, como ϕ es sobreyectiva, debe existir u en A tal que $\phi(u) = w$ por lo que $x < u < y$ lo que es una contradicción por lo que el elemento w con esa propiedad no puede existir. En otras palabras $\phi(x) \ll \phi(y)$. Esto nos lleva a que 2) implica 3).

Supongamos ahora 3). Si $x < y$ entonces existen elementos

$$x \ll x_1 \ll \cdots \ll x_n \ll y,$$

en ese caso

$$\phi(x) \ll \phi(x_1) \ll \cdots \ll \phi(x_n) \ll \phi(y),$$

y por tanto $\phi(x) < \phi(y)$. Esto prueba que 3) implica 2), lo que termina la prueba de las equivalencias entre los enunciados. $\square$

Falta ahora usar estos resultados para construir una gráfica a partir de un orden. Para esto usaremos la relación de cobertura.

Definición 2.6. Sea A un conjunto parcialmente ordenado. *La gráfica dirigida asociada a A*, en símbolos $\mathcal{G}(A)$, es la gráfica $(A, E(A))$ donde

$$E(A) = \{(x, y) \mid x \ll y\}.$$

Estamos finalmente en la antesala del teorema que deseamos probar.

Teorema 2.6. *Sean A y B conjuntos finitos parcialmente ordenados. Entonces, A es isomorfo a B si y sólo $\mathcal{G}(A)$ es isomorfa a $\mathcal{G}(B)$*

Demostración. Supongamos que son isomorfos, entonces existe una inmersión $\phi\colon A \to B$ biyectiva. Como las gráficas $\mathcal{G}(A)$ y $\mathcal{G}(B)$ tienen como vertices a los conjuntos A y B bastará probar que $(x, y) \in E(A)$ si y sólo si $(\phi(x), \phi(y)) \in E(B)$. En efecto, $(x, y) \in E(A)$ sucede si y sólo si $x \ll y$ y aplicando el lema anterior, lo anterior pasa si y sólo si $\phi(x) \ll \phi(y)$, como queríamos probar.

Supongamos ahora que las gráficas son isomorfas, entonces existe una función $f\colon A \to B$ que es un isomorfismo entre las gráficas $\mathcal{G}(A)$ y $\mathcal{G}(B)$. Entonces $x \ll y$ que por definición sucede si y sólo si $(x, y) \in E(A)$ lo que por la definición de isomorfismo si y sólo si $(f(x), f(y)) \in E(B)$ lo que por definición sucede si y sólo si $f(x) \ll f(y)$. Por el lema anterior eso implica que f es un isomorfismo de orden. $\square$

Este teorema es de relevancia pues existen muchos aspectos computacionales en la teoría de gráficas que pueden ser transferidas directamente a la teoría del orden gracias al teorema anterior. En la siguiente sección desarrollaremos una de estas para mostrar y clasificar algunas gráficas. Finalizamos esta sección con un par corolario que debe resultar inmediato respecto a algunas observaciones que se pueden realizar en las gráficas asociadas a un conjunto parcialmente ordenado.

Corolario 2.7. *La gráfica de un conjunto parcialmente ordenado no es transitiva, no contiene bucles y no contiene ciclos.*

Corolario 2.8. *Si la gráfica de un conjunto finito parcialmente ordenado A contiene un camino, entonces para algún número natural n,*

$$\mathbf{n} \hookrightarrow A.$$

2.3. Un vistazo computacional

Para poder introducir este elemento computacional, primero y manera inesperada haremos uso de la teoría del orden para construir un resultado en teoría de gráficas. Este resultado nos dejará representar un orden parcial de manera computacional y terminaremos el tratamiento obteniendo un algoritmo interesante para construir un orden total dado un orden parcial.

Comenzaremos tomando el conjunto de las matrices de tamaño de $m \times n$ sobre el anillo $\mathbf{1} = \{0, 1\}$. Denotemos este conjunto $\mathbf{1}_{n\times m}$. De manera natural podemos definir la suma, el producto y producto booleano de las matrices de la siguiente manera: Sean $A = (a_{ij})$ matrices de $n \times m$ sobre $\{0, 1\}$, definimos

$$(A + B)_{ij} = a_{ij} + b_{ij}$$

y

$$(A \odot B)_{ij} = a_{ij} \cdot b_{ij}.$$

Sean ahora $A = (a_{ij})$ es una matriz de $n \times m$ y $B = (b_{ij})$ de $m \times p$ sobre $\{0, 1\}$, definimos

$$(AB)_{ij} = \sum_{k=1} a_{ik} b_{kj}.$$

Aparte de estas operaciones, volveremos $\mathbf{1}_{n\times m}$ un conjunto parcialmente ordenado, para esto tomamos dos matrices $A = (a_{ij})$ y $B = (b_{ij})$ en este conjunto, entonces $A \leq B$ si y sólo si $a_{ij} \leq b_{ij}$ para cada $1 \leq i \leq n$ y $1 \leq j \leq m$.

