INFORME TECNICO INTERNO

N°. 66

INSTITUTO DE MATEMATICA DE BAHIA BLANCA

INMABB (UNS - CONICET)

UNIVERSIDAD NACIONAL DEL SUR
Avda. ALEM 1253 - 8000 BAHIA BLANCA
República Argentina

INFORME TÉCNICO INTERNO N° 66

ÁLGEBRAS DE BOOLE

Luiz F. Monteiro

Universidad Nacional del Sur

INMABB

CONICET - UNS

AÑO 1998

Versión revisada 2000 – 2001 - 2002

INFORME TÉCNICO INTERNO

N° 66

INSTITUTO DE MATEMÁTICA DE BAHIA BLANCA

INMABB (CONICET - UNS)

UNIVERSIDAD NACIONAL DEL SUR

Avda. ALEM 1253 - 8000 BAHIA BLANCA

1998

Versión revisada 2000 – 2001 - 2002

ALGEBRAS DE BOOLE

Luiz F. Monteiro

Estas notas estan basadas, fundamentalmente, en partes de diversos cursos, que dictara en la Universidad Nacional del Sur, entre 1957 y 1975, el Dr. Antonio A. R. Monteiro. En las mismas hemos introducido algunas modificaciones que fueron incluídas en sucesivos cursos que dictaramos en la misma Universidad, entre 1974 y 1997, así como resultados propios.
Agradecemos la colaboración del Licenciado Ignacio D. Viglizzo, y en la corrección de estas notas a las Licenciadas Sonia Savini y Estela Bianco, y a los alumnos Cecilia Cimadamore, Martín Figallo, Romina Coppola, Melina Verdecchia y Yanina González.

INMABB - CONICET -UNS

1998

Versión revisada - 2.000 - 2.001 - 2.002

Índice General

1 CONJUNTOS ORDENADOS

1.1 Definición de conjunto ordenado

Sea $I\!N$ el conjunto de los números naturales y $I\!N_0 = I\!N \cup \{0\}$. Existen dos relaciones binarias definidas sobre $I\!N_0$ que tienen gran importancia, a saber:

(1) La relación *menor ó igual* que se representa por "$\leq$" y que se define del siguiente modo:

$$x \leq y \text{ si existe } n \in I\!N_0 \text{ tal que } x + n = y.$$

(2) La relación *divide* que se representa por "/" y que se define del siguiente modo:

$$x/y \text{ si existe } n \in I\!N_0 \text{ tal que } x.n = y.$$

La relación $\leq$ tiene las siguientes propiedades

O1) (*Propiedad Reflexiva*): $x \leq x$ cualquiera que sea $x \in I\!N_0$.

O2) (*Propiedad Antisimétrica*): Si $x, y \in I\!N_0$ son tales que $x \leq y$ e $y \leq x$ entonces $x = y$.

O3) (*Propiedad Transitiva*): Si $x, y, z \in I\!N_0$ son tales que $x \leq y$ e $y \leq z$ entonces $x \leq z$.

La relación divide también tiene las propiedades Reflexiva, Antisimétrica y Transitiva.

Ejercicio 1.1.1 *Demostrar la propiedades indicadas anteriormente.*

Existen muchas otras relaciones binarias que poseen las tres propiedades citadas anteriormente. Ello lleva en forma natural a introducir la siguiente definición:

Definición 1.1.1 *Dado un conjunto, no vacío, A y una relación binaria definida sobre A, que representaremos por "$\leq$" que verifica las propiedades* O1), O2) *y* O3) *indicadas anteriormente, diremos que "$\leq$" es una* **relación de orden sobre** *A y que el sistema $(A, \leq)$ es un* **conjunto ordenado.**

Para simplificar el lenguaje diremos muchas veces, mas sencillamente que A es un conjunto ordenado. Si se verifica la relación "$x \leq y$" diremos que "x precede a y", o que " x es menor o igual que y".
Observemos que varios autores denominan *orden parcial* a toda relación binaria que verifica O1), O2) y O3). En la literatura inglesa es habitual denominar a estos conjuntos **poset** (partial ordered **set**).
De acuerdo con la definición precedente las relaciones "$\leq$" y "/" son relaciones de orden definidas sobre $I\!N_0$, por lo tanto $(I\!N_0, \leq)$ y $(I\!N_0, /)$ son conjuntos ordenados.

Observación 1.1.1 *Dadas dos relaciones binarias R_1 y R_2 sobre un conjunto A, se dice que ellas son iguales, y se nota $R_1 = R_2$, si $(x, y) \in R_1 \iff (x, y) \in R_2$. Luego las relaciones R_1 y R_2 son diferentes, en notación $R_1 \neq R_2$ si existen elementos $a, b \in A$ tales que:*

$$(a, b) \in R_1 \text{ y } (a, b) \notin R_2 \text{ ó } (a, b) \in R_2 \text{ y } (a, b) \notin R_1.$$

Luego las relaciones "$\leq$" y "/" son diferentes dado que $2 \leq 3$, y 2 no divide a 3. Esto nos muestra que sobre el conjunto $I\!N_0$ se puede definir mas de una relación de orden.

Ejemplo 1.1.1 *Dado un conjunto, no vacío, A, sea $\mathcal{P}(A)$ la familia de todos los subconjuntos de A, entonces es claro que $(\mathcal{P}(A), \subseteq)$ es un conjunto ordenado. Este es uno de los ejemplos mas importantes, pues veremos mas adelante que el estudio de una relación de orden se puede reducir al estudio de una relación de inclusión entre subconjuntos de un cierto conjunto.*

Ejercicio 1.1.2 *1) Sea A el conjunto de todas las personas. Si $a, b \in A$, pongamos por definición $a\, R\, b \iff$* estatura de a $\leq$ estatura de b. *¿Es R una relación de orden?*

2) Sea I un conjunto no vacío y $\mathbb{R}$ el conjunto de los números reales. Consideremos el conjunto F de todas las funciones definidas sobre I y que toman valores en $\mathbb{R}$. Dadas $f, g \in F$ pongamos por definición:

$$f \leq g \iff f(x) \leq g(x),\ \forall\, x \in I.$$

Probar que $(F, \leq)$ es un conjunto ordenado.

3) Si i_0 es un elemento fijo de I y ponemos por definición:

$$f \leq g \iff f(i_0) \leq g(i_0),$$

¿ Será $(F, \leq)$ un conjunto ordenado ?

4) En $\mathbb{N}_0$ definamos:

$$x\, R\, y \iff \text{existe } a \in \mathbb{N}_0 \text{ tal que } x^2 + a = y^2.$$

¿ Es $(\mathbb{N}_0, R)$ un conjunto ordenado? En caso afirmativo ¿será la relación binaria "$\leq$" definida anteriormente igual a la relación R?

Observación 1.1.2 *Los axiomas* O1), O2) *y* O3) *son independientes,* [30]. *Esto significa que ninguno de ellos se puede deducir a partir de los restantes. Sea $A = \{a, b, c\}$ y definamos sobre A las siguientes relaciones binarias:*

	a	b	c	a	b	c	a	b	c
a		R	R	S	S		T	T	
b			R	S	S			T	T
c						S			T

1) O1) *es independiente de* O2) *y* O3.
La relación R verifica O2) *y* O3) *y no verifica* O1), *ya que $a \not R\, a$.*

2) O2) *es independiente de* O1) *y* O3).
La relación S verifica O1) *y* O3) *y no verifica* O2), *ya que $a\, S\, b$, $b\, S\, a$ y $a \neq b$.*

3) O3) *es independiente de* O1) *y* O2).
La relación T verifica O1) *y* O2) *y no verifica* O3), *ya que $a\, T\, b$, $b\, T\, c$ y $a \not T\, c$.*

Notaremos $a_1 \leq a_2 \leq \ldots \leq a_{n-1} \leq a_n$, para indicar que $a_1 \leq a_2$, $a_2 \leq a_3, \ldots, a_{n-1} \leq a_n$.

Ejercicio 1.1.3 *Probar que si* $a_1 \leq a_2 \leq \ldots \leq a_{n-1} \leq a_n \leq a_1$, *entonces:* $a_1 = a_2 = \ldots = a_{n-1} = a_n$.

Definición 1.1.2 *Si* $(A, \leq)$ *es un conjunto ordenado, escribiremos* $a < b$ *(a* **menor que** *b) para indicar que* $a \leq b$ *y* $a \neq b$. *Caso contrario notaremos* $a \not< b$.

Análogamente notaremos $a_1 < a_2 < \ldots < a_{n-1} < a_n$, para indicar que: $a_1 < a_2, \;\; a_2 < a_3, \ldots, a_{n-1} < a_n$.

Lema 1.1.1 *La relación* $<$ *tiene las siguientes propiedades:*

O'1) Propiedad Irreflexiva: $x \not< x, \;\; \forall\, x \in A$.

O'2) Propiedad Transitiva: Si $a, b, c \in A$ *verifican* $a < b$ *y* $b < c$ *entonces* $a < c$.

y además se cumple la condición:

D) $a \leq b \iff a < b$ *o* $a = b$.

Dem.

O'1) Supongamos que existe $x \in A$ tal que $x < x$, luego $x \leq x$ y $x \neq x$, absurdo.

O'2) Si $a < b$ y $b < c$ entonces (1) $a \leq b$, (2) $a \neq b$, (3) $b \leq c$, y (4) $b \neq c$. De (1) y (3) resulta por la propiedad O3) que $a \leq c$. Para probar que $a < c$, nos falta demostrar que $a \neq c$. Supongamos que $a = c$, entonces por (3) tendremos que (5) $b \leq a$ y de (1) y (5) resulta por O2) que $a = b$, lo que contradice (2).
Observemos que de $a \neq b$ y $b \neq c$ no se puede concluir que $a \neq c$. En efecto $2 \neq 3, \;\; 3 \neq 2$ y no se verifica que $2 \neq 2$.

D) $\Longrightarrow$) Si $a = b$ no hay nada que demostrar. Si $a \neq b$ como por hipótesis $a \leq b$ entonces $a < b$.

$\Longleftarrow$) Dados $a, b \in A$ si $a = b$ como $a \leq a = b$ entonces $a \leq b$.
Si $a < b$ entonces $a \leq b$ y $a \neq b$, luego en particular $a \leq b$.

■

El resultado precedente muestra que la relación "$\leq$" se puede definir a partir de la relación "$<$" usando la propiedad D.

Teorema 1.1.1 *Sea* $(A, <)$ *un sistema formado por un conjunto, no vacío,* A *y una relación binaria "*$<$*" definida sobre* A *que verifica las propiedades* O'1) *y* O'2). *Entonces, si definimos sobre* A *la siguiente relación binaria:*

$$\text{D)} \;\; a \leq b \iff a < b \;\text{ ó }\; a = b,$$

el sistema $(A, \leq)$ *es un conjunto ordenado y además:*

$$a < b \iff a \leq b \;\text{ y }\; a \neq b.$$

Dem.

O1) $a \leq a, \ \forall\, a \in A$.
De acuerdo con la definición D) esto equivale a probar que $a < a$ ó $a = a$, luego $a \leq a$.

O2) Supongamos que $a \leq b$ y $b \leq a$, esto es, (1) $a < b$ ó (2) $a = b$ y (3) $b < a$ ó (4) $a = b$.
Si se verificaran (1) y (3) entonces por O'2) tendríamos que $a < a$ lo que contradice O'1). Si se verificaran (1) y (4) también tendríamos que $a < a$. Si se verificaran (3) y (2) también llegamos a que $a < a$. Por lo tanto $a = b$.

O3) Supongamos que $a \leq b$ y $b \leq c$, esto es, (1) $a < b$ ó (2) $a = b$, y (3) $b < c$ ó (4) $b = c$.
De (1) y (3) resulta por O'2) que $a < c$, luego $a \leq c$. De (1) y (4) resulta que $a < c$ luego $a \leq c$. De (2) y (3) resulta $a < c$ luego $a \leq c$. De (2) y (4) resulta que $a = c$, luego $a \leq c$.

$\Rightarrow$) Supongamos que $a < b$ luego por D) resulta que $a \leq b$. Si $a = b$ entonces $a < a$, absurdo luego $a \neq b$.
$\Leftarrow$) Supongamos que (1) $a \leq b$ y (2) $a \neq b$, luego por D) $a < b$ ó (3) $a = b$, como (2) contradice a (3) tenemos que $a < b$. ■

El resultado precedente muestra que la noción de conjunto ordenado se puede definir de dos modos diferentes.

Observemos que si $(A, \leq)$ es un conjunto ordenado y X es una parte no vacía de A entonces $(X, \leq)$ es un conjunto ordenado.

Definición 1.1.3 *Si $(A, \leq)$ es un conjunto ordenado, $a, b \in A$ se dicen* **comparables** *y se nota $a \parallel b$ si $a \leq b$ ó $b \leq a$, caso contrario se dicen* **incomparables** *y se nota $a \nparallel b$.*

En el conjunto ordenado $(\mathbb{N}_0, \leq)$ los elementos 2 y 7 son comparables dado que $2 \leq 7$, pero en el conjunto ordenado $(\mathbb{N}_0, /)$ son incomparables dado que 2 no divide a 7 y 7 no divide a 2.

Definición 1.1.4 *Un conjunto ordenado A se dice* **una cadena, conjunto linealmente ordenado,** *ó* **totalmente ordenado** *si todo par de elementos de A es comparable.*

$(\mathbb{N}_0, \leq)$ y $(\mathbb{R}, \leq)$ son cadenas. Si $(A, \leq)$ es un conjunto ordenado, $X \subseteq A$, $X \neq \emptyset$ y $(X, \leq)$ es una cadena se dice que X es **cadena de** A. Por ejemplo, sabemos que $(\mathbb{N}_0, /)$ no es una cadena, pero el subconjunto $\{2, 4, 8\}$ es una cadena de $\mathbb{N}_0$ ya que $2/4$, $2/8$ y $4/8$.
Si $(A, \leq)$ es un conjunto ordenado y $a \in A$ entonces $\{a\}$ es una cadena de A y si $a, b \in A$ son tales que $a \leq b$ también $\{a, b\}$ es una cadena de A.

Definición 1.1.5 *Una parte L de un conjunto ordenado A se dice* **una parte libre de** *A, si dados dos elementos diferentes de L ellos son incomparables. También se suele decir que L es* **una anticadena de** *A. Si $L = A$ se dice que A es una anticadena.*

Ejemplo 1.1.2 *El conjunto $\{2, 3, 5\}$ es una anticadena del conjunto ordenado $(\mathbb{N}_0, /)$.*

1.2 Elementos especiales. Diagrama de Hasse

Un conjunto ordenado $(A, \leq)$ puede o no contener elementos con algunas de las propiedades que se indican a continuación.

Definición 1.2.1 *Un elemento m de un conjunto ordenado $(A, \leq)$ se dice* **un elemento máximo o maximal** *de A si:*

M) Si $x \in A$ es tal que $m \leq x$ entonces $x = m$.

Un elemento $m \in A$ se dice **un elemento mínimo o minimal** *de A si:*

m) Si $x \in A$ es tal que $x \leq m$ entonces $x = m$.

Ejemplo 1.2.1

1) Consideremos el conjunto ordenado $(\mathbb{N}_0, \leq)$, entonces 0 es elemento mínimo de $\mathbb{N}_0$. Este conjunto no tiene elementos máximos.

2) Es claro que $(\{x \in \mathbb{Z} : x \leq 0\}, \leq)$ es un conjunto ordenado, 0 es elemento máximo. Este conjunto no tiene elementos mínimos.

3) Sea $A = \{1, 2, 4, 8, 12\}$, como $A \subseteq \mathbb{N}_0$ entonces $(A, /)$ es un conjunto ordenado. ¿A tiene elementos máximos? Si en efecto, 12 y 8 son elementos máximos. Luego si un conjunto ordenado tiene un elemento máximo, en general, él no es único. El 1 es el único elemento mínimo de A.

4) En $(\mathbb{Z}, \leq)$ no existen elementos máximos ni mínimos.

Lema 1.2.1 *Todo conjunto ordenado finito $(A, \leq)$ tiene, por lo menos, un elemento mínimo (máximo).*

Dem. Por inducción sobre el número n de elementos de A. Si $n = 1$, el lema es evidentemente verificado.
Supongamos el lema verdadero para todo conjunto ordenado con k elementos, y sea $(A = \{x_1, x_2, \ldots, x_k, x_{k+1}\}, \leq)$, un conjunto ordenado, entonces por la hipótesis de inducción, el conjunto $X = \{x_1, x_2, \ldots, x_k\}$, tiene por lo menos un elemento mínimo x_t , $1 \leq t \leq k$. Además, $A = X \cup \{x_{k+1}\}$.
Probemos que si (1) $x_{k+1} \leq x_t$ entonces x_{k+1} es un elemento mínimo de A. En efecto sea (2) $a \in A$ tal que (3) $a \leq x_{k+1}$. De (2) resulta que (4) $a \in X$ ó (5) $a = x_{k+1}$. De (1) y (3) se deduce (6) $a \leq x_t$. Si ocurre (4), como $a, x_t \in X$ y x_t es un elemento mínimo de X tenemos (7) $a = x_t$. Luego de (3) y (7) resulta (8) $x_t \leq x_{k+1}$ y de (1) y (8) concluímos que $x_t = x_{k+1}$. Pero $x_t \in X$ y $x_{k+1} \notin X$. Por lo tanto, debe ocurrir (5), lo que prueba que x_{k+1} es minimal de A.
Si (9) $x_{k+1} \not\leq x_t$, veamos que x_t es minimal de A. En efecto, si $a \in A$ verifica (10) $a \leq x_t$ entonces por (9) $a \neq x_{k+1}$ y en consecuencia $a \in X$, por lo tanto, como x_t es minimal de X, de (10) resulta $a = x_t$. ■

Los conjuntos ordenados finitos pueden representarse por un diagrama denominado **diagrama de Hasse**.

Definición 1.2.2 *Sea* $(A, \leq)$ *un conjunto ordenado, se dice que el elemento* $b \in A$ **cubre** *al elemento* $a \in A$ *si*

1) $a < b$,

2) No existe ningún elemento $x \in A$ *tal que* $a < x < b$.

Ejemplo 1.2.2

1) En $(I\!N_0, \leq)$, 4 cubre a 3.

2) En $(I\!N_0, /)$, 4 cubre a 2, pués $2/4$ y no existe ningún $x \in I\!N_0$, $x \neq 2$, $x \neq 4$ tal que $2/x$ y $x/4$.

Dado un conjunto ordenado finito $(A, \leq)$, su diagrama de Hasse se construye de acuerdo con las siguientes reglas.

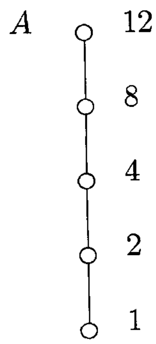
H1) Si $a \in A$, a será representado por un pequeño círculo, denominado **el afijo de** a.

H2) Si $b \in A$ cubre al elemento $a \in A$, el afijo de b se "coloca por arriba" del afijo de a.

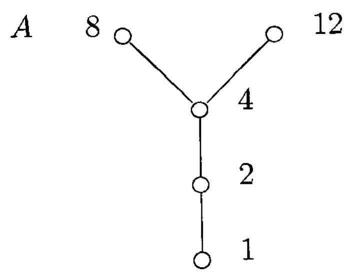
H3) Si $b \in A$ cubre al elemento $a \in A$, los afijos de a y b se unen por un segmento de extremos a y b.

Ejemplo 1.2.3

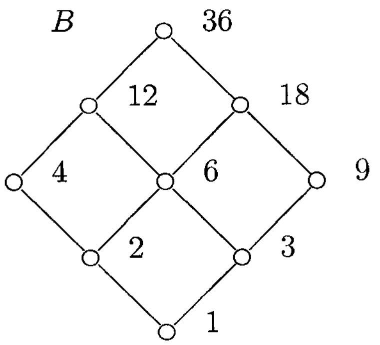
1) Sea $A = \{1, 2, 4, 8, 12\} \subseteq I\!N_0$, luego $(A, \leq)$ es un conjunto ordenado, que tiene por diagrama:



2) El conjunto ordenado $(A, /)$ tiene por diagrama:

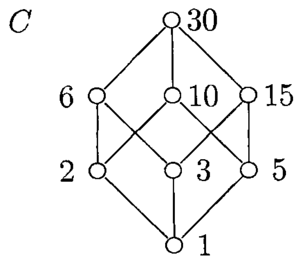


3) $B = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$ es el conjunto de los divisores naturales de 36. Luego $(B, /)$ es un conjunto ordenado que tiene por diagrama de Hasse:



Observemos que *mcd* $\{2, 3\} = 1$, *mcm* $\{2, 3\} = 6$, etc.

4) $C = \{1, 2, 3, 5, 6, 10, 15, 30\}$ es el conjunto de los divisores naturales de 30. Luego $(C, /)$ es un conjunto ordenado que tiene por diagrama de Hasse:



Ejercicio 1.2.1

Sea $D = \{1, 2, , 4, 6, 8, 10, 18, 28, 42, 50, 52, 70\}$. Luego $(D, /)$ es un conjunto ordenado. ¿ Cuál es su diagrama de Hasse?

El uso de diagramas de Hasse tiene su importancia, fundamentalmente en investigaciones teóricas.

Teorema 1.2.1 *Todo conjunto ordenado finito tiene un diagrama de Hasse.*
(G. Birkhoff, [7])

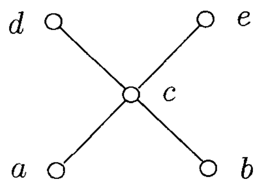
Dem. Por inducción sobre el número n de elementos del conjunto. Si $n = 1$ el teorema es evidentemente verdadero (su diagrama se reduce a un pequeño círculo). Supongamos que el teorema es válido para todos los conjuntos ordenados con $k-1$ elementos. Sea A un conjunto ordenado con k elementos. Como A es finito, entonces por el Lema 1.2.1 A tiene por lo menos un elemento máximo m. Entonces el conjunto ordenado $A' = A - \{m\}$ tiene $k - 1$ elementos y por la hipótesis de inducción tiene un diagrama de Hasse. Poniendo el afijo de m *"por arriba"* del diagrama de A' y uniendo el afijo de m con todos los afijos de elementos de A' a los cuales cubre m, eventualmente ninguno, obtenemos el diagrama de A. ■

Para dar ejemplos de conjuntos ordenados finitos basta dibujar diagramas de Hasse y el conjunto ordenado queda determinado en virtud del siguiente:

Lema 1.2.2 *Conocido el diagrama de Hasse de un conjunto ordenado A (finito) entonces el orden "$<$" de A queda unívocamente determinado por el diagrama correspondiente.* (G. Birkhoff, [7]).

Dem. Si $a, b \in A$, $a \neq b$ entonces $a < b \iff$ gráficamente es posible pasar del afijo de a al afijo de b por medio de segmentos ascendentes del diagrama, esto es $a < b \iff$ existe una sucesión $x_0, x_1, \ldots, x_n$ de elementos de A tales que $x_0 = a$, $x_n = b$ y el afijo de x_i está por arriba del afijo de x_{i-1}, para $i = 1, 2, \ldots, n$. ■

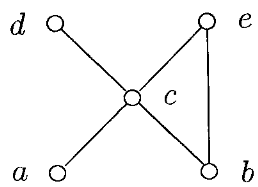
Ejemplo 1.2.4 *Dado el siguiente diagrama:*



La relación binaria está indicada en la siguiente tabla:

$<$	a	b	c	d	e
a			•	•	•
b			•	•	•
c				•	•
d					
e					

Observemos que la siguiente figura no es un diagrama de Hasse:



Definición 1.2.3 *Sea $(A, \leq)$ un conjunto ordenado. Se dice que un elemento $0 \in A$ es* **primer elemento** *de A si:*

$$0 \leq x, \quad \text{para todo } x \in A.$$

Se dice que un elemento $1 \in A$ es **último elemento** *de A si:*

$$x \leq 1, \quad \text{para todo } x \in A.$$

Lema 1.2.3 *Si un conjunto ordenado tiene primer (último) elemento este es único.*

Dem. Supongamos que p y p' son primer elemento de A, entonces:

$$(1)\ \ p \leq x, \qquad \text{para todo } x \in A, \text{ y } \quad (2)\ \ p' \leq x, \qquad \text{para todo } x \in A.$$

Luego como $p' \in A$, de (1) resulta (3) $p \leq p'$, y como $p \in A$, de (2) resulta (4) $p' \leq p$. De (3) y (4) se concluye por la propiedad antisimétrica que $p = p'$. En forma análoga se demuestra la unicidad del último elemento. ∎

Si un conjunto ordenado tiene primer (último) elemento es habitual notarlo A_0 (A_1), y si tiene primer y último elemento $A_{0,1}$.

Lema 1.2.4 *Si A es un conjunto ordenado, entonces*

1) *Si A tiene primer (último) elemento este es un elemento minimal (maximal).*

2) *Si A es finito y tiene un único elemento minimal (maximal) entonces él es el primer (último) elemento de A.*

3) *Si A es finito y no tiene primer (último) elemento entonces tiene más de un elemento minimal (maximal).*

Dem.

1) Sea 0 primer elemento de A, esto es $0 \leq x$ cualquiera que sea $x \in A$, luego si $x \leq 0$ entonces $x = 0$, por lo tanto 0, es minimal.

2) Sea m el único elemento minimal de A y supongamos que m no es primer elemento de A, esto es existe $x_0 \in A$ tal que $m \not\leq x_0$, por lo tanto, $m \not< x_0$ y (1) $m \neq x_0$. De (1) y la hipótesis resulta que x_0 no es minimal, luego como A es finito existe un elemento minimal que lo precede, y como existe un único minimal, debe ser $m < x_0$, absurdo.

3) Como A es finito tiene elementos minimales. Si tuviese un único elemento minimal m entonces por 2) m sería primer elemento de A, absurdo.

∎

Definición 1.2.4 *Dado un conjunto ordenado A con primer elemento 0 se dice que $a \in A$ es* **un átomo** *de A si "a" cubre a "0," esto es, $0 < a$ y no existe $x \in A$ tal que $0 < x < a$.*

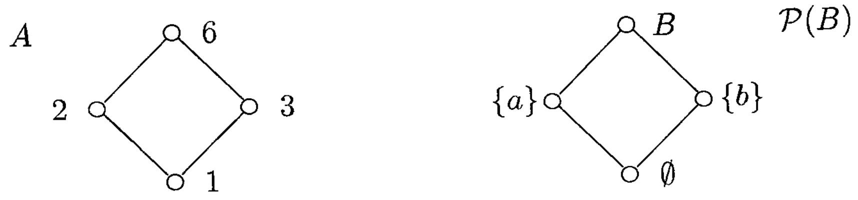
Sea E un conjunto no vacío, luego $(\mathcal{P}(E), \subseteq)$ es un conjunto ordenado.

1) ¿ Este conjunto tiene átomos? ¿Cúales son?
$\emptyset$ es el primer elemento de este conjunto ordenado. Los conjuntos $\{x\}$, donde $x \in E$ son átomos de $\mathcal{P}(E)$, dado que no existe $Y \in \mathcal{P}(E)$ tal que $\emptyset \subset Y \subset \{x\}$. Estos elementos son los únicos átomos de $\mathcal{P}(E)$, dado que si $X \subseteq E$ tiene más de un elemento entonces $\emptyset \subset X \setminus \{p\} \subset X$, con $p \in X$.

2) ¿Todo conjunto ordenado finito con primer elemento, siempre tiene átomos? No, por ejemplo si el conjunto tiene un sólo elemento.

1.3 Isomorfismos e involuciones

Consideremos el conjunto $A = \{1, 2, 3, 6\}$ ordenado por la relación divide y el conjunto ordenado $(\mathcal{P}(B), \subseteq)$, donde $B = \{a, b\}$. Tenemos así dos conjuntos ordenados cuyos diagramas de Hasse se indican a continuación:



Los conjuntos A y $\mathcal{P}(B)$ están formados por elementos de naturaleza diferente, pero sus diagramas de Hasse son *semejantes.*

Definición 1.3.1 *Sean $(A, \leq)$, $(A', \leq')$ conjuntos ordenados. A toda función suryectiva $f : A \rightarrow A'$ que verifica:*

I1) Si $x, y \in A$ verifican $x \leq y$ entonces $f(x) \leq' f(y)$,

I2) Si $x, y \in A$ son tales que $f(x) \leq' f(y)$ entonces $x \leq y$,

daremos el nombre de **isomorfismo** *(de orden) de A sobre A' y notaremos $A' \cong A$.*

Observemos que todo isomorfismo es una función inyectiva. En efecto si $f(x) = f(y)$ entonces $f(x) \leq' f(y)$ y $f(y) \leq' f(x)$, de donde resulta por I2) que $x \leq y$ e $y \leq x$, y por lo tanto, $x = y$.

Definición 1.3.2 *A toda función $f : A \rightarrow A'$ que verifica la condición I1) se denomina* **isótona** *o* **monótona**. *Esto es, respeta el orden de ambos conjuntos.*

Consideremos los conjuntos ordenados indicados anteriormente y pongamos $f(1) = \emptyset$, $f(2) = \{a\}$, $f(3) = \{b\}$, $f(6) = \{a, b\}$. Es fácil ver que f es un isomorfismo de A sobre $\mathcal{P}(B)$.

Lema 1.3.1 *Si A, B y C son conjuntos ordenados, entonces:*

1) $A \cong A$.

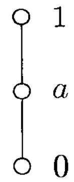
2) Si $A \cong B$, entonces $B \cong A$.

3) Si $A \cong B$, y $B \cong C$, entonces $A \cong C$.

Definición 1.3.3 *Dos conjuntos ordenados A y B se dicen* **isomorfos** *si existe un isomorfismo de uno de ellos sobre el otro.*
Un isomorfismo de un conjunto ordenado A sobre el mismo se denomina un **automorfismo.**

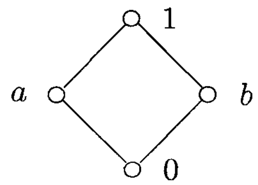
Ejemplo 1.3.1 *1) Es claro que si A es un conjunto ordenado entonces la transformación identidad, $e(x) = x$, $\forall x \in A$, es un automorfismo, denominado automorfismo trivial.*

2) Consideremos el conjunto ordenado A cuyo diagrama de Hasse indicamos a continuación:



Vamos a demostrar que el único automorfismo que admite es el trivial. En efecto: si f es un automorfismo de A entonces (1) f es una función suryectiva. Como $x \leq 1$, $\forall x \in A$ entonces (2) $f(x) \leq f(1)$, $\forall x \in A$. De (1) y (2) resulta que $f(1)$ es el último elemento de A y en consecuencia $f(1) = 1$. Análogamente de $0 \leq x$, $\forall x \in A$ se deduce que $f(0) = 0$. Por lo tanto como f es inyectiva debe ser $f(a) = a$.

3) Consideremos el conjunto ordenado B cuyo diagrama de Hasse se indica:



Es fácil verificar que la función f definida por : $f(0) = 0$, $f(1) = 1$, $f(a) = b$, $f(b) = a$, es un automorfismo no trivial.

Definición 1.3.4 *Sean $(A, \leq)$, $(A', \leq')$ conjuntos ordenados. A toda función suryectiva $f : A \to A'$ que verifica:*

A1) Si $x, y \in A$ verifican $x \leq y$ entonces $f(y) \leq' f(x)$,

A2) Si $x, y \in A$ son tales que $f(x) \leq' f(y)$ entonces $y \leq x$,

daremos el nombre de **antiisomorfismo** *(de orden) de A sobre A'.*

Es claro todo antiisomorfismo es una función inyectiva.

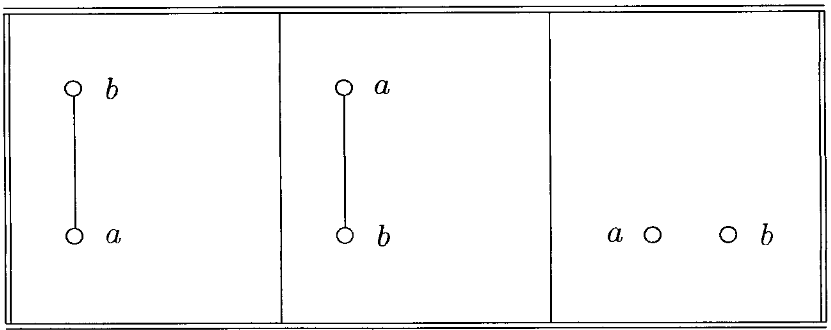
Definición 1.3.5 *A toda función $f : A \to A'$ que verifica la condición A1) se denomina* **antítona** *o* **antimonótona**.
A todo antiisomorfismo de A sobre A se denomina **antiautomorfismo** *de A.*

Consideremos el conjunto ordenado B indicado en el ejemplo 1.3.1, 3) entonces la función f definida por : $f(0) = 1$, $f(1) = 0$, $f(a) = b$, $f(b) = a$, es un antiautomorfismo de A.