Definición 2.7. Sean los conjuntos $A = \{a_1, \dots, a_n\}$ y $B = \{b_1, \dots, b_m\}$ y sea también R una relación de A en B. Se llama *la matriz de adyacencia de R* a la matriz

$$(M(R))_{ij} = \begin{cases} 1 & \text{si } (a_i, b_j) \in R. \\ 0 & \text{en otro caso.} \end{cases}$$

Para una gráfica (V, E), su matriz de adyacencia es la matriz $M(E)$. Esto presenta una motivación para representar una gráfica por una matriz. No sólo eso, esto implica que además, al ser las gráficas un marco perfectamente válido para trabajar los conjuntos finitos parcialmente ordenados, un conjunto parcialmente ordenado podrá ser representado por una matriz. Una matriz es un elemento perfectamente válido para ser manipulado de manera computacional y muchas más ocasiones que en menos, será deseable expresarlo de esa forma. El siguiente teorema (y su más importante demostración) presentan de alguna manera un conocido problema computacional: El problema del isomorfismo entre gráficas.

Teorema 2.9. *Sean G y H gráficas y sean (a_{ij}) y (b_{ij}) sus matrices de adyacencia respectivamente. Entonces, G y H son isomorfas si y sólo si existe una permutación p de forma que $a_{ij} = b_{p(i)p(j)}$.*

Demostración. Sean $G = (V, E)$ y $H = (W, F)$ las gráficas en cuestión. Debemos suponer además que los conjuntos V y W tienen el mismo número de elementos, si éste no fuera el caso sería imposible encontrar una biyección entre ellos y de la misma forma tampoco se podrían comparar las matrices. Sean entonces $V = \{v_1, \ldots, v_n\}$ y $W = \{w_1, \ldots, w_n\}$, en ese caso las matrices (a_{ij}) y (b_{ij}) tienen tamaño $n \times n$.

Supongamos primero que G y H son gráficas isomorfas. Entonces podemos encontrar una biyección f entre V y W. Al ser V y W finitos, esta función dará lugar a una permutación p del conjunto $\{1, \ldots, n\}$ de la siguiente manera: $p(i)$ será el único elemento tal que $w_{p(i)} = f(v_i)$. Por la existencia del isomorfismo, debemos tener que $(v_i, v_j) \in E$ si y sólo si $(f(v_i), f(v_j)) \in F$. Esto se verá reflejado en la matriz asociada a las gráficas pues $a_{ij} = 1$ si y sólo si $(v_i, v_j) \in E$ lo que sucede si y sólo si $(w_{p(i)}, w_{p(j)}) \in F$ lo que también sucede si y sólo si $b_{p(i)p(j)} = 1$. Como las matrices involucradas sólo presentan ceros y unos lo anterior es suficiente para afirmar que $a_{ij} = b_{p(i)p(j)}$, y esto prueba lo que deseábamos.

Procederemos ahora de modo contrario, afirmando que existe una permutación de forma tal que $a_{ij} = b_{p(i)p(j)}$ para alguna permutación p. Definimos entonces la función $f \colon V \to W$ como $f(v_i) = w_{p(j)}$ y como p es una permutación, f debe ser una biyección. En ese caso tenemos que $(v_i, v_j) \in E$ si y sólo si $a_{ij} = 1$ lo que sucede por hipótesis si y sólo si $b_{p(i)p(j)} = 1$ y en sucede si y sólo si $(w_{p(i)}, w_{p(j)}) \in F$ o lo que es lo mismo $(f(v_i), f(v_j)) \in F$. Por lo que f resulta ser un homomorfismo de gráficas que es además una función biyectiva. Entonces las gráficas G y H son en verdad isomorfas lo que concluye la prueba. □

La demostración de teorema anterior, se puede utilizar (¡aunque a una alto costo computacional!) para decidir cuando dos conjuntos parcialmente ordenados son isomorfos utilizando solamente la matriz de adyacencia de sus gráficas. Conectaremos ahora otro resultado interesante en teoría del orden y presentaremos el algoritmo que este genera.