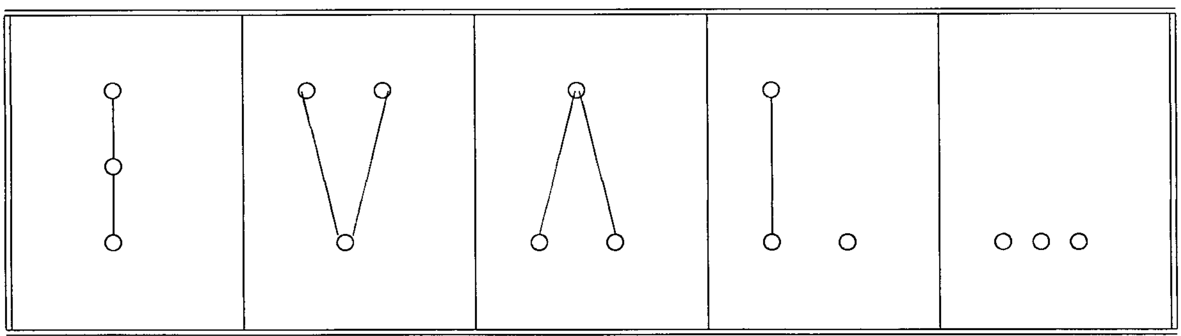
Si A y B son los conjuntos ordenados cuyos diagramas se indican, entonces el conjunto de todas las funciones isótonas de A en B está indicado en la tabla siguiente.

f	a	b	c
f_1	0	0	0
f_2	0	0	1
f_3	0	1	0
f_4	0	1	1
f_5	1	1	0
f_6	1	1	1

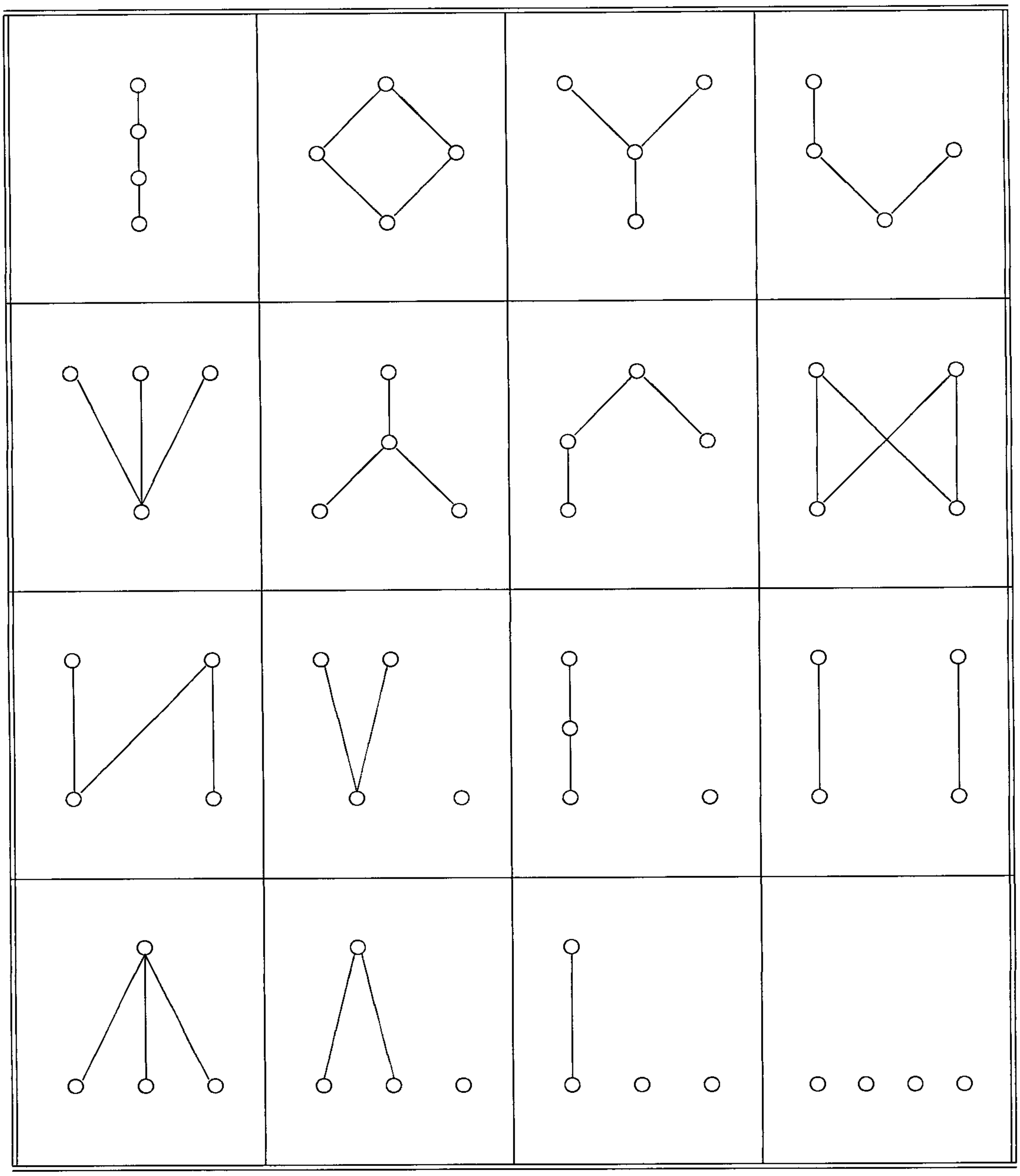
Es claro que sobre un conjunto con un sólo elemento solamente se puede definir una única relación de orden. Si el conjunto tiene 2 elementos entonces se pueden definir 3 relaciones de orden, cuyos diagramas se indican a continuación:



Si el conjunto tiene 3 elementos entonces se pueden definir 19 relaciones de orden, 5 de las cuales no son isomorfas entre si y cuyos diagramas se indican:

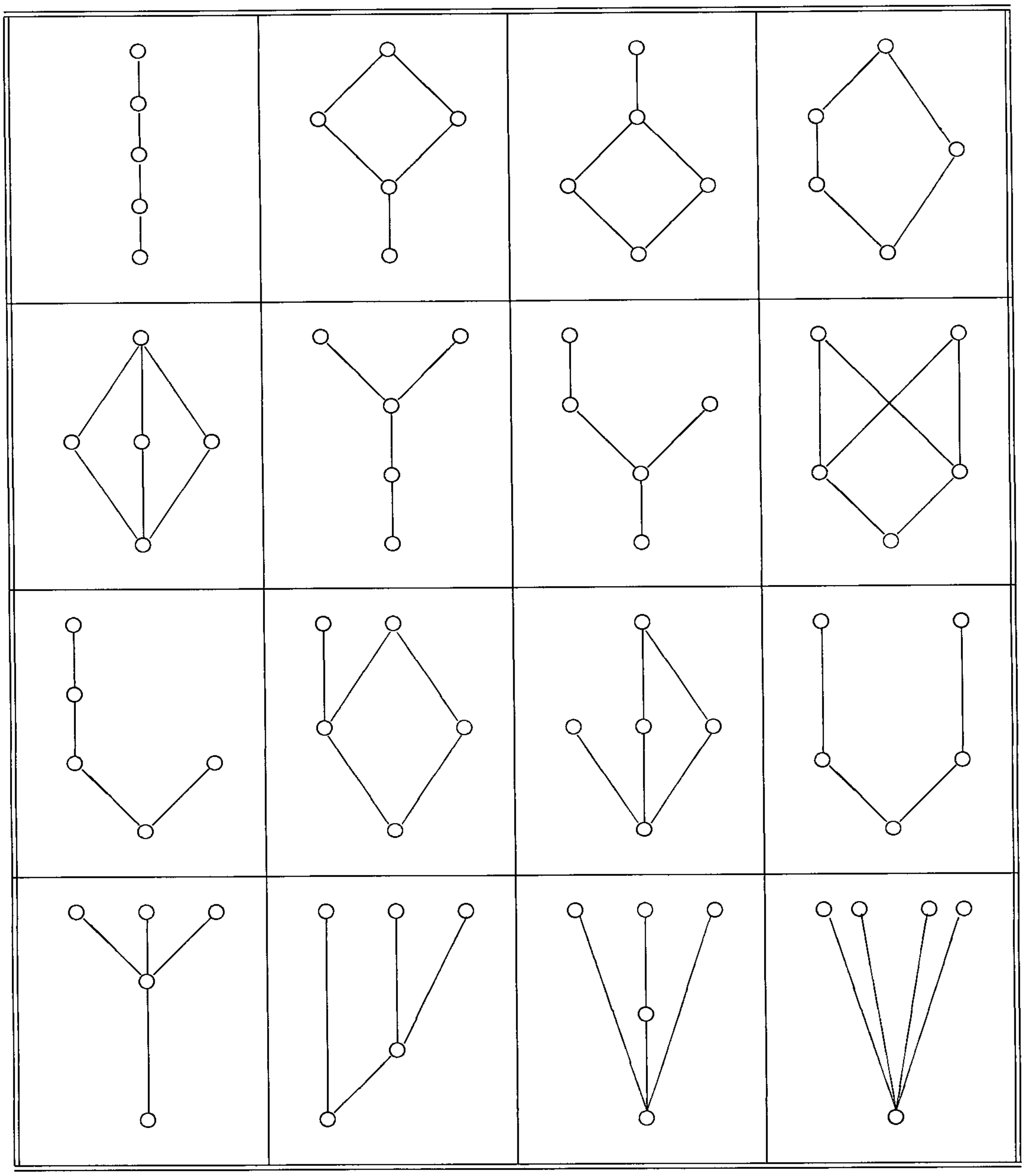


Si el conjunto tiene 4 elementos entonces se pueden definir 219 relaciones de orden, de las cuales 16 no son isomorfas entre si y cuyos diagramas se indican:

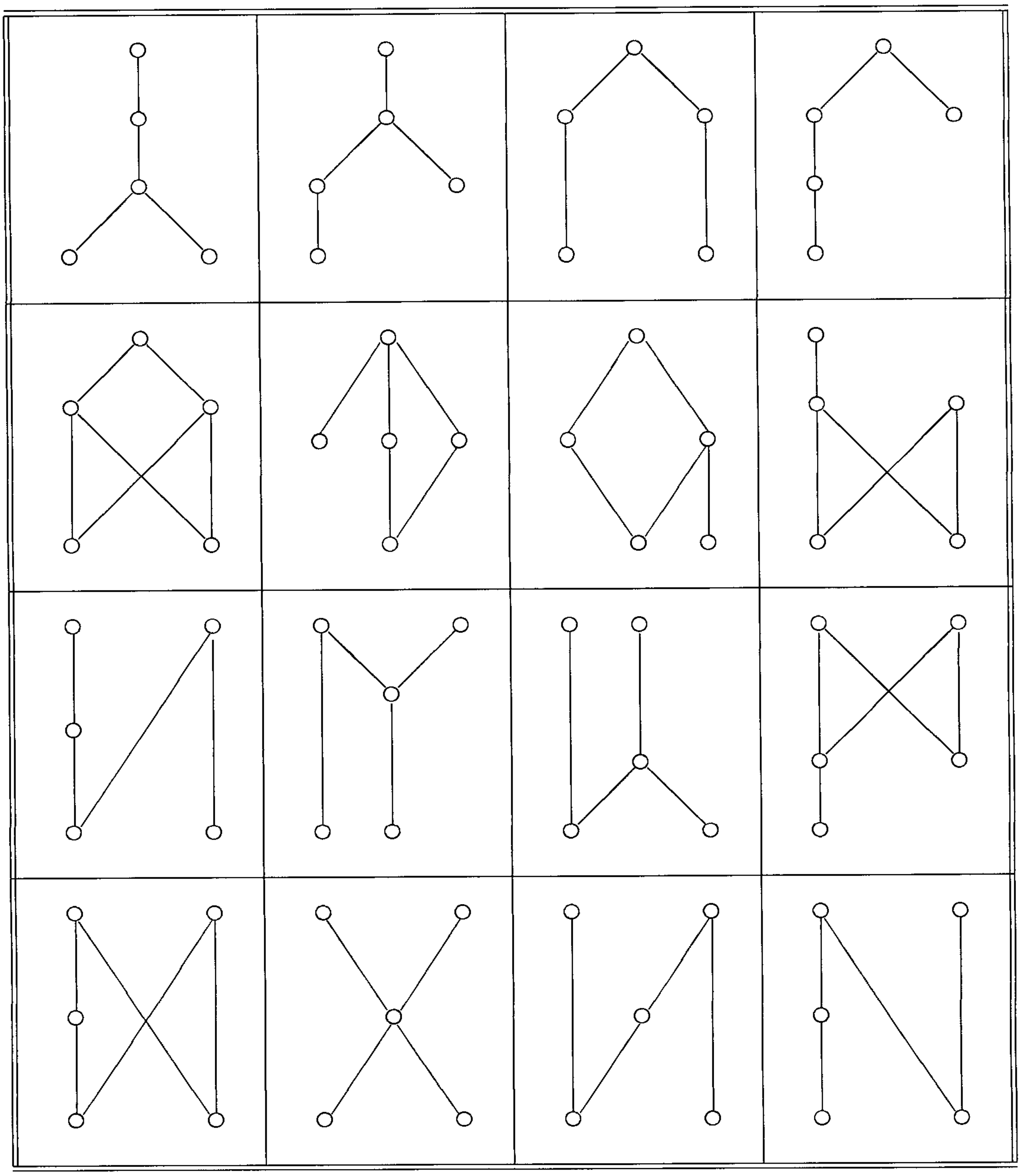


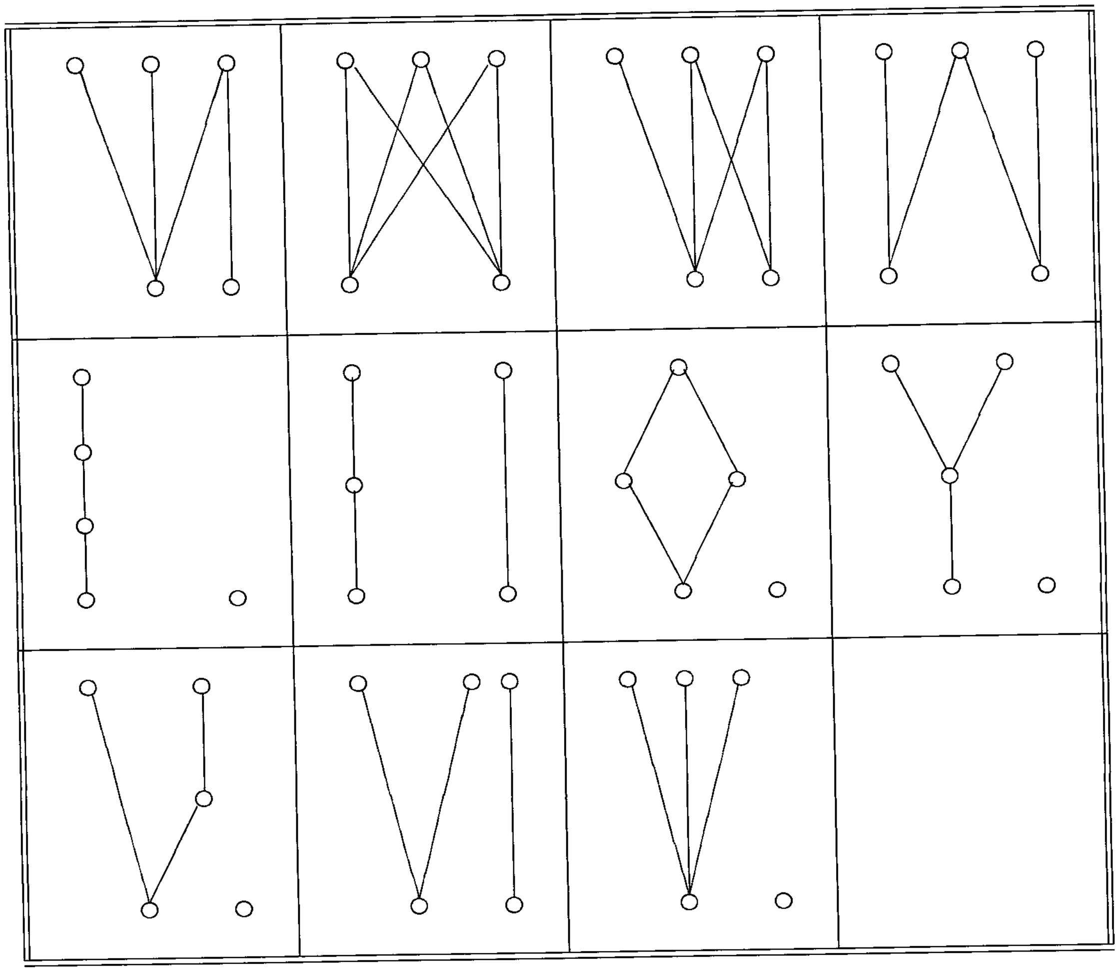
Si el conjunto tiene 5 elementos entonces se pueden definir 4.231 relaciones de orden, de las cuales 63 no son isomorfas entre si y cuyos diagramas se indican:

Conjuntos ordenados con 5 elementos y 1 minimal:

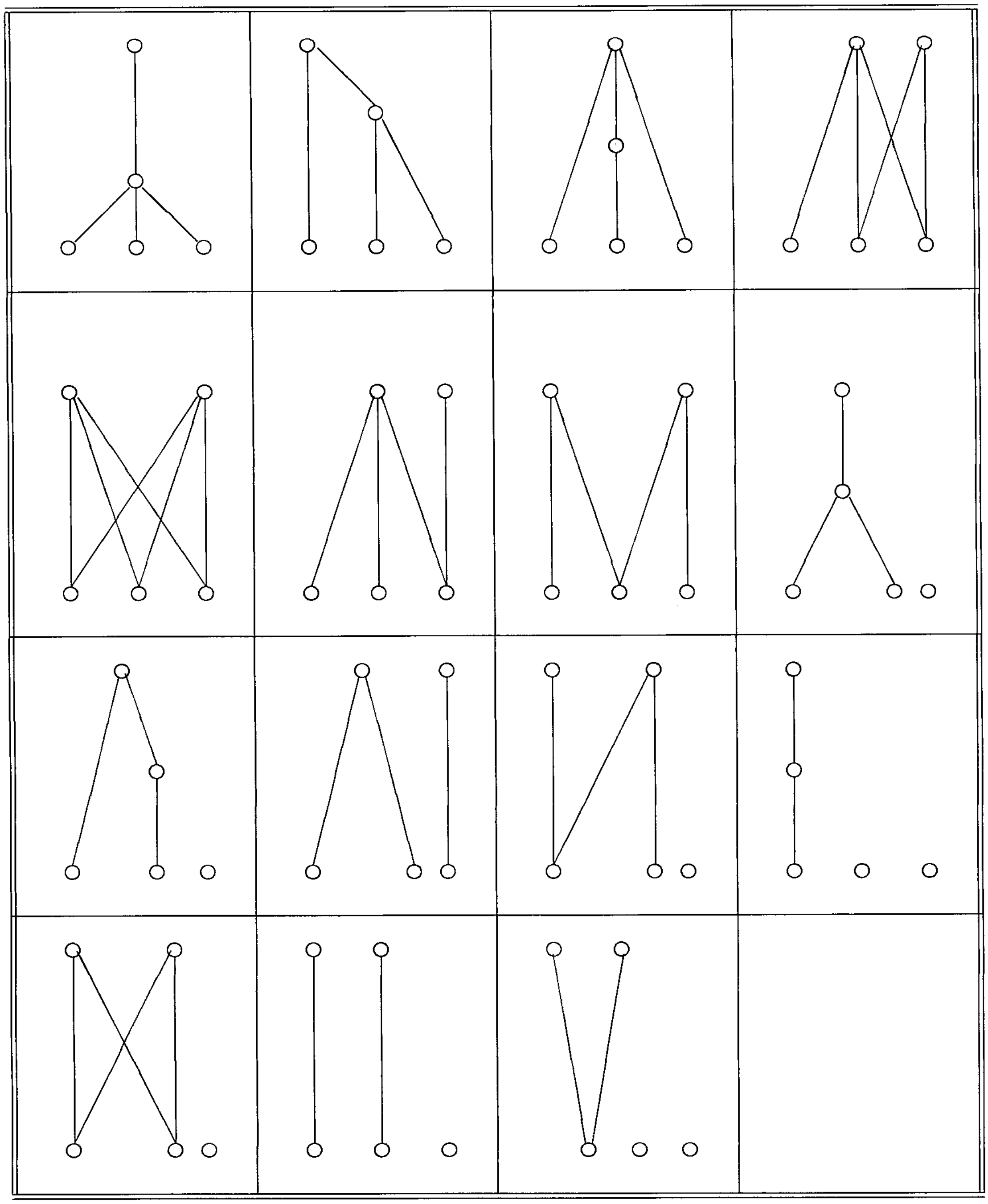


Conjuntos ordenados con 5 elementos y 2 elementos minimales

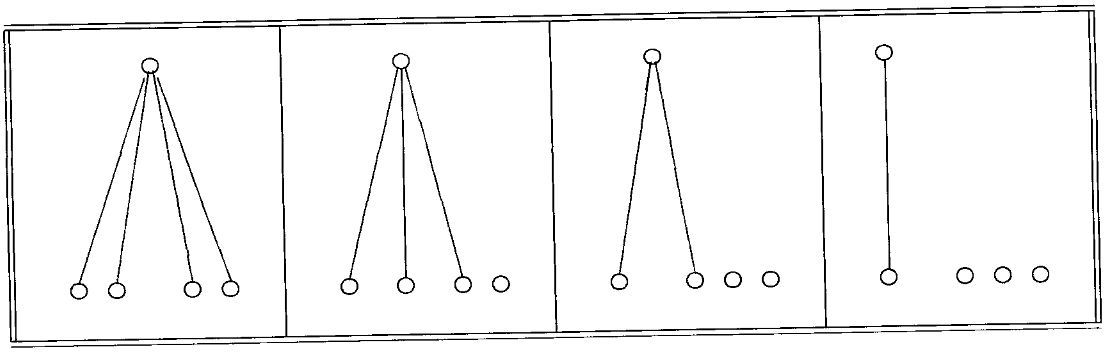




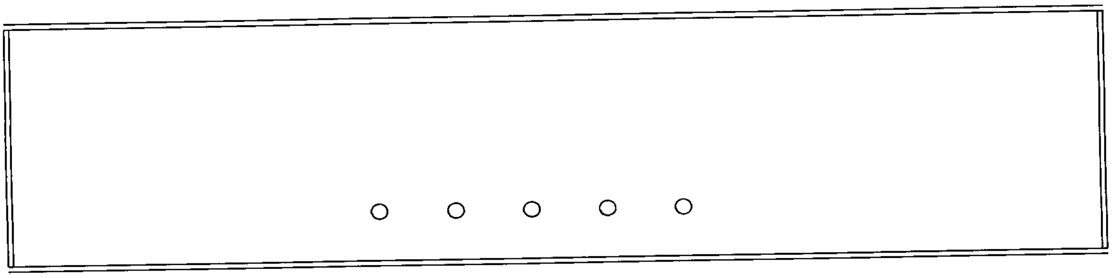
Conjuntos ordenados con 5 elementos y 3 elementos minimales



Conjuntos ordenados con 5 elementos y 4 elementos minimales



Conjunto ordenado con 5 elementos y 5 elementos minimales



Si un conjunto tiene n elementos, no se conoce una fórmula en función de n que indique el número de relaciones de orden que se pueden definir sobre el mismo, como así tampoco el número de relaciones de orden no isomorfas.

A continuación indicamos una tabla con los resultados conocidos, ver por ejemplo: [7], [8], M. Erné and K. Stege *Counting finite posets and topologies*, Order 8, (1991), 247-265:

n	Nro. de Ordenes
1	1
2	3
3	19
4	219
5	4.231
6	130.023
7	6.129.859
8	431.723.379
9	44.511.042.511
10	6.611.065.248.783
11	1.396.281.677.105.899
12	414.864.951.055.853.499
13	171.850.728.381.587.059.351
14	98.484.324.257.128.207.032.183

n	Nro. de Ordenes no isomorfos
1	1
2	2
3	5
4	16
5	63
6	318
7	2.045
8	16.999
9	183.231
10	2.567.284
11	46.749.427
12	1.104.891.746
13	33.823.827.452

ver: C. Chaunier and N. Lygerõs, *The number of orders with thirteen elements*, Order 9, (1992), 203-204.

Ejercicio 1.3.1 *Si X es un conjunto finito con n elementos, notaremos $N[X] = n$. Sea $I_n = \{1, 2, \ldots, n\}$, se denomina* **sustitución** *de orden n a toda biyección de I_n. Al conjunto de todas las sustituciones de orden n se lo representa por S_n, que se denomina* **grupo simétrico**. *Es bien conocido que $N[S_n] = n!$. Dada $f \in S_n$ pongamos por definición: $a \sqsubseteq_f b \iff a \leq b$ y $f^{-1}(a) \leq f^{-1}(b)$, donde $a, b \in I_n$ y $\leq$ indica el orden natural de I_n.*

1) *Probar que $\sqsubseteq_f$ es una relación de orden.*

2) *Probar que si $f \in S_n$ entonces $(I_n, \sqsubseteq_f)$ y $(I_n, \sqsubseteq_{f^{-1}})$ son conjuntos ordenados isomorfos.*

1.4 Representación de conjuntos ordenados

Hemos visto que si X es un conjunto, no vacío, entonces $(\mathcal{P}(X), \subseteq)$ es un conjunto ordenado.

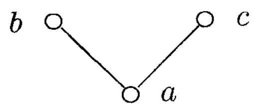
Lema 1.4.1 *Todo conjunto ordenado $(A, \leq)$ es isomorfo a una familia de conjuntos ordenada por la relación de inclusión.*

Dem. Dado $x \in A$, sea $A_x = \{y \in A : y \leq x\}$. Entonces tenemos que: (1) $A_x \neq \emptyset$, $\forall x \in A$, ya que $x \in A_x$ y (2) $A_x \subseteq A$, $\forall x \in A$.
Sea $\mathcal{A} = \{A_x\}_{x \in A}$, como $(\mathcal{P}(A), \subseteq)$ es un conjunto ordenado y $\mathcal{A} \subseteq \mathcal{P}(A)$ entonces $(\mathcal{A}, \subseteq)$, es un conjunto ordenado. Pongamos:

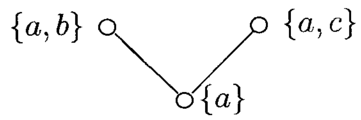
$$f(x) = A_x, \ \forall x \in A,$$

entonces f es una función de A sobre $\mathcal{A}$.
Sean $x, y \in A$ tales que (1) $x \leq y$, luego si $z \in f(x) = A_x$, esto es, (2) $z \leq x$. De (1) y (2) resulta $z \leq y$ esto es $z \in A_y = f(y)$. Acabamos así de probar que $f(x) \subseteq f(y)$.
Supongamos ahora que $x, y \in A$ son tales que $A_x = f(x) \subseteq f(y) = A_y$, entonces como $x \in A_x$ tenemos que $x \in A_y$ esto es $x \leq y$. ■

Ejemplo 1.4.1 *Sea A el conjunto ordenado cuyo diagrama de Hasse se indica.*



Entonces $A_a = \{a\}$, $A_b = \{a, b\}$, $A_c = \{a, c\}$. Estos subconjuntos de A ordenados por inclusión tiene el siguiente diagrama:



1.5 Conjunto ordenado dual

Dada una relación binaria R sobre un conjunto A se denomina **relación dual** ó **inversa** de R a la relación binaria R^* definida del siguiente modo:

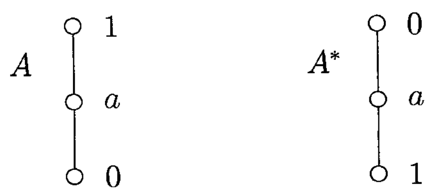
$$x\, R^*\, y \iff y\, R\, x$$

esto es $(x, y) \in R^* \iff (y, x) \in R$.
La relación dual de la relación "divide a" se denomina "es múltiplo de", la relación dual de "contenido" ($\subseteq$) se denomina "contiene a" ($\supseteq$) y la relación dual de "menor o igual" ($\leq$) se denomina "mayor o igual " ($\geq$). Es claro que:

Lema 1.5.1 *La relación dual de una relación de orden es una relación de orden.*

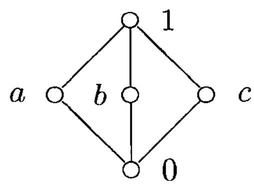
Se denomina **dual** de un conjunto ordenado $(A, \leq)$ al conjunto ordenado $(A, \leq^*)$ donde con $\leq^*$ indicamos la relación dual de $\leq$. También notaremos $\geq$ en vez de $\leq^*$. Para simplificar la notación, notaremos con A^* al dual del conjunto ordenado A. Es claro que $(A^*)^* \cong A$. Un conjunto ordenado A se dice **autodual** si es isomorfo a su dual.

Ejemplo 1.5.1 *El siguiente conjunto ordenado es autodual.*

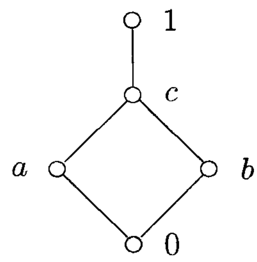


Definición 1.5.1 *Sea $(A, \leq)$ un conjunto ordenado, con último elemento 1. Se dice que $b \in A$ es* **un átomo dual** *de A si "1" cubre a "b", esto es, $b < 1$ y no existe $x \in A$ tal que $b < x < 1$.*

Ejemplo 1.5.2 *1) En el siguiente conjunto ordenado, los elementos a, b y c son átomos duales del mismo, y también átomos.*



2) El único átomo dual del siguiente conjunto ordenado es el elemento c



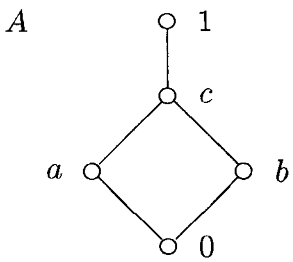
Es claro que si un teorema es válido en un conjunto ordenado también es válido si cambiamos entre si los símbolos $\leq$ y $\geq$ en el enunciado.

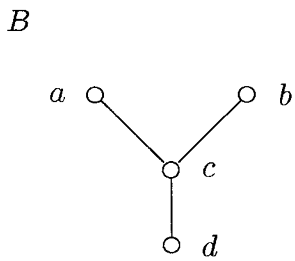
1.6 Cotas superiores e inferiores

Definición 1.6.1 *Sea $(A, \leq)$ un conjunto ordenado. Un elemento $c \in A$ se dice* **una cota superior** *o* **un mayorante** *de un subconjunto, no vacío, X de A si:*

$$x \leq c, \quad \forall\, x \in X.$$

Ejemplo 1.6.1 *Consideremos los conjuntos ordenados, cuyos diagramas se indican a continuación:*





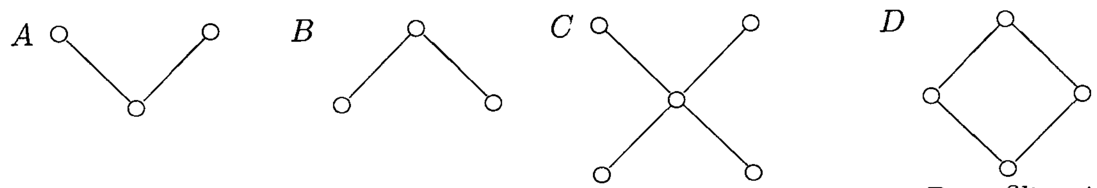
Si $X = \{a, b\} \subseteq A$ entonces c y 1 son cotas superiores de X. El subconjunto $Y = \{a, b\}$ de B no tiene cotas superiores.

En forma análoga se define la noción de **una cota inferior** o **minorante** de un subconjunto, no vacío. En los ejemplos anteriores 0 es una cota inferior de X y c y d son cotas inferiores de Y.

Definición 1.6.2 *Un conjunto ordenado A se dice* **filtrante superiormente** *si todos los subconjuntos de A con 2 elementos tienen una cota superior.*

En forma análoga se define el concepto de **filtrante inferiormente**.

Ejemplo 1.6.2 *Consideremos los conjuntos ordenados cuyos diagramas se indican:*



Entonces A es filtrante inferiormente, pero no lo es superiormente, B es filtrante superiormente, pero no lo es inferiormente, C no es filtrante superiormente ni inferiormente y D es filtrante superiormente e inferiormente.

Definición 1.6.3 *Si $(A, \leq)$ es un conjunto ordenado, una parte X de A se denomina* **sección superior** *de A si:*

$$X = \emptyset \qquad \text{ó} \qquad \text{Si } a \in X, \text{ y } a \leq b \text{ entonces } b \in X.$$

Por ejemplo, si A es un conjunto ordenado y $a \in A$ entonces el conjunto

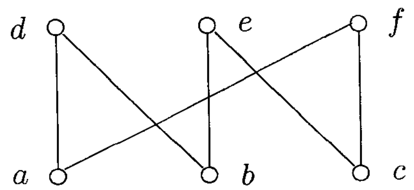
$$[a) = \{x \in A : a \leq x\}$$

es una sección superior, que se suele denominar **sección superior generada por** a. Análogamente se define el concepto de **sección inferior**. Si $a \in A$ el conjunto

$$(a] = \{x \in A : x \leq a\}$$

es una sección inferior, que se suele denominar **sección inferior generada por** a.

Ejercicio 1.6.1 *Determinar las secciones superiores* (son 18) *del conjunto ordenado cuyo diagrama se indica:*



Definición 1.6.4 *Si $(A, \leq)$ es un conjunto ordenado, y $a, b \in A$ verifican $a \leq b$ se denomina:*

- **segmento** *al conjunto* $[a, b] = \{x \in A : a \leq x \leq b\}$,
- **intervalo** *al conjunto* $(a, b) = \{x \in A : a < x < b\}$,
- **intervalo semiabierto a izquierda o segmento cerrado a derecha** *al conjunto* $(a, b] = \{x \in A : a < x \leq b\}$,
- **intervalo semiabierto a derecha o segmento cerrado a izquierda** *al conjunto* $[a, b) = \{x \in A : a \leq x < b\}$.

1.7 Producto cartesiano de conjuntos ordenados

Dada una familia de conjuntos ordenados $\{(A_i, \leq_i)\}_{i\in I}$, sea $A = \prod_{i\in I} A_i$ el producto cartesiano de la familia de conjuntos $\{A_i\}_{i\in I}$, esto es, el conjunto de todas las funciones $x : I \to \bigcup_{i\in I} A_i$ tales que en cada elemento $i \in I$ toman un valor $x(i) = x_i \in A_i$. Se dice que x_i es la coordenada de indice i del elemento $x \in A$ y se nota $x = [x_i]_{i\in I}$, $x = [x_i]$, $x = (x_i)_{i\in I}$ ó $x = (x_i)$.
Dados $x = (x_i)_{i\in I} \in A$, $y = (y_i)_{i\in I} \in A$, pongamos por definición:

$$x \leq y \iff x(i) \leq_i y(i), \ \forall \ i \in I.$$

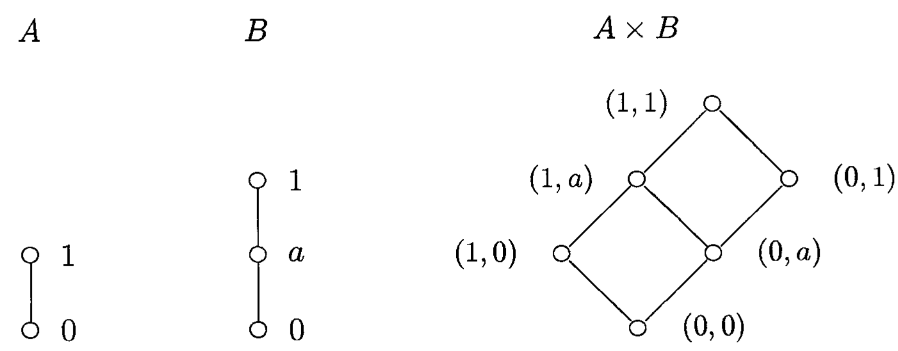
Se prueba sin dificultad que la relación binaria definida precedentemente es una relación de orden definida sobre A, por lo tanto $(A, \leq)$ es un conjunto ordenado al que se denomina **producto cartesiano** o **directo** de la familia de conjuntos ordenados $\{(A_i, \leq_i)\}_{i\in I}$. A veces se suele escribir $(A, \leq) = \prod_{i\in I}(A_i, \leq_i)$. Cada uno de los conjuntos A_i recibe el nombre de **i-ésimo eje de coordenadas** ó **i-ésimo eje** .
Para cada $i \in I$, la función $p_i : \prod_{i\in I} A_i \to A_i$, definida por $p_i(x) = x_i$ se denomina **proyección i-ésima**. Es claro que p_i es una función suryectiva e isótona.

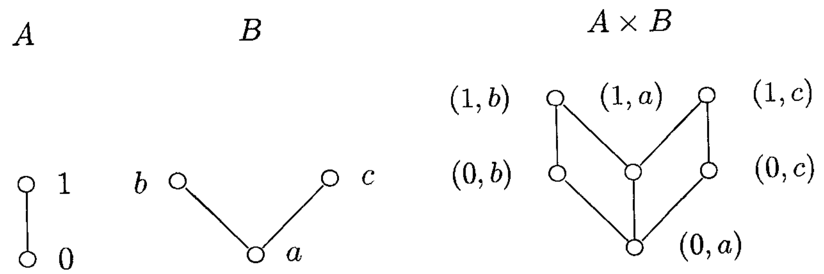
Si $A_i = C$, $\forall \ i \in I$, entonces $\prod_{i\in I} A_i$ es el conjunto de todas las funciones de I en C, por ello se nota C^I. Si el conjunto I es finito, por ejemplo $I = \{1, 2, \ldots, n\}$ entonces se utiliza cualquiera de las notaciones siguientes:

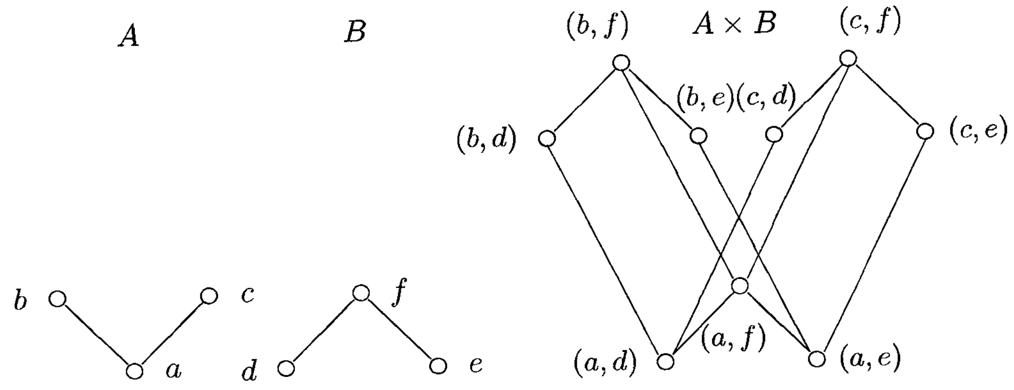
$$\prod_{i=1}^{n} A_i \qquad \text{ó} \qquad A_1 \times A_2 \times \ldots \times A_n$$

En este caso, si $x \in \prod_{i=1}^{n} A_i$ entonces: $x = (x(1), x(2), \ldots, x(n)) = (x_1, x_2, \ldots, x_n)$.
Es claro que $A_1 \times A_2 \neq A_2 \times A_1$, pero $A_1 \times A_2$ y $A_2 \times A_1$ son conjuntos ordenados isomorfos. Tambien se prueba sin dificultad que $A_1 \times (A_2 \times A_3) \cong (A_1 \times A_2) \times A_3$ y que $(A \times B)^* = A^* \times B^*$.
Observemos que si A, B son conjuntos ordenados y a es un elemento fijo de A entonces el subconjunto $\{(a, y) : y \in B\}$ de $A \times B$ es un conjunto ordenado isomorfo a B y si b es un elemento fijo de B entonces el subconjunto $\{(x, b) : x \in A\}$ de $A \times B$ es un conjunto ordenado isomorfo a A.