Teorema 2.10. *Sea $(A, \leq)$ un conjunto finito parcialmente ordenado. Entonces, existe un orden total $\leq'$ de forma que $a \leq b$ implica que $a \leq' b$.*

Demostración. Si el conjunto es vacío, el orden en es total por lo que el resultado sigue; supongamos entonces A no vacío. Elegimos v_1 como un elemento maximal de $H_1 = A$ (en un conjunto finito parcialmente ordenado, estos elementos siempre existen). Preguntamos ahora si $H_2 = A \backslash \{v_1\} \neq \varnothing$; si lo es, el orden original es total y si no es vacío, entonces podemos tomar $v_2 \in H_2$ como un elemento maximal de H_2 y definir $v_2 <' v_1$. Podemos continuar este proceso y como A es finito, existirá una n en los naturales tal que H_{n+1} será un conjunto vacío mientras habremos formado la cadena

$$v_n <' v_{n-1} <' \ldots <' v_2 <' v_1.$$

Basta ahora comprobar que este orden tiene la propiedad propuesta. Supongamos entonces $a \leq b$, entonces, como la anterior cadena es exhaustiva, podemos encontrar el conjunto H_j para el cual b es un maximal, entonces $a \in H_j$, por lo que a será el maximal de algún conjunto H_i con $i \leq j$ por lo que $a \leq' b$ como queríamos probar. $\square$

La demostración de este teorema se puede ver desde otro punto de vista, un punto de vista algorítmico, que nos permite transitar de un orden parcial no necesariamente total a un orden total. A este algoritmo se le denomina *algoritmo de ordenación topológica*.

Ejercicios

Ejercicio 2.1. Sean (V, E), (W, F) y (Z, G) gráficas y sean $f\colon V \to W$ y $g\colon W \to Z$ homomorfismos entre las gráficas correspondientes. Demuestra que $g \circ f$ es también un homomorfismo.

Ejercicio 2.2. Demuestra que si f es un isomorfismo entre las gráficas (V, E) y (W, F), debemos tener que $(x, y) \in E$ si y sólo si $(f(x), f(y)) \in F$.

Ejercicio 2.3. Sean R y S relaciones en un conjunto finito A. Calcule la matriz de adyacencia de la composición $R \circ S$.

Ejercicio 2.4. Sea R una relación. La matriz de adyacencia de la relación se puede usar para demostrar algunas propiedades de las relaciones. Sea $A = \{a_1, \ldots, a_n\}$ un conjunto con n elementos y sea R una relacion en A. Si $M(R)$ es la matriz de adyacencia de la relación, demuestra que

1. R es reflexiva si y sólo si $I_n \leq M(R)$.
2. R es simétrica si y sólo si $(M(R))^t = M(R)$.
3. R es transitiva si y sólo si $M(R) \cdot M(R) \leq M(R)$.
4. R es antisimetrica si y sólo si $M(R) \odot M(R) \leq I_n$.

Ejercicio 2.5. Desarrolle un programa usando la matriz de adyacencia que reconozca relaciones de orden sobre un conjunto finito.

Ejercicio 2.6. En una gráfica (V, E), un subconjunto de S de V se dice *una cuenca* si $(x, y) \in E$ y $x \in S$ implica que $y \in S$. es vacío. ¿Cómo prodríamos usar la matriz de adyacencia para deducir si un subconjunto es una cuenca?

Ejercicio 2.7. Sea $\mathcal{G}(A)$ la gráfica asociada a un conjunto finito parcialmente ordenado A. Demuestra que si S es una cuenca en $\mathcal{G}(A)$ entonces S es un conjunto creciente en A.

Ejercicio 2.8. Sea A un conjunto parcialmente ordenado. Si $M(A)$ es la matriz de incidencia de la gráfica asociada de A, ¿cómo sería posible reconocer a un elemento maximal de A? ¿cómo sería posible reconocer a un elemento minimal de A?

Ejercicio 2.9. Sean A y B conjuntos parcialmente ordenado. Si $M(A)$ y $M(B)$ son las matrices de incidencia de las gráficas asociadas a los conjuntos A y B respectivamente, calcule $M(A\dot{\cup}B)$, usando $M(A)$ y $M(B)$.

Ejercicio 2.10. Sean A y B conjuntos parcialmente ordenado. Si $M(A)$ y $M(B)$ son las matrices de incidencia de las gráficas asociadas a los conjuntos A y B respectivamente, calcule $M(A \oplus B)$, siendo esta la matriz asociada al conjunto parcialmente ordenado $A \oplus B$ usando $M(A)$ y $M(B)$.

3. Retículas

3.1. Retículas como conjuntos ordenados

Muchas de las propiedades de conjuntos parcialmente ordenados se pueden expresar a través de la existencia de ciertas cotas. Dos importantes estructuras en este sentido son las retículas y las retículas completas. Presentamos ahora algunas definiciones necesarias para transitar sobre estas estructuras.