Ejemplo 1.7.1 *Para cada par de conjuntos ordenados dados por sus diagramas de Hasse, indicamos el diagrama de Hasse del producto cartesiano de los mismos.*







Ejercicio 1.7.1 *Si $A_1, A_2, \ldots A_n$ son conjuntos ordenados y $A = \prod_{i=1}^{n} A_i$, ¿Cuál es la condición necesaria y suficiente para que $(y_1, y_2, \ldots, y_n) \in A$ cubra a $(x_1, x_2, \ldots, x_n) \in A$?*

1.8 Suma cardinal de conjuntos ordenados

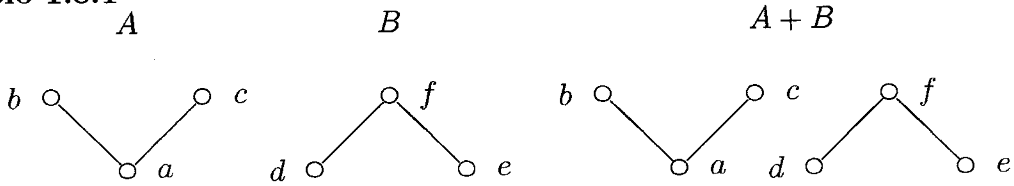
Observación 1.8.1 *Dados dos conjuntos ordenados $(A, \leq_1)$, $(B, \leq_2)$ donde $A \cap B \neq \emptyset$, sean u, v elementos tales que $u \neq v$. Como $\{u\}$ y $\{v\}$ son conjuntos ordenados, podemos considerar los conjuntos ordenados $A' = A \times \{u\}$ y $B' = B \times \{v\}$. Entonces es claro que $A' \cap B' = \emptyset$, dado que $u \neq v$. Si ponemos por definición $f(a) = (a, u)$, $\forall a \in A$, entonces se prueba sin dificultad que f establece un isomorfismo entre A y A'. Análogamente B es isomorfo a B'.*

Dados dos conjuntos ordenados $(A, \leq_1)$, $(B, \leq_2)$ tales que $A \cap B = \emptyset$, consideremos el conjunto $C = A \cup B$ y definamos sobre C la siguiente relación:
Dados $c, d \in C$

$$c \leq d \iff \begin{cases} c, d \in A \quad \text{y} \quad c \leq_1 d \\ \text{ó} \\ c, d \in B \quad \text{y} \quad c \leq_2 d \end{cases}$$

Es claro que "$\leq$" es una relación de orden definida sobre C, por lo tanto $(C, \leq)$ es un conjunto ordenado, al cual se dá el nombre de **suma cardinal de** A y B, y se nota $C = A + B$. A y B se denominan las **componentes** de la suma cardinal de los dos conjuntos ordenados. Es claro de acuerdo a la definición precedente que si $a \in A$ y $b \in B$ entonces a y b no estan relacionados por "$\leq$" en C, y que además si A y B son finitos, el diagrama de Hasse de C se obtiene colocando el diagrama de B *al lado* del diagrama de A.

Ejemplo 1.8.1



Lema 1.8.1 *La suma cardinal tiene las siguientes propiedades:*

1) $A + B \cong B + A$.

2) $(A + B) + C \cong A + (B + C)$.

3) $A \times (B + C) \cong (A \times B) + (A \times C)$.

4) $(A + B)^* = A^* + B^*$.

Observemos que si A y B son conjuntos ordenados, no disjuntos, entonces la suma cardinal de los mismos se define por $A' + B'$, donde A' y B' son conjuntos ordenados disjuntos, isomorfos respectivamente a A y B, (ver observación 1.8.1).

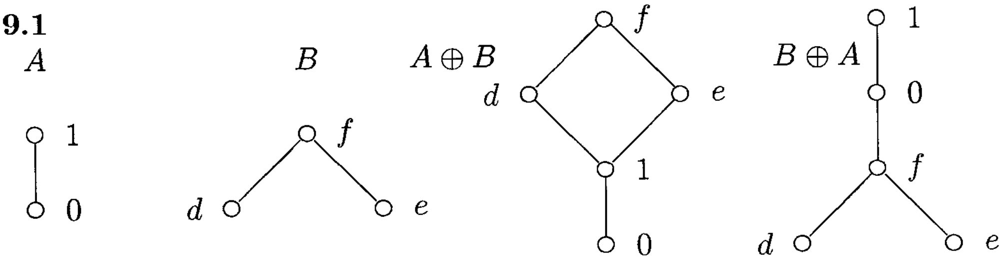
1.9 Suma ordinal de conjuntos ordenados

Dados dos conjuntos ordenados $(A, \leq_1)$, $(B, \leq_2)$ tales que $A \cap B = \emptyset$, consideremos el conjunto $C = A \cup B$ y definamos sobre C la siguiente relación:
Dados $c, d \in C$

$$c \leq d \iff \begin{cases} & c \in A \quad \text{y} \quad d \in B \\ \text{ó} & c, d \in A \quad \text{y} \quad c \leq_1 d \\ \text{ó} & c, d \in B \quad \text{y} \quad c \leq_2 d \end{cases}$$

Es claro que "$\leq$" es una relación de orden definida sobre C, por lo tanto $(C, \leq)$ es un conjunto ordenado, al cual se dá el nombre de **suma ordinal de** A y B, y se nota $C = A \oplus B$.

Ejemplo 1.9.1



El ejemplo precedente nos muestra que la suma ordinal no es, en general, conmutativa.

Lema 1.9.1 *La suma ordinal tiene las siguientes propiedades:*

1) $(A \oplus B) \oplus C \cong A \oplus (B \oplus C)$.

2) $(A \oplus B)^* \cong B^* \oplus A^*$.

Observemos que si A y B son conjuntos ordenados, no disjuntos, entonces la suma ordinal de los mismos se define por $A' \oplus B'$, donde A' y B' son conjuntos ordenados disjuntos, isomorfos respectivamente a A y B. (ver observación 1.8.1).

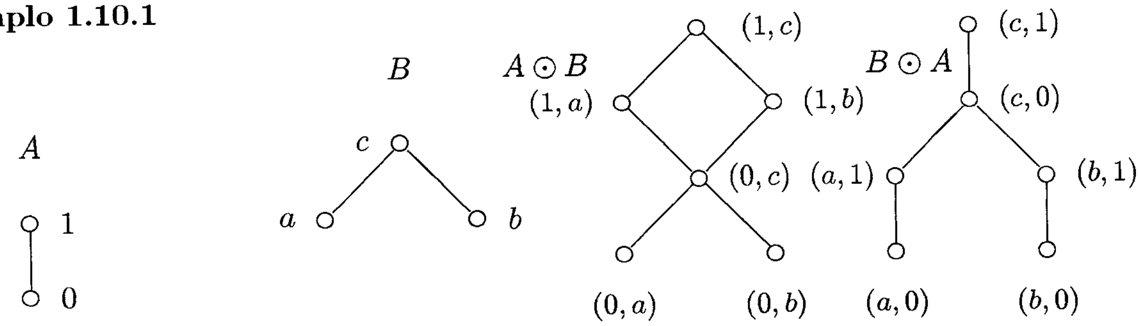
1.10 Producto ordinal de conjuntos ordenados

Dados dos conjuntos ordenados $(A, \leq_1)$, $(B, \leq_2)$ tales que $A \cap B = \emptyset$, consideremos el conjunto $C = A \times B$ y definamos sobre C la siguiente relación, dados (x, y), $(z, w) \in C$

$$(x,y) \leq (z,w) \iff \begin{cases} x <_1 z \\ \text{ó} \\ x = z \quad \text{e} \quad y \leq_2 w \end{cases}$$

Es fácil ver que "$\leq$" es una relación de orden definida sobre C, por lo tanto $(C, \leq)$ es un conjunto ordenado, al cual se dá el nombre de **producto ordinal de** A por B, y se nota $C = A \odot B$.
Observemos que para cada elemento $x_0 \in A$, el conjunto de los pares $\{(x_0, y)\}_{y \in B} \subseteq A \times B$ es un conjunto ordenado isomorfo a B, luego para el caso en que A y B son finitos el diagrama de B *se repite* en el diagrama de $A \odot B$ tantas veces como elementos tiene A.

Ejemplo 1.10.1



El ejemplo precedente nos muestra que el producto ordinal no es, en general, conmutativo.

Lema 1.10.1 *$(A \odot B) \odot C \cong A \odot (B \odot C)$ y $(A \odot B)^* = A^* \odot B^*$.*

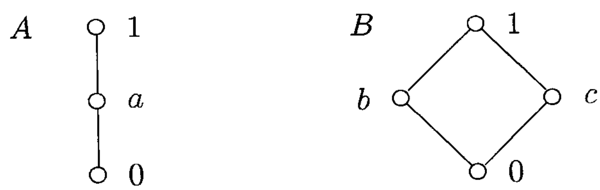
1.11 Potencia (cardinal) de conjuntos ordenados

Dados dos conjuntos ordenados $(A, \leq_1)$, $(B, \leq_2)$ sea C el conjunto de todas las funciones isótonas de A en B, que notaremos $C = B^A$. Sobre C definamos la siguiente relación, dadas $f, g \in C$

$$f \leq g \iff f(a) \leq_2 g(a), \quad \forall a \in A$$

Es fácil ver que "$\leq$" es una relación de orden definida sobre C, por lo tanto $(C, \leq)$ es un conjunto ordenado, al cual se dá el nombre de **potencia (cardinal)**.

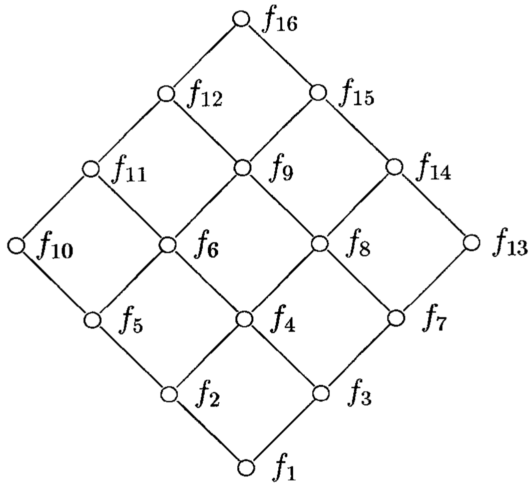
Ejemplo 1.11.1 *Sean A y B los conjuntos ordenados cuyos diagramas de Hasse se indican:*



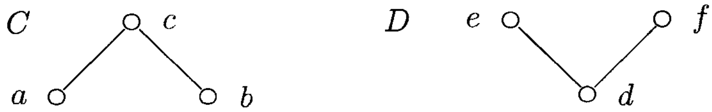
entonces B^A tiene los siguientes elementos:

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{12}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	b	b	b	c	c	c	1
a	0	0	0	0	b	b	c	c	1	b	b	1	c	c	1	1
1	0	b	c	1	b	1	c	1	1	b	1	1	c	1	1	1

y su diagrama de Hasse es:



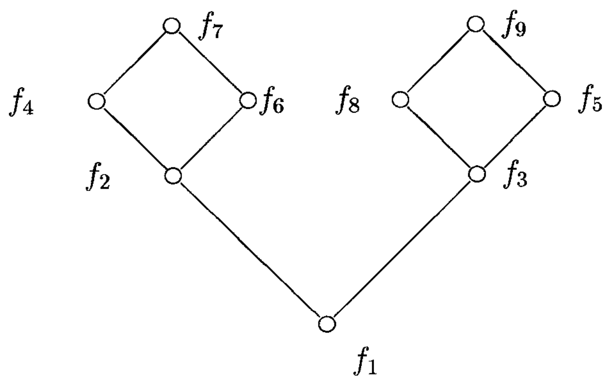
Ejemplo 1.11.2 *Sean C y D los conjuntos ordenados cuyos diagramas de Hasse se indican:*



entonces D^C tiene los siguientes elementos:

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9
a	d	d	d	d	d	e	e	f	f
b	d	d	d	e	f	d	e	d	f
c	d	e	f	e	f	e	e	f	f

y su diagrama de Hasse es:



Ejercicio 1.11.1 *La potencia de conjuntos ordenados tiene las siguientes propiedades:*

P1) $A^B \times A^C \cong A^{B+C}$.

P2) $A^C \times B^C \cong (A \times B)^C$.

P3) $(A^B)^C \cong A^{(B \times C)}$.

P4) $(A^B)^* = (A^*)^{B^*}$.

P1) Sean $(A, \leq_1), (B, \leq_2), (C, \leq_3)$ *conjuntos ordenados. Dadas* $f \in A^B$, $g \in A^C$ *consideremos la siguiente función de* $B + C$ *en* A.

$$h_{(f,g)}(r) = \begin{cases} f(r) & \text{si} \quad r \in B \\ g(r) & \text{si} \quad r \in C. \end{cases}$$

Probar que $h_{(f,g)}$ *es isótona y que la transformación de* $A^B \times A^C$ *en* A^{B+C} *definida por:* $\varphi((f,g)) = h_{(f,g)}$ *es un isomorfismo de orden.*

P2) Dado $(f,g) \in A^C \times B^C$ *consideremos la siguiente función de* C *en* $A \times B$: $h_{(f,g)}(c) = (f(c), g(c))$. *Probar que* $h_{(f,g)}$ *es isótona y que la transformación de* $A^C \times B^C$ *en* $(A \times B)^C$ *definida por:* $\varphi((f,g)) = h_{(f,g)}$ *es un isomorfismo de orden.*

P3) Dada $f \in (A^B)^C$ *entonces* $f(c) = g_f \in A^B$ *y* $g_f(b) = a \in A$, *donde* $b \in B$. *Consideremos la función de* $B \times C$ *en* A *definida por:* $h((b,c)) = g_f(b)$. *Probar que* h *es isótona y que la transformación de* $(A^B)^C$ *en* $A^{B \times C}$ *definida por* $\varphi(f) = h$ *es un isomorfismo de orden.*

P4) Dada $f \in (A^B)^*$ *entonces* f *es una función isótona de* B *en* A, f *también es una función isótona de* B^* *en* A^*. *En efect, si* $x, y \in B$ *son tales que* $x \leq_2 y$ *entonces* $f(x) \leq_1 f(y)$, *esto es,* $y \leq_2 x$ *entonces* $f(y) \leq_1 f(x)$, *luego* $f \in (A^*)^{B^*}$. *Esto prueba que* $(A^B)^* \subseteq (A^*)^{B^*}$. *En forma análoga se prueba la otra inclusión.*

1.12 Conjuntos ordenados conexos

Un conjunto ordenado A se dice **conexo** si *no existen* conjuntos ordenados A_1 y A_2, no vacíos, tales que $A \cong A_1 + A_2$, esto es, tales que A sea isomorfo a la suma cardinal de A_1 con A_2.

Observación 1.12.1 *Si un conjunto ordenado* A *es isomorfo a la suma cardinal* $A_1 + A_2$ *de dos conjuntos ordenados, entonces existen subconjuntos* $A_1^{'}$ *y* $A_2^{'}$ *de* A *tales que* $A = A_1^{'} + A_2^{'}$, *esto es,* $A_1^{'} \cap A_2^{'} = \emptyset$, $A = A_1^{'} \cup A_2^{'}$ *y* $a \leq b$, *donde* $a, b \in A \iff a \leq b$, $a, b \in A_1^{'}$ *ó* $a \leq b$, $a, b \in A_2^{'}$.
En efecto, por hipótesis existe una función $f : A_1 + A_2 \to A$, *que es un isomorfismo de orden. Sean* $A_1^{'} = f(A_1)$ *y* $A_2^{'} = f(A_2)$. *Si* $A_1^{'} \cap A_2^{'} \neq \emptyset$ *entonces existe* $z \in A_1^{'} \cap A_2^{'}$, *luego* $z = f(a_1)$ *con* $a_1 \in A_1$ *y* $z = f(a_2)$ *con* $a_2 \in A_2$, *entonces* $f(a_1) = f(a_2)$ *de donde resulta por ser* f *inyectiva que* $a_1 = a_2$, *absurdo dado que* $A_1 \cap A_2 = \emptyset$. *Veamos que* $f(A_1) \cup f(A_2) = A$. *En efecto, es claro que* $f(A_1) \cup f(A_2) \subseteq A$. *Sea* $w \in A$, *luego existe (1)* $y \in A_1 + A_2$ *tal que* $f(y) = w$. *De (1) resulta que* $y \in A_1$ *ó* $y \in A_2$, *luego* $f(y) = w \in f(A_1)$ *ó* $f(y) = w \in f(A_2)$.

Sean $x, y \in A$ tales que $x \leq y$, luego como f^{-1} también es un isomorfismo entonces $x' = f^{-1}(x) \leq f^{-1}(y) = y'$, donde $x', y' \in A_1 + A_2$, y por lo tanto, $x', y' \in A_1$ ó $x', y' \in A_2$, esto es $x, y \in f(A_1) = A_1^{'}$ ó $x, y \in f(A_1) = A_2^{'}$. La recíproca es obvia.

Definición 1.12.1 *Se dice que los elementos a, b de un conjunto ordenado A están* **conectados** *si existe una sucesión finita $a_1, a_2, \ldots, a_n$ de elementos de A tales que:*

- $a_1 = a$,
- $a_n = b$,
- a_i *es comparable con* a_{i+1}, *para* $i = 1, 2, \ldots, n-1$.

y en ese caso notaremos $a \equiv b$.

Ejemplo 1.12.1 *En el conjunto ordenado cuyo diagrama está indicado en el Ejemplo 1.2.4, el elemento a está conectado con b, ya que la sucesión $a_1 = a, a_2 = c, a_3 = b$ verifica las condiciones de la definición anterior. Observemos que a y b son incomparables.*

Lema 1.12.1 *La relación de conectabilidad es una relación de equivalencia.*

Por lo tanto, la relación $\equiv$ dá origen a una partición de A. Dado $a \in A$, notaremos con $C(a) = \{x \in A : x \equiv a\}$, la clase de equivalencia que contiene al elemento $a \in A$.

Definición 1.12.2 *Sea $(A, \leq)$ un conjunto ordenado y $\emptyset \neq X \subseteq A$. Se dice que X es* **una parte conexa de** *A, si $(X, \leq)$ es un conjunto ordenado conexo.*

Lema 1.12.2 *$C(x)$ es una parte conexa de A, cualquiera que sea $x \in A$.*

Dem. Supongamos que $C(x) = Y + Z$, donde $\emptyset \neq Y \subseteq C(x)$, $\emptyset \neq Z \subseteq C(x)$. Dados $y \in Y$, $z \in Z$ entonces $y, z \in Y \cup Z = C(x)$, y por lo tanto $y \equiv z$. Luego, existe una sucesión finita $a_1, a_2, \ldots, a_n$ de elementos de $C(x)$ tales que: $a_1 = y$, $a_n = z$, a_i es comparable con a_{i+1}, para $i = 1, 2, \ldots, n-1$. Observemos que $n > 1$, pues si $n = 1$ entonces $a_1 = y = z$, absurdo, ya que $Y \cap Z = \emptyset$.
Sea $S = \{a_1, a_2, \ldots, a_n\}$ y $W = S \cap Z$, entonces como $a_n \in S$ y $a_n = z \in Z$ tenemos que $a_n \in W$.
Sea (1) i_0 *el menor índice* tal que $a_{i_0} \in W$, luego $a_{i_0} \in Z$. Como $a_1 = y \in Y$ e $Y \cap Z = \emptyset$ entonces $a_1 \notin Z$ y por lo tanto $a_1 \notin W$, entonces tenemos que $i_0 \neq 1$, y por lo tanto $i_0 > 1$. Como $a_{i_0-1} \in S$, entonces por (1) resulta que $a_{i_0-1} \notin Z$, y en consecuencia como $a_{i_0-1} \in C(x) = Y \cup Z$ e $Y \cap Z = \emptyset$ tenemos que $a_{i_0-1} \in Y$.
Como a_{i_0-1} es comparable con a_{i_0}, entonces tendríamos un elemento de Y,(el a_{i_0-1}), comparable con un elemento de Z (el a_{i_0}), lo que contradice que $C(x)$ es la suma cardinal de Y con Z. ■
Este resultado justifica que a los conjuntos $C(a)$, donde $a \in A$, se los denomine **componente conexa** del elemento $a \in A$.

Teorema 1.12.1 *La familia $\mathcal{K}$ de las partes conexas de un conjunto ordenado A, ordenada por inclusión, es inductiva superiormente, esto es, toda cadena de $\mathcal{K}$ tiene una cota superior en $\mathcal{K}$.*

Dem. Sea $\{C_i\}_{i\in I}$ una cadena de partes conexas de A, es claro que $S = \bigcup_{i\in I} C_i$ es un conjunto ordenado. Como $C_i \subseteq S$, para todo $i \in I$ si probamos que S es una parte conexa de A, entonces S es una cota superior, en $\mathcal{K}$, de la familia $\{C_i\}_{i\in I}$.
Supongamos que S no es un conjunto ordenado conexo, esto es, $S = S_1 + S_2$, donde $S_1 \neq \emptyset$, $S_2 \neq \emptyset$, $S_1 \cap S_2 = \emptyset$, $S_1 \cup S_2 = S$, y ningún elemento de S_1 es comparable con ningún elemento de S_2.
Veamos que existe por lo menos un C_i tal que (1) $S_1 \cap C_i \neq \emptyset$. En efecto, si $S_1 \cap C_i = \emptyset$, $\forall i \in I$ entonces $C_i \subseteq S \setminus S_1 = S_2$, $\forall i \in I$, y por lo tanto, $S = \bigcup_{i\in I} C_i \subseteq S_2$ y en consecuencia $S = S_2$, luego $S_1 = \emptyset$, absurdo.
En forma análoga se demuestra que existe por lo menos un C_j tal que (2) $S_2 \cap C_j \neq \emptyset$.
Como por hipótesis $\mathcal{K}$ es una cadena entonces (3) $C_i \subseteq C_j$ ó (4) $C_j \subseteq C_i$. Si se verifica (3) entonces por (1) tenemos $\emptyset \neq S_1 \cap C_i \subseteq S_1 \cap C_j$, esto es, (5) $S_1 \cap C_j \neq \emptyset$.
Sean $D_1 = S_1 \cap C_j$ y $D_2 = S_2 \cap C_j$, luego ambos son subconjuntos de C_j y por (5) y (2) respectivamente, ellos no son vacíos. Además, $D_1 \cup D_2 = (S_1 \cap C_j) \cup (S_2 \cap C_j) = (S_1 \cup S_2) \cap C_j = S \cap C_j = C_j$ y $D_1 \cap D_2 = (S_1 \cap C_j) \cap (S_2 \cap C_j) = S_1 \cap S_2 \cap C_j = \emptyset \cap C_j = \emptyset$.
Como los elementos de S_1 son incomparables con los elementos de S_2 también los elementos de D_1 y D_2 son incomparables. Por lo tanto, $C_j = D_1 + D_2$ lo que contradice la hipótesis de que C_j es conexo. Si se verifica (4) por un razonamiento análogo se llega a una contradicción. Luego S es una parte conexa de A. ■
De este resultado se deduce por el lema de Zorn que:

Teorema 1.12.2 *Toda parte conexa de un conjunto ordenado está contenida en una parte conexa máxima.*

Lema 1.12.3 *Si M es una parte conexa máxima de A y $a \in M$ entonces $C(a) = M$.*

Dem. Sea $a \in M$, si probamos que $M \subseteq C(a)$, entonces como M es una parte conexa máxima de A tendremos que $M = C(a)$.
Supongamos que $M \not\subseteq C(a)$, donde $a \in M$ y sea $M_1 = M \cap C(a)$ luego $M_1 \neq \emptyset$ ya que $a \in M$ y $a \in C(a)$. Consideremos el conjunto $M_2 = M \setminus C(a)$. Si $\emptyset = M_2 = M \setminus C(a)$ entonces $M \subseteq C(a)$, absurdo .
Tenemos asi que $M = M_1 \cup M_2$, $M_1 \cap M_2 = \emptyset$ $M_1 \neq \emptyset$ $M_2 \neq \emptyset$. Veamos que ningún elemento de M_1 es comparable con ningún elemento de M_2. En efecto, si $m_1 \in M_1$ es comparable con $m_2 \in M_2$ entonces $m_1 \equiv m_2$ y como $m_1 \in M \cap C(a)$, en particular, $m_1 \in C(a)$ y por lo tanto $m_1 \equiv a$ y en consecuencia $m_2 \equiv a$, esto es $m_2 \in C(a)$, absurdo ya que $m_2 \in M_2 = M \setminus C(a)$. ■

Corolario 1.12.1 *$C(a)$ es una parte conexa máxima de A cualquiera que sea $a \in A$.*

Dem. Por el Lema 1.12.2 sabemos que $C(a)$ es una parte conexa, luego por el Teorema 1.12.2, existe una parte conexa máxima M tal que $C(a) \subseteq M$, luego como $a \in C(a)$ tenemos que $a \in M$ de donde resulta por el Lema 1.12.3 que $C(a) = M$. ■

La noción de suma cardinal de dos conjuntos ordenados se puede generalizar para el caso de una familia arbitraria de conjuntos ordenados.
Dada una familia arbitraria $\{(A_i, \leq_i)\}_{i\in I}$ tales que

$$(*) \qquad A_i \cap A_j = \emptyset \quad \text{para} \quad i, j \in I \;\; i \neq j,$$

consideremos el conjunto $A = \bigcup_{i\in I} A_i$ y dados $a, b \in A$ definimos $a \leq b \iff$ existe $i \in I$, tal que (1) $a, b \in A_i$ y (2) $a \leq_i b$. Entonces se verifica facilmente que $(A, \leq)$ es un conjunto ordenado, que se denomina **suma cardinal de la familia** $\{(A_i, \leq_i)\}_{i\in I}$ y se nota

$$A = \sum_{i\in I} A_i.$$

Observemos que si la familia de conjuntos ordenados no verifica la condición

$$(*),$$

entonces para cada $i \in I$, considerando los conjuntos ordenados $A_i' = A_i \times \{i\}$, ellos verifican

$$(*),$$

y entonces se define la suma cardinal de la familia dada como:

$$\sum_{i\in I} A_i'.$$

Utilizando la definición precedente se puede afirmar que:

Teorema 1.12.3 *Dado un conjunto ordenado $(A, \leq)$, entonces A es conexo ó A es la suma cardinal de conjuntos ordenados conexos.*

Dem. Si A es conexo no hay nada que probar. Supongamos que A no es conexo. Como "$\equiv$" es una relación de equivalencia, ella induce una partición de A, $\{A_i\}_{i\in I}$ donde $A_i = C(a)$ para algún $a \in A$, esto es, $A = \bigcup_{i\in I} A_i$, los conjuntos A_i son no vacíos para todo $i \in I$ y $A_i \cap A_j = \emptyset$, para $i \neq j$, $i, j \in I$. Por lo tanto, $(A_i, \leq_i)$ es un conjunto ordenado cualquiera que sea $i \in I$, y la relación $\leq_i$ es la relación $\leq$ restringida al subconjunto A_i de A. Además si $a, b \in A$ y $a \leq b$ es claro que $a \equiv b$, y por lo tanto $a, b \in C(a) = A_i$, luego $a \leq_i b$, y si $a, b \in A_i$ y $a \leq_i b$, entonces $a \leq b$. Por lo tanto $A = \sum_{i\in I} A_i$. ■

2 RETICULADOS

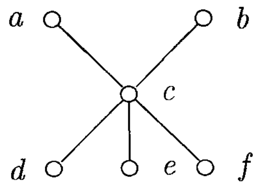
2.1 Reticulados inferiores

Definición 2.1.1 *Si $(A, \leq)$ es un conjunto ordenado, dados $a, b \in A$ se dice que el elemento $c \in A$ es* **el ínfimo** *de a y b y se nota $c = a \wedge b$ si:*

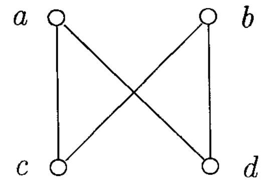
I1) $c \leq a$ y $c \leq b$, esto es, c es una cota inferior del conjunto $\{a, b\}$.

I2) Si $x \in A$ verifica $x \leq a$ y $x \leq b$, entonces $x \leq c$, esto es, c es la "mayor" de las cotas inferiores del conjunto $\{a, b\}$, ó c es el último elemento del conjunto de las cotas inferiores del conjunto $\{a, b\}$.

Ejemplo 2.1.1 *1) Sea A el conjunto ordenado cuyo diagrama se indica:*



Entonces el conjunto de las cotas inferiores de $\{a, b\}$ es $\{c, d, e, f\}$ y por lo tanto $c = a \wedge b$.
2) Si B el conjunto ordenado cuyo diagrama se indica:



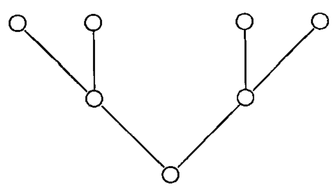
entonces no existe el ínfimo de a y b dado que el conjunto $\{c, d\}$ de las cotas inferiores de $\{a, b\}$ no tiene último elemento.

Observación 2.1.1 *Es claro que $a \wedge a = a$.*

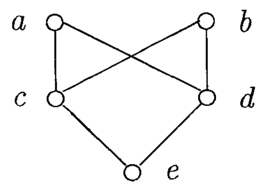
Definición 2.1.2 *Un conjunto ordenado $(A, \leq)$, se dice un* **reticulado inferior** *si todo par de elementos de A tiene ínfimo.*

Observación 2.1.2 *Como $a \wedge a = a$, cualquiera que sea $a \in A$, es claro que la definición precedente debe verificarse para todo par, a, b de elementos de A tales que $a \neq b$.*

Ejemplo 2.1.2 *El conjunto ordenado cuyo diagrama se indica es un reticulado inferior.*



Observación 2.1.3 *Todo reticulado inferior es un conjunto filtrante inferiormente, pero la recíproca no es verdadera, por ejemplo el conjunto ordenado cuyo diagrama de Hasse se indica:*



es filtrante inferiormente; pero no es un reticulado inferior pues el conjunto de las cotas inferiores del conjunto $\{a, b\}$ *es* $\{c, d, e\}$, *y este conjunto no tiene último elemento.*

Lema 2.1.1 *En un conjunto ordenado si existe el ínfimo de dos elementos, él es único.*

Dem. Supongamos que (1) $c = a \wedge b$ y (2) $d = a \wedge b$. De (1) resulta por I1) que $c \leq a$ y $c \leq b$, luego como d es el ínfimo de a y b por I2) resulta que $c \leq d$. En forma análoga se deduce que $d \leq c$ y por lo tanto $c = d$. ■

Lema 2.1.2 $a \leq b \iff a \wedge b = a$.

Dem. $\Longrightarrow$) Supongamos que $a \leq b$, luego tenemos I1) $a \leq a$ y $a \leq b$. Si $x \leq a$ y $x \leq b$, en particular $x \leq a$, por lo tanto se verifica I2).
$\Longleftarrow$) Si $a = a \wedge b$ entonces, en particular $a \leq b$. ■

Corolario 2.1.1 *Toda cadena A es un reticulado inferior.*

Dem. Sean $a, b \in A$ entonces $a \leq b$ ó $b \leq a$, y por lo tanto $a \wedge b = a$ ó $b \wedge a = b$. ■

Lema 2.1.3 *En todo reticulado inferior R se verifican las siguientes propiedades:*

RI1) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ *(Propiedad asociativa)*

RI2) $a \wedge b = b \wedge a$ *(Propiedad conmutativa)*

RI3) $a \wedge a = a$ *(Propiedad idempotente)*

La propiedad RI1) nos dice que $(A, \wedge)$ es un semigrupo, la RI2) que es conmutativo y la RI3) que es idempotente.

Lema 2.1.4 *Sea* $(R, \wedge)$ *un sistema formado por un conjunto, no vacío, R y una operación binaria definida sobre R, que verifica RI1), RI2) y RI3), entonces R es un reticulado inferior.*

Dem. En primer lugar debemos probar que R es un conjunto ordenado. Para ello vamos a definir:

$$a \leq b \iff a = a \wedge b.$$

O1) Probar que $a \leq a$ equivale a probar que $a = a \wedge a$, lo que verifica por la hipótesis RI3).

O2) Supongamos que $a \leq b$ y $b \leq a$, esto es, que $a = a \wedge b$ y $b = b \wedge a$, entonces por RI2) resulta que $a = b$.

O3) Supongamos que $a \leq b$ y $b \leq c$, esto es, $a = a \wedge b$ y $b = b \wedge c$, entonces teniendo en cuenta las hipótesis y RI1) tenemos $a = a \wedge b = a \wedge (b \wedge c) = (a \wedge b) \wedge c = a \wedge c$, esto es, $a \leq c$.

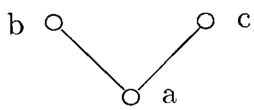
Acabamos así de probar que $(R, \leq)$ es un conjunto ordenado, que se denomina conjunto ordenado **asociado**. Para verificar que R es un reticulado inferior falta probar que todo par de elementos de R tiene un ínfimo. Vamos a demostrar que $c = a \wedge b$ es precisamente el ínfimo de a y b.

I1) $a \wedge b \leq a$ y $a \wedge b \leq b$. Esto equivale a probar que $(a \wedge b) \wedge a = a \wedge b$ y $(a \wedge b) \wedge b = a \wedge b$. $(a \wedge b) \wedge a =$ (*por RI*1) $= a \wedge (b \wedge a) =$ (*por RI*2) $= a \wedge (a \wedge b) =$ (*por RI*1) $=$ $(a \wedge a) \wedge b =$ (*por RI*3) $= a \wedge b$. En forma análoga se prueba la otra condición.

I2) Sea $x \in R$ tal que $x \leq a$ y $x \leq b$, esto es, (1) $x = x \wedge aa$ y (2) $x = x \wedge b$. Entonces $x \wedge (a \wedge b) =$ (*por RI*1) $= (x \wedge a) \wedge b =$ (*por* (1)) $= x \wedge b =$ (*por* (2)) $= x$, esto es, $x \leq a \wedge b$.

■

Acabamos así de probar que la noción de reticulado inferior es equivalente a la de semigrupo conmutativo idempotente. Entonces para dar ejemplos de semigrupos conmutativos idempotentes, basta indicar conjuntos ordenados en los cuales cada par de elementos tenga un ínfimo. Por ejemplo si A es el conjunto ordenado cuyo diagrama de Hasse se indica:



entonces la operación binaria "$\wedge$" tiene la siguiente tabla:

$\wedge$	a	b	c
a	a	a	a
b	a	b	a
c	a	a	c

Si damos el conjunto $A = \{a, b, c\}$ y la operación binaria $\wedge$ indicada en la tabla precedente para probar que $(A, \wedge)$ es un semigrupo conmutativo idempotente, debemos verificar que se verifican RI1), RI2) y RI3). A partir de la tabla se ve inmediatamente que se verifican RI2) y RI3). Para comprobar que se verifica RI1) hay que hacer $3^3 = 27$ sustituciones y los cálculos correspondientes.

Definición 2.1.3 *Sean* $(A, \wedge)$, $(A', \wedge)$ *reticulados inferiores. A toda función* $h : A \to A'$ *tal que* $h(a \wedge b) = h(a) \wedge h(b)$, *cualesquiera que sean* $a, b \in A$, *se denomina* **homomorfismo** *de* A *en* A'. *Si* h *es suryectiva, se denomina* **epimorfismo** *y si* h *es biyectiva se denomina* **isomorfismo**.

Definición 2.1.4 *Una familia* $\mathcal{F}$, *no vacía, de subconjuntos de un conjunto fijo* A *se denomina* **multiplicativa** *si verifica:*

$$\text{Si} \quad X, Y \in \mathcal{F} \Longrightarrow X \cap Y \in \mathcal{F}.$$

Como la intersección de conjuntos tiene las propiedades RI1), RI2) y RI3) indicadas anteriormente, entonces si $\mathcal{F}$ es multiplicativa, $(\mathcal{F}, \cap)$ es un reticulado inferior.

Lema 2.1.5 *Todo reticulado inferior es isomorfo a una familia multiplicativa de conjuntos.*

Dem. Sea $(R, \wedge)$ un reticulado inferior y $(R, \leq)$ el conjunto ordenado asociado, esto es $a \leq b \iff a = a \wedge b$. Si $x \in R$ pongamos $R_x = \{y \in R : y \leq x\} = (x]$ y $h(x) = R_x$. Vimos en el Lema 1.4.1 que h es un isomorfismo de orden entre los conjuntos ordenados $(R, \leq)$ y $(\{R_x\}_{x \in R}, \subseteq)$. Probemos que $h(a \wedge b) = h(a) \cap h(b)$. Sea $x \in h(a \wedge b)$, esto es, $x \leq a \wedge b$. Como $a \wedge b \leq a$ y $a \wedge b \leq b$ entonces tenemos $x \leq a$ y $x \leq b$, esto es, $x \in h(a)$ y $x \in h(b)$, por lo tanto $x \in h(a) \cap h(b)$. Supongamos ahora que $x \in h(a) \cap h(b)$, luego $x \in h(a)$ y $x \in h(b)$, esto es, $x \leq a$ y $x \leq b$ y en consecuencia, por definición, $x \leq a \wedge b$, esto es, $x \in h(a \wedge b)$. Acabamos así de probar que $h(a \wedge b) = h(a) \cap h(b)$. De esta igualdad se deduce que la familia $\mathcal{F} = \{R_x\}_{x \in R}$ es multiplicativa, ya que si $A, B \in \mathcal{F}$ entonces $A = h(a)$ y $B = h(b)$, $a, b \in R$ y por lo tanto $A \cap B = h(a) \cap h(b) = h(a \wedge b)$, donde $a \wedge b \in R$, esto es, $A \cap B \in \mathcal{F}$. ■

Definición 2.1.5 *Sea $(R, \wedge)$ un reticulado inferior.*

1) *Se dice que un elemento $1 \in R$ es una* **unidad** *si $1 \wedge x = x, \quad \forall\, x \in R$. Esto equivale a decir que $x \leq 1 \quad \forall\, x \in R$, esto es, el conjunto ordenado $(R, \leq)$ tiene último elemento 1.*

2) *Se dice que un elemento $0 \in R$ es* **nulo** *si $0 \wedge x = 0, \quad \forall\, x \in R$. Esto equivale a decir que $0 \leq x \quad \forall\, x \in R$, esto es, el conjunto ordenado $(R, \leq)$ tiene primer elemento 0.*

En un reticulado inferior vamos a notar $\bigwedge_{i=1}^{n} a_i$ ó $a_1 \wedge a_2 \wedge \ldots \wedge a_n$ al elemento:

$$(\ldots((a_1 \wedge a_2) \wedge a_3) \wedge \ldots) \wedge a_n.$$

Lema 2.1.6 *Todo reticulado inferior finito tiene primer elemento.*

Dem. Sea $R = \{a_1, a_2, \ldots, a_n\}$ y $p = \bigwedge_{i=1}^{n} a_i$ luego $p \in R$ y $p \leq a_i, \quad i = 1, 2, \ldots, n$. ■

Observemos que los reticulados inferiores finitos pueden no tener último elemento, como lo demuestra el Ejemplo 2.1.2.

2.2 Reticulados superiores

En forma similar se define el concepto de **reticulado superior** y se prueban resultados análogos, cuyas demostraciones quedan a cargo del lector.

Definición 2.2.1 *Si $(A, \leq)$ es un conjunto ordenado, dados $a, b \in A$ se dice que el elemento $c \in A$ es* **el supremo** *de a y b y se nota $c = a \vee b$ si:*

S1) $a \leq c$ y $b \leq c$, esto es, c es una cota superior del conjunto $\{a, b\}$.

S2) Si $x \in A$ verifica $a \leq x$ y $b \leq x$, entonces $c \leq x$, esto es, c es la "menor" de las cotas superiores del conjunto $\{a, b\}$, ó c es el primer elemento del conjunto de las cotas superiores del conjunto $\{a, b\}$.

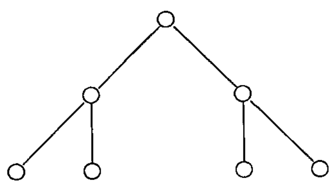
Sea A el conjunto ordenado indicado en el Ejemplo 2.1.1, 1) Entonces el conjunto de las cotas superiores de $\{d, e\}$ es $\{a, b, c\}$ y por lo tanto $c = d \vee e$.
Si B el conjunto ordenado indicado en el Ejemplo 2.1.1, 2) entonces no existe el supremo de c y d dado que el conjunto $\{a, b\}$ de las cotas superiores de $\{c, d\}$ no tiene primer elemento.

Observación 2.2.1 *Es claro que* $a \vee a = a$.

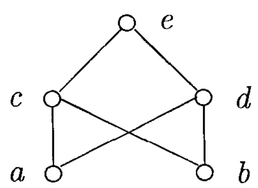
Definición 2.2.2 *Un conjunto ordenado* $(A, \leq)$, *se dice un* **reticulado superior** *si* <u>*todo*</u> *par de elementos de* A *tiene supremo.*

Observación 2.2.2 *Como* $a \vee a = a$, *cualquiera que sea* $a \in A$, *es claro que la definición precedente debe verificarse para todo par,* a, b *de elementos de* A *tales que* $a \neq b$.

Ejemplo 2.2.1 *El conjunto ordenado cuyo diagrama se indica es un reticulado superior.*



Observación 2.2.3 *Todo reticulado superior es un conjunto filtrante superiormente, pero la recíproca no es verdadera, por ejemplo el conjunto ordenado cuyo diagrama de Hasse se indica:*



es filtrante superiormente, pero no es un reticulado superior pues el conjunto de las cotas superiores del conjunto $\{a, b\}$ *es* $\{c, d, e\}$ *y este conjunto no tiene primer elemento.*

Lema 2.2.1 *En un conjunto ordenado si existe el supremo de dos elementos, el es único.*

Lema 2.2.2 $a \leq b \iff a \vee b = b$.

Corolario 2.2.1 *Todo conjunto totalmente ordenado* A *es un reticulado superior.*

Lema 2.2.3 *En todo reticulado superior* R *se verifican las siguientes propiedades:*

RS1) $a \vee (b \vee c) = (a \vee b) \vee c$ *(Propiedad asociativa)*

RS2) $a \vee b = b \vee a$ *(Propiedad conmutativa)*

RS3) $a \vee a = a$ *(Propiedad idempotente)*

La propiedad RS1) nos dice que $(A, \vee)$ es un semigrupo, la RS2) que es conmutativo y la RS3) que es idempotente.

Lema 2.2.4 *Sea* $(R, \vee)$ *un sistema formado por un conjunto, no vacío,* R *y una operación binaria definida sobre* R, *que verifica RS1), RS2) y RS3), entonces* R *es un reticulado superior.*

Dem. Se define: $a \leq b \iff b = a \vee b$ y la demostración se hace en forma análoga a la indicada en el Lema 2.1.4. ■

Acabamos así de probar que la noción de reticulado superior es equivalente a la de semigrupo conmutativo idempotente. Entonces para dar ejemplos de semigrupos conmutativos idempotentes, basta indicar conjuntos ordenados en los cuales cada par de elementos tenga un supremo.

Definición 2.2.3 *Sean $(A, \vee)$, $(A', \vee)$ reticulados superiores. A toda función $h : A \to A'$ tal que $h(a \vee b) = h(a) \vee h(b)$, cualesquiera que sean $a, b \in A$ se denomina* **homomorfismo** *de A en A'. Si h es suryectiva, se denomina* **epimorfismo** *y si h es biyectiva se denomina* **isomorfismo**.

Definición 2.2.4 *Una familia $\mathcal{F}$, no vacía, de subconjuntos de un conjunto fijo A se denomina* **aditiva** *si verifica:*

$$\text{Si} \quad X, Y \in \mathcal{F} \Longrightarrow X \cup Y \in \mathcal{F}.$$

Como la unión de conjuntos tiene las propiedades RS1), RS2) y RS3) indicadas anteriormente, entonces si $\mathcal{F}$ es aditiva, $(\mathcal{F}, \cup)$ es un reticulado superior.

Lema 2.2.5 *Todo reticulado superior es isomorfo a una familia aditiva de conjuntos.*

Dem. Considerar la transformación $h(x) = \{y \in R : x \leq y\}$. ■

En un reticulado superior vamos a notar $\bigvee_{i=1}^{n} a_i$ o $a_1 \vee a_2 \vee \ldots \vee a_n$ al elemento:

$$(\ldots((a_1 \vee a_2) \vee a_3) \vee \ldots) \vee a_n.$$

Lema 2.2.6 *Todo reticulado superior finito tiene último elemento.*

Dem. Si $R = \{a_1, a_2, \ldots, a_n\}$ entonces $u = \bigvee_{i=1}^{n} a_i$ es el último elemento de R. ■

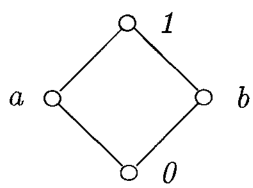
Observemos que los reticulados superiores finitos pueden no tener primer elemento, como lo demuestra el Ejemplo 2.2.1.

2.3 Reticulados

Definición 2.3.1 *Un conjunto ordenado $(A, \leq)$ se dice un* **reticulado** *si es reticulado inferior y superior, esto es, si cualesquiera que sean $a, b \in A$ existen $a \wedge b$ y $a \vee b$.*

Ejemplo 2.3.1 *1) Toda cadena es un reticulado (ver Corolarios 2.1.1 y 2.2.1).*

2) El conjunto ordenado cuyo diagrama de Hasse se indica, es un reticulado, las operaciones de $\wedge$ y $\vee$ se indican en las tablas siguientes:



$\wedge$	0	a	b	1
0	0	0	0	0
a	0	a	0	a
b	0	0	b	b
1	0	a	b	1

$\vee$	0	a	b	1
0	0	a	b	1
a	a	a	1	1
b	b	1	b	1
1	1	1	1	1

3) La recta es un reticulado donde $x \wedge y = min\{x, y\}$ *y* $x \vee y = max\{x, y\}$.

De acuerdo con los Lemas 2.1.6 y 2.2.6 tenemos:

Lema 2.3.1 *Todo reticulado finito tiene primer y último elemento.*

Lema 2.3.2 *En todo reticulado R se verifican las siguientes propiedades:*

RI1) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ *(Propiedad asociativa)*

RI2) $a \wedge b = b \wedge a$ *(Propiedad conmutativa)*

RI3) $a \wedge a = a$ *(Propiedad idempotente)*

C1) $a \wedge (a \vee b) = a$ *(Ley de absorción)*

RS1) $a \vee (b \vee c) = (a \vee b) \vee c$ *(Propiedad asociativa)*

RS2) $a \vee b = b \vee a$ *(Propiedad conmutativa)*

RS3) $a \vee a = a$ *(Propiedad idempotente)*

C2) $a \vee (a \wedge b) = a$ *(Ley de absorción)*

Dem. Como R es un reticulado inferior sabemos por el Lema 2.1.3 que se verifican RI1), RI2) y RI3) y como es un reticulado superior sabemos por el Lema 2.2.3 que se verifican RS1), RS2) y RS3). Por la definición de supremo tenemos que $a \leq a \vee b$ de donde resulta por el Lema 2.1.2 $a \wedge (a \vee b) = a$. Por la definición de ínfimo tenemos que $a \wedge b \leq a$ de donde resulta por el Lema 2.2.2 $a \vee (a \wedge b) = a$. ■

Lema 2.3.3 *Sea* $(R, \wedge, \vee)$ *un sistema formado por un conjunto, no vacío, R y dos operaciones binarias definidas sobre R,* $\wedge$ *y* $\vee$, *que verifican RI1), RI2), RI3), C1), RS1), RS2), RS3) y C2), entonces R es un reticulado, en el cual cada par de elementos* $a, b \in R$ *tiene un ínfimo que es precisamente* $a \wedge b$ *y un supremo que es precisamente* $a \vee b$.

Dem. Como se verifican $RI1), RI2), RI3)$ sobre R sabemos por el Lema 2.1.4 que podemos definir una relación de orden "$\leq$" ($a \leq b \iff a = a \wedge b$) y que el ínfimo de dos elementos $a, b \in R$ es precisamente $a \wedge b$. Como también se verifican RS1), RS2), RS3) sabemos por el Lema 2.2.3 que podemos definir una relación de orden "$\leq'$" ($a \leq' b \iff a \vee b = b$) y que el supremo de dos elementos $a, b \in R$ es precisamente $a \vee b$. Vamos a demostrar que $a \leq b \iff a \leq' b$.
Si $a \leq b$, esto es $a = a \wedge b$, entonces teniendo en cuenta C2) tenemos que $a \vee b = (a \wedge b) \vee b = b$, esto es, $a \leq' b$. Recíprocamente, si $a \leq' b$, esto es $b = a \vee b$ entonces teniendo en cuenta C1) tenemos que $a \wedge b = a \wedge (a \vee b) = a$, esto es, $a \leq b$. ■

Ejercicio 2.3.1 *Probar que en cualquier reticulado valen la siguientes reglas de cálculo:*

1) *Si* $a \leq b$ *entonces* $a \wedge c \leq b \wedge c$ *y* $a \vee c \leq b \vee c$.

2) *Si* $a \leq b$ *y* $a' \leq b'$ *entonces* $a \wedge a' \leq b \wedge b'$ *y* $a \vee a' \leq b \vee b'$.

3) *Si* $a \wedge b = a \vee b$ *entonces* $a = b$.

4) Leyes semidistributivas:

4a) $(a \wedge c) \vee (b \wedge c) \leq (a \vee b) \wedge c$.

4b) $(a \vee c) \wedge (b \vee c) \geq (a \wedge b) \vee c$.

Un reticulado R con primer y último elemento se denomina **reticulado acotado** ó **$(0,1)$-reticulado**

El producto cartesiano de reticulados se define en forma análoga a la indicada en el capítulo de Conjuntos Ordenados. Si A y B son reticulados en $A \times B$ el ínfimo y el supremo estan dados por $(a_1,b_1) \wedge (a_2,b_2) = (a_1 \wedge a_2, b_1 \wedge b_2)$ y $(a_1,b_1) \vee (a_2,b_2) = (a_1 \vee a_2, b_1 \vee b_2)$.

2.4 Elementos irreducibles y primos de un reticulado

Definición 2.4.1 *Un elemento i de un reticulado R se dice* **irreducible** (ó **$\vee$-irreducible)** *si:*

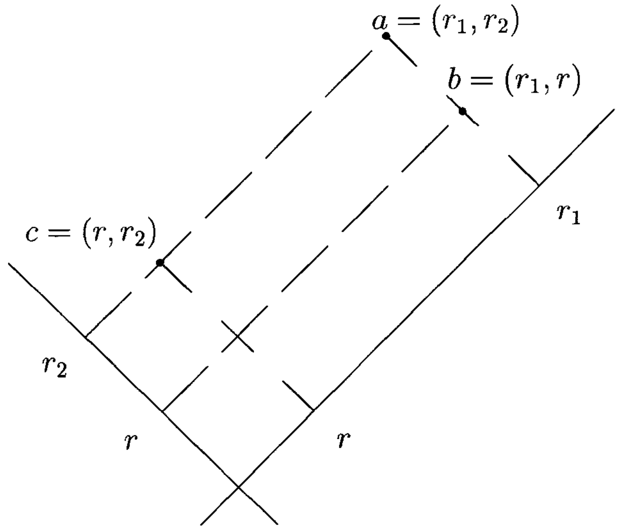
I1) i no es primer elemento de R.

I2) Si $i = a \vee b$ entonces $i = a$ ó $i = b$.

Observemos que si el reticulado R no tiene primer elemento la condición I1) es *trivialmente verificada.*
Existen reticulados que no tienen elementos irreducibles:

1) Cualquier reticulado con un sólo elemento.

2) Sea $\mathbb{R}$ la recta con su orden natural. Sabemos que $\mathbb{R}$ es un reticulado y consideremos el reticulado $A = \mathbb{R} \times \mathbb{R}$, el cual no tiene primer elemento.
Sea $a = (r_1, r_2) \in A$ y $r < min\{r_1, r_2\}$, entonces los elementos $b = (r_1, r)$ y $c = (r, r_2)$ verifican: 1) $a = b \vee c$, 2) $b \neq a$, 3) $c \neq a$.



3) Existen reticulados cuyos elementos son todos irreducibles. Por ejemplo $\mathbb{R}$.

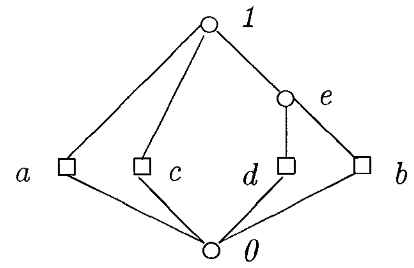
4) En toda cadena sin primer elemento todos los elementos son irreducibles y si C es una cadena con primer elemento 0 todos los elementos de C diferentes de 0 son irreducibles.

El siguiente teorema nos dá un método para determinar los elementos irreducibles de un reticulado finito cuando conocemos su diagrama de Hasse.

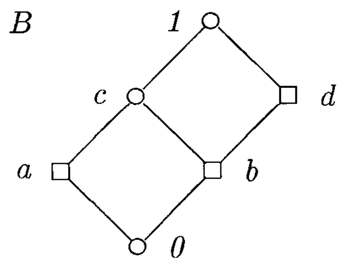
Teorema 2.4.1 *Sea R un reticulado finito, luego tiene primer elemento que notaremos con 0. Para que $i \in R - \{0\}$ sea irreducible es necesario y suficiente que el conjunto $I = \{x \in R : x < i\}$ tenga último elemento.*

Dem. $\Longrightarrow$) Sea $i \in R - \{0\}$ un elemento irreducible de R y consideremos el conjunto $I = \{x \in R : x < i\}$. Como $0 \leq i$ y por hipótesis $i \neq 0$ entonces $0 < i$, por lo tanto $I \neq \emptyset$. Por lo tanto, como R es un conjunto finito tenemos que I es un conjunto finito no vacío. Sea $I = \{a_1, a_2, \ldots, a_n\}$ y $a = \bigvee_{j=1}^{n} a_j$, luego $a_j \leq a$ para $j = 1, 2, \ldots, n$. Si probamos que $a \in I$, la demostración está terminada. Probar que $a \in I$ equivale a probar que $a < i$. Como $a_j \in I$ para $j = 1, 2, \ldots, n$, esto es, (1) $a_j < i$, para $j = 1, 2, \ldots, n$ y por lo tanto $a = \bigvee_{j=1}^{n} a_j \leq i$. Veamos que $a \neq i$. En efecto si $i = a = a_1 \vee (a_2 \vee \ldots \vee a_n)$ como i es irreducible entonces (2) $i = a_1$ ó (3) $i = a_2 \vee \ldots \vee a_n$. La condición (2) se contradice con (1), luego se debe verificar (3). Reiterando este procedimiento llegaremos a que $i = a_n$, absurdo. Luego $i \neq a$.
$\Longleftarrow$) Sea $i \in R - \{0\}$ tal que el conjunto $I = \{x \in R : x < i\}$ tenga último elemento. Sea m el último elemento de I, luego (1) $m \in I$, (2) $m < i$ y (3) $x \leq m$ para todo $x \in I$. Supongamos que i no es irreducible, esto es, que (4) $i = a \vee b$, (5) $i \neq a$ y (6) $i \neq b$. De (4) resulta que (7) $a \leq i$ y (8) $b \leq i$. De (7) y (5) resulta $a < i$, esto es, (9) $a \in I$ y de (8) y (6) : $b < i$, luego (10) $b \in I$. De (9) y (3) tenemos que $a \leq m$ y de (10) y (3) que $b \leq m$. Luego (11) $i = a \vee b \leq m$. De (11) y (2) resulta $i < i$, absurdo. Luego i es irreducible. ■

Ejemplo 2.4.1 *1) Sea A el reticulado cuyo diagrama de Hasse se indica. Los elementos irreducibles de A estan marcados con □.*



2) Sea B el reticulado cuyo diagrama de Hasse se indica. Los elementos irreducibles de B estan marcados con $\Box$.



Lema 2.4.1 *Sea R un reticulado con primer elemento 0. Si a es un átomo de R entonces a es un elemento irreducible de R.*

Dem. Supongamos que $a = b \vee c$, donde $b, c \in R$, luego tenemos que (1) $0 \leq b \leq a$ y (2) $0 \leq c \leq a$. De (1) resulta por ser a un átomo que:

$$(3) \quad b = 0 \ \text{ó} \ (4) \quad b = a.$$

Y de (2) resulta por ser a un átomo que:

$$(5) \quad c = 0 \ \text{ó} \ (6) \quad c = a.$$

Si se verifican (3) y (5), entonces $b = c = 0$ y por lo tanto $a = 0$, absurdo. Si se verifican (3) y (6), entonces $b = 0$ y por lo tanto $c = a$. Si se verifican (4) y (5), entonces $b = a$ y $c = 0$. Finalmente si se verifican (4) y (6), entonces $b = c = a$. ■

La recíproca de este resultado no es válida. En el Ejemplo 2.4.1, 2), el elemento d es irreducible y no es átomo.

Teorema 2.4.2 *Si R es un reticulado finito, no trivial, esto es, con más de un elemento, y $a, b \in R$ son tales que $a \not\leq b$, entonces existe un elemento irreducible i tal que : 1) $i \leq a$, e (2) $i \not\leq b$.*

Dem. Representemos con 0 al primer elemento de R. Observemos en primer lugar que $a \neq 0$, dado que si $a = 0$ como $0 \leq x$ cualquiera que sea $x \in R$ entonces $0 = a \leq b$, lo que contradice la hipótesis. Sea $X = \{x \in R : x \leq a \ \text{ y } \ x \not\leq b\}$, luego $a \in X$. Tenemos así que X es un conjunto ordenado finito no vacío y en consecuencia por el Lema 1.2.1 tiene por lo menos un elemento mínimo. Sea i un elemento mínimo de X, luego (1) $i \leq a$, (2) $i \not\leq b$ y (3) si $x \in X$ verifica $x \leq i$ entonces $x = i$. Si probamos que i es irreducible el teorema está demostrado. En efecto: $i \neq 0$ pues si $i = 0$ entonces $i \leq b$ lo que contradice (2). Supongamos ahora que $i = x \vee y$. Si $x \leq b$ e $y \leq b$ entonces tendríamos que $i = x \vee y \leq b$ lo que contradice (2). Por lo tanto (4) $x \not\leq b$ o (5) $y \not\leq b$. Como $x \leq x \vee y = i$ entonces por (1) $x \leq a$, por lo tanto si se cumple (4) resulta $x \in X$ y como $x \leq x \vee y = i$ resulta por (3) que $x = i$. Como (6) $y \leq x \vee y = i$ entonces de (6) y (1) resulta que (7) $y \leq a$. Por lo tanto si se verifica (5), de (7) y (5) resulta (8) $y \in X$. De (6), y (8) se deduce por (3) que $y = i$. ■

Ejemplo 2.4.2 *Consideremos el reticulado indicado en el Ejemplo 2.4.1, 2). Tenemos que* $c \not\leq 0$, *a es un elemento irreducible que verifica* $a \leq c$ *y* $a \not\leq 0$. *El elemento b que también es irreducible verifica* $b \leq c$ *y* $b \not\leq 0$. *También ocurre que* $c \not\leq d$, *en este caso el único elemento irreducible que verifica ambas condiciones es el elemento a.*

Corolario 2.4.1 *En todo reticulado R finito, no trivial, existen elementos irreducibles.*

Dem. Como R es finito tiene primer elemento 0, y como R es no trivial existe por lo menos un elemento $x \in R$, $x \neq 0$, por lo tanto $x \not\leq 0$ y en consecuencia por el Teorema 2.4.2 existe un elemento irreducible i tal que $i \leq x$, $i \not\leq 0$. ■

Teorema 2.4.3 *Si R es un reticulado finito, no trivial, todo elemento diferente del primer elemento es supremo de elementos irreducibles.*

Dem. Sea $a \in R$, $a \neq 0$, luego $a \not\leq 0$, entonces por el Teorema 2.4.2 existe un elemento irreducible i tal que $i \leq a$. Sea $X = \{i_1, i_2, \ldots, i_n\}$ el conjunto de todos los elementos irreducibles de R que verifican $i_j \leq a$ para $j = 1, 2, \ldots, n$. Luego $b = \bigvee_{j=1}^{n} i_j \leq a$. Si $b \neq a$, esto es, $b < a$, entonces $a \not\leq b$; luego por el teorema anterior existe un elemento irreducible i tal que (1) $i \leq a$ y (2) $i \not\leq b$. De (1) resulta que $i \in X$, luego $i = i_j$ para algún j, $1 \leq j \leq n$. Luego (3) $i = i_j \leq \bigvee_{j=1}^{n} i_j = b$. Como (2) y (3) se contradicen tenemos que $a = b = \bigvee_{j=1}^{n} i_j$. ■

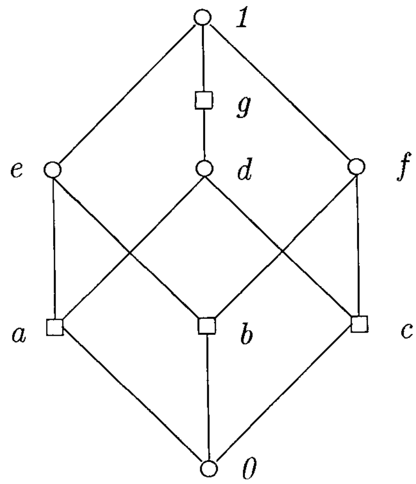
Acabamos así de probar que si R es un reticulado finito no trivial, $a \in R$, y $a \neq 0$, entonces a es supremo de todos los elementos irreducibles que lo preceden.

Consideremos el reticulado indicado en el Ejemplo 2.4.1, 1). Entonces tenemos que: $1 = a \vee b \vee c \vee d$ y también que $1 = a \vee b$, $1 = a \vee c$, y $1 = b \vee c$. Esto nos indica que existen varias *representaciones* del elemento 1 como supremo de elementos irreducibles.

Definición 2.4.2 *Una representación de un elemento* $a \neq 0$ *como supremo de elementos irreducibles* $a = i_1 \vee i_2 \vee \ldots \vee i_n$ *se dice* **irredundante** *si* $a \neq \bigvee_{x \in X_j} x$ *para todo* j, $1 \leq j \leq n$, *donde* $X_j = \{i_1, i_2, \ldots, i_n\} - \{i_j\}$.

En el Ejemplo 2.4.1, 1) todas las representaciones irredundantes del elemento 1 tienen la misma cantidad de elementos. Veamos que esto no siempre ocurre.

Ejemplo 2.4.3 *Sea R el reticulado cuyo diagrama se indica:*



Entonces $1 = b \vee g$ y $1 = a \vee b \vee c$ son representaciones irredundantes del elemento 1.

Definición 2.4.3 *Un elemento p de un reticulado se dice* **primo** *si:*

P1) p no es primer elemento de R.

P2) Si $p \leq a \vee b$ entonces $p \leq a$ ó $p \leq b$.

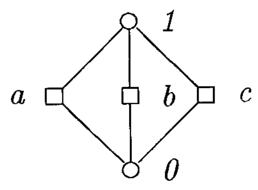
Observemos que si el reticulado R no tiene primer elemento la condición P1) es *trivialmente verificada.*

Lema 2.4.2 *En un reticulado R todo elemento primo es irreducible.*

Dem. Si p es un elemento primo de R entonces p no es primer elemento de R, luego se verifica I1). Supongamos que $p = a \vee b$, luego en particular tenemos que $p \leq a \vee b$ y como p es primo resulta que $p \leq a$ ó $p \leq b$. Pero $a \leq a \vee b = p$ y $b \leq a \vee b = p$ luego, $p = a$ ó $p = b$. ■

La recíproca de este lema no es verdadera. En efecto:

Ejemplo 2.4.4 *Consideremos el reticulado A cuyo diagrama se indica:*



El elemento a es irreducible, dado que es un átomo de A. Se verifica que $a \leq b \vee c = 1$ y $a \not\leq b$ y $a \not\leq c$, por lo tanto a no es primo.

3 RETICULADOS DISTRIBUTIVOS

3.1 Conceptos preliminares

Definición 3.1.1 *Un reticulado R se dice* **distributivo** *si verifica la siguiente propiedad* (ley distributiva del ínfimo con respecto al supremo)*:*

$$\text{(D)} \quad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \quad \textit{cualesquiera que sean } x, y, z \in R.$$

El reticulado indicado en el ejemplo 2.4.4 no es distributivo, ya que $a \wedge (b \vee c) = a \wedge 1 = a$ y $(a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0$.

Lema 3.1.1 *En todo reticulado la condición* (D) *es equivalente a:*

$$\text{(D}'\text{)} \quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

que se denomina: ley distributiva del supremo con respecto al ínfimo.

Dem. (D) $\Longrightarrow$ (D'). $(x \vee y) \wedge (x \vee z) = \text{(porD)} = [(x \vee y) \wedge x] \vee [(x \vee y) \wedge z] = x \vee [(x \wedge z) \vee (y \wedge z)] = [x \vee (x \wedge z)] \vee (y \wedge z) = x \vee (y \wedge z)$.
(D') $\Longrightarrow$ (D). Se demuestra en forma análoga. ■

Lema 3.1.2 *En todo reticulado las condiciones* (D) *y* (D') *son equivalentes a :*

$$\text{(D'')} \quad (x \vee y) \wedge (x \vee z) \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z).$$

Dem. (D') $\Longrightarrow$ (D"). Vimos que (D') $\Longleftrightarrow$ (D). Por lo indicado en el capítulo anterior tenemos que $(*)$ $x \wedge y \leq x \vee y$. Entonces:

$$(x \wedge y) \vee (x \wedge z) \vee (y \wedge z) = [\text{por (D)}] = (x \wedge y) \vee [(x \vee y) \wedge z] = [\text{por (D}')] =$$
$$[(x \wedge y) \vee (x \vee y)] \wedge [(x \wedge y) \vee z] = [\text{por } (*)] = (x \vee y) \wedge [(x \wedge y) \vee z] = [\text{por (D}')] =$$
$$(x \vee y) \wedge (x \vee z) \wedge (y \vee z).$$

(D") $\Longrightarrow$ (D). Probemos en primer lugar que:

$$(**) \quad \text{Si } x \leq z \Longrightarrow (x \vee y) \wedge z = x \vee (y \wedge z) = (x \wedge z) \vee (y \wedge z).$$

En efecto de $x \leq z$ resulta (1) $x = x \wedge z$ y (2) $x \vee z = z$. Por (D"):

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

luego teniendo en cuenta (1) y (2) tenemos que:

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

luego por las leyes de absorción, C1) y C2):

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

y teniendo en cuenta (1), resulta:

$$(3) \quad (x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z).$$

Por (D") tenemos que:

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

Haciendo el ínfimo de ambos miembros con z tenemos:

$$(x \vee y) \wedge (x \vee z) \wedge (y \vee z) \wedge z = [(x \wedge y) \vee (x \wedge z) \vee (y \wedge z)] \wedge z.$$

Luego teniendo en cuenta, sucesivamente una de las leyes de absorción:

$$(x \vee y) \wedge (x \vee z) \wedge z = [(x \wedge y) \vee (x \wedge z) \vee (y \wedge z)] \wedge z.$$

$$(4) \quad (x \vee y) \wedge z = [(x \wedge y) \vee (x \wedge z) \vee (y \wedge z)] \wedge z.$$

Como $x' = (x \wedge z) \vee (y \wedge z) \leq z$ resulta por $(**)$ que:

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

luego

$$[(x \wedge z) \vee (y \wedge z) \vee (x \wedge y)] \wedge z = [((x \wedge z) \vee (y \wedge z)) \wedge z] \vee (x \wedge y \wedge z),$$

esto es,

$$[(x \wedge z) \vee (y \wedge z) \vee (x \wedge y)] \wedge z = (x \wedge z) \vee (y \wedge z) \vee (x \wedge y \wedge z)$$

y como $x \wedge y \wedge z \leq x \wedge z$ y $x \wedge y \wedge z \leq y \wedge z$, tenemos finalmente que:

$$(5) \quad [(x \wedge z) \vee (y \wedge z) \vee (x \wedge y)] \wedge z = (x \wedge z) \vee (y \wedge z).$$

De (4) y (6) se deduce (D). ■

Lema 3.1.3 *En todo reticulado distributivo vale la ley de simplificación (o de cancelación), que dice: Si* $a \wedge x = a \wedge y$ *y* $a \vee x = a \vee y$ *entonces* $x = y$.

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

Lema 3.1.4 *Si R es un reticulado que verifica la ley de simplificación entonces:*

$$\text{(C)} \qquad [(x \wedge z) \vee y] \wedge z = (x \wedge z) \vee (y \wedge z).$$

Dem. Sean $p = (x \wedge z) \vee (y \wedge z)$ y $q = [(x \wedge z) \vee y] \wedge z$. Como $x \wedge z \leq z$ y $x \wedge z \leq (x \wedge z) \vee y$ entonces (1) $x \wedge z \leq q$. Análogamente como $y \wedge z \leq z$ e $y \wedge z \leq y \leq (x \wedge z) \vee y$ entonces (2) $y \wedge z \leq q$. De (1) y (2) resulta $p \leq q$ y por lo tanto $p \wedge y \leq q \wedge y$ y $p \vee y \leq q \vee y$. Como $q \wedge y = [(x \wedge z) \vee y] \wedge z \wedge y = z \wedge y \leq p \wedge y$. Como $z \leq z \vee y$ entonces (3) $[(x \wedge z) \vee y] \wedge z \leq [(x \wedge z) \vee y] \wedge (z \vee y)$. Además (4) $y \leq [(x \wedge z) \vee y] \wedge (z \vee y)$. De (3) y (4) resulta que $[(x \wedge z) \vee y] \wedge z] \vee y \leq [(x \wedge z) \vee y] \wedge (z \vee y)$ y por lo tanto tenemos que $q \vee y = [[(x \wedge z) \vee y] \wedge z] \vee y \leq [(x \wedge z) \vee y] \wedge (z \vee y) \leq (x \wedge z) \vee y = p \vee y$. Luego tenemos que $p \wedge y = q \wedge y$ y $p \vee y = q \vee y$, de donde se deduce por la ley de simplificación que $p = q$. ■

Lema 3.1.5 *En todo reticulado la condición* (C) *es equivalente a la condición:*

$$\text{(C')} \qquad [(x \vee z) \wedge y] \vee z = (x \vee z) \wedge (y \vee z).$$

Dem. (C) $\Rightarrow$ (C'). Como

$$(x \vee z) \wedge (y \vee z) = (z \vee y) \wedge (x \vee z) = [[z \wedge (x \vee z)] \vee y] \wedge (x \vee z) = \text{ (por (C))}$$

$$[z \wedge (x \vee z)] \vee [y \wedge (x \vee z)] = z \vee [y \wedge (x \vee z)] = [(x \vee z) \wedge y] \vee z.$$

(C') $\Rightarrow$ (C).

$$(x \wedge z) \vee (y \wedge z) = (z \wedge y) \vee (x \wedge z) = [[z \vee (x \wedge z)] \wedge y] \vee (x \wedge z) = \text{ (por (C'))}$$

$$[z \vee (x \wedge z)] \wedge [y \vee (x \wedge z)] = z \wedge [y \vee (x \wedge z)] = [(x \wedge z) \vee y] \wedge z.$$

■

Lema 3.1.6 *Todo reticulado donde vale la ley de simplificación es distributivo.*
(O. Ore, *On the foundations of abstract algebra I,* Annals of Math. 36 (1935), 406-443 *y On the foundations of abstract algebra II,* Annals of Math. 37 (1936), 265-292).

Dem. Sean $r = [(x \vee z) \wedge y] \vee (x \wedge z)$ y $s = [(y \vee z) \wedge x] \vee (y \wedge z)$, entonces

$$r \wedge z = \Big[[(x \vee z) \wedge y] \vee (x \wedge z)\Big] \wedge z = \Big[(x \wedge z) \vee [(x \vee z) \wedge y]\Big] \wedge z = \text{ (por (C))}$$

$$(x \wedge z) \vee [(x \vee z) \wedge y \wedge z] = (x \wedge z) \vee (y \wedge z).$$

$$s \wedge z = \Big[[(y \vee z) \wedge x] \vee (y \wedge z)\Big] \wedge z = \Big[(y \wedge z) \vee [(y \vee z) \wedge x]\Big] \wedge z = \text{ (por (C))}$$

$$(y \wedge z) \vee [(y \vee z) \wedge x \wedge z] = (y \wedge z) \vee (x \wedge z).$$

Acabamos así de probar que $r \wedge z = s \wedge z$. Vamos a demostrar que tambien $r \vee z = s \vee z$, de donde resultará por la ley de simplificación que $r = s$.
En virtud de la condición (C') indicada en el Lema 3.1.5 tenemos

$$r \vee z = [(x \vee z) \wedge y] \vee (x \wedge z) \vee z = [(x \vee z) \wedge y] \vee z = (x \vee z) \wedge (y \vee z),$$

y tambien que $s \vee z = [(y \vee z) \wedge x] \vee (y \wedge z) \vee z = [(y \vee z) \wedge x] \vee z = (y \vee z) \wedge (x \vee z)$.
Acabamos así de probar que $r = s$ y por lo tanto tenemos que (1) $r \vee s = r \wedge s$.

$$r \vee s = [(x \vee z) \wedge y] \vee (x \wedge z) \vee [(y \vee z) \wedge x] \vee (y \wedge z) =$$

$$[(x \vee z) \wedge y] \vee (y \wedge z) \vee [(y \vee z) \wedge x] \vee (x \wedge z)$$

Luego como $y \wedge z \leq (x \vee z) \wedge y$ y $x \wedge z \leq (y \vee z) \wedge x$ tenemos que

$$r \vee s = [(x \vee z) \wedge y] \vee [(y \vee z) \wedge x]$$

y como $(y \vee z) \wedge x \leq x \leq x \vee z$ podemos escribir

$$r \vee s = \Big[\Big[[(y \vee z) \wedge x] \vee (x \vee z)\Big] \wedge y\Big] \vee [(y \vee z) \wedge x] = \text{ (por (C'))}$$

$$\Big[[(y \vee z) \wedge x] \vee (x \vee z)\Big] \wedge \Big[y \vee [(y \vee z) \wedge x]\Big]$$

y nuevamente como $(y \vee z) \wedge x \leq x \vee z$ tenemos

$$(2)\ r \vee s = (x \vee z) \wedge \Big[[(y \vee z) \wedge x] \vee y\Big] = (x \vee z) \wedge \Big[[(z \vee y) \wedge x] \vee y\Big] = \text{ (por (C'))}$$

$$(x \vee z) \wedge (z \vee y) \wedge (x \vee y).$$

En forma análoga se prueba que:

$$(3)\ r \wedge s = (x \wedge y) \vee (y \wedge z) \vee (z \wedge x).$$

De (1), (2) y (3) se deduce que:

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

esto es se verifica la condición (D") indicada en el Lema 3.1.2 y en consecuencia el reticulado es distributivo. ■

Lema 3.1.7 *Un sistema $(A, \wedge, \vee)$ es un reticulado distributivo si y solamente si se verifican:*

S1) $a \wedge (a \vee b) = a$

S2) $a \wedge (b \vee c) = (c \wedge a) \vee (b \wedge a)$

(M. Sholander, *Postulates for distributive lattices,* Canad. Journ. Math., 3 (1951), 28-30).