Definición 3.1. Sea A un conjunto parcialmente ordenado y sea $S \subset A$. Un elemento $a \in A$ se dice *una cota superior de* S si para cada $s \in S$ tenemos $s \leq a$. Por dualidad, una cota inferior de S es un elemento $a \in A$ de forma que para cada $s \in S$, tenemos $a \leq s$.

Dado un subconjunto S de un conjunto parcialmente ordenado de L podemos definir el conjunto de cotas superiores de S como el conjunto

$$S^u = \{x \in A \mid s \leq x \text{ para cada } s \in S\}$$

y por dualidad definimos también el conjunto de cotas inferiores de S, S^l. Como un orden es transitivo, no es difícil observar que S^u es creciente y S^l es decreciente.

Definición 3.2. Sea A un conjunto parcialmente ordenado y sea $S \subset A$. Si el conjunto S^u tiene un mínimo, a éste se le llama *el supremo de* S y se denota por $\sup(S)$. Si el conjunto S^l tiene un máximo a éste se llama *el ínfimo de* S y se denota por $\operatorname{ínf}(S)$.

Introduciremos ahora una notación que nos permita operar de manera algebraica algunos conjuntos parcialmente ordenados. Para elementos a y b de un conjunto parcialmente ordenado, escribiremos

$$a \vee b = \sup\{x, y\}$$

cuando dicho supremo exista; lo anterior se lee como «a disyunción b». También escribiremos

$$a \wedge b = \operatorname{ínf}\{x, y\}$$

cuando dicho ínfimo exista; lo anterior se lee como «a conjunción b». De manera similar, para un subconjunto S de un conjunto parcialmente ordenado, escribiremos

$$\bigvee S = \sup S$$

y

$$\bigwedge S = \text{ínf}\, S$$

cuando estos existan y leyéndose de nueva cuenta como *la disyunción y la conjunción de S* respectivamente. Presentamos ahora la definición de retícula.

Definición 3.3. Sea L un conjunto parcialmente ordenado. Si para cualesquiera elementos a y b en A, existe $x \vee y$ y $x \wedge y$, entonces L se dice *una retícula*. De manera complementaria, si para cualquier subconjunto $S \subset L$, existen los conjuntos $\bigvee S$ y $\bigwedge S$, entonces L se dice *una retícula completa*.

Es interesante preguntar en que casos fallará en existir la conjunción y la disyunción de dos elementos en un conjunto parcialmente ordenado. Si la disyunción de los elementos a y b no existe, esto sólo se puede deber a dos razones, que a y b no tienen un cota superior común o que no existe una mínima cota superior para ellos.

Probaremos ahora algunos lemas de transición entre las retículas como orden y como estructura algebraica.

Proposición 3.1. *Sea L una retícula. Entonces, $a \leq b$ implica $a \vee b = b$ y $a \wedge b = a$.*

Demostración. Debemos notar que bajo la hipótesis

$$\{a, b\}^u = \{x \in L \mid b \leq x\}$$

y también

$$\{a, b\}^l = \{x \in L \mid x \leq a\}.$$

Entonces el mínimo del conjunto $\{a, b\}^u$ es el elemento b mientras que el máximo del conjunto $\{a, b\}^l$ es el elemento a. En otras palabras $a \vee b = b$ y $a \wedge b = a$ como buscábamos. □

Corolario 3.2. *Sea L una retícula. Entonces, $a \vee a = a$ y $a \wedge a = a$.*

Proposición 3.3. *Sea L una retícula. Entonces, para cualesquiera a, b, c y d tenemos que si $a \leq b$ y $c \leq d$, entonces $a \vee c \leq b \vee d$ y $a \wedge c \leq b \wedge d$.*

Demostración. Supongamos que $a \leq b$ y $c \leq d$. Afirmamos que $\{b, d\}^u \subset \{a, c\}^u$, en efecto si $x \in \{b, d\}^u$ y por definición $a \leq b \leq x$ $c \leq d \leq x$ y en consecuencia $x \in \{a, c\}^u$. Como el $\sup\{b, d\} = \text{mín}\{b, d\}^u$ es por definición un elemento de $\{b, d\}^u$, por la afirmación anterior debemos tener $\sup\{b, d\} \in \{a, c\}^u$ y en consecuencia $\sup\{a, c\} = \text{mín}\{a, c\}^u \leq \sup\{b, d\}$. Lo anterior significa simplemente que $a \vee c \leq b \vee d$.