Definición 3.1.2 *Una familia $\mathcal{F}$, no vacía, de subconjuntos de un conjunto fijo A se denomina* **un anillo de conjuntos** *si verifica:*

$$\text{Si} \quad X, Y \in \mathcal{F} \Longrightarrow X \cap Y,\ X \cup Y \in \mathcal{F}.$$

Indicaremos a continuación ejemplos de reticulados distributivos.

1) Si $\mathcal{F}$ es un anillo de conjuntos entonces $(\mathcal{F}, \cap, \cup)$. es un reticulado distributivo.

2) Toda cadena C es un reticulado distributivo. Para ello basta considerar elementos $a, b, c \in C$ y probar que vale una de las leyes distributivas en los siguientes casos posibles $a \leq b \leq c$, $a \leq c \leq b$, $b \leq a \leq c$, $b \leq c \leq a$, $c \leq a \leq b$, $c \leq b \leq a$.

3) $(\mathbb{N}_0, /)$ es un reticulado distributivo.
Ya vimos que $(\mathbb{N}_0, /)$ es un conjunto ordenado. Este conjunto ordenado tiene por primer elemento al número 1 y por último elemento al número 0, ya que:

$$(*)\ \ 1/a, \quad a/0, \quad \forall\, a \in \mathbb{N}_0.$$

Para probar que es un reticulado distributivo, hay que demostrar en primer lugar que <u>todo par</u> de elementos de $\mathbb{N}_0$ tiene un ínfimo y un supremo y luego que vale la ley distributiva (D).
De $(*)$ resulta por lemas anteriores que: $1 = 1 \wedge a, a = 1 \vee a, a = 0 \wedge a$ y $0 = 0 \vee a$, $\forall\, a \in \mathbb{N}_0$.
Sean $a, b \in \mathbb{N}_0 - \{0, 1\}$ entonces como (i) $mcd\{a, b\}/a$, $mcd\{a, b\}/b$ y (ii) Si x/a y x/b entonces $x/mcd\{a, b\}$ resulta que $mcd\{a, b\} = a \wedge b$. Análogamente se demuestra que $mcm\{a, b\} = a \vee b$. Por lo tanto $(\mathbb{N}_0, /)$ es un reticulado.
Recordemos que si $a, b \neq 0, 1$ y $a = p_1^{e_1}.p_2^{e_2}. \ \ldots \ .p_t^{e_t}$, $b = p_1^{f_1}.p_2^{f_2}. \ \ldots \ .p_t^{f_t}$, donde

$p_1, p_2, \ldots, p_t$ son números primos positivos y $e_1, e_2, \ldots, e_t, f_1, f_2, \ldots, f_t$ son enteros no negativos entonces:

$$a \wedge b = mcd\{a, b\} = \prod p_i^{min\{e_i, f_i\}} = \prod p_i^{(e_i \wedge f_i)}$$

y

$$a \vee b = mcm\{a, b\} = \prod p_i^{max\{e_i, f_i\}} = \prod p_i^{(e_i \vee f_i)}.$$

Antes de probar que se verifica la ley distributiva vamos a demostrar algunas propiedades de este reticulado:

3.1) p es un átomo de $\mathbb{N}_0$ $\Longleftrightarrow$ p es primo (aritmético) de $\mathbb{N}_0$.
$\Longrightarrow$) Si p es átomo de $\mathbb{N}_0$ entonces p cubre a 1, esto es $1/p$, $p \neq 1$ y no existe ningún $x \in \mathbb{N}_0$ tal que $1 \,/\, x \,/ p$ con $x \neq 1$, $x \neq p$.
Queremos probar que p es primo aritmético de $\mathbb{N}_0$ esto es que (1) $p \neq 0, p \neq 1$ y que (2) Si $d \in \mathbb{N}_0$ verifica d/p entonces $d = 1$ ó $d = p$.
Por hipótesis $p \neq 1$. Si $p = 0$ como $1 \,/ 2 \,/ 0 = p$, p no sería átomo de $\mathbb{N}_0$. Supongamos que $d \in \mathbb{N}_0$ verifica d/p, luego como p es átomo de $\mathbb{N}_0$ tenemos que $d = 1$ ó $d = p$.
$\Longleftarrow$) Si $p \in \mathbb{N}_0$ es un primo aritmético entonces $p \neq 0, 1$, en particular $p \neq 1$ esto es p es diferente del primer elemento de $\mathbb{N}_0$. Supongamos que existe $x \in \mathbb{N}_0$ tal que $1 \,/\, x \,/ p$. Como p es primo aritmético de $\mathbb{N}_0$ entonces de x/p resulta que $x = p$ ó, $x = 1$. Luego no existe ningún $x \in \mathbb{N}_0$, $x \neq p$, $x \neq 1$ tal que $1 \,/\, x \,/ p$, lo que prueba que p es un átomo.

3.2) $x \in \mathbb{N}_0$ es irreducible $\Longleftrightarrow$ $x = 0$ ó x es potencia natural de un primo aritmético.
$\Longrightarrow$) Supongamos que $x \in \mathbb{N}_0$ es irreducible, luego es diferente del primer elemento de $\mathbb{N}_0$, esto es $x \neq 1$. En consecuencia $x = 0$ ó $x > 1$.
Si $x > 1$ entonces $x = p_1^{e1}.p_2^{e2}. \ldots .p_t^{et} = a \vee b$, donde $a = p_1^{e1}$ y $b = p_2^{e2}. \ldots .p_t^{et}$, y $p_1, p_2, \ldots, p_t$ son números primos y $e_1, e_2, \ldots, e_t$ enteros positivos.
Como x es irreducible entonces (1) $x = a = p_1^{e1}$, ó (2) $x = b = p_2^{e2}. \ldots .p_t^{et}$, etc.
$\Longleftarrow$) Supongamos que $x = 0$ ó $x = p^n$ donde p es un número primo y n un entero positivo. Si $x = 0$ entonces $x \neq 1$, esto es x es diferente del primer elemento. Supongamos que $a \vee b = 0$, esto es que $mcm\{a, b\} = 0$, y que $a \neq 0$, $b \neq 0$. Entonces $a = 1$ ó $a > 1$ y $b = 1$ ó $b > 1$. Si $a = 1$ entonces $1 \vee b = b \neq 0$. Si $a > 1$ entonces $a = p_1^{e1}.p_2^{e2}. \ldots .p_r^{er}$.Luego si $b = 1$ tenemos $a \vee b = a \vee 1 = a \neq 0$ y en el otro caso $a \vee b \neq 0$.
Si $x = p^n$, donde p es primo aritmético entonces $x \neq 1$. Supongamos que $x = p^n = a \vee b = mcm\{a, b\} = p_1^{(e_1 \vee f_1)}.p_2^{(e_2 \vee f_2)}. \ldots .p_t^{(e_t \vee f_t)}$, como la descomposición en factores primos es única, a menos del orden de los factores, entonces $p^n = p_s^{(e_s \vee f_s)}$ y como $e_s \vee f_s = e_s$ ó $e_s \vee f_s = f_s$, entonces $p^n = p_s^{e_s}$ ó $p^n = p_s^{f_s}$. Ahora bien $mcm\{a, b\} = p_s^{(e_s \vee f_s)} \Longleftrightarrow a = p_s^{e_s}$ y $b = p_s^{f_s}$ ó $a = p_s^{f_s}$ y $b = p_s^{e_s}$, luego $p^n = a$ ó $p^n = b$.

Probemos que el reticulado $\mathbb{N}_0$ es distributivo.
Si $a = 0$ entonces: $a \wedge (b \vee c) = 0 \wedge (b \vee c) = b \vee c$ y $(0 \wedge b) \vee (0 \wedge c) = b \vee c$.

En forma análoga se demuestra para los casos $b = 0$, $c = 0$.
Si $a = 1$ entonces: $a \wedge (b \vee c) = 1 \wedge (b \vee c) = 1$ y $(1 \wedge b) \vee (1 \wedge c) = 1 \vee 1 = 1$.
En forma análoga se demuestra para los casos $b = 1$, $c = 1$.
Si $a, b, c \neq 0, 1$ entonces:

$$a \wedge (b \vee c) = \prod p_i^{[e_i \wedge (f_i \vee g_i)]}$$

y

$$(a \wedge b) \vee (a \wedge c) = \prod p_i^{(e_i \wedge f_i)} \vee \prod p_i^{(e_i \wedge g_i)} =$$

$$\prod p_i^{[(e_i \wedge f_i) \vee (e_i \wedge g_i)]} = \prod p_i^{[e_i \wedge (f_i \vee g_i)]}.$$

4) Sea E un conjunto no vacío, y $\mathcal{F}$ una familia de partes de E que verifican: (1) $\emptyset, E \in \mathcal{F}$, (2) Si $\{F_i\}_{i \in I}$ es una familia no vacía, donde $F_i \in \mathcal{F}$, para todo $i \in I$, entonces $\bigcap\limits_{i \in I} F_i \in \mathcal{F}$, (3) Si $X, Y \in \mathcal{F}$ entonces $X \cup Y \in \mathcal{F}$.
Al par $(E, \mathcal{F})$ se denomina espacio topológico, y todo elemento $F \in \mathcal{F}$ se lo denomina conjunto cerrado del espacio topológico. Observemos que de las condiciones (2) y (3) resulta que $\mathcal{F}$ es un anillo de conjuntos, por lo tanto $(\mathcal{F}, \cap, \cup)$ es un reticulado distributivo con primer elemento $(\emptyset)$ y último elemento (E).

Dada una familia de reticulados $\{(R_i, \wedge_i, \vee_i)\}_{i \in I}$, sea $P = \prod\limits_{i \in I} R_i$ el producto cartesiano de la familia de conjuntos $\{R_i\}_{i \in I}$, esto es el conjunto de todas las funciones $x : I \to \bigcup\limits_{i \in I} R_i$ tales que en cada elemento $i \in I$ toman un valor $x(i) = x_i \in R_i$. Se dice que x_i es la coordenada de indice i del elemento $x \in P$ y se nota $x = [x_i]_{i \in I}$, $x = [x_i]$, $x = (x_i)_{i \in I}$ ó $x = (x_i)$.
Dados $x = (x_i)_{i \in I} \in P$, $y = (y_i)_{i \in I} \in P$, pongamos por definición:

$$x \wedge y = (x_i \wedge_i y_i) \ \text{ y } \ x \vee y = (x_i \vee_i y_i).$$

Se prueba sin dificultad $(P, \vee, \wedge)$ es un reticulado, al que se denomina **producto cartesiano** ó **directo** de la familia de reticulados $\{(R_i, \wedge_i, \vee_i)\}_{i \in I}$. A veces se suele escribir $(R, \wedge, \vee) = \prod\limits_{i \in I} (R_i, \wedge_i, \vee_i)_{i \in I}$. Cada uno de los reticulados R_i recibe el nombre de **i-ésimo eje de coordenadas** ó **i-ésimo eje** .
Para cada $i \in I$ la función $p_i : \prod\limits_{i \in I} R_i \to R_i$, definida por $p_i(x) = x_i$ se denomina **proyección i-ésima**. Es claro que p_i es una función suryectiva.

Si $R_i = C$, $\forall\, i \in I$, entonces $\prod\limits_{i \in I} R_i$ es el conjunto de todas las funciones de I en C, por ello se nota C^I. Si el conjunto I es finito, por ejemplo $I = \{1, 2, \ldots, n\}$ entonces se utiliza cualquiera de las notaciones siguientes:

$$\prod_{i=1}^{n} R_i \qquad \text{ó} \qquad R_1 \times R_2 \times \ldots \times R_n$$

En este caso si $x \in \prod\limits_{i=1}^{n} R_i$ entonces: $x = (x(1), x(2), \ldots, x(n)) = (x_1, x_2, \ldots, x_n)$.

Lema 3.1.8 *El producto cartesiano de reticulados distributivos es un reticulado distributivo.*

Corolario 3.1.1 *El producto cartesiano de cadenas es un reticulado distributivo.*

Lema 3.1.9 *Si R es un reticulado distributivo entonces todo elemento irreducible de R es un elemento primo.*

Dem. Sea i un elemento irreducible de R, luego (1) i no es primer elemento de R. Probemos ahora que (ii) Si $i \leq a \vee b$, donde $a, b \in R$ entonces $i \leq a$ ó $i \leq b$. En efecto de $i \leq a \vee b$ resulta que $i = i \wedge (a \vee b)$ y como R es distributivo tenemos $i = (i \wedge a) \vee (i \wedge b)$, de donde resulta por ser i irreducible que $i = i \wedge a$ ó $i = i \wedge b$, esto es $i \leq a$ ó $i \leq b$. ■

Del Lema 3.1.9 y el Lema 2.4.2 resulta que en los reticulados distributivos las nociones de elemento irreducible y elemento primo coinciden.

Lema 3.1.10 *Para que en un reticulado finito, no trivial, R las nociones de elemento irreducible y elemento primo coincidan es necesario y suficiente que R sea distributivo.*

Dem. Por el Lema 3.1.9 es claro que la condición es suficiente. Sabemos que en cualquier reticulado vale la ley semidistributiva (ver Ejercicio 2.3.1.)

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

Supongamos que

$$a \wedge (b \vee c) \not\leq (a \wedge b) \vee (a \wedge c),$$

entonces como R es finito, no trivial, resulta por el Teorema 2.4.2 que existe un elemento irreducible (que por la hipótesis hecha es primo) $i \in R$ tal que: (1) $i \leq a \wedge (b \vee c)$ y (2) $i \not\leq (a \wedge b) \vee (a \wedge c)$.
De (1) resulta que (3) $i \leq a$ y (4) $i \leq b \vee c$. De (4) resulta por ser i un elemento primo que (5) $i \leq b$ ó (6) $i \leq c$. De (3) y (5) deducimos $i \leq a \wedge b \leq (a \wedge b) \vee (a \wedge c)$ lo que contradice (2). De (3) y (6) resulta $i \leq a \wedge c \leq (a \wedge b) \vee (a \wedge c)$ lo que contradice (2). ■

Dado un reticulado finito, no trivial, R por intermedio de su diagrama de Hasse, se plantea el problema de saber si R es distributivo, sin comprobar que se verifica alguna de las propiedades (D) ó (D'). De acuerdo con el resultado anterior basta demostrar que todo elemento irreducible es primo. El Teorema 2.4.1 nos da un método para determinar los elementos irreducibles de un reticulado finito, no trivial. Vamos a indicar un método para determinar los elementos primos de un reticulado finito, no trivial.

Lema 3.1.11 *En un reticulado finito, no trivial, R, p es un elemento primo $\Longleftrightarrow$ el conjunto ordenado $Z_p = \{z \in R : p \not\leq z\}$ tiene último elemento.*

Dem. $\Longrightarrow$) Dado un elemento primo p de R, consideremos el conjunto:

$$Z_p = \{z \in R : p \not\leq z\}.$$

Como $p \not\leq 0$, entonces $0 \in Z_p$, esto es $Z_p \neq \emptyset$. Luego como R es finito, no trivial, tenemos que Z_p es un conjunto finito no vacío. Sea $Z_p = \{z_1, z_2, \ldots, z_t\}$ y $z = \bigvee_{i=1}^{t} z_i$, luego $z_i \leq z$

para $i = 1, 2, \ldots, t$. Si probamos que $z \in Z_p$ entonces z será el último elemento de Z_p. Supongamos que $z \notin Z_p$, entonces $p \leq z = \bigvee_{i=1}^{t} z_i$, luego como p es primo resulta que $p \leq z_i$, para algún i, $1 \leq i \leq t$, absurdo.
$\Longleftarrow$) Sea p un elemento del reticulado, finito no trivial, R tal que el conjunto $Z_p = \{z \in R : p \not\leq z\}$ tiene último elemento. Luego, existe $u \in Z_p$ ($p \not\leq u$) tal que (i) $z \leq u$ para todo $z \in Z_p$. Probemos que p es primo.
(1) $p \neq 0$. En efecto, si $p = 0$, como $0 = p \leq z$ para todo $z \in R$ resultaría que Z_p es vacío, absurdo.
(2) Supongamos que (ii) $p \leq a \vee b$ y que $p \not\leq a$ y $p \not\leq b$, luego $a, b \in Z_p$, luego de (i) resulta que $a \leq u$, $b \leq u$ y en consecuencia (iii) $a \vee b \leq u$. De (ii) e (iii) resulta que $p \leq u$, absurdo.
Observemos que si notamos $W_p = \{w \in R : p \leq w\}$ entonces $Z_p = R \setminus W_p$. ■

Consideremos el reticulado indicado en el Ejemplo 2.4.1,2. Vimos que el conjunto de los elementos irreducibles es $\{a, b, d\}$. Determinemos los elementos primos: $W_a = \{a, c, 1\}$, luego $Z_a = \{0, b, d\}$ tiene último elemento y en consecuencia es primo. En forma análoga se ve que b y d son primos. Como $W_c = \{c, 1\}$, entonces $Z_c = \{0, a, b, d\}$ no tiene último elemento y por lo tanto no es primo. Lo mismo ocurre con el elemento 1.

Definición 3.1.3 *Sean* $(A, \wedge, \vee)$, $(A', \wedge, \vee)$ *reticulados. A toda función* $h : A \rightarrow A'$ *tal que:*

H2) $h(a \wedge b) = h(a) \wedge h(b)$,

H3) $h(a \vee b) = h(a) \vee h(b)$,

cualesquiera que sean $a, b \in A$, *se denomina* **homomorfismo** *de* A *en* A'. *Si* h *es suryectiva, se denomina* **epimorfismo** *y si* h *es biyectiva se denomina* **isomorfismo**.

Observación 3.1.1 *1) De cualquiera de las condiciones H2) ó H3) se deduce en forma inmediata que todo homomorfismo es una función isótona.*

2) Si A *y* A' *son reticulados con primer (*0 *y* $0'$ *respectivamente) y último elemento (*1 *y* $1'$ *respectivamente) a toda función* $h : A \rightarrow A'$ *que verifica H2), H3), H0)* $h(0) = 0'$ *y H1)* $h(1) = 1'$ *se denomina* $(0,1)$-**homomorfismo**.

3) Si A *y* A' *tienen primer y último elemento, y* $h : A \rightarrow A'$ *es un epimorfismo, entonces* h *es un* $(0,1)$*-homomorfismo. En efecto, como* $0 \leq a$ *cualquiera que sea* $a \in A$ *entonces como* h *es isótona tenemos que (1)* $h(0) \leq h(a)$, *cualquiera que sea* $a \in A$, *y como (2)* $h(A) = A'$, *de (1) y (2) resulta que* $h(0)$ *es primer elemento de* A', *esto es* $h(0) = 0'$. *Análogamente se prueba que* $h(1) = 1'$.

Teorema 3.1.1 (de Representación de Birkhoff) *Todo reticulado distributivo finito es isomorfo a un anillo de conjuntos.*

Dem. Sea R un reticulado distributivo finito. Si R tiene un sólo elemento es claro que R es isomorfo a $\mathcal{F} = \{\emptyset\}$.
Supongamos que R tiene más de un elemento y sea $\Pi = \Pi(R)$ el conjunto de todos sus elementos irreducibles (primos). Como R es finito, no trivial, sabemos por el Corolario 2.4.1 que $\Pi \neq \emptyset$.
Pongamos por definición:

$$\psi(a) = \{p \in \Pi : p \leq a\}, \; a \in R,$$

luego $\psi(a) \subseteq \Pi, \;\; \forall \;\, a \in R$.
Sea $\mathcal{F} = \{\psi(a)\}_{a \in R}$. Vamos a demostrar que R es isomorfo a $(\mathcal{F}, \cap, \cup)$. Es claro que ψ es una función de R sobre $\mathcal{F}$. Observemos que:

1) $\psi(x) = \emptyset \iff x = 0$.
Si $x = 0$ no existe $p \in \Pi$ tal que $p \leq 0$, luego $\psi(x) = \emptyset$. Si $\psi(x) = \emptyset$ con $x \neq 0$ entonces $x \not\leq 0$, luego existiría $p \in \Pi$ tal que $p \leq x$ y por lo tanto $p \in \psi(x)$, absurdo.

2) $\psi(1) = \{p \in \Pi : p \leq 1\} = \Pi$.

3) ψ es inyectiva.
Supongamos que $\psi(a) = \psi(b)$. Si $\psi(a) = \psi(b) = \emptyset$ entonces $a = 0 = b$. Si $\psi(a) = \psi(b) \neq \emptyset$ entonces $a \neq 0$ y $b \neq 0$ y sabemos por el Teorema 2.4.3 que todo elemento diferente de 0 es supremo de todos los elementos irreducibles (primos) que lo preceden, luego de

$$\{p \in \Pi : p \leq a\} = \{q \in \Pi : q \leq b\}$$

resulta

$$a = \bigvee\{p \in \Pi : p \leq a\} = \bigvee\{q \in \Pi : q \leq b\} = b.$$

4) $\psi(a \wedge b) = \psi(a) \cap \psi(b)$. Si $\psi(a) = \emptyset$ ó $\psi(b) = \emptyset$ es claro que se verifica 4).
$p \in \psi(a \wedge b) \iff p \in \Pi$ y $p \leq a \wedge b \iff p \in \Pi$, $p \leq a$ y $p \leq b \iff p \in \psi(a)$ y $p \in \psi(b) \iff p \in \psi(a) \cap \psi(b)$.

5) $\psi(a \vee b) = \psi(a) \cup \psi(b)$. Si $\psi(a) = \emptyset$ ó $\psi(b) = \emptyset$ es claro que se verifica 5).
$p \in \psi(a \vee b) \iff p \in \Pi$ y $p \leq a \vee b$, luego teniendo en cuenta que p es primo podemos afirmar que la condición precedente es equivalente a $p \in \Pi$ y $p \leq a$ ó $p \in \Pi$ y $p \leq b$ lo que equivale a: $p \in \psi(a)$ ó $p \in \psi(b) \iff p \in \psi(a) \cup \psi(b)$.

De 4) y 5) resulta que $\mathcal{F}$ es un anillo de conjuntos. ∎

Vimos en el Ejemplo 2.4.3 que en un reticulado finito, un elemento $a \neq 0$ puede tener varias representaciones irredundantes (como supremo de irreducibles).

Lema 3.1.12 *En un reticulado distributivo finito R, si $a \neq 0$, a tiene una única representación irredundante como supremo de elementos irreducibles (primos), única a menos del orden en que aparecen los factores.*

Dem. Sea $a \neq 0$ y supongamos que:

$$a = i_1 \vee i_2 \vee \ldots \vee i_s = p_1 \vee p_2 \vee \ldots \vee p_t$$

donde $i_j, p_k \in \Pi = \Pi(R)$, $1 \leq j \leq s$ $1 \leq k \leq t$, son representaciones irredundantes de a. Por lo tanto si (1) $1 \leq j_1, j_2 \leq s$ y $j_1 \neq j_2$ entonces $i_{j_1} \neq i_{j_2}$ y si (2) $1 \leq k_1, k_2 \leq t$ y $k_1 \neq k_2$ entonces $p_{k_1} \neq p_{k_2}$. Sean $I = \{i_1, i_2, \ldots, i_s\}$, $P = \{p_1, p_2, \ldots, p_t\}$, luego

$$\forall\, j,\ 1 \leq j \leq s,\ a \neq \bigvee \{x : x \in X_j\},\ \text{ donde } X_j = I \setminus \{i_j\},$$

$$\forall\, k,\ 1 \leq k \leq t,\ a \neq \bigvee \{y : y \in Y_k\},\ \text{ donde } Y_k = P \setminus \{p_k\}.$$

Probemos que $I = P$. Sea $x \in I$, luego $x = i_j$, $1 \leq j \leq s$. Como

$$x = i_j \leq i_1 \vee i_2 \vee \ldots \vee i_s = p_1 \vee p_2 \vee \ldots \vee p_t$$

e $i_j \in \Pi$ existe k tal que (3) $i_j \leq p_k$.
Como

$$p_k \leq p_1 \vee p_2 \vee \ldots \vee p_t = i_1 \vee i_2 \vee \ldots \vee i_s$$

y $p_k \in \Pi$ existe r, $1 \leq r \leq s$ tal que (4) $p_k \leq i_r$. De (3) y (4) resulta que $i_j \leq i_r$. Si $i_j < i_r$, esto es $i_j \vee i_r = i_r$ entonces la representación no sería irredundante, luego $i_j = i_r$ y en consecuencia $j = r$ pues caso contrario $i_j = i_r$ con $j \neq r$ contradice (1). Tenemos así que $i_j \leq p_k \leq i_j$, esto es $i_j = p_k \in P$. Análogamente se muestra que $P \subseteq I$, y como los elementos de cada conjunto son diferentes dos a dos tenemos que $s = t$. ■

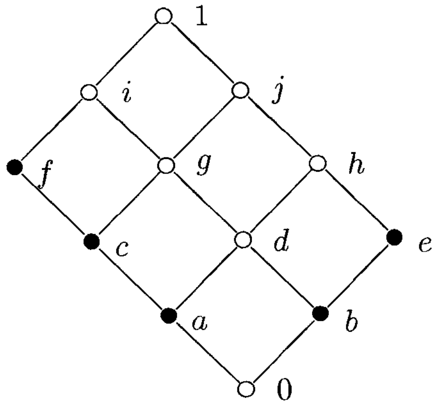
Sea R un reticulado distributivo finito, no trivial, 0 y 1 el primer y último elemento de R. Si $a \in R$, $a \neq 0$ notaremos $\Pi(a) = \{p \in \Pi : p \leq a\}$. Sabemos que $\Pi(a) \neq \emptyset$. Como R es finito entonces $\Pi(a)$ es un conjunto ordenado finito, luego tiene por lo menos un elemento máximo.

Lema 3.1.13 *Si $m_1, m_2, \ldots, m_t$ son los elementos máximos de $\Pi(a)$, entonces la única representación irredundante de a es $a = \bigvee_{i=1}^{t} m_i$.*

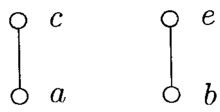
Dem. Como $m_i \in \Pi(a)$, para $1 \leq i \leq t$, esto es $m_i \leq a$, para $1 \leq i \leq t$ y por lo tanto $m = \bigvee_{i=1}^{t} m_i \leq a$. Supongamos que $m \neq a$ luego $a \not\leq m$ y en consecuencia por el Teorema 2.4.2 existe un elemento irreducible (primo) p que precede al elemento a y no precede a m. Esto esto, existe (1) $p \in \Pi$ tal que (2) $p \leq a$ y (3) $p \not\leq m$. De (1) y (2) resulta que $p \in \Pi(a)$, luego existe un indice i tal que $p \leq m_i$ y como $m_i \leq m$ tenemos que $p \leq m$, lo que contradice (3). Acabamos así de probar que $a = \bigvee_{i=1}^{t} m_i$.

Probemos que esta descomposición es irredundante. En efecto si $a = \bigvee_{i=1,\, i=i_0}^{t} m_i$, entonces $m_{i_0} \leq \bigvee_{i=1}^{t} m_i = a = \bigvee_{i=1,\, i=i_0}^{t} m_i$, luego como m_{i_0} es un elemento primo tenemos que $m_{i_0} \leq m_i$ para algún i, $1 \leq i \leq n$, $i \neq i_0$, absurdo. ■

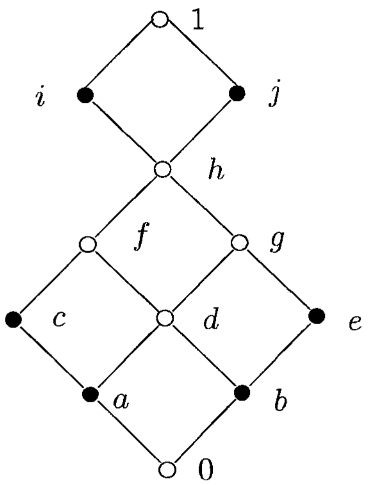
Observemos que si $p \in \Pi(R)$ entonces la representación irredundante de p es el propio elemento p.
Consideremos el reticulado R cuyo diagrama se indica, donde los elementos primos están marcados con •.



Entonces el diagrama de Hasse de $\Pi(j) = \{a, b, c, e\}$ es

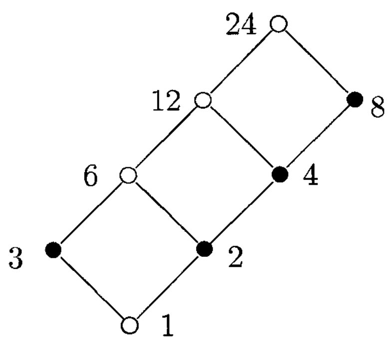


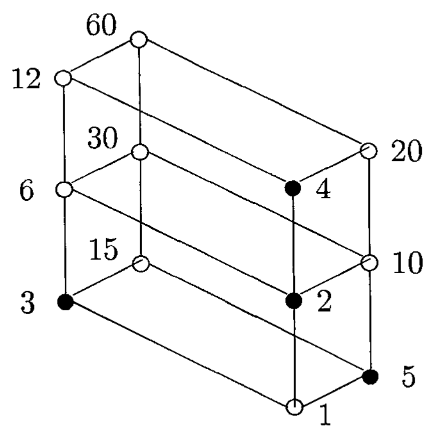
luego sus elementos máximos son c y e y en consecuencia la representación irredundante de j es $j = c \vee e$. Análogamente $i = f \vee b$, $h = a \vee e$, son representacinones irredundantes En el reticulado S cuyo diagrama se indica, donde los elementos primos están marcados con $\bullet$



tenemos que $1 = i \vee j$, $f = c \vee b$, $h = c \vee e$ son representaciones irredundantes.

Observación 3.1.2 *El reticulado distributivo* $(\mathbb{N}_0, /)$ *no es finito pero si consideramos el subconjunto* $D(u) = \{y \in \mathbb{N}_0 : y/u\}$, *donde* $u \in \mathbb{N}_0$, $u \neq 0$, *entonces* $D(u)$ *es un reticulado distributivo finito con primer elemento* 1 *y último elemento* u. *Si la descomposición en primos de* $x \in D(u)$ *es* $x = p_1^{e_1}.p_2^{e_2}.\dots.p_n^{e_n}$, *los elementos irreducibles (primos) de* $D(u)$ *son* $p_i^{f_i}$ $1 \leq i \leq n$, $1 \leq f_i \leq e_i$. *Todo elemento* $y \in D(u)$, $y \neq 1$ *se expresa en forma única como supremo de elementos irreducibles (primos) máximos de* $D(u)$ *que lo preceden y estos son precisamente los primos aritméticos que aparecen en la descomposición de* y *elevados a la máxima potencia. Indiquemos dos ejemplos:*





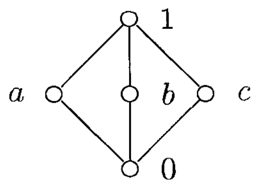
En el primer ejemplo tenemos que $12 = 2^2 \vee 3 = mcm\{4,3\}$. En el segundo ejemplo $60 = 2^2 \vee 3 \vee 5 = mcm\{12,20\}$.

3.2 Complemento de un elemento

Un elemento b de un reticulado R con primer (0) y último elemento (1) se denomina **el complemento de** $a \in R$ si :

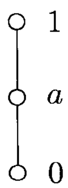
$$a \wedge b = 0 \qquad \text{y} \qquad a \vee b = 1.$$

Consideremos el reticulado cuyo diagrama de Hasse se indica:



Como $a \wedge b = 0$, $a \vee b = 1$, $a \wedge c = 0$, $a \vee c = 1$ tenemos que b y c son complementos de a.

Si R es distributivo y a tiene complemento entonces él es único. En efecto si $a \wedge b = 0 = a \wedge c$ y $a \vee b = 1 = a \vee c$ entonces por la ley de cancelación resulta que $b = c$.
Observemos que el elemento a del reticulado cuyo diagrama de Hasse se indica a continuación no tiene complemento.



Si R es un reticulado distributivo con primer (0) y último (1) elemento, y $a \in R$ tiene complemento, lo notaremos con $-a$ y diremos que a es un **elemento booleano** de R. Al conjunto de todos los elementos booleanos de R lo notaremos $B(R)$. Es claro que $0, 1 \in B(R)$.

Lema 3.2.1 *Si $R = R_{0,1}$ es un reticulado distributivo entonces:*

1) *Si $a \in B(R)$ entonces $--a = a$.*

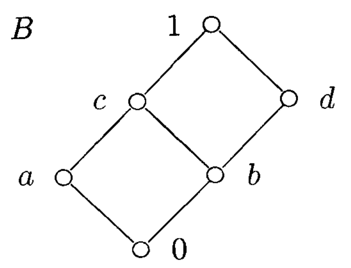
2) *Si $a, b \in B(R)$ entonces existen $-(a \wedge b), -(a \vee b)$ y se verifican las* **Leyes de De Morgan**
$$-(a \wedge b) = -a \vee -b, \quad -(a \vee b) = -a \wedge -b.$$

Definición 3.2.1 *Sea R un reticulado con primer elemento 0, se dice que un elemento $y \in R$ es* **ortogonal** *al elemento $b \in R$ si $b \wedge y = 0$.*
Un elemento que notaremos $\neg b$ se denomina el **ortocomplemento** *de b si:*

1) *$b \wedge \neg b = 0$ (esto es $\neg b$ es ortogonal a b).*

2) *Si $b \wedge x = 0$ entonces $x \leq \neg b$. (esto es $\neg b$ es el mayor elemento ortogonal a b.)*

A continuación indicamos el ortocomplemento de todos los elementos del reticulado indicado en la siguiente figura:



x	0	a	b	c	d	1
$\neg$ x	1	d	a	0	a	0

Lema 3.2.2 *Si existe el ortocomplemento de un elemento b perteneciente a un reticulado con primer elemento 0, él es único.*

Dem. Supongamos que a y c son ortocomplementos de b esto es:

$$(1)\ b \wedge a = 0 \qquad (2)\ Si\ \ b \wedge x = 0 \Longrightarrow\ x \leq a$$

$$(3)\ b \wedge c = 0 \qquad (4)\ Si\ \ b \wedge x = 0 \Longrightarrow\ x \leq c.$$

De (1) y (4) resulta que $a \leq c$ y de (3) y (2) $c \leq a$, luego $a = c$. ■

Observación 3.2.1 *1) De acuerdo con la definición anterior, es claro que para que un elemento b tenga ortocomplemento es necesario y suficiente que el conjunto de todos los elementos ortogonales al elemento b tenga último elemento.*

2) No todo elemento de un reticulado con primer elemento tiene ortocomplemento. El conjunto de los elementos ortogonales al elemento a del reticulado indicado en el Ejemplo 2.4.4, es $\{0, b, c\}$ y este conjunto no tiene último elemento.

Lema 3.2.3 *Si R es un reticulado distributivo, finito, entonces todos los elementos tienen ortocomplemento.*

Dem. Dado $a \in R$, sea $X_a = \{x \in R : a \wedge x = 0\}$. Como $0 \in X_a$, entonces $X_a \neq \emptyset$. Sea $X_a = \{x_1, x_2, \ldots, x_n\}$ y $x = \bigvee_{i=1}^{n} x_i$, entonces $a \wedge x = a \wedge (\bigvee_{i=1}^{n} x_i) = \bigvee_{i=1}^{n} (a \wedge x_i) = 0$, por lo tanto $x \in X_a$, y como $x_i \leq x$ para $1 \leq i \leq n$ tenemos que x es el último elemento de X_a, por lo tanto a tiene ortocomplemento. ■

Si R es un reticulado distributivo finito, no trivial, sabemos que R tiene primer elemento 0. Esto es, $0 \leq x$ cualquiera que sea $x \in R$, y como R es no trivial existe $x_0 \in R$ tal que $0 < x_0$. Sea $X = \{x \in R : 0 < x\}$ luego X es un subconjunto finito, no vacío, de R y por lo tanto X es un conjunto ordenado (finito). En consecuencia X tiene por lo menos un elemento minimal. Sea m un elemento minimal de X, entonces m es un átomo de R. En efecto, de $m \in X$ resulta $0 < m$ y si existiera $x \in R$ tal que $0 < x < m$ entonces el elemento $x \in X$ sería un elemento menor que un elemento minimal de X, absurdo. Tenemos así que el conjunto $\mathcal{A}$ de todos los átomos de R es no vacío.
Observemos ahora que si $x \in R$, $x \neq 0$ entonces:

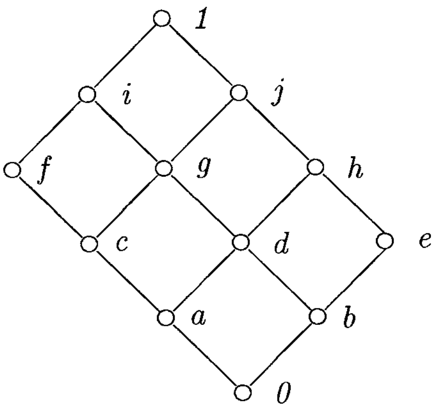
$$a \wedge x \neq 0, \ \ \forall a \in \mathcal{A} \iff \bigvee\{a : a \in \mathcal{A}\} \leq x.$$

En efecto, (1) $0 \leq x \wedge a \leq a$ cualquiera que sea $a \in \mathcal{A}$ y como a es átomo entonces de (1) resulta (2) $x \wedge a = 0$ ó (3) $x \wedge a = a$, pero por la hipótesis hecha solo se puede verificar la condición (3), luego $a \leq x$, $\forall a \in \mathcal{A}$ y por lo tanto $\bigvee\{a : a \in \mathcal{A}\} \leq x$.
Supongamos ahora que $b = \bigvee\{a : a \in \mathcal{A}\} \leq x$, entonces si existiera $a \in \mathcal{A}$ tal que $a \wedge x = 0$, tendríamos que:

$$b \wedge a \leq a \wedge x = 0,$$

y como $a \leq b$, esto es $a \wedge b = a$ entonces $a = 0$, absurdo. Luego $a \wedge x \neq 0 \ \ \forall a \in \mathcal{A}$.
De lo anterior resulta que si $\bigvee\{a : a \in \mathcal{A}\} \leq x$, entonces $\neg x = 0$. En efecto, si $\neg x \neq 0$ existe un átomo a tal que $a \leq \neg x$ y por lo tanto $a \wedge x \leq \neg x \wedge x = 0$, esto es, $a \wedge x = 0$, absurdo.
Esto nos permite, en forma inmediata determinar el ortocomplemento de todos los elementos que son mayores o iguales que el supremo de todos los átomos de un reticulado distributivo finito, no trivial.

Ejemplo 3.2.1 *Sea R el reticulado distributivo cuyo diagrama de Hasse se indica.*



Luego como el conjunto de los átomos de R es $\{a, b\}$ y $a \vee b = d$ entonces $\neg d = \neg g = \neg h = \neg i = \neg j = \neg 1 = 0$. El ortocomplemento de los restantes elementos se obtiene determinando el mayor elemento ortogonal a cada uno de ellos.

Lema 3.2.4 *En un reticulado distributivo con primer y último elemento si un elemento a tiene complemento entonces $-a = \neg a$.*

Dem. Por hipótesis (1) $a \wedge -a = 0$ y (2) $a \vee -a = 1$. De (1) resulta que $-a$ es ortogonal al elemento a. Supongamos que $a \wedge x = 0$, luego $(a \wedge x) \vee -a = 0 \vee -a = -a$, y por lo tanto

$$x \vee -a = 1 \wedge (x \vee -a) = (a \vee -a) \wedge (x \vee -a) = (a \wedge x) \vee -a = -a,$$

luego $x \leq -a$, lo que prueba que el mayor elemento ortogonal al elemento a es $-a$, y por lo tanto $\neg a = -a$. ■

Observación 3.2.2 *En los reticulados distributivos finitos siempre existe el ortocomplemento de cualquier elemento x, pero pueden existir elementos sin complemento (booleano). En el ejemplo precedente $a \vee \neg a = h \neq 1$, y solo existen 4 elementos que tienen complemento.*

Lema 3.2.5 *Para que $\neg x$ sea el complemento de x es necesario y suficiente que $x \vee \neg x = 1$.*

3.3 Subreticulados

A todo subconjunto S, no vacío, de un reticulado R se denomina un **subreticulado** de R si se verifican:

1) Si $x, y \in S$ entonces $x \wedge y \in S$,

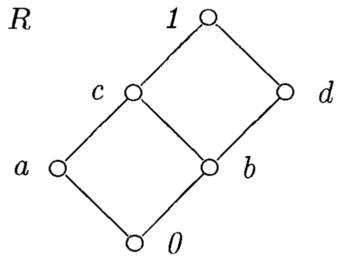
2) Si $x, y \in S$ entonces $x \vee y \in S$.

Es claro, de acuerdo con esta definición, que S es un reticulado y que si R es distributivo entonces S es distributivo, pero puede ocurrir que S sea distributivo sin que R lo sea. El reticulado indicado en el Ejemplo 2.4.4 no es distributivo, y sin embargo $S = \{0, 1\}$ es un subreticulado de R que es distributivo.
Si R es el reticulado indicado en el Ejemplo 3.2.1 entonces $S_1 = \{0, a, b, d\}$ es un subreticulado de R que tiene primer elemento 0 y último elemento d. También son subreticulados de R: $S_2 = \{d, g, h, j, 1\}$, $S_3 = \{c, f, i\}$, $S_4 = \{a, g, 1\}$.
Si a, b son elementos de un reticulado R tales que $a \leq b$ entonces $S = [a, b] = \{x : a \leq x \leq b\}$ es un subreticulado de R que tiene primer elemento a y último elemento b. En particular las secciones inferiores $(a]$, $a \in R$ y las secciones superiores $[a)$, $a \in R$, son subreticulados de R.
Observemos que los subreticulados S_2 y S_3, indicados precedentemente, verifican $S_2 \cap S_3 = \emptyset$, por lo tanto, la intersección de dos subreticulados no es necesariamente un subreticulado.

Lema 3.3.1 *Si $\{S_i\}_{i \in I}$ es una familia de subreticulados de un reticulado R tal que $S = \bigcap_{i \in I} S_i \neq \emptyset$ entonces S es un subreticulado de R.*

Dado un subconjunto, no vacío, G de un reticulado R siempre existe un subreticulado de R que contiene a G, a saber el propio R. Por lo tanto, la familia $\{S_i\}_{i \in I}$ de todos los subreticulados de R que contienen a G, no es vacía. Además, como $\emptyset \subset G \subseteq S_i$, $\forall i \in I$, entonces $\bigcap_{i \in I} S_i \neq \emptyset$ y por lo tanto $\overline{G} = \bigcap_{i \in I} S_i$ es un subreticulado de R, que verifica $G \subseteq \overline{G}$. $\overline{G}$ se denomina el subreticulado **generado** por G. Es fácil ver que $\overline{G}$ es el menor subreticulado de R que contiene a G. Si $\overline{G} = R$ se dice que G es un **conjunto de generadores** de R.

Ejemplo 3.3.1 *Sea R el reticulado cuyo diagrama de Hasse se indica:*



entonces la familia de todos los subreticulados de R está indicada en la siguiente tabla:

1 elemento	*2 elementos*	*3 elementos*	*4 elementos*	*5 elementos*	*6 elementos*
$\{0\}$	$\{0,a\}$	$\{0,a,c\}$	$\{0,a,c,1\}$	$\{0,a,b,c,1\}$	R
$\{a\}$	$\{0,b\}$	$\{0,a,1\}$	$\{0,a,b,c\}$	$\{0,b,c,d,1\}$	
$\{b\}$	$\{0,c\}$	$\{0,b,c\}$	$\{0,a,d,1\}$		
$\{c\}$	$\{0,d\}$	$\{0,b,d\}$	$\{0,b,c,1\}$		
$\{d\}$	$\{0,1\}$	$\{0,b,1\}$	$\{0,b,d,1\}$		
$\{1\}$	$\{a,c\}$	$\{0,c,1\}$	$\{b,c,d,1\}$		
	$\{a,1\}$	$\{0,d,1\}$			
	$\{b,c\}$	$\{a,c,1\}$			
	$\{b,d\}$	$\{b,c,1\}$			
	$\{b,1\}$	$\{b,d,1\}$			
	$\{c,1\}$				
	$\{d,1\}$				

Si $G = \{a,d\}$ entonces $\overline{G} = \{0,a,d,1\} \cap R = \{0,a,d,1\}$, y si $G = \{a,b\}$ entonces $\overline{G} = \{0,a,b,c\} \cap \{0,a,b,c,1\} \cap R = \{0,a,b,c\}$.

Con este ejemplo vemos que no es fácil o por lo menos no es cómodo determinar la familia de todos los subreticulados de un reticulado R y por lo tanto no es cómodo o fácil determinar $\overline{G}$ utilizando la definición de subreticulado generado. A continuación vamos a indicar como se obtiene $\overline{G}$ a partir de cálculos efectuados sobre los elementos de un subconjunto G, no vacío, de un reticulado distributivo.

Si X es un subconjunto no vacío de un reticulado R notaremos con $i(X)$ el conjunto de todos los elementos que son el ínfimo de un número finito de elementos de X, esto es :

$$i(X) = \{ \bigwedge_{x \in F} x : F \subseteq X, \quad F \text{ finito, } \quad \text{no vacío}\}.$$

Si $F = \{f\}$ se sobreentiende que $\bigwedge_{x \in F} x = f$. Análogamente:

$$s(X) = \{ \bigvee_{x \in F} x : F \subseteq X, \quad F \text{ finito, } \quad \text{no vacío}\}.$$

Es claro que, de acuerdo con estas definiciones: $X \subseteq i(X)$ y $X \subseteq s(X)$, y que:

1) Si $x, y \in i(X)$ entonces $x \wedge y \in i(X)$,

2) Si $x, y \in s(X)$ entonces $x \vee y \in s(X)$.

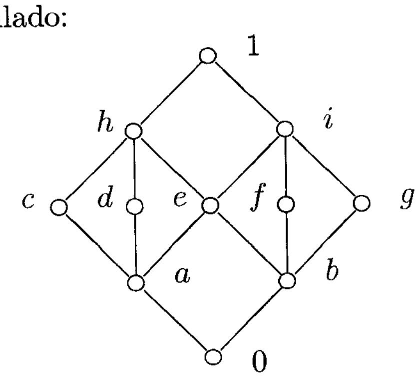
Lema 3.3.2 *Si R es un reticulado distributivo y G un subconjunto, no vacío, de R entonces: $\overline{G} = s(i(G)) = i(s(G))$.*

Dem. Probaremos que $\overline{G} = s(i(G))$, la otra igualdad se prueba en forma análoga.
Si probamos que (I) $G \subseteq s(i(G))$ y que (II) $s(i(G))$ es un subreticulado entonces por la definición de subreticulado generado tendremos que (III) $\overline{G} \subseteq s(i(G))$.
Como $G \subseteq i(G)$ e $i(G) \subseteq s(i(G))$, luego $G \subseteq s(i(G))$.
Por 2) sabemos que si $x, y \in s(i(G))$ entonces $x \vee y \in s(i(G))$. Probemos ahora que tambien $x \wedge y \in s(i(G))$. Por hipótesis $x = \bigvee_{j=1}^{n} x_j$ donde $x_j \in i(G)$ para $1 \leq j \leq n$ e $y = \bigvee_{k=1}^{m} y_k$ donde $y_k \in i(G)$ para $1 \leq k \leq m$ luego:

$$x \wedge y = x \wedge (\bigvee_{k=1}^{m} y_k) = \bigvee_{k=1}^{m} (x \wedge y_k) = \bigvee_{k=1}^{m} ((\bigvee_{j=1}^{n} x_j) \wedge y_k) = \bigvee_{k=1}^{m} (\bigvee_{j=1}^{n} (x_j \wedge y_k)).$$

Como $xj, y_k \in i(G)$, para todo j y todo k entonces $x_j \wedge y_k \in i(G)$ para todo j y todo k; por lo tanto, $\bigvee_{j=1}^{n} (x_j \wedge y_k) \in s(i(G))$ y en consecuencia $\bigvee_{k=1}^{m} (\bigvee_{j=1}^{n} (x_j \wedge y_k)) \in s(i(G))$.
Probemos ahora que (IV) $s(i(G)) \subseteq \overline{G}$. Sea $x \in s(i(G))$, esto es $x = \bigvee_{j=1}^{n} x_j$ donde $x_j \in i(G)$ para $1 \leq j \leq n$, luego $x_j = \bigwedge_{k=1}^{n_j} y_k^j$ donde $y_k^j \in G \subseteq \overline{G}$ luego por ser $\overline{G}$ un subreticulado de R tenemos que $x_j \in \overline{G}$ para todo j de donde resulta por ser $\overline{G}$ un subreticulado de R que $x = \bigvee_{j=1}^{n} x_j \in \overline{G}$. ■

En la demostración anterior solamente se utilizó la propiedad distributiva en la primera parte. Por lo tanto, en cualquier reticulado siempre se verifica $s(i(G)) \subseteq \overline{G}$.
En el reticulado distributivo indicado precedentemente si $G = \{a, b\}$, entonces $i(G) = \{a, b, 0\}$ y $\overline{G} = s(i(G)) = \{a, b, 0, c = a \vee b\}$, y si $G = \{a, d\}$, entonces $i(G) = \{a, d, 0\}$ y $\overline{G} = s(i(G)) = \{a, d, 0, 1 = a \vee d\}$.
Consideremos el siguiente reticulado:



y $G = \{c, f, g\}$. Entonces $i(G) = \{c, f, g, 0 = c \wedge f, b = f \wedge g\}$, $X = s(i(G)) = \{c, f, g, 0, b, 1 = c \vee f, h = c \vee b, i = f \vee g\}$. El conjunto X no es un subreticulado dado que $h, i \in X$ y $e = h \wedge i \notin X$. Este reticulado no es distributivo, dado que su conjunto de elementos irreducibles es $\{a, c, d, f, g, b\}$ y el elemento c no es primo. En efecto $c \leq d \vee e$ y $c \not\leq d$ y $c \not\leq e$.

Lema 3.3.3 *Si G es una parte finita, no vacía, de R entonces $\overline{G}$ es finito.*

Dem. Sea n el número de elementos de G, esto es $N[G] = n$. Pongamos $i_1(G) = G$ y si $1 < j \leq n$, : $i_j(G) = \{\bigwedge y : y \in Y, Y \subseteq G, N[Y] = j\}$. Entonces es claro que:

$$i(G) = \bigcup_{j=1}^{n} i_j(G)$$

$$N[i_1(G)] = \binom{n}{1} \quad \text{y} \quad N[i_j(G)] \leq \binom{n}{j}, \quad 1 < j \leq n,$$

y por lo tanto

$$N[i(G)] \leq \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = 2^n - 1.$$

Esto prueba que si G es finito entonces $i(G)$ es finito. En forma análoga se demuestra que si G es finito entonces $s(G)$ es finito, y por lo tanto como $i(G)$ es finito resulta que $s(i(G))$ es finito. Además:

$$N[s(i(G))] \leq 2^{(2^n - 1)} - 1.$$

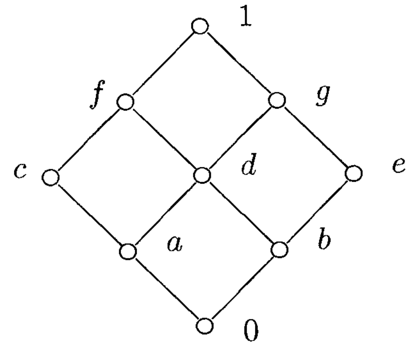
■

Sea R un reticulado distributivo con primer (0) y último elemento (1). Diremos que un subconjunto S de R es un $(0,1)$-**subreticulado** de R si:

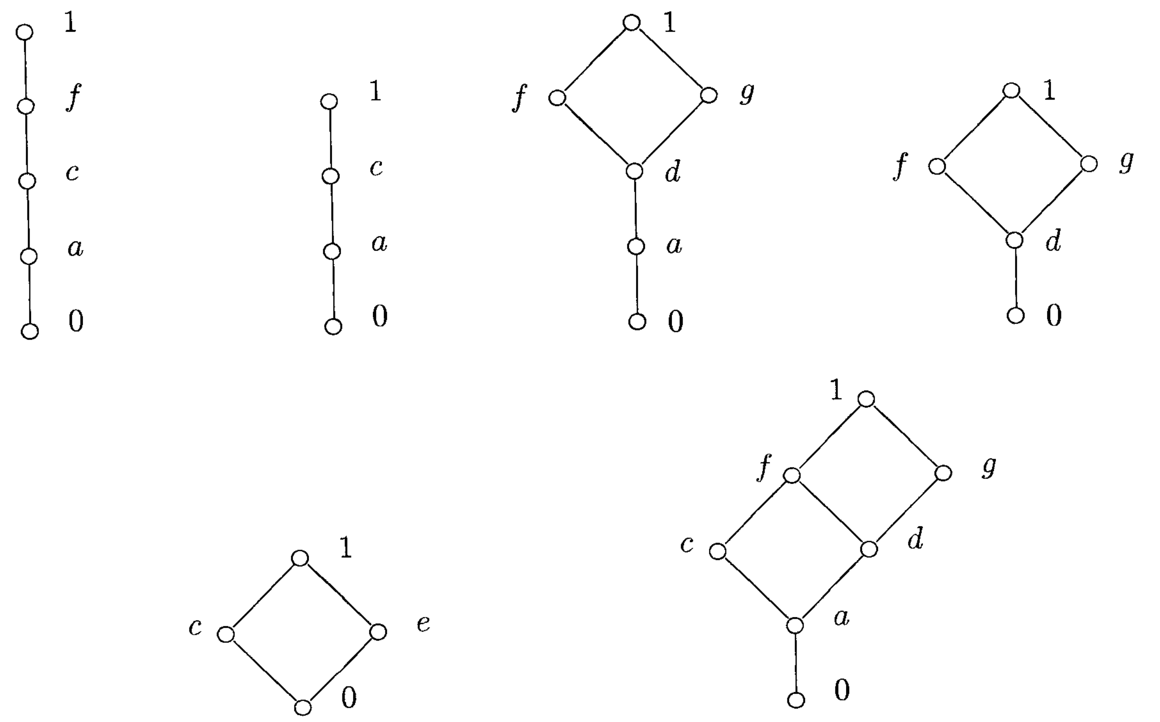
1) $0, 1 \in S$,

2) Si $x, y \in S$ entonces $x \wedge y, x \vee y \in S$.

Esto es un $(0,1)$-subreticulado de R es un subreticulado de R que contiene al primer y al último elemento de R. Es claro que S es un reticulado distributivo con primer (0) y último elemento (1). El reticulado distributivo indicado en el Ejemplo 3.3.1 tiene los siguientes $(0,1)$-subreticulados: $S_1 = \{0,1\}$; $S_2 = \{0, a, 1\}$, $S_3 = \{0, b, 1\}$; $S_4 = \{0, c, 1\}$; $S_5 = \{0, d, 1\}$; $S_6 = \{0, a, c, 1\}$; $S_7 = \{0, a, d, 1\}$; $S_8 = \{0, b, c, 1\}$; $S_9 = \{0, b, d, 1\}$; $S_{10} = \{0, a, b, c, 1\}$; $S_{11} = \{0, b, c, d, 1\}$; $S_{12} = R$. Recordemos que R tiene 37 subreticulados.
Consideremos el siguiente reticulado distributivo:



$S_1 = \{0,1\}$, $S_x = \{0,x,1\}$ donde $x \in R \backslash \{0,1\}$ son $(0,1)$-subreticulados de R. Indiquemos otros $(0,1)$-subreticulados:



Es claro que si S es un $(0,1)$-subreticulado del reticulado distributivo R, entonces $\{0,1\} \subseteq S \subseteq R$, y $\{0,1\}$, R son $(0,1)$-subreticulados de R, y que si $\{S_i\}_{i \in I}$ es una familia de $(0,1)$-subreticulados de R entonces $\bigcap\limits_{i \in I} S_i$ es un $(0,1)$-subreticulado de R.

Dada una parte G de R, se denomina $(0,1)$-**subreticulado generado** por G a la intersección de todos los $(0,1)$-subreticulados de R que contienen a G y lo notaremos $SR(G)$. En la forma habitual se demuestra que $SR(G)$ es el menor $(0,1)$-subreticulado que contiene a G. De acuerdo con la definición precedente es claro que $SR(\emptyset) = \{0,1\}$.
Si R es el reticulado distributivo indicado en el Ejemplo 3.3.1 y $G = \{d\}$ entonces $\overline{G} = \{d\}$ y $SR(G) = \{0,d,1\}$, luego $\overline{G} \neq SR(G)$ y si $G = \{a,d\}$ entonces $\overline{G} = \{0,a,d,1\} = SR(G)$.

Lema 3.3.4 $SR(G) = \{0,1\} \cup \overline{G}$.

Dem. (1) $\{0,1\} \cup \overline{G} \subseteq SR(G)$.
Como $SR(G)$ es un subreticulado que contiene a G entonces (i) $G \subseteq SR(G)$, y como $SR(G)$ es un $(0,1)$-subreticulado entonces (ii) $\{0,1\} \subseteq SR(G)$, de (i) e (ii) resulta (1).
(2) $SR(G) \subseteq \{0,1\} \cup \overline{G}$.
(iii) $G \subseteq \overline{G} \subseteq \overline{G} \cup \{0,1\}$. Probemos que: (iv) $\overline{G} \cup \{0,1\}$ es un $(0,1)$-subreticulado. En efecto, si $x, y \in \overline{G}$, como $\overline{G}$ es un subreticulado tenemos que $x \wedge y, x \vee y \in \overline{G} \subseteq \overline{G} \cup \{0,1\}$. Si $x, y \in \{0,1\}$ es claro que $x \wedge y, x \vee y \in \{0,1\} \subseteq \{0,1\} \cup \overline{G}$. Si $x \in \overline{G}$ e $y \in \{0,1\}$ entonces $x \wedge 0 = 0$, $x \wedge 1 = x$, $x \vee 0 = x$, o $x \vee 1 = 1$, por lo tanto, también $x \wedge y, x \vee y \in \{0,1\} \cup \overline{G}$.
De (iii) y (iv) resulta (2). ■

Si $G = \{g\}$ notaremos $SR(g)$ en vez de $SR(\{g\})$. Observemos que $SR(g) = \{0,g,1\}$ si $g \neq 0,1$ y si $g = 0$ ó $g = 1$ entonces $SR(g) = \{0,1\}$.
Si S es un $(0,1)$-subreticulado y $g \in R \backslash S$ vamos a notar $SR(S,g)$ en vez de $SR(S \cup \{g\})$.

Lema 3.3.5 $SR(S,g) = \{s \wedge (t \vee g) : s,t \in S\} = \{s \vee (t \wedge g) : s,t \in S\}$.
[L. Monteiro, (1975)].

Dem. Sea $H = \{s \wedge (t \vee g) : s,t \in S\}$. Probemos que:
(1) $\underline{H \subseteq SR(S,g)}$.
Sea $h \in H$, esto es $h = s \wedge (t \vee g)$ donde $s,t \in S$, como $S \subseteq S \cup \{g\} \subseteq SR(S,g)$ y $g \in SR(S,g)$ entonces $h \in SR(S,g)$.
(2) $\underline{SR(S,g) \subseteq H}$.
Para ello probaremos que (2a) $S \cup \{g\} \subseteq H$, y (2b) H es un $(0,1)$-subreticulado de R.
Sea $x \in S \cup \{g\}$ entonces $x \in S$ o $x = g$ y por lo tanto, $x = x \wedge (x \vee g)$ ó $x = 1 \wedge (0 \vee g)$. Luego, en ambos casos, $x \in H$, lo que prueba (2a). Como $S \subseteq S \cup \{g\}$ entonces por la condición (2a) resulta que $S \subseteq H$. Como $0,1 \in S$ entonces $0,1 \in H$.
Sean $x, y \in H$, luego $x = s_1 \wedge (t_1 \vee g), y = s_2 \wedge (t_2 \vee g)$ donde $s_1, s_2, t_1, t_2 \in S$, luego:

$$x \wedge y = s_1 \wedge (t_1 \vee g) \wedge s_2 \wedge (t_2 \vee g) = (s_1 \wedge s_2) \wedge ((t_1 \wedge t_2) \vee g)$$

donde $s_1 \wedge s_2, t_1 \wedge t_2 \in S$, y por lo tanto $x \wedge y \in H$.

$$x \vee y = [s_1 \wedge (t_1 \vee g)] \vee [s_2 \wedge (t_2 \vee g)] = (s_1 \vee s_2) \wedge (s_1 \vee t_2 \vee g) \wedge (s_2 \vee t_1 \vee g) \wedge (t_1 \vee t_2 \vee g) =$$

$$(s_1 \vee s_2) \wedge [[(s_1 \vee t_2) \wedge (s_2 \vee t_1) \wedge (t_1 \vee t_2)] \vee g]$$

donde $s_1 \vee s_2, (s_1 \vee t_2) \wedge (s_2 \vee t_1) \wedge (t_1 \vee t_2) \in S$, y por lo tanto $x \vee y \in H$. ■

Observemos que la forma de los elementos de $SR(S,g)$ no es única. En efecto consideremos el reticulado R indicado en el Ejemplo 3.3.1. $S = \{0, d, 1\}$ es un $(0,1)$-subreticulado de R, $SR(S,a) = \{0, a, d, 1\}$, $d = d \wedge (d \vee a)$ y $d = d \wedge (1 \vee a)$.

Sea $G = \{g_1, g_2, \ldots g_n\}$ un subconjunto de un reticulado distributivo R con primer y último elemento. Consideremos:

$$S_1 = SR(g_1), \quad S_2 = SR(S_1, g_2), \ldots, S_n = SR(S_{n-1}, g_n)$$

Probaremos que $SR(G) = S_n$. Como $g_1 \in G$ entonces $\{g_1\} \subseteq G \subseteq SR(G)$ luego $S_1 = SR(g_1) \subseteq SR(G)$ y por lo tanto $S_1 \cup \{g_2\} \subseteq SR(G)$ y en consecuencia $S_2 = SR(S_1, g_2) \subseteq SR(G)$. Entonces tenemos que:

$$S_1 \subseteq S_2 \subseteq \ldots \subseteq S_n \subseteq SR(G).$$

Por la construcción indicada tenemos que $g_i \in S_i$ para $i = 1, 2, \ldots, n$ y como $S_i \subseteq S_{i+1}$ para $i = 1, 2, ..., n-1$ resulta que (1) $G \subseteq S_n$. Además, por construcción (2) S_n es un $(0,1)$-subreticulado de R. De (1) y (2) resulta que $SR(G) \subseteq S_n$.

Lema 3.3.6 *Si R es un reticulado distributivo con primer (0) y último elemento (1) entonces el conjunto $B(R)$ de todos los elementos booleanos de R tiene las siguientes propiedades (ver Lema 3.2.1):*

1) $0, 1 \in B(R)$,

2) Si $x, y \in B(R)$ entonces $x \wedge y, x \vee y \in B(R)$,

3) Si $x \in B(R)$ entonces $-x \in B(R)$.

De 1) y 2) resulta que $B(R)$ es un $(0,1)$-subreticulado de R. Además este $(0,1)$-subreticulado tiene la propiedad 3).

3.4 Factorización de un reticulado distributivo

Es claro que todo reticulado A es isomorfo al producto cartesiano de dos reticulados, en efecto $A \times \{0\} \cong A \cong \{0\} \times A$. Vamos a determinar cuando un reticulado distributivo finito, no trivial, es isomorfo al producto cartesiano de dos reticulados distributivos no triviales.

Lema 3.4.1 *Si A_1 y A_2 son reticulados distributivos, no triviales, con primer* $(0_1, 0_2$ *respectivamente*) *y último elemento* $(1_1, 1_2$ *respectivamente*) *entonces en* $A_1 \times A_2$ *existe un elemento booleano, diferente del primer y último elemento de* $A = A_1 \times A_2$.

Dem. Es claro que el primer elemento de A es $0 = (0_1, 0_2)$ y que el último elemento de A es $1 = (1_1, 1_2)$. Sea $b = (0_1, 1_2) \in A$. Es claro que $b \neq 0, 1$. Sea $b' = (1_1, 0_2)$ entonces $b \wedge b' = (0_1, 1_2) \wedge (1_1, 0_2) = (0_1, 0_2) = 0$ y $b \vee b' = (0_1, 1_2) \vee (1_1, 0_2) = (1_1, 1_2) = 1$. ■

Corolario 3.4.1 *Si A_1 y A_2 son reticulados distributivos finitos, no triviales, en $A_1 \times A_2$ existe un elemento booleano, diferente del primer y último elemento de $A = A_1 \times A_2$.*

Observemos que si R es un reticulado con un sólo elemento, R es un reticulado distributivo con primer y último elemento, y no existe ningún elemento booleano diferente del primer y último elemento.

Lema 3.4.2 *Sean A y A' reticulados y $h : A \to A'$ un isomorfismo de orden de A sobre A', entonces h es un isomorfismo de reticulado.*

Dem. Debemos probar que se verifican las condiciones $H2$) y $H3$). Como $x \wedge y \leq x$ y $x \wedge y \leq y$, resulta por ser h una función isótona que $h(x \wedge y) \leq h(x)$ y $h(x \wedge y) \leq h(y)$. Por lo tanto, el elemento $h(x \wedge y)$ es una cota inferior del conjunto $X = \{h(x), h(y)\}$. Supongamos que $z' \in A'$ es una cota inferior del conjunto X, esto es $z' \leq h(x)$ y $z' \leq h(y)$. Como h es una función suryectiva $z' = f(z)$ con $z \in A$, entonces tenemos que $h(z) \leq h(x)$ y $h(z) \leq h(y)$, de donde resulta por ser h un isomorfismo de orden que $z \leq x$ y $z \leq y$, y por lo tanto $z \leq x \wedge y$, de donde se deduce $z' = h(z) \leq h(x \wedge y)$. En forma análoga se demuestra $H3$). ■

Lema 3.4.3 *Si R es un reticulado distributivo, no trivial, con primer y último elemento* (0 *y* 1 *respectivamente*) *tal que existe $b \in B(R) \setminus \{0, 1\}$ entonces existen reticulados distributivos no triviales R_1 y R_2 tales que $R \cong R_1 \times R_2$.*

Dem. Por hipótesis $(*)$ $b \in B(R) \setminus \{0, 1\}$ luego R no es trivial. Consideremos los siguientes subconjuntos de R: $R_1 = [0, b]$, $R_2 = [0, -b]$. Sabemos que R_1 y R_2 son reticulados distributivos con primer elemento 0 (en ambos casos) y b es el último elemento de R_1, y $-b$ es el último elemento de R_2. Además ambos son no triviales, pués de $(*)$ resulta que $b \neq 0$ y si $-b = 0$ entonces $b = 1$, lo que contradice $(*)$. Probemos que:
(I) $\underline{R_1 \cap R_2 = \{0\}}$. En efecto si $x \in R_1 \cap R_2$ entonces $0 \leq x \leq b$ y $0 \leq x \leq -b$ y por lo tanto $0 \leq x \leq b \wedge -b = 0$, y como $\{0\} \subseteq R_1 \cap R_2$, queda probada la igualdad (I).
Si X, Y son subconjuntos de R notaremos $X \vee Y = \{x \vee y : x \in X,\ y \in Y\}$.
(II) $\underline{R_1 \vee R_2 = R}$. Es claro que $R_1 \vee R_2 \subseteq R$. Sea $r \in R$ entonces $r = r \wedge 1 = r \wedge (b \vee -b) = (r \wedge b) \vee (r \wedge -b)$ y como $0 \leq r \wedge b \leq b$ y $0 \leq r \wedge -b \leq -b$ tenemos que $r \wedge b \in R_1$ y $r \wedge -b \in R_2$, lo que prueba que $R \subseteq R_1 \vee R_2$. Por lo tanto, todo elemento del reticulado

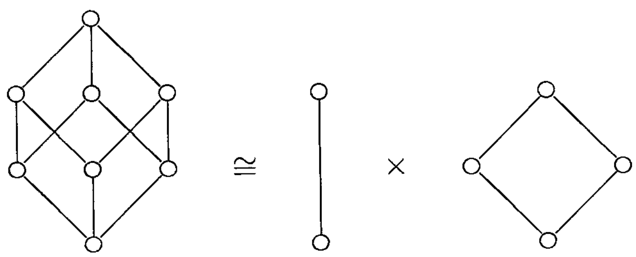
R se puede expresar como supremo de un elemento de R_1 con un elemento de R_2.
(III) Si $x = r_1 \vee r_2$ donde $r_i \in R_i$ para $i = 1, 2$ entonces $r_1 = x \wedge b$ y $r_2 = x \wedge -b$. De $x = r_1 \vee r_2$ resulta que (1) $x \wedge b = (r_1 \vee r_2) \wedge b = (r_1 \wedge b) \vee (r_2 \wedge b)$. Como $r_1 \in R_1$, esto es $0 \leq r_1 \leq b$, por lo tanto (2) $r_1 \wedge b = r_1$. Como $r_2 \in R_2$, esto es $0 \leq r_2 \leq -b$, entonces $0 \leq r_2 \wedge b \leq -b \wedge b = 0$, luego (3) $r_2 \wedge b = 0$. De (1), (2) y (3) resulta que $x \wedge b = r_1$. En forma análoga se demuestra que $x \wedge -b = r_2$. Acabamos así de probar que la representación es única.
Sea $P = R_1 \times R_2$. Vamos a demostrar que $R \cong P$. Dado $r \in R$, sea $h(r) = (r \wedge b, r \wedge -b)$ luego $h : R \to P$.
(IV) h es sobreyectiva. Dado $p = (r_1, r_2) \in P$, entonces $r = r_1 \vee r_2 \in R$, y como $r_1 \in R_1$ y $r_2 \in R_2$ tenemos que $r_1 = r \wedge b$ y $r_2 = r \wedge -b$, luego $h(r) = (r \wedge b, r \wedge -b) = (r_1, r_2) = p$.
(V) Si $x \leq y$ entonces $h(x) \leq h(y)$. De $x \leq y$ resulta que $x \wedge b \leq y \wedge b$ y $x \wedge -b \leq y \wedge -b$ por lo tanto $h(x) = (x \wedge b, x \wedge -b) \leq (y \wedge b, y \wedge -b) = h(y)$.
(VI) Si $x, y \in R$ son tales que $h(x) \leq h(y)$ entonces $x \leq y$. De $h(x) = (x \wedge b, x \wedge -b) \leq (y \wedge b, y \wedge -b) = h(y)$, resulta que $x \wedge b \leq y \wedge b$ y $x \wedge -b \leq y \wedge -b$, luego

$$x = x \wedge (b \vee -b) = (x \wedge b) \vee (x \wedge -b) \leq (y \wedge b) \vee (y \wedge -b) = y \wedge (b \vee -b) = y.$$

■

Ejemplo 3.4.1 *1) Sea R el reticulado distributivo indicado en el Ejemplo 3.3.1 entonces $B(R) = \{0, a, d, 1\}$ luego $B(R) \setminus \{0, 1\} = \{a, d\}$. $R_1 = [0, a]$, $R_2 = [0, d]$. luego $R \cong R_1 \times R_2$.*

2) El reticulado indicado a continuación es isomorfo al producto cartesiano de los siguientes reticulados:



Lema 3.4.4 *Si R es un reticulado distributivo con primer y último elemento (0 y 1 respectivamente) tal que existe $b \in B(R) \setminus \{0, 1\}$, $R_1 = [0, b]$, $R_2 = [0, -b]$ entonces:*

1) $B(R_1) = R_1 \cap B(R)$, $B(R_2) = R_2 \cap B(R)$.

2) Si $a \in B(R)$ entonces $a = a_1 \vee a_2$ donde $a_1 \in B(R_1)$ y $a_2 \in B(R_2)$.

y si R es finito, no trivial, se verifica:

3) Si $p \in \Pi(R)$ entonces $p \in R_1$ ó $p \in R_2$.

4) $\Pi(R) = \Pi(R_1) + \Pi(R_2)$. Esto es, el conjunto ordenado de los elementos primos de R es la suma cardinal de dos conjuntos ordenados.

Dem. Sabemos que si un reticulado tiene primer y último elemento ellos son elementos booleanos. Por lo tanto $0, b \in B(R_1)$.

1) Sea $a \in B(R_1)$ luego $a \in R_1$, esto es (i) $0 \leq a \leq b$ y existe $a' \in R_1$ tal que $a \wedge a' = 0$ y $a \vee a' = b$. Sea $c = a' \vee -b \in R$ luego $a \wedge c = a \wedge (a' \vee -b) = (a \wedge a') \vee (a \wedge -b) = 0 \vee (a \wedge -b)$, pero de (i) resulta $a \wedge -b \leq b \wedge -b = 0$ y por lo tanto $a \wedge c = 0$. Por otro lado $a \vee c = a \vee a' \vee -b = b \vee -b = 1$. Esto prueba que $a \in B(R)$, y por lo tanto $B(R_1) \subseteq R_1 \cap B(R)$.
Sea $t \in R_1 \cap B(R)$, luego $t \in R_1$ y $t \in B(R)$ por lo tanto (1) $0 \leq t \leq b$, y existe $-t \in R$ tal que (2) $t \wedge -t = 0$ y (3) $t \vee -t = 1$. De (1) resulta (4) $t \vee b = b$. Sea $t' = -t \wedge b$, luego $t' \in R_1$, entonces teniendo en cuenta (2), (3) y (4) tenemos que $t \wedge t' = t \wedge -t \wedge b = 0$ y $t \vee t' = t \vee (-t \wedge b) = (t \vee -t) \wedge (t \vee b) = 1 \wedge b = b$, lo que prueba que $t \in B(R_1)$.

2) Si $a \in B(R)$ entonces $a = a \wedge 1 = a \wedge (b \vee -b) = (a \wedge b) \vee (a \wedge -b) = a_1 \vee a_2$ donde (1) $a_1 = a \wedge b \in R_1$ y $a_2 = a \wedge -b \in R_2$. Como $a, b \in B(R)$ entonces por el Lema 3.3.6: (2) $a_1 = a \wedge b \in B(R)$. De (1) y (2) resulta que $a_1 \in R_1 \cap B(R) = B(R_1)$. Análogamente se prueba que $a_2 \in B(R_2)$.