Para la segunda desigualdad, afirmamos que $\{a, c\}^l \subset \{b, d\}^l$, en efecto si $x \in \{a, c\}^l$ y por definición $x \leq a \leq b$ $x \leq c \leq d$ por lo que $x \in \{b, d\}^l$. Además, como el $\text{ínf}\{a, c\} = \text{máx}\{a, c\}^l$ es por definición un elemento de $\{a, c\}^l$, de la afirmación anterior debemos obtener que $\text{ínf}\{a, c\} \in \{b, d\}^l$ y en consecuencia $\text{ínf}\{b, d\} = \text{máx}\{b, d\}^l \geq \text{ínf}\{a, c\}$. Lo anterior significa que $a \wedge c \leq b \wedge d$. Esto termina la demostración. □

Proposición 3.4. *Sea L una retícula y sean a, b y c elementos de L.*

- *Si $b \leq a \leq b \vee c$, entonces $b \vee c = a \vee c$.*
- *Si $b \wedge c \leq a \leq b$ entonces $b \wedge c = a \wedge a$.*

Demostración. Por definición, tenemos que $c \leq \sup\{b, c\} = b \vee c$ y por la proposición 3.1 $(b \vee c) \vee c = b \vee c$, además por la proposición **??** y como $c \leq c$,

$$b \vee c \leq a \vee c \leq (b \vee c) \vee c = b \vee c.$$

Por la antisimetría del orden, entonces $b \vee c = a \vee c$. La prueba del segundo enunciado es inmediata al ser el enunciado dual del primero. □

Antes de continuar, hemos expuesto algunos ejemplos que resultarán en retículas de manera inmediata. Por ejemplo, una cadena en general es una retícula pues pues de acuerdo a la proposición **??**, si $x \leq y$ entonces $x \vee y = y$ y $x \wedge y = x$; como en una cadena cualesquiera elementos son comparables, entonces estos elementos siempre existen. De manera curiosa las retículas $\mathbb{R}$, $\mathbb{Z}$ y $\mathbb{Z}$ no son completas. Sin embargo, si tomamos un intervalo cerrado en $\mathbb{R}$, $[a, b]$ con $a < b$, entonces como conjunto parcialmente ordenado es completo, lo cual no sucede con un intervalo de $\mathbb{Q}$ por ejemplo $[0, \sqrt{2}]$.

El orden parcial $(\mathcal{P}(A), \subset)$ es una retícula. No sólo una retícula, una retícula completa. Es posible probar que si $S \subset \mathcal{P}(A)$, entonces

$$\bigvee S = \bigcup S$$

y

$$\bigwedge S = \bigcap S.$$

Otro ejemplo que resulta en una retícula es el conjunto de conjuntos decrecientes de un conjunto parcialmente ordenado A, $\mathcal{O}(A)$, resulta una retícula completa. A ésta se le denomina *la retícula decreciente de A*.

Un último ejemplo resulta en introducir un nuevo orden en los naturales. Consideremos para esto el conjunto parcialmente ordenado $(\mathbb{N}_0, \preceq)$en donde definimos $m \preceq n$ si y sólo si m divide a n, i.e., existe un número en $\mathbb{N}_0$ tal que $n = mk$. Este nuevo orden define una retícula, donde $m \vee n = [m, n]$ y $m \wedge n = (m, n)$.

Probaremos ahora un lema y un teorema que nos describen con toda precisión el comportamiento de $\vee$ y $\wedge$, con lo que podremos tomarlas como operaciones y proponer una lattice no como un orden sino como una estructura puramente algebraica.

Lema 3.5 (de la conexión)**.** *Sea L una retícula y sean $a, b \in L$. Entonces son equivalentes:*

1. $a \leq b$.
2. $a \vee b = b$.

3. $a \wedge b = a$.

Demostración. En 3.1 hemos probado que 1) implica ambos 2) y 3). Asumamos 2), entonces b es una cota superior de $\{a, b\}$ por lo tanto $a \leq b$; esto afirma que 2) implica 1). De manera similar, si asumimos 3), entonces a es una cota inferior de $\{a, b\}$ por lo que $a \leq b$. □

Teorema 3.6. *Sea L una retícula. Entonces para cualesquiera a y b elementos de L, se cumple*

$$(a \vee b) \vee c = a \vee (b \vee c). \tag{L1}$$
$$(a \wedge b) \wedge c = a \wedge (b \wedge c). \tag{L1'}$$
$$a \vee b = b \vee a. \tag{L2}$$
$$a \wedge b = b \wedge a. \tag{L2'}$$
$$a \vee a = a. \tag{L3}$$
$$a \wedge a = a. \tag{L3'}$$
$$a \vee (a \wedge b) = a. \tag{L4}$$
$$a \wedge (a \vee b) = a. \tag{L4'}$$

Demostración. L1: Supongamos $s = a \vee b$, $t = s \vee c$ y también que $s' = b \vee c$ y $t' = a \vee s'$. Probaremos primero que $t' \leq t$: como s es el supremo del conjunto $\{a, b\}$ entonces $b \leq t$ y bajo un argumento similar, podemos ver que $c \leq t$, esto quiere decir que t es una cota superior del conjunto $\{b, c\}$, por lo que debemos tener que $s' \leq t$ al ser s el supremo del conjunto $\{b, c\}$. Ahora, debemos tener también que $a \leq t$ y por tanto debemos tener que t es una cota superior del conjunto $\{a, s'\}$ y en consecuencia, $t' \leq t$ al ser t' el supremo del conjunto $\{a, s'\}$.

Probemos ahora que $t \leq t'$: por definición $a \leq t'$ y $s' \leq t'$, pero como s' es el supremo entre b y c, debemos tener que $b \leq t$ y por tanto t' es una cota superior de a, b. En ese caso $s \leq t'$ y eso deriva en que t' es una cota superior de $\{s, c\}$ y por tanto $t \leq t'$. Junto con el párrafo anterior, debemos tener $t = t'$ como deseábamos.

L2: Basta notar que $\{a, b\} = \{b, a\}$ es cierto, pues al considerar cotas superiores e inferiores y mínimos y máximos de estas, ni su existencia ni los elementos que resultan cambian.

L3: Corolario 3.2.

L4: Por definición $a \wedge b \leq a$ y por el lema de la conexión, debemos tener que $(a \wedge b) \vee a = a$ por L2 esto implica L4.

Los enunciados L1', L2', L3' y L4' son inmediatos por dualidad. □

3.2. Retículas como estructura algebraica

El teorema 3.6 es un resultado relevante. La hipótesis resulta en suponer el conjunto parcialmente ordenado como una retícula, sin embargo en ninguna parte del teorema aparece mención alguna al orden, toda mención es sólo de manera implícita. Esto es una sugerencia importante, pues podríamos definir una retícula sin más trámite que operaciones binarias sobre un conjunto. Comencemos hablando del significado de una operación sobre un conjunto.

Definición 3.4. Sea A un conjunto. A una función $\sigma\colon A^n \to A$ se le denomina una operación n-aria sobre A.

Definición 3.5. Sea L un conjunto y sean $\wedge\colon L^2 \to L$ y $\vee\colon L^2 \to L$ operaciones binarias sobre L. A la tercia $(L, \wedge, \vee)$ se le denomina *retícula* si las operaciones satisfacen L1, L1', L2, L2', L3, L3', L4, L4'

Hemos visto que cualquier retícula, como conjunto parcialmente ordenado, resulta en una retícula, como estructura algebraica. Para asegurar que son en realidad la misma definición habría que garantizar que una retícula como estructura deriva en un orden.

Teorema 3.7. *Sea L una retícula. Para cualesquiera a y b en L se cumple que $a \vee b = b$ si y sólo si $a \wedge b = a$.*

Demostración. Supongamos que $a \vee b = b$, entonces

$$\begin{aligned} a &= a \wedge (b \vee a) && \text{L4}' \\ &= a \wedge (a \vee b) && \text{L2}' \\ &= a \wedge b. \end{aligned}$$

De manera inversa, si $a \wedge b = b$, entonces

$$\begin{aligned} a &= a \vee (b \wedge a) && \text{L4} \\ &= a \vee (a \wedge b) && \text{L2} \\ &= a \vee b. \end{aligned}$$

□

Teorema 3.8. *Sea $(L, \wedge, \vee)$ una retícula. Entonces la relación $\leq$ en L, definida como $a \leq b$ si y sólo si $a \wedge b = a$, resulta en un orden.*

Demostración. Como $a \wedge a = a$ por L3, entonces $a \leq a$ por lo que $\leq$ es una reflexión reflexiva. Supongamos ahora que $a \leq b$ y $b \leq c$, entonces $a \wedge b = a$ y $b \wedge c = b$. En ese caso, por L1

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

y en consecuencia $a \leq c$, por lo que la relación es reflexiva. Por último, debemos de probar que la relación es antisimétrica. Para esto supongamos que $a \leq b$ y