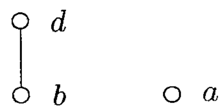
Supongamos ahora que R es finito, no trivial.

3) Sea $p \in \Pi(R)$, como $p \leq b \vee -b = 1$ entonces $p \leq b$ ó $p \leq -b$ y por lo tanto $p \in R_1$ ó $p \in R_2$. Observemos que como $R_1 \cap R_2 = \{0\}$ las dos condiciones anteriores no se pueden verificar simultáneamente.

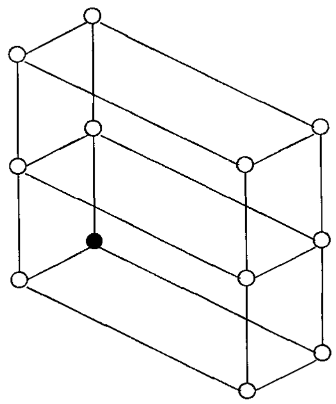
4) De 3) resulta que $\Pi(R) \subseteq R_1 \cup R_2$. Observemos que $\Pi(R) = \Pi(R) \cap (R_1 \cup R_2) = (\Pi(R) \cap R_1) \cup (\Pi(R) \cap R_2)$ y que además $(\Pi(R) \cap R_1) \cap (\Pi(R) \cap R_2) = \Pi(R) \cap R_1 \cap R_2 = \Pi(R) \cap \{0\} = \emptyset$. Por lo tanto $\Pi(R)$ es la unión disjunta de dos conjuntos, uno contenido en R_1 y otro contenido en R_2.
Vamos a demostrar que $\Pi(R_1) = \Pi(R) \cap R_1$.
Observemos que $\Pi(R) \cap R_1 = \{p \in \Pi(R) : p \leq b\} = \Pi(b)$, y que además este conjunto es no vacío dado que $b \neq 0$ entonces $b \not\leq 0$ y por lo tanto existe $p \in \Pi(R)$ tal que $p \leq b$, y en consecuencia $p \in \Pi(R) \cap R_1$. Probemos que $\Pi(R) \cap R_1 \subseteq \Pi(R_1)$. Si $p \in \Pi(R) \cap R_1$ entonces $p \in R_1$ y $p \neq 0$. Supongamos que $p \leq a_1 \vee b_1$ donde $a_1, b_1 \in R_1 \subseteq R$, luego como $p \in \Pi(R)$ resulta que $p \leq a_1$ ó $p \leq b_1$, por lo tanto $p \in \Pi(R_1)$. Probemos que $\Pi(R_1) \subseteq \Pi(R) \cap R_1$. Sea $q \in \Pi(R_1)$ luego $q \in R_1 \subseteq R$ y $q \neq 0$. Supongamos que $q \leq x \vee y$, donde $x, y \in R$, luego $q = q \wedge b \leq (x \vee y) \wedge b = (x \wedge b) \vee (y \wedge b)$ y como $x \wedge b, y \wedge b \in R_1$ y $q \in \Pi(R_1)$ resulta que $q \leq x \wedge b \leq x$ ó $q \leq y \wedge b \leq y$.
Análogamente se prueba que $\Pi(R) \cap R_2 \neq \emptyset$ y que $\Pi(R_2) = \{p \in \Pi(R) : p \leq -b\} = \Pi(-b)$.
Por lo visto anteriormente tenemos que $\Pi(b) \cap \Pi(-b) = \emptyset$ y que $\Pi(b) \cup \Pi(-b) = \Pi(R)$. Nos resta probar que todo elemento de $\Pi(b)$ es incomparable con todo elemento de $\Pi(-b)$. En efecto si $p \in \Pi(b)$, $q \in \Pi(-b)$ son comparables, por ejemplo si $p \leq q$ como $q \leq -b$ entonces $p \leq -b$. Pero $p \leq b$ y por lo tanto $p \leq b \wedge -b = 0$, absurdo.

■

En el reticulado indicado en el Ejemplo 3.3.1 $\Pi(d) = \{b, d\}$ y $\Pi(-d) = \Pi(a) = \{a\}$, y el diagrama de $\Pi(R)$ es el siguiente:



En este ejemplo todo elemento booleano diferente de 0 y 1 es primo. Veamos que no siempre ocurre esto. En el reticulado distributivo indicado a continuación el elemento marcado con • es un booleano diferente de 0 y 1 que no es primo.



Observación 3.4.1 *1) Vimos en 2.4 que si* $R_1 = R_2 = \mathbb{R}$ *entonces* $\mathbb{R} = \Pi(R_1) = \Pi(R_2) \neq \emptyset$ *y que* $\Pi(R_1 \times R_2) = \emptyset$. *Esto es, existen reticulados distributivos* R_1 *y* R_2 *cuyos conjuntos de elementos primos son no vacíos y* $R_1 \times R_2$ *no tiene elementos primos.*

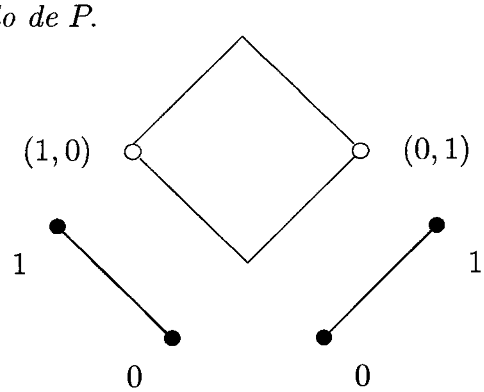
2) Existen reticulados distributivos A *con primer y último elemento tales que:*

$$\Pi(A) = \Pi_1 + \Pi_2$$

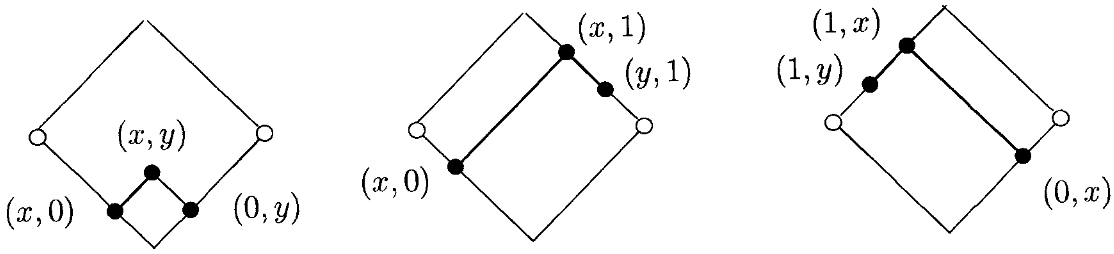
y no existen reticulados distributivos, no triviales tales que

$$A \cong A_1 \times A_2.$$

Por ejemplo, sea $[0,1] \subseteq \mathbb{R}$, $P = [0,1] \times [0,1]$ *y* $A = P \setminus \{(0,1),(1,0)\}$. *Entonces* A *es un subreticulado de* P.



Observando las siguientes figuras se deduce inmediatamente que ninguno de los elementos (x,y), $(x,1)$, $(1,x) \in A$, *indicados, es un elemento primo de* A.



Se prueba sin dificultad que $\Pi(A) = \{(p,0) : 0 < p < 1\} \cup \{(0,p) : 0 < p < 1\}$. Si existieran reticulados A_1 y A_2 tales que $A \cong A_1 \times A_2$ entonces en A tendría que existir (ver Lema 3.4.1) un elemento booleano diferente del primer y último elemento de A, absurdo.

Lema 3.4.5 *Si R_1 y R_2 son reticulados distributivos, no triviales, y $R = R_1 \times R_2$ entonces $p = (p_1, p_2) \in \Pi(R) \iff p_1 = 0$ y $p_2 \in \Pi(R_2)$ ó $p_1 \in \Pi(R_1)$ y $p_2 = 0$.*

Dem. Empezemos por observar que como R_1 y R_2 son reticulados distributivos, no triviales, entonces $\Pi(R_1) \neq \emptyset$, $\Pi(R_2) \neq \emptyset$ y también $\Pi(R_1 \times R_2) \neq \emptyset$.
Sea $p = (p_1, p_2) \in \Pi(R)$, luego $p \neq (0,0)$ luego $p_1 \neq 0$ ó $p_2 \neq 0$. Supongamos que $p_1 \neq 0$ y probemos que $p_1 \in \Pi(R_1)$ y $p_2 = 0$. Como $p = (p_1, p_2) = (p_1, 0) \vee (0, p_2)$ y p es primo entonces $(p_1, p_2) = (p_1, 0)$ ó $(p_1, p_2) = (0, p_2)$, y como $p_1 \neq 0$ tenemos que $p_2 = 0$ y $p = (p_1, 0)$. Supongamos que $p_1 = x_1 \vee y_1$ con $x_1, y_1 \in R_1$ entonces $p = (x_1 \vee y_1, 0) = (x_1, 0) \vee (y_1, 0)$ de donde resulta por ser p primo que $(p_1, 0) = (x_1, 0)$ ó $(p, 0) = (y_1, 0)$ y en consecuencia $p_1 = x_1$ ó $p_1 = y_1$. En caso en que $p_2 \neq 0$ se prueba que $p_1 = 0$ y $p_2 \in \Pi(R_2)$.
Supongamos ahora que $p_1 = 0$ y $p_2 \in \Pi(R_2)$ y probemos que $p = (0, p_2) \in \Pi(R)$. Como $p_2 \in \Pi(R_2)$ entonces $p_2 \neq 0$ y en consecuencia $p = (0, p_2) \neq (0,0)$. Si $(0, p_2) = (x_1, x_2) \vee (y_1, y_2) = (x_1 \vee y_1, x_2 \vee y_2)$, luego $0 = x_1 \vee y_1$ y en consecuencia $x_1 = y_1 = 0$ y $p_2 = x_2 \vee y_2$. Como $p_2 \in \Pi(R_2)$ entonces $p_2 = x_2$ ó $p_2 = y_2$, luego $x_2 \vee y_2 = x_2$ ó $x_2 \vee y_2 = y_2$ y por lo tanto $(0, p_2) = (0, x_2) = (x_1, x_2)$ ó $(0, p_2) = (0, y_2) = (y_1, y_2)$. ■

Lema 3.4.6 *Sean A y A' reticulados distributivos con primer elemento y $h : A \to A'$ un isomorfismo de orden de A sobre A'. Si $\Pi(A) \neq \emptyset$ entonces $\Pi(A') \neq \emptyset$, y $\Pi(A)$ y $\Pi(A')$ son conjuntos ordenados isomorfos.*

Dem.

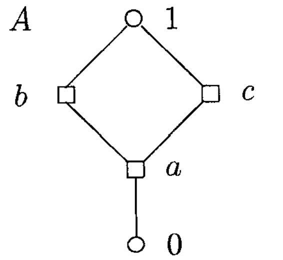
1) Si $p \in \Pi(A) \Longrightarrow h(p) \in \Pi(A')$.
De $p \in \Pi(A)$ resulta que $p \neq 0$ y como h es biunívoca tenemos que $h(p) \neq h(0) = 0'$. Supongamos que $h(p) = a' \vee b'$, con $a', b' \in A'$. Como h es suryectiva $a' = h(a), b' = h(b)$, con $a, b \in A$, luego $h(p) = h(a) \vee h(b) = h(a \vee b)$ de donde resulta por ser h biunívoca que $p = a \vee b$ y como $p \in \Pi(A)$ resulta $p = a$ ó $p = b$ y en consecuencia $h(p) = h(a) = a'$ ó $h(p) = h(b) = b'$. Por lo tanto:
$$h : \Pi(A) \longrightarrow \Pi(A').$$

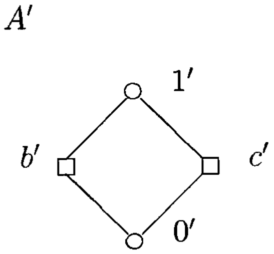
2) h es suryectiva.
Sea $p' \in \Pi(A')$, como h^{-1} es un isomorfismo entonces por 1) $p = h^{-1}(p') \in \Pi(A)$ y por lo tanto $h(p) = h(h^{-1}(p')) = p'$.

3) Si $x, y \in \Pi(A)$ entonces $x \leq y \iff h(x) \leq h(y)$
Como todo homomorfismo de reticulado es una función isótona, entonces h es isótona sobre $\Pi(A)$. Si $h(x) \leq h(y)$ entonces $h(x) = h(x) \wedge h(y) = h(x \wedge y)$, luego como h es biunívoca tenemos $x = x \wedge y$, esto es $x \leq y$.

■

Observación 3.4.2 *1) Consideremos los reticulados distributivos cuyos diagramas se indican:*



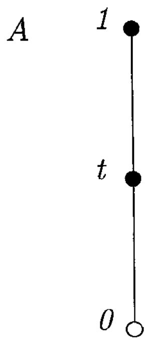


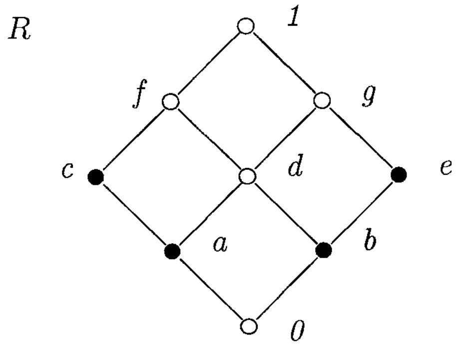
y la función $h : A \to A'$ definida por $h(0) = h(a) = 0'$, $h(b) = b'$, $h(c) = c'$, $h(1) = 1'$. Se verifica fácilmente que h es un homomorfismo suryectivo, y que:

1a) $a \in \Pi(A)$ y $h(a) = 0' \notin \Pi(A')$.

1b) Dado $p' \in \Pi(A')$ existe $p \in \Pi(A)$ tal que $h(p) = p'$.

2) Sean A y R los reticulados distributivos indicados a continuación:





y la función $h : A \to R$ definida por $h(0) = 0$, $h(t) = d$, $h(1) = 1$. Se verifica fácilmente que h es un homomorfismo biunívoco. En este caso, $t \in \Pi(A)$ y $h(t) = d \notin \Pi(R)$. Además, dado $p \in \Pi(R)$ no existe ningún $x \in A$ tal que $h(x) = p$, en particular no existe ningún $q \in \Pi(A)$ tal que $h(q) = p$.

Observación 3.4.3 *En el reticulado R, indicado precedentemente, tenemos que: $\Pi(R) = \{a, b, c, e\}$. Sea $I = \{a, e\}$ entonces $\bigvee_{i \in I} i = a \vee e = g$ y $\Pi(g) = \{a, b, e\}$, por lo tanto $I \neq \Pi(g)$.*

Teorema 3.4.1 *Sean A, A' reticulados distributivos finitos, no triviales. Si $\Pi = \Pi(A)$ y $\Pi' = \Pi(A')$ son conjuntos ordenados isomorfos entonces A y A' son reticulados isomorfos.*

Dem. Sea $\varphi : \Pi \to \Pi'$ un isomorfismo de orden de Π sobre Π'. Sabemos que si $a \in A$, $a \neq 0$ entonces $a = \bigvee_{p\in\Pi(a)} p$.

$$\psi(a) = \begin{cases} 0' & si \;\; a = 0, \\ \bigvee\limits_{p\in\Pi(a)} \varphi(p) & si \;\; a \neq 0. \end{cases}$$

Tenemos así una función $\psi : A \to A'$. Vamos a probar que ψ es un isomorfismo entre los reticulados A y A'. Para ello nos basta probar, de acuerdo con el Lema 3.4.2, que ψ es un isomorfismo de orden.
Observemos en primer lugar que $\psi_{|\Pi} = \varphi$, donde $\psi_{|\Pi}$ representa la función ψ restringida al conjunto Π. En efecto, si $p \in \Pi$ entonces $p = \bigvee_{q\in\Pi(p)} q$, luego $q \leq p$ para todo $q \in \Pi(p)$ y por lo tanto, $\varphi(q) \leq \varphi(p)$ para todo $q \in \Pi(p)$ y en consecuencia $\psi(p) = \bigvee_{q\in\Pi(p)} \varphi(q) = \varphi(p)$.

1) Si $a, b \in A$, $a \leq b \implies \psi(a) \leq \psi(b)$.
   Si $a = 0$ entonces $\psi(0) = 0' \leq \psi(b)$. Si $a \neq 0$ entonces $b \neq 0$, luego como $a \leq b$ resulta que $\Pi(a) \subseteq \Pi(b)$ y en consecuencia $\varphi(\Pi(a)) \subseteq \varphi(\Pi(b))$ y por lo tanto

$$\psi(a) = \bigvee_{p\in\Pi(a)} \varphi(p) \leq \bigvee_{q\in\Pi(b)} \varphi(q) = \psi(b).$$

2) Si $a, b \in A$, son tales que $\psi(a) \leq \psi(b) \implies a \leq b$.
   Si $\psi(a) = 0'$, de acuerdo con la definición de ψ, $a = 0$ y por lo tanto $a = 0 \leq b$. Supongamos que $\psi(a) \neq 0'$, entonces $a \neq 0$ y $b \neq 0$ (si $b = 0$ entonces $\psi(a) \leq \psi(b) = 0'$ y en consecuencia $\psi(a) = 0'$, absurdo).
   Probemos que $\Pi(a) \subseteq \Pi(b)$ de donde resultará que $a \leq b$. Sea $p \in \Pi(a)$, luego $\varphi(p) \leq \bigvee_{t\in\Pi(a)} \varphi(t) = \psi(a) \leq \psi(b) = \bigvee_{q\in\Pi(b)} \varphi(q)$, entonces como $\varphi(p) \in \Pi'$ tenemos que $\varphi(p) \leq \varphi(q)$ para algún $q \in \Pi(b)$, luego como φ es un isomorfismo de orden $p \leq q$ con $q \in \Pi(b)$ esto es, $q \in \Pi$ y $q \leq b$, luego $p \leq b$ y $p \in \Pi$, lo que prueba que $p \in \Pi(b)$.

3) ψ es una función suryectiva.
   Dado $a' \in A'$, si $a' = 0'$ entonces $\psi(0) = 0' = a'$. Supongamos que $a' \neq 0'$, luego $a' = \bigvee_{p'\in\Pi(a')} p'$. Sea $I = \varphi^{-1}(\Pi(a'))$ entonces $I \neq \emptyset$, dado que φ es suryectiva, y además $I \subseteq \Pi$. Consideremos el elemento $a = \bigvee_{p\in I} p$ y probemos que $\psi(a) = a'$. Para ello nos basta probar que (*) $I = \Pi(a)$, (ver observación 3.4.3), dado que entonces (**) $\varphi(\Pi(a)) = \varphi(I) = \varphi(\varphi^{-1}(\Pi(a'))) = \Pi(a')$ y por lo tanto teniendo en cuenta (*) y (**) $\psi(a) = \bigvee_{p\in\Pi(a)} \varphi(p) = \bigvee_{p\in I} \varphi(p) = \bigvee_{x\in\varphi(I)} x = \bigvee_{x\in\Pi(a')} x = a'$.

   Probemos (*). En efecto:

   (i) $I \subseteq \Pi(a)$. Sea $p \in I$, luego $p \in \Pi$ y como $p \leq \bigvee_{q\in I} q = a$ resulta que $p \in \Pi(a)$.

(ii) $\Pi(a) \subseteq I$. Sea $q \in \Pi(a)$, esto es $q \in \Pi$ y $q \leq a = \bigvee_{p \in I} p$, luego como q es un elemento primo, $q \leq p$ para algún $p \in I$, por lo tanto (***) $\varphi(q) \leq \varphi(p)$. Como $p \in I$ entonces $\varphi(p) \in \varphi(I) = \Pi(a')$ esto es, $\varphi(p) \in \Pi'$ y $\varphi(p) \leq a'$, luego por (***) tenemos $\varphi(q) \leq a'$ y como $\varphi(q) \in \Pi'$ tenemos que $\varphi(q) \in \Pi(a')$ y por lo tanto $q \in \varphi^{-1}(\Pi(a')) = I$.

∎

Acabamos así de probar que si A es un reticulado distributivo finito, no trivial, y A' es un reticulado distributivo finito, no trivial, tal que $\Pi(A)$ y $\Pi(A')$ son conjuntos ordenados isomorfos entonces A y A' son isomorfos.

Corolario 3.4.2 *Todo reticulado distributivo finito, no trivial, A es determinado, a menos de isomorfismos, por el conjunto ordenado $\Pi(A)$ de sus elementos primos.*

Teorema 3.4.2 *Si A es un reticulado distributivo finito, no trivial, $\Pi = \Pi(A)$, $\Pi = \Pi_1 + \Pi_2$ y A_1 y A_2 son reticulados distributivos finitos tales que $\Pi(A_i) \cong \Pi_i$, para $i = 1,2$ entonces $A \cong A_1 \times A_2$.*

Dem. De acuerdo con el Teorema 3.4.1 nos basta demostrar que $\Pi \cong \Pi(A_1 \times A_2)$. Por el Lema 3.4.5 sabemos que (*) $p = (p_1, p_2) \in \Pi(A_1 \times A_2) \iff p_1 = 0$ y $p_2 \in \Pi(A_2)$ ó $p_1 \in \Pi(A_1)$ y $p_2 = 0$.
Sean $\varphi_1 : \Pi_1 \to \Pi(A_1)$ y $\varphi_2 : \Pi_2 \to \Pi(A_2)$, isomorfismos de orden. Pongamos por definición:

$$\varphi(p) = \begin{cases} (\varphi_1(p), 0) & si\ \ p \in \Pi_1, \\ & \\ (0, \varphi_2(p)) & si\ \ p \in \Pi_2. \end{cases} \qquad p \in \Pi$$

Por (*) tenemos que $\varphi : \Pi \to \Pi(A_1 \times A_2)$.

1) φ es suryectiva.
Dado $p' \in \Pi(A_1 \times A_2)$, por (*) $p' = (p'_1, 0)$ con $p'_1 \in \Pi(A_1)$ ó $p' = (0, p'_2)$ con $p'_2 \in \Pi(A_2)$. En el primer caso $p'_1 = \varphi_1(p_1)$ con $p_1 \in \Pi_1$, luego $\varphi(p_1) = (\varphi_1(p_1), 0) = (p'_1, 0) = p'$. En el segundo caso la demostración es análoga.

2) Si $p, q \in \Pi$ verifican $p \leq q$ entonces $\varphi(p) \leq \varphi(q)$.
Si $p, q \in \Pi = \Pi_1 + \Pi_2$ verifican $p \leq q$ entonces $p, q \in \Pi_1$ ó $p, q \in \Pi_2$. En el primer caso como φ_1 es un isomorfismo de orden $\varphi_1(p) \leq \varphi_1(q)$, esto es $\varphi(p) = (\varphi_1(p), 0) \leq (\varphi_1(q), 0) = \varphi(q)$. En el otro caso la demostración es análoga.

3) Si $p, q \in \Pi$ verifican $\varphi(p) \leq \varphi(q)$ entonces $p \leq q$.
Sean $X_1 = \{(p, 0) : p \in \Pi(A_1)\}$, $X_2 = \{(0, q) : q \in \Pi(A_2)\}$. Sabemos que $\Pi(A_1 \times A_2)$ es la suma cardinal de los conjuntos ordenados X_1 y X_2. Luego como $\varphi(p), \varphi(q) \in \Pi(A_1 \times A_2)$ y $\varphi(p) \leq \varphi(q)$ resulta que $\varphi(p), \varphi(q) \in X_1$ ó $\varphi(p), \varphi(q) \in X_2$. En el primer caso $\varphi(p) = (\varphi_1(p), 0) \leq (\varphi_1(q), 0) = \varphi(q)$ y por lo tanto $\varphi_1(p) \leq \varphi_1(q)$ y en consecuencia $p \leq q$. En el segundo caso la demostración es análoga.

∎

De acuerdo con los resultados precedentes tenemos el siguiente:

Teorema 3.4.3 *Para que un reticulado distributivo, finito, no trivial A sea isomorfo al producto cartesiano $A_1 \times A_2$ de dos reticulados distributivos no triviales A_1 y A_2 es necesario y suficiente que el conjunto ordenado $\Pi(A)$ de sus elementos primos sea la suma cardinal de dos conjuntos ordenados (esto es que $\Pi(A)$ no sea conexo.)*

Definición 3.4.1 *Un reticulado distributivo A se denomina* **reducible** *si no es trivial y $A \cong A_1 \times A_2$ donde A_1 y A_2 son reticulados distributivos no triviales. A se denomina* **irreducible**, *si no es trivial, y no es reducible.*

Todo reticulado formado por un sólo elemento, no es reducible, ni irreducible.

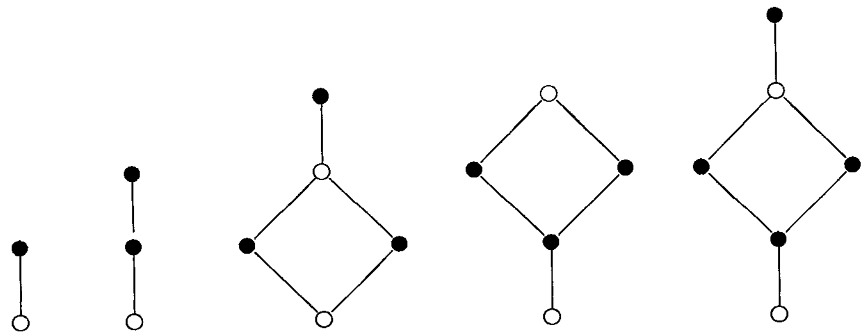
De acuerdo con la definición precedente y resultados anteriores tenemos que:

Lema 3.4.7 *Sea A un reticulado distributivo, finito, no trivial, entonces:*

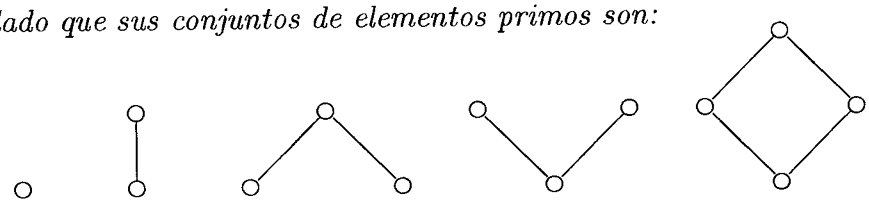
1) A es irreducible $\iff$ $B(A) = \{0,1\}$,

2) A es irreducible $\iff$ $\Pi(A)$ es un conjunto ordenado conexo.

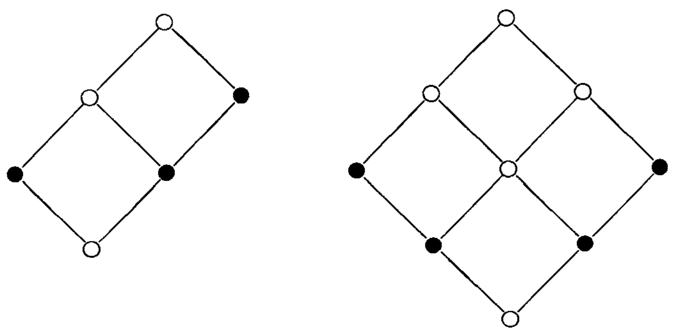
Ejemplo 3.4.2 *1) Los siguientes reticulados son irreducibles:*



dado que sus conjuntos de elementos primos son:



2) Los siguientes reticulados son reducibles:



dado que sus conjuntos de elementos primos son:

Lema 3.4.8 *Si A es un reticulado distributivo, finito, y no trivial, $b \in B(A) \setminus \{0,1\}$, $A_1 = [0,b]$ entonces para que A_1 sea irreducible es necesario y suficiente que b sea un átomo de $B(A)$.*

Dem. Por el Lema 3.4.4 sabemos que $B(A_1) = A_1 \cap B(A)$, luego por el Lema 3.4.7 para que A_1 sea irreducible es necesario y suficiente que $B(A_1) = \{0, b\}$. Vamos a demostrar que esto equivale a decir que b es un átomo de $B(A)$.
$\Longrightarrow$) Por hipótesis $b \in B(A)$ y $b \neq 0$. Supongamos que (1) $0 \leq a \leq b$ con (2) $a \in B(A)$. De (1) resulta que (3) $a \in A_1$ y de (2) y (3) $a \in A_1 \cap B(A) = \{0, b\}$, esto es $a = 0$ ó $a = b$ y por lo tanto b es un átomo de $B(A)$.
$\Longleftarrow$) Supongamos que (1) b es un átomo de $B(A)$. Como $0, b \in A_1 \cap B(A)$ entonces $\{0,b\} \subseteq A_1 \cap B(A)$. Sea $a \in A_1 \cap B(A)$ entonces $a \in A_1$, esto es (2) $0 \leq a \leq b$ y (3) $a \in B(A)$. De (1), (2) y (3) resulta que $a = 0$ ó $a = b$, por lo tanto $a \in \{0, b\}$. Esto prueba que $A_1 \cap B(A) \subseteq \{0, b\}$ y en consecuencia $A_1 \cap B(A) = \{0, b\}$. ■

Sea R un reticulado distributivo con primer y último elemento, $B(R)$ el $(0,1)$-subreticulado de R, de todos los elementos booleanos de R, entonces:

Lema 3.4.9 *Si p es un elemento primo de $B(R)$ entonces p es un átomo de $B(R)$.*

Dem. Como p es un elemento primo de $B(R)$ entonces $p \neq 0$. Supongamos que (1) $0 \leq q \leq p$, con $q \in B(R)$, luego existe $-q \in B(R)$ tal que $q \vee -q = 1$ y $q \wedge -q = 0$. Como $p \leq 1 = q \vee -q$ y p es primo de $B(R)$ entonces (2) $p \leq q$ ó (3) $p \leq -q$. Si ocurre (2) entonces por (1) tenemos que $q = p$. Si ocurre (3) entonces $p \wedge q \leq -q \wedge q = 0$, esto es (4) $p \wedge q = 0$, pero por (1) tenemos (5) $p \wedge q = q$. De (4) y (5) resulta $q = 0$. ■

Corolario 3.4.3 *Si R es un reticulado distributivo finito, no trivial, y $\mathcal{A}$ el conjunto de los átomos de $B(R)$ entonces $\bigvee\{a : a \in \mathcal{A}\} = 1$.*

Dem. Como R es finito, no trivial, entonces $B(R)$ es un reticulado finito, no trivial, y en consecuencia $\Pi(B(R)) \neq \emptyset$. Por el lema anterior $\Pi(B(R)) \subseteq \mathcal{A}$ y sabemos que todo átomo es un elemento primo, esto es $\mathcal{A} \subseteq \Pi(B(R))$. Por lo tanto $\Pi(B(R)) = \mathcal{A}$. Como el supremo de todos los primos de un reticulado distributivo finito es igual a 1, entonces $1 = \bigvee\{p : p \in \Pi(B(R))\} = \bigvee\{a : a \in \mathcal{A}\}$. ■

Lema 3.4.10 *Si R es un reticulado distributivo con primer y último elemento tal que el conjunto $\mathcal{A}$ de los átomos de $B(R)$ es no vacío, entonces:*

I) Si $a, b \in \mathcal{A}$ y $a \neq b$ entonces $a \wedge b = 0$,

II) Si $a \in \mathcal{A}$ y $b \in B(R)$ entonces $a \wedge b = 0$ ó $a \wedge b = a$.

III) Si $a \in \mathcal{A}$ y $b_1, b_2, \ldots, b_t \in \mathcal{A}$ son tales que $a \neq b_i$ para $i = 1, 2, \ldots, t$ entonces $a \wedge (\bigvee_{i=1}^{t} b_i) = 0$.

IV) Si $a_1, a_2, \ldots, a_s, b_1, b_2, \ldots, b_t \in \mathcal{A}$ *son tales que* $a_i \neq b_j$, $\forall\, i,j$ *entonces*

$$(\bigvee_{i=1}^{s} a_i) \wedge (\bigvee_{j=1}^{t} b_j) = 0.$$

Dem.

I) Supongamos que $a \wedge b \neq 0$ luego (1) $0 < a \wedge b \leq a$ y (2) $0 < a \wedge b \leq b$. De (1) resulta por ser a átomo que $a \wedge b = a$ y de (2) resulta por ser b átomo que $a \wedge b = b$. Entonces tendríamos que $a = b$, absurdo.

II) Como $0 \leq a \wedge b \leq a$ y a es átomo entonces $a \wedge b = 0$ ó $a \wedge b = a$.

III) Utilizando la propiedad distributiva, las hipótesis y (I) tenemos que: $a \wedge (\bigvee_{i=1}^{t} b_i) = \bigvee_{i=1}^{t} (a \wedge b_i) = 0$.

IV) Utilizando la propiedad distributiva, las hipótesis y (III) tenemos que:

$$(\bigvee_{i=1}^{s} a_i) \wedge (\bigvee_{j=1}^{t} b_j) = \bigvee_{i=1}^{s} (a_i \wedge (\bigvee_{j=1}^{t} b_j)) = 0.$$

■

Lema 3.4.11 *Si* R *es un reticulado distributivo finito, no trivial, tal que todo elemento primo de* R *es un átomo de* R *entonces todos los elementos de* R *tienen complemento booleano.*

Dem. Sabemos que $0, 1 \in B(R)$. Sea $a \in R \setminus \{0,1\}$, luego como $a \neq 0$, $a = \bigvee\{p : p \in \Pi(a)\}$ y además $\Pi(a) \neq \Pi = \Pi(R)$ pués si $\Pi(a) = \Pi$ entonces por el Corolario 3.4.3, $a = \bigvee\{p : p \in \Pi\} = 1$, contradicción. Sea $\Pi' = \Pi \setminus \Pi(a)$ y $b = \bigvee\{q : q \in \Pi'\}$, entonces:

(1) $a \vee b = \bigvee\{p : p \in \Pi(a)\} \vee \bigvee\{q : q \in \Pi'\} = \bigvee\{p : p \in \Pi\} = 1,$ y

(2) $a \wedge b = (\bigvee\{p : p \in \Pi(a)\}) \wedge (\bigvee\{q : q \in \Pi'\})$.

Sea $\mathcal{A}$ el conjunto de los átomos de R, por hipótesis $\Pi \subseteq \mathcal{A}$, luego los elementos de los conjuntos $\Pi(a)$ y Π' son átomos. Además $\Pi(a) \cap \Pi' = \emptyset$, por lo tanto si $p \in \Pi(a)$ y $q \in \Pi'$ tenemos que $p \neq q$, luego por el Lema 3.4.10,(IV) tenemos que: (3) $a \wedge b = 0$. De (1) y (2) resulta que $a \in B(R)$. ■

Lema 3.4.12 *Sea* A *un reticulado distributivo finito, no trivial, reducible entonces* $A \cong A_1 \times A_2 \times \ldots \times A_n$, *donde los* A_i, $1 \leq i \leq n$ *son reticulados distributivos irreducibles y* n *es el número de átomos de* $B(A)$.

Dem. Por hipótesis A es reducible luego $B(A) \neq \{0,1\}$, luego tiene átomos. Sea $\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$, $n \geq 2$, el conjunto de los átomos de $B(A)$. Por el Lema 3.4.8 sabemos que $A_i = [0, a_i]$, $1 \leq i \leq n$ es un reticulado distributivo irreducible. Sea $P = \prod_{i=1}^{n} A_i$ y probemos que $A \cong P$. Dado $x \in A$ pongamos por definición:

$$\varphi(x) = (x \wedge a_1, x \wedge a_2, \ldots, x \wedge a_n),$$

como $0 \leq x \wedge a_i \leq a_i$ para $1 \leq i \leq n$ entonces $x \wedge a_i \in A_i$ para $1 \leq i \leq n$.
Vamos a demostrar que φ es un isomorfismo de orden de A sobre P.

1) φ es suryectiva.
Si $y = (y_1, y_2, \ldots, y_n) \in P$ entonces $y_i \in A_i \subseteq A$, para $1 \leq i \leq n$. Sea $x = \bigvee_{i=1}^{n} y_i$. Vamos a demostrar que $x \wedge a_j = y_j$, cualquiera que sea j, de donde resultará que $\varphi(x) = y$.
En efecto $x \wedge a_j = (\bigvee_{i=1}^{n} y_i) \wedge a_j = \bigvee_{i=1}^{n} (y_i \wedge a_j)$. Como $y_j \in A_j = [0, a_j]$ entonces $y_j \leq a_j$ y por lo tanto $y_j \wedge a_j = y_j$. Si $j \neq i$, de $y_i \leq a_i$ resulta que $y_j = y_j \wedge a_j \leq a_i \wedge a_j = 0$. Luego $x \wedge a_j = y_j$, cualquiera que sea j, $1 \leq j \leq n$.

2) Si $x, y \in A$ son tales que $x \leq y$ entonces $\varphi(x) \leq \varphi(y)$.
De $x \leq y$ resulta que $x \wedge a_i \leq y \wedge a_i$ para $1 \leq i \leq n$, luego $\varphi(x) \leq \varphi(y)$.