$b \leq a$, en ese caso tenemos que $a \wedge b = a$ y $b \wedge a = b$. Entonces, por L3

$$\begin{aligned} a &= a \wedge b \\ &= b \wedge a \\ &= b, \end{aligned}$$

por lo que podemos concluir que la relación es antisimétrica. □

Corolario 3.9. *Para cualesquiera elementos a y b en L, ambos* $\sup\{a, b\}$ *e* $\operatorname{inf}\{a, b\}$ *existen y*

$$\sup\{a, b\} = a \vee b \text{ y } \operatorname{inf}\{a, b\} = a \wedge b.$$

Demostración. Probaremos primero que $a \vee b$ es una cota superior de $\{a, b\}$. En efecto, por L4', $a \wedge (a \vee b) = a$ y por tanto $a \leq a \vee b$, de igual forma $b \leq a \vee b$. Entonces $a \vee b \in \{a, b\}^u$; supongamos ahora que $s \in \{a, b\}^u$, como $a \leq s$ y $b \leq s$, debemos tener que $a = a \wedge s$ y $b = b \wedge s$, lo que por el teorema 3.7, significa que $s = s \vee a$ y $s = s \vee b$, en ese caso

$$\begin{aligned} s &= s \vee b \\ &= (s \vee a) \vee b \\ &= s \vee (a \vee b) \end{aligned}$$

De nuevo, por el teorema 3.7, debemos tener que $a \vee b = s \wedge (a \vee b)$ por lo que $a \vee b \leq s$ convirtiendo $a \vee b$ en la mínima cota superior de a y b. En ese caso $\sup\{a, b\} = a \vee b$ como queríamos.

Ahora, debemos tener que $a \wedge b$ es una cota inferior de $\{a, b\}$. En efecto, como

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

debemos tener que $a \wedge b \leq a$. De la misma forma $a \wedge b \leq b$, por lo que podemos concluir que $a \wedge b \in \{a, b\}^l$; supongamos ahora que $s \in \{a, b\}^l$, como $s \leq a$ y $s \leq b$, debemos tener que $s = s \wedge a$ y $s = s \wedge b$, entonces,

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

En ese caso, $s \leq a \wedge b$ por lo que $a \wedge b$ es la máxima cota inferior de a y b, en ese caso $\operatorname{inf}\{a, b\} = a \wedge b$, como deseábamos. □

En ese caso, al escribir $(L, \leq)$ o $(L, \wedge, \vee)$ se entenderá que es una retícula, entendiendo que podemos tomar cualquiera de las dos definiciones. Por un lado, si es un conjunto parcialmente ordenado las operaciones derivan de los supremos e ínfimos, por otro, si es una estructura con dos operaciones binarias, es posible asociar un orden a esta. De cualquier forma, una retícula de manera implícita contendrá un orden y dos operaciones.

Desde punto de vista algebraico llamar a los elementos cima y fondo $\top$ y $\perp$ resulta extraño. Por eso, en el caso de retículas preferimos llamarlos 1 y 0. Cuando una retícula contenga los elementos 1 y 0 se dirá *acotada*. En un ejemplo que puede parecer extraño, la retícula $(\mathbb{N}_0, \preceq)$ resulta acotada con ¡$1 = 0$ y $0 = 1$!

Una de las ventajas del punto de vista algebraico, es que revela con mucha facilidad la estructura del conjunto. Para analizar esto, propondremos algunos de los conceptos que surgen naturalmente cuando tenemos una estructura algebraica.

Definición 3.6. Sea L una retícula. Si $\varnothing \neq M \subset L$, entonces M se dice una subretícula cuando $a, b \in M$ implica $a \vee b \in M$ y $a \wedge b \in M$.

A diferencia de otras estructuras algebraicas, en una retícula L es posible que un subconjunto $M \subset L$, podría ser una retícula sin ser una subretícula de la retícula L.

Definición 3.7. Sean L y K retículas. Entonces, el producto $L \times K$ se define usando las expresiones

$$(l_1, k_1) \wedge (l_2, k_2) = (l_1 \wedge l_2, k_1 \wedge k_2)$$
$$(l_1, k_1) \vee (l_2, k_2) = (l_1 \vee l_2, k_1 \vee k_2).$$

Ejercicios

Ejercicio 3.1. Demuestra que S^u es un conjunto creciente y que S^l es un conjunto decreciente

Ejercicio 3.2. Sea $S \subset \mathcal{P}(A)$ y considérese $(\mathcal{P}(A), \subset)$ como conjunto parcialmente ordenado. Demuestra que $\bigcap S$ es una cota inferior de S y también $\bigcup S$ es una cota superior de S.

Ejercicio 3.3. Sea $S \subset \mathcal{P}(A)$ y considérese $(\mathcal{P}(A), \subset)$ como conjunto parcialmente ordenado. Demuestra que $\bigcap S$ es la máxima cota inferior de S y que también $\bigcup S$ es la mínima cota superior de S.

Ejercicio 3.4. Sea $S \subset \mathcal{O}(A)$ donde A es un conjunto parcialmente ordenado. Entonces $\bigcup S$ y $\bigcap S$ son también conjuntos decrecientes. Esto en particular prueba que $(\mathcal{O}(A), \subset)$ es una retícula.

Ejercicio 3.5. Sea $(L, \wedge, \vee)$ una retícula. Demuestra que la relación definida por $a \leq b$ si y sólo si $a \vee b = a$, es un orden parcial.

Ejercicio 3.6. Demuestra que si L y K son retícuas, el conjunto $L \times K$ puede resultar de igual forma en retícula definiendo

$$(l_1, k_1) \wedge (l_2, k_2) = (l_1 \wedge l_2, k_1 \wedge k_2)$$

y

$$(l_1, k_1) \vee (l_2, k_2) = (l_1 \vee l_2, k_1 \vee k_2).$$

En los siguientes ejercicios probaremos que $(\mathbb{N}_0, \mathrm{mcd}, \mathrm{mcm})$ resulta en una retícula desarrollando conceptos de divisibilidad. Comencemos con las definiciones.

Definición 3.8. Para números m y n en $\mathbb{N}_0$, decimos que n divide a m o m es un múltiplo de n, en símbolos $m|n$, si existe $k \in \mathbb{N}_0$ tal que $km = n$.

Definición 3.9. Sean m, n y s números en $\mathbb{N}_0$. Decimos que s es *un divisor común de n y m* si $s|n$ y $s|m$. Decimos también que s es *un mútiplo común de n y m* si $n|s$ y $m|s$.

Ejercicio 3.7. Sean m y n números en $\mathbb{N}_0$. Demuestra que los siguiente conjuntos son no vacíos.

$$D(m, n) = \{x \in \mathbb{N}_0 \mid x \text{ es divisor común de } m \text{ y } n\}$$

$$M(m, n) = \{x \in \mathbb{N}_0 \mid x \text{ es múltiplo común de } m \text{ y } n\}$$

Ejercicio 3.8. Sean m y n números. Demuestra que existe un número K tal que para todo $s \in D(m, n)$ se tiene que $s \leq K$. En otras palabras, demuestra que $D(m, n)$ está acotado.

Ejercicio 3.9. De estos últimos ejercicios concluye a través del principio de buen orden, que existe máximo común divisor y el mínimo común múltiplo para cualesquiera dos números en $\mathbb{N}_0$.

Definición 3.10. Sean m y n números cualesquiera. Definimos $\mathrm{mcd}(m, n)$ como el máximo común divisor de m y n, y $\mathrm{mcm}(m, n)$ como el mínimo común mútiplo de m y n.

Ejercicio 3.10. Para cualesquiera n, m y l, demuestra que

$$\mathrm{mcd}\left(\mathrm{mcd}(m, n), l\right) = \mathrm{mcd}\left(m, \mathrm{mcd}(n, l)\right)$$

$$\mathrm{mcm}\left(\mathrm{mcm}(m, n), l\right) = \mathrm{mcm}\left(m, \mathrm{mcm}(n, l)\right)$$

Ejercicio 3.11. Para cualquier n demuestra que

$$\mathrm{mcd}(n, n) = n$$

$$\mathrm{mcm}(n, n) = n$$

Ejercicio 3.12. Para cualesquiera n y m, demuestra que

$$\mathrm{mcd}\left(n, \mathrm{mcm}(m, n)\right) = n$$

$$\mathrm{mcm}\left(n, \mathrm{mcd}(m, n)\right) = n$$

Ejercicio 3.13. Convencete con lo anterior que $(\mathbb{N}_0, \mathrm{mcd}, \mathrm{mcm})$ es una retícula. No ya desde el punto de vista de orden, sino desde la definición algebraica.

Ejercicio 3.14. Demuestra que la retícula $(\mathbb{N}_0, \mathrm{mcd}, \mathrm{mcm})$ posee una cima con $\top = 0$ y un fondo con $\perp = 1$.

4. Retículas completas

5. Retículas modulares, distributivas y booleanas

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.

[HN04] Hell, Pavol y Nesetril, Jaroslav: *Graphs and homomorphisms.* Oxford University Press, 2004.

Comentario. Las notas anteriores juegan algunas veces a ser un simple resumen de lo que otros autores han presentado, otras menos a reinterpretarlo y en una cantidad ínfima de ocasiones intentan pobremente aumentalo. El único objectivo al que sirven, es preparar el curso de Matemáticas Discretas impartido en la carrera de Matemáticas Aplicadas y Computación de la FES Acatlán. Su versión es, en consecuencia, susceptible a errores gramaticales, imprecisiones técnicas y cambios constantes.

El contenido original que aparezca en estas notas (si es que lo hay), se distribuye bajo la Licencia Creative Commons Atribución-NoComercial 4.0 Internacional (CC BY-NC 4.0). ©Eduardo Antonio Gomezcaña Alanis.