3) Si $x, y \in A$ son tales que $\varphi(x) \leq \varphi(y)$ entonces $x \leq y$.
De $\varphi(x) \leq \varphi(y)$ resulta que $x \wedge a_i \leq y \wedge a_i$ para $1 \leq i \leq n$, luego $x \wedge (\bigvee_{i=1}^{n} a_i) = \bigvee_{i=1}^{n} (x \wedge a_i) \leq \bigvee_{i=1}^{n} (y \wedge a_i) = y \wedge (\bigvee_{i=1}^{n} a_i)$, y como (ver Corolario 3.4.3), $\bigvee_{i=1}^{n} a_i = 1$ tenemos finalmente que $x \leq y$.

■

Observemos que por el Teorema 3.4.3 y el Lema 3.4.4 tenemos que:

$$\Pi(P) \cong \sum_{i=1}^{n} \Pi(A_i) = \sum_{i=1}^{n} \Pi([0, a_i]).$$

Veamos otra forma de probar el resultado anterior: Como $a_1 \in B(A) \setminus \{0,1\}$, por el Lema 3.4.11 el complemento de a_1 es $b_1 = \bigvee_{i=2}^{n} a_i$, luego por el Lema 3.4.3 tenemos que:

$$A \cong [0, a_1] \times [0, b_1]$$

y por el Lema 3.4.4

$$\Pi(A) = \Pi([0, a_1]) + \Pi([0, b_1]).$$

Si $n = 2$ entonces $b_1 = a_2$, luego

$$A \cong [0, a_1] \times [0, a_2] \qquad \text{y} \qquad \Pi(A) = \Pi([0, a_1]) + \Pi([0, a_2]).$$

Supongamos que (*) $n > 2$. Como $0 \leq a_2 \leq \bigvee_{i=2}^{n} a_i = b_1$ tenemos que $a_2 \in [0, b_1]$. Por el Lema 3.4.4 sabemos que $B([0, b_1]) = [0, b_1] \cap B(A)$, por lo tanto $a_2 \in B([0, b_1])$. Además $a_2 \neq 0$ y por (*) $a_2 \neq b_1$ tenemos que $a_2 \in B([0, b_1]) \setminus \{0, b_1\}$. Como el complemento booleano de a_2 en $[0, b_1]$ es $b_2 = \bigvee_{i=3}^{n} a_i$ tenemos que:

$$[0, b_1] \cong [0, a_2] \times [0, b_2]$$

y

$$\Pi([0, b_1]) = \Pi([0, a_2]) + \Pi([0, b_2]).$$

Reiterando este procedimiento $n - 1$ veces tenemos:

$$A \cong \prod_{i=1}^{n} [0, a_i] \qquad \text{y} \qquad \Pi(A) = \sum_{i=1}^{n} \Pi([0, a_i]).$$

3.5 Caracterización de un reticulado distributivo finito, no trivial, por intermedio del conjunto de sus elementos primos

3.5.1 Teorema de Birkhoff

Vimos que si R es un reticulado distributivo finito, no trivial, entonces el conjunto de sus elementos primos, $\Pi(R)$ no es vacío. Entonces a cada reticulado distributivo finito, no trivial, R le podemos hacer corresponder un conjunto ordenado finito, a saber $\Pi(R)$:

$$R \longrightarrow \Pi(R).$$

Se plantea en forma natural el siguiente problema. *Dado un conjunto ordenado finito* Π, *¿existirá algún reticulado distributivo finito, no trivial,* R *tal que* $\Pi(R) \cong \Pi$? La respuesta es afirmativa y fué dada por G. Birkhoff.
Recordemos que si Π es un conjunto ordenado se dice que un subconjunto Y de Π es una <u>sección inferior</u> de Π si $Y = \emptyset$ ó Y verifica: *Si* $y \in Y$ *y* $t \leq y$ *entonces* $t \in Y$. Vimos que si $y \in \Pi$ entonces $(y] = \{t \in \Pi : t \leq y\}$ es una sección inferior de Π.

Sea $\mathcal{A}$ el conjunto de todas las secciones inferiores de Π, entonces:

I) $\emptyset, \Pi \in \mathcal{A}$,

II) Si $X, Y \in \mathcal{A}$ entonces $X \cap Y, X \cup Y \in \mathcal{A}$.

En efecto:

I) Por definición $\emptyset \in \mathcal{A}$, y es obvio que $\Pi \in \mathcal{A}$.

II) Si $X \cap Y = \emptyset$ entonces $X \cap Y \in \mathcal{A}$. Si $X \cap Y \neq \emptyset$ sea $t \in X \cap Y$ y $z \leq t$ luego como $X, Y \in \mathcal{A}$, $t \in X$ y $t \in Y$ tenemos que $z \in X$ y $z \in Y$, por lo tanto $z \in X \cap Y$.
Si $X, Y = \emptyset$ entonces $X \cup Y = \emptyset \in \mathcal{A}$. Si uno de los subconjuntos es vacío y el otro no es vacío, por ejemplo $X = \emptyset$ e $Y \neq \emptyset$ entonces $X \cup Y = Y \in \mathcal{A}$. Si $X \neq \emptyset$ e $Y \neq \emptyset$, entonces $X \cup Y \neq \emptyset$. Sea $t \in X \cup Y$ y $z \leq t$, luego $t \in X$ ó $t \in Y$, y por lo

tanto como $X, Y \in \mathcal{A}$ tenemos que $z \in X$ ó $z \in Y$ y en consecuencia $z \in X \cup Y$.
Acabamos así de probar que $\mathcal{A}$ es un anillo de conjuntos (formado por subconjuntos de Π), y en consecuencia $(\mathcal{A}, \cap, \cup)$ es un reticulado distributivo. Además, como $\emptyset, \Pi \in \mathcal{A}$ tenemos que $\mathcal{A}$ es un reticulado distributivo con primer y último elemento, que es claramente finito.
Vamos a demostrar que: (a) $\Pi(\mathcal{A}) = \{(x] : x \in \Pi\}$.
Sabemos que (1) $(x] \in \mathcal{A}$ y como $x \in (x]$ entonces (2) $(x] \neq \emptyset$.
(3) Supongamos que $(x] = S_1 \cup S_2$ donde $S_1, S_2 \in \mathcal{A}$. Entonces por hipótesis $S_1 \subseteq S_1 \cup S_2 = (x]$ y $S_2 \subseteq S_1 \cup S_2 = (x]$. Como $x \in (x] = S_1 \cup S_2$ entonces (i) $x \in S_1$ ó (ii) $x \in S_2$. Si ocurre (i) entonces $(x] \subseteq S_1$. En efecto si $y \in (x]$ esto es $y \leq x$, como $x \in S_1 \in \mathcal{A}$ entonces $y \in S_1$. Análogamente, si ocurre (ii) se deduce que $(x] \subseteq S_2$.
Acabamos así de probar que: $\{(x] : x \in \Pi\} \subseteq \Pi(\mathcal{A})$.
Sea $X \in \Pi(\mathcal{A})$, luego $X \neq \emptyset$ y $X \in \mathcal{A}$. Como X es un subconjunto, no vacío, del conjunto finito Π entonces $X = \{x_1, x_2, \ldots, x_n\}$. Probemos que (iii) $X = \bigcup_{i=1}^{n} (x_i]$.
En efecto como $x_i \in (x_i]$, para $i = 1, 2, \ldots, n$ entonces $X = \bigcup_{i=1}^{n} \{x_i\} \subseteq \bigcup_{i=1}^{n} (x_i]$. Sea $t \in \bigcup_{i=1}^{n} (x_i]$, luego $t \in (x_i]$ para algún i, $1 \leq i \leq n$, y por lo tanto $t \leq x_i$. Como $x_i \in X \in \mathcal{A}$ entonces $t \in X$.
De (iii) resulta por ser X un elemento primo de $\mathcal{A}$ que $X = (x_i]$ para algún i.
Acabamos así de probar que $\Pi(\mathcal{A}) \subseteq \{(x] : x \in \Pi\}$.

Vimos en el capítulo 1 que si definimos:

$$\varphi(p) = (p], \qquad p \in \Pi,$$

entonces $\varphi : \Pi \to \Pi(\mathcal{A})$ es un isomorfimo de orden.

Vamos a notar $RB(\Pi)$ al reticulado distributivo que terminamos de construir. Acabamos de probar que dado un conjunto ordenado finito Π, $RB(\Pi)$ verifica $\Pi(RB(\Pi)) \cong \Pi$, luego por el Corolario 3.4.2 si A' es un reticulado distributivo finito, no trivial, tal que el conjunto ordenado $\Pi(A')$ es isomorfo a Π, entonces A' es isomorfo a $RB(\Pi)$.

Sabemos que todo elemento $X \in \mathcal{A} = RB(\Pi)$, $X \neq \emptyset$ es supremo de elementos primos de $\mathcal{A}$, luego para construir $RB(\Pi)$ nos basta considerar los conjuntos $(x]$, con $x \in \Pi$ y hacer reuniones finitas de ellos.
Recordemos que si R es un reticulado trivial entonces $\Pi(R) = \emptyset$. Pongamos $RB(\emptyset) = \{1\}$.

Ejemplo 3.5.1 *1) Si Π es la suma cardinal de n conjuntos ordenados cada uno de los cuales tienen un sólo elemento, esto es Π es una anticadena. Por lo tanto tiene el siguiente diagrama:*

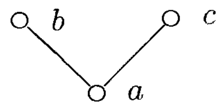
$$\begin{array}{cccc} \circ & \circ & \cdots & \circ \\ x_1 & x_2 & & x_n \end{array}$$

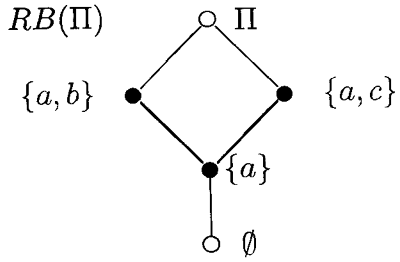
Luego $(x_i] = \{x_i\}$ para $i = 1, 2, \ldots, n$, y por lo tanto $RB(\Pi)$ es igual a $\mathcal{P}(\Pi)$.

2) Si Π es una cadena con n elementos, $\Pi = \{x_1, x_2, \ldots, x_n\}$, donde $x_1 < x_2 < \ldots < x_n$ entonces $(x_i] = \{x_1, x_2, \ldots, x_i\}$ para $i = 1, 2, \ldots, n$, y por lo tanto $(x_1] \subset (x_2] \subset \ldots \subset (x_n]$. Luego $RB(\Pi)$ es una cadena con $n + 1$ elementos.

3) Sea Π *el conjunto ordenado cuyo diagrama se indica.*

Π



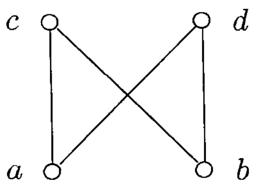


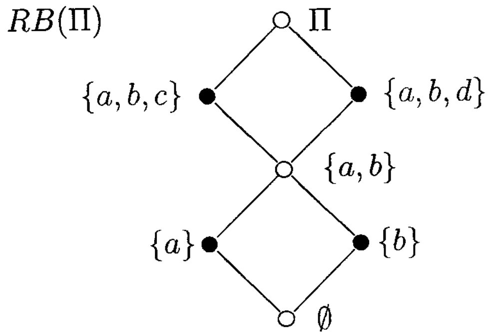
	$(a]$	$(b]$	$(c]$	
$\cup$	$\{a\}$	$\{a,b\}$	$\{a,c\}$	Π
$\{a\}$				
$\{a,b\}$			Π	
$\{a,c\}$				

Por lo tanto, $RB(\Pi)$ *tiene el diagrama indicado precedentemente.*

4) Sea Π *el conjunto ordenado cuyo diagrama se indica.*

Π

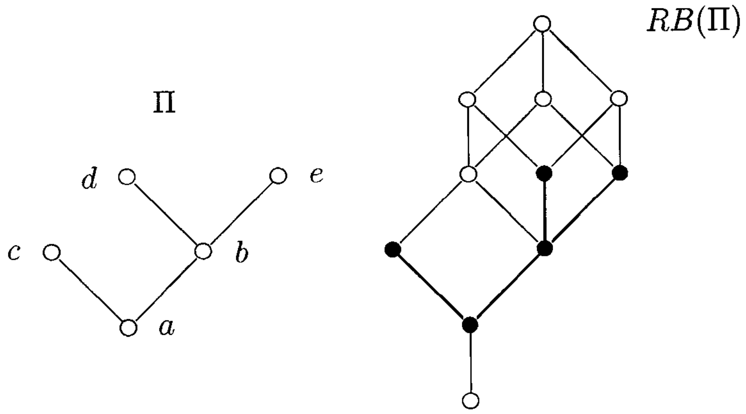




	$(a]$	$(b]$	$(c]$	$(d]$	
$\cup$	$\{a\}$	$\{b\}$	$\{a,b,c\}$	$\{a,b,d\}$	Π
$\{a\}$		$\{a,b\}$			
$\{b\}$					
$\{a,b,c\}$				Π	
$\{a,b,d\}$					

Por lo tanto, $RB(\Pi)$ *tiene el diagrama indicado.*

5) Si Π *es el conjunto ordenado cuyo diagrama se indica,* $RB(\Pi)$ *está indicado a continuación.*

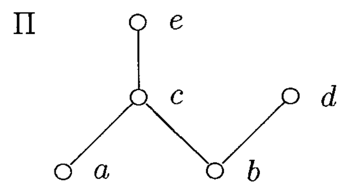


3.5.2 Número de elementos de $RB(X)$

Si Π es un conjunto ordenado y $x \in \Pi$ pongamos:

$$\text{Cono}(x) = (x] \cup [x).$$

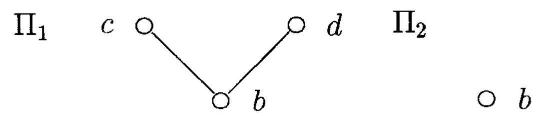
Por ejemplo, si Π tiene el diagrama que se indica:



entonces $Cono(c) = \{a, b, c, e\}$.
J. Berman and P. Köhler, *Cardinalities of finite distributive lattices*, Mitt. Math Sem. Gieβen 121 (1976), 103-124, probaron que si Π es un conjunto ordenado finito, entonces cualquiera que sea $x \in \Pi$, se tiene:

$$N[RB(\Pi)] = N[RB(\Pi \setminus \{x\})] + N[RB(\Pi \setminus Cono(x))].$$

Este resultado nos dá información sobre el número de elementos de $RB(\Pi)$ pero no sobre su estructura. En el ejemplo 4) indicado anteriormente, si $x = a$ entonces $Cono(a) = \{a, c, d\}$, $\Pi_1 = \Pi \setminus \{a\}$, $\Pi_2 = \Pi \setminus Cono(a)$ tienen los diagramas indicados a continuación:

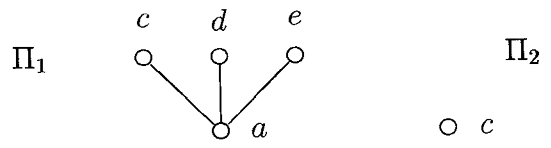


y en consecuencia $N[RB(\Pi_1)] = 5$ y $N[RB(\Pi_2)] = 2$. Por lo tanto, $N[RB(\Pi)] = 5+2 = 7$.

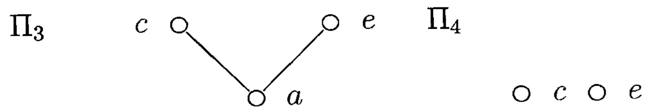
Observemos que si p es primer elemento del conjunto ordenado Π entonces $\Pi \setminus Cono(p) = \Pi \setminus \Pi = \emptyset$ y si u es último elemento de Π entonces $\Pi \setminus Cono(u) = \Pi \setminus \Pi = \emptyset$. Por lo tanto, en estos casos $RB(\emptyset)$ tiene un solo elemento. En el ejemplo 3) indicado anteriormente si consideramos $x = a$ entonces $\Pi_1 = \Pi \setminus Cono(a) = \emptyset$, y $\Pi_2 = \Pi \setminus \{a\}$ tiene el siguiente diagrama:

Π_2 ○ b ○ c

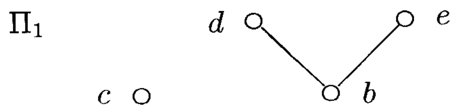
por lo tanto $N[RB(\Pi_1)] = 1$ y $N[RB(\Pi_2)] = 4$, luego $N[RB(\Pi)] = 5$.
Consideremos en el ejemplo 5) $x = b$ entonces $\Pi_1 = \Pi \setminus \{b\}$, $\Pi_2 = \Pi \setminus Cono(b)$ tienen los diagramas indicados a continuación:



y en consecuencia $N[RB(\Pi_2)] = 2$. En el conjunto ordenado Π_1 consideremos $x = d$ luego $\Pi_3 = \Pi_1 \setminus \{d\}$, $\Pi_4 = \Pi_1 \setminus Cono(d)$ tienen los diagramas indicados a continuación:



y en consecuencia $N[RB(\Pi_3)] = 5$ y $N[RB(\Pi_4)] = 4$, luego $N[RB(\Pi)] = 2 + 5 + 4 = 11$, como habíamos visto anteriormente.
Si hubiésemos considerado en Π, $x = a$ entonces $\Pi_1 = \Pi \setminus \{a\}$, $\Pi_2 = \emptyset$, luego $N[RB(\Pi_2)] = 2$. El conjunto Π_1 tiene el siguiente diagrama:



luego es la suma cardinal de dos conjuntos ordenados Π_2 y Π_3, esto es $\Pi_1 = \Pi_2 + \Pi_3$ luego por el Teorema 3.4.2 $RB(\Pi_1) = RB(\Pi_2) \times RB(\Pi_3)$, por lo tanto $N[RB(\Pi_1)] = 2 \times 5 = 10$, y en consecuencia $N[RB(\Pi)] = 11$.

Sea X un conjunto no vacío, R un reticulado distributivo con 0 y 1 y $F(X, R)$ el conjunto de todos las funciones de X en R. Si $f, g \in F(X, R)$, pongamos por definición:

$$\begin{cases} (f \wedge g)(x) = f(x) \wedge g(x) \\ \\ (f \vee g)(x) = f(x) \vee g(x) \end{cases} \qquad \forall \ x \in X$$

entonces $F(X, R)$ es un reticulado distributivo. Ademas $\mathbf{0}(x) = 0, \mathbf{1}(x) = 1$ cqs. $x \in X$ son el primer y último elemento de $F(X, R)$ respectivamente.

Si X es un conjunto ordenado y R^X es el conjunto de todas las funciones isótonas de X en R, entonces $R^X \subseteq F(X, R)$, $\mathbf{0}, \mathbf{1} \in R^X$ y es claro que si $f, g \in R^X$ entonces $f \wedge g, f \vee g \in R^X$. Por lo tanto, R^X es un $(0, 1)$-subreticulado de $F(X, R)$ y en consecuencia es un reticulado distributivo con primer y último elemento.

Sea X un conjunto ordenado finito y $\mathbf{2} = \{0, 1\}$, donde $0 < 1$. Como $\mathbf{2}$ es una cadena entonces es un reticulado distributivo. Además tiene primer y último elemento. En este caso $\mathbf{2}^X$ es un reticulado distributivo finito ya que es un subreticulado del reticulado distributivo finito $F(X, \mathbf{2})$.

Vamos a probar que $RB(X)$ y $(\mathbf{2}^X)^*$ son reticulados distributivos isomorfos.

Observemos que como $\mathbf{2} \cong \mathbf{2}^*$ entonces $\mathbf{2}^{(X^*)} \cong (\mathbf{2}^*)^{(X^*)}$, y como $(\mathbf{2}^X)^* \cong (\mathbf{2}^*)^{(X^*)}$ entonces $\mathbf{2}^{(X^*)} \cong (\mathbf{2}^X)^*$.

Vamos a definir una función $\varphi : \mathbf{2}^X \to RB(X)$ y vamos a probar que φ es un isomorfismo de orden entre los conjuntos ordenados $(\mathbf{2}^X, \leq^*)$ y $(RB(X), \subseteq)$ de donde resultará por el Lema 3.4.2, que los reticulados distributivos $(\mathbf{2}^X)^*$ y $RB(X)$ son isomorfos.

Sea $f \in \mathbf{2}^X$, esto es una función isótona de X en $\mathbf{2}$, y pongamos por definición:

$$\varphi(f) = f^{-1}(0),$$

luego $f^{-1}(0) \subseteq X$.
Si $f^{-1}(0) = \emptyset$, lo que ocurre cuando $0 \notin Im(f)$ entonces $f^{-1}(0) \in RB(X)$.
Si $f^{-1}(0) \neq \emptyset$, esto es cuando $0 \in Im(f)$. Veamos que $f^{-1}(0) \in RB(X)$. En efecto si $x \in f^{-1}(0)$, esto es $f(x) = 0$, sea $y \leq x$ como f es isótona $f(y) \leq f(x) = 0$ y en consecuencia $f(y) = 0$ esto es $y \in f^{-1}(0)$. Por lo tanto en ambos casos $f^{-1}(0)$ es una sección inferior de X, esto es $f^{-1}(0) \in RB(X)$.

1) φ es suryectiva.
Sea $Y \in RB(X)$, esto es, $Y \subseteq X$ e Y es una sección inferior de X.

$$f_Y(x) = \begin{cases} 0 \in \mathbf{2}, & \text{si } x \in Y \\ \\ 1 \in \mathbf{2}, & \text{si } x \notin Y \end{cases} \qquad , x \in X$$

Tenemos así una función f_Y de X en $\mathbf{2}$.

1a) $f_Y \in \mathbf{2}^X$.
Sean $x, y \in X$, $x \leq y$. Si $f_Y(y) = 1$ entonces $f_Y(x) \leq f_Y(y) = 1$. Si $f_Y(y) = 0$ entonces $y \in Y$ y como $x \leq y$ tenemos que $x \in Y$, luego $f_Y(x) = 0$ y por lo tanto $0 = f_Y(x) \leq f_Y(y) = 0$.

1b) $\varphi(f_Y) = Y$.
En efecto $\varphi(f_Y) = f_Y^{-1}(0) = Y$.

2) Si $f_1, f_2 \in \mathbf{2}^X$, y $f_1 \leq^* f_2$, esto es $f_2 \leq f_1$ entonces $\varphi(f_1) \subseteq \varphi(f_2)$.
Si $\varphi(f_1) = \emptyset$, es claro que se verifica la inclusión. Si $\varphi(f_1) \neq \emptyset$ sea $x \in \varphi(f_1) = f_1^{-1}(0)$, luego $f_1(x) = 0$ y como $f_2 \leq f_1$ tenemos que $f_2(x) = 0$, luego $x \in f_2^{-1}(0) = \varphi(f_2)$.

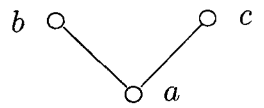
3) Si $f_1, f_2 \in \mathbf{2}^X$, son tales que $\varphi(f_1) \subseteq \varphi(f_2)$, entonces $f_1 \leq^* f_2$, esto es $f_2 \leq f_1$.
Si $f_2 \not\leq f_1$ existe $x \in X$ tal que $f_2(x) \not\leq f_1(x)$ y como ambas funciones toman valores en $\mathbf{2} = \{0, 1\}$, debe ser $f_2(x) = 1$ y $f_1(x) = 0$ entonces $x \in \varphi(f_1) \subseteq \varphi(f_2) = f_2^{-1}(0)$, luego $f_2(x) = 0$, absurdo.
Otro modo de demostrar 3) es el siguente: Por hipótesis, $f_1^{-1}(0) \subseteq f_2^{-1}(0)$ luego $f_2^{-1}(1) = X \setminus f_2^{-1}(0) \subseteq X \setminus f_1^{-1}(0) = f_1^{-1}(1)$. Por lo tanto si $f_2(x) = 0$ entonces $f_2(x) = 0 \leq f_1(x)$, y si $f_2(x) = 1$, $x \in f_2^{-1}(1)$, luego $x \in f_1^{-1}(1)$ esto es $f_1(x) = 1$ y en consecuencia $f_2(x) \leq f_1(x)$.

De 1), 2) y 3) resulta que $(\mathbf{2}^X)^* \cong RB(X)$.

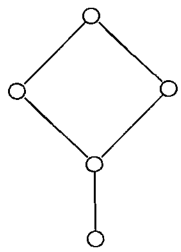
Vamos a indicar otra demostración del Teorema 3.4.2 cuyo enunciado es el siguiente:
Si A es un reticulado distributivo finito, no trivial, $\Pi = \Pi(A)$, $\Pi = \Pi_1 + \Pi_2$ *y* A_1 *y* A_2 *son reticulados distributivos finitos tales que* $\Pi(A_i) \cong \Pi_i$, *para* $i = 1, 2$ *entonces* $A \cong A_1 \times A_2$.
Por lo demostrado anteriormente tenemos que $A_1 \cong RB(\Pi_1) \cong \mathbf{2}^{(\Pi_1^*)}$ y $A_2 \cong RB(\Pi_2) \cong \mathbf{2}^{(\Pi_2^*)}$, luego:

$$A_1 \times A_2 \cong \mathbf{2}^{(\Pi_1^*)} \times \mathbf{2}^{(\Pi_2^*)} \cong \mathbf{2}^{(\Pi_1^* + \Pi_2^*)} \cong \mathbf{2}^{(\Pi_1 + \Pi_2)^*} \cong \mathbf{2}^{\Pi^*} \cong RB(\Pi) \cong A.$$

Ejemplo 3.5.2 *Sea X el conjunto ordenado que se indica a continuación.*



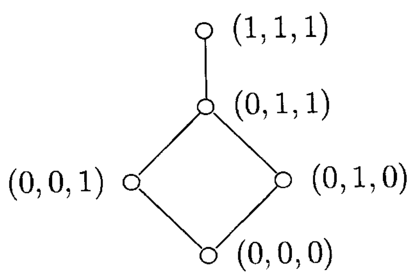
Vimos anteriormente que $RB(X)$ tiene el siguiente diagrama:

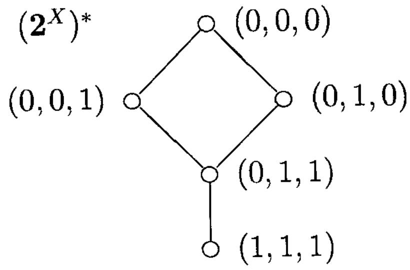


A continuación indicamos los elementos de $\mathbf{2}^X$, su diagrama y el diagrama de $(\mathbf{2}^X)^*$.

	f_1	f_2	f_3	f_4	f_5
a	*0*	*0*	*0*	*0*	*1*
b	*0*	*0*	*1*	*1*	*1*
c	*0*	*1*	*0*	*1*	*1*

$\mathbf{2}^X$





Los siguientes resultados se deben a L. Monteiro. [1] Sea t un elemento fijo de X y

$$F_{t,0} = \{f \in \mathbf{2}^X : f(t) = 0\}, \qquad F_{t,1} = \{f \in \mathbf{2}^X : f(t) = 1\},$$

luego

$$F_{t,0} \cup F_{t,1} = \mathbf{2}^X \text{ y } F_{t,0} \cap F_{t,1} = \emptyset$$

por lo tanto

$$N[\mathbf{2}^X] = N[F_{t,0}] + N[F_{t,1}].$$

En el caso anterior tenemos: si $t = a$, $N[\mathbf{2}^X] = 4 + 1$, si $t = b$, $N[\mathbf{2}^X] = 2 + 3$, y si $t = c$, $N[\mathbf{2}^X] = 2 + 3$.

Lema 3.5.1 *1) Si p es primer elemento de X entonces $F_{p,1} = \{\mathbf{1}\}$.*

2) Si u es último elemento de X entonces $F_{u,0} = \{\mathbf{0}\}$.

3) p es primer elemento de X $\iff$ $X \setminus [p) = \emptyset$.

4) u es último elemento de X $\iff$ $X \setminus (u] = \emptyset$.

5) t no es primer ni último elemento de X $\iff$ $X \setminus [t) \neq \emptyset$ y $X \setminus (t] \neq \emptyset$

Dem. 1) y 2) se prueban sin dificultad.

3) $\Longrightarrow$) Como $p \leq x$, $\forall\, x \in X$ entonces $X = [p)$.
$\Longleftarrow$) Si $X \setminus [p) = \emptyset$ entonces $X \subseteq [p)$ y como $[p) \subseteq X$ entonces $X = [p)$, por lo tanto p es primer elemento de X.

4) Se prueba en forma similar a la anterior.

5) Es una consecuencia inmediata de 3) y 4).

■

Lema 3.5.2 *Si t no es primer ni último elemento de X entonces $N[F_{t,0}] = N[\mathbf{2}^{(X\setminus(t])}]$ y $N[F_{t,1}] = N[\mathbf{2}^{(X\setminus[t))}]$.*

Dem. Sea $f \in F_{t,0}$, esto es $f \in \mathbf{2}^X$ y $f(t) = 0$ luego:

$$\text{(i)} \qquad f(x) = 0, \quad \forall\ x \in (t].$$

Sea $f^* = f_{|X\setminus(t]}$, luego $f^* : X \setminus (t] \to \mathbf{2}$ y es claro que f^* es isótona, luego $f^* \in \mathbf{2}^{X\setminus(t]}$. Pongamos $H(f) = f_{|X\setminus(t]}$, luego:

$$H : F_{t,0} \to \mathbf{2}^{X\setminus(t]}.$$

[1] *Los mismos fueron obtenidos en 1990 y expuestos en diversos cursos que dictara en la Universidad Nacional del Sur y en el Congreso "Lógica 98" realizado en la Universidade de Évora, Portugal (13 al 17 de julio de 1998)* en homenaje al Dr. Antonio A. R. Monteiro y publicados en "Multiple Valued Logic (2000), 1-18 (volumen de homenaje al Dr. Gr. C. Moisil).

Sea $f^* \in \mathbf{2}^{X\setminus(t]}$, esto es $f^* : X \setminus (t] \to \mathbf{2}$ y f^* es isótona. Pongamos por definición:

$$f(x) = \begin{cases} f^*(x) & \text{si } x \in X \setminus (t] \iff x \notin (t], \\ 0 & \text{si } x \in (t] \end{cases} \quad , x \in X \ .$$

luego $f : X \to \mathbf{2}$ y por definición $f(t) = 0$.
Probemos que f es isótona. Sean $x, y \in X$ tales que $x \leq y$, entonces no puede ocurrir que $x \in X \setminus (t]$ e $y \in (t]$, pués en este caso $y \leq t$ y como $x \leq y$ entonces tendríamos que $x \leq t$, esto es $x \in (t]$, absurdo. Luego, sólo se pueden presentar los siguientes casos:

a) $x, y \in (t]$.
Entonces $f(x) = 0 \leq 0 = f(y)$.

b) $x, y \in X \setminus (t]$.
$f(x) = f^*(x) \leq f^*(y) = f(y)$.

c) $x \in (t]$, $y \in X \setminus (t]$.
$f(x) = 0 \leq f^*(y) = f(y)$.

Además es claro que $H(f) = f_{|X\setminus(t]} = f^*$, esto es H es suryectiva.
Vamos a probar que los conjuntos ordenados $F_{t,0}$ y $\mathbf{2}^{X\setminus(t]}$ son isomorfos.
Sean $f, g \in F_{t,0}$, tales que $f \leq g$, esto es $f(x) \leq g(x)$, para todo $x \in X$, luego en particular $f(x) \leq g(x)$, para todo $x \in X \setminus (t]$, entonces

$$H(f) = f_{|X\setminus(t]} \leq g_{|X\setminus(t]} = H(g).$$

Recíprocamente si $f, g \in F_{t,0}$ son tales que $f_{|X\setminus(t]} = H(f) \leq H(g) = g_{|X\setminus(t]}$, como $f, g \in F_{t,0}$ esto es $f(x) = g(x) = 0$ para todo $x \in (t]$ entonces $f \leq g$. Acabamos así de probar que los conjuntos $F_{t,0}$ y $\mathbf{2}^{X\setminus(t]}$ son isomorfos y por lo tanto coordinables. En forma análoga se demuestra que $F_{t,1}$ y $\mathbf{2}^{X\setminus[t)}$ son coordinables.
Observemos que la hipótesis de que t no es primer ni último elemento de X sólo tiene importancia para que $X \setminus (t] \neq \emptyset$ y $X \setminus [t) \neq \emptyset$. ■

Tenemos asi que:

1) Si t es primer elemento de X entonces $N[\mathbf{2}^X] = N[F_{t,0}] + 1$.

2) Si t es último elemento de X entonces $N[\mathbf{2}^X] = 1 + N[F_{t,1}]$.

3) Si t no es primer ni último elemento de X entonces $N[\mathbf{2}^X] = N[\mathbf{2}^{X\setminus(t]}] + N[\mathbf{2}^{X\setminus[t)}]$ y por lo tanto:
$$N[RB(X)] = N[RB(X \setminus (t])] + N[RB(X \setminus [t))].$$

El problema consiste en determinar un elemento $t \in X$ de forma tal que sea fácil calcular $F_{t,0}$ y $F_{t,1}$ ó $\mathbf{2}^{X\setminus(t]}$ y $\mathbf{2}^{X\setminus[t)}$.
Observemos que el número de funciones isótonas de una cadena C_n con n elementos en una cadena C_m con m elementos es:

$$N[C_m^{C_n}] = \binom{m+n-1}{n}.$$

Luego si $m = 2$, que es el caso que nos interesa tenemos que

$$N[\mathbf{2}^{C_n}] = \binom{2+n-1}{n} = n+1.$$

Vimos que si X, Y, Z son conjuntos ordenados entonces:

$$X^Y \times X^Z \cong X^{Y+Z},$$

luego, si ellos son finitos:

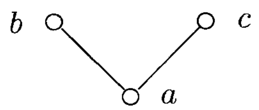
$$N[X^{Y+Z}] = N[X^Y] \,.\, N[X^Z],$$

luego si $X = \mathbf{2}$ e Y, Z son cadenas finitas tenemos que:

$$N[\mathbf{2}^{Y+Z}] = (N[Y]+1) \,.\, (N[Z]+1).$$

Por lo tanto si mediante la elección de un elemento $t \in X$ obtenemos que $X \setminus (t]$ y $X \setminus [t)$ son cadenas, o suma cardinal de cadenas, el cálculo de $N[\mathbf{2}^X]$ es inmediato.

Ejemplo 3.5.3 *1) Sea X el conjunto ordenado cuyo diagrama se indica:*



$t = a)$ *Entonces* $N[\mathbf{2}^X] = N[F_{a,0}] + N[F_{a,1}] = N[F_{a,0}] + 1 = N[\mathbf{2}^{X\setminus(a]}] + 1$. *Como* $X \setminus (a]$ *tiene el siguiente diagrama, (es suma cardinal de 2 cadenas):*

entonces $N[RB(X)] = N[\mathbf{2}^X] = (2 \times 2) + 1$.

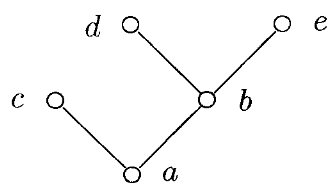
$t = b)$ *Entonces* $X \setminus (b]$ *y* $X \setminus [b)$ *tienen los diagramas que se indican a continuación:*

y por lo tanto $N[RB(X)] = N[\mathbf{2}^X] = 2 + 3 = 5$.

$t = c)$ *Entonces* $X \setminus (c]$ *y* $X \setminus [c)$ *tienen los diagramas que se indican a continuación:*

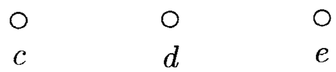
y por lo tanto $N[RB(X)] = N[\mathbf{2}^X] = 2 + 3 = 5$.

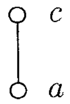
2) Sea Y el conjunto ordenado cuyo diagrama se indica:



Entonces:

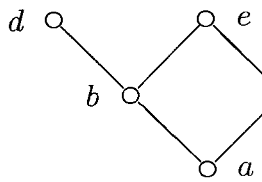
$$Y \setminus (b] = \{c, d, e\} \qquad\qquad Y \setminus [b) = \{a, c\}$$





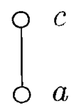
luego $N[RB(Y)] = N[\mathbf{2}^Y] = (2 \times 2 \times 2) + 3 = 11.$

3) Sea Z el conjunto ordenado cuyo diagrama se indica:



Entonces:

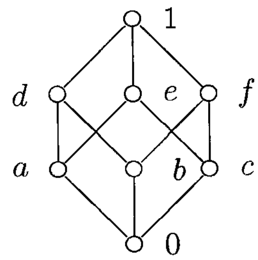
$$Z \setminus (b] \qquad\qquad\qquad Z \setminus [b)$$



luego $N[RB(Z)] = N[\mathbf{2}^Z] = (2 \times 3) + 3 = 9.$

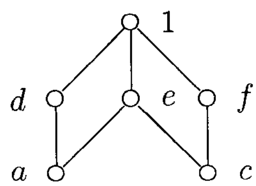
Vamos a determinar el número de elementos del reticulado de Birkhoff determinado por cada uno de los conjuntos ordenados indicados a continuación, así como el diagrama de los reticulados.

A

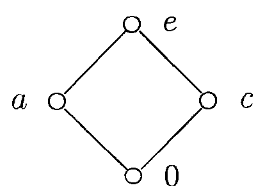


entonces los conjuntos $A_1 = A \setminus (b]$ y $A_2 = A \setminus [b)$ tienen los siguientes diagramas:

A_1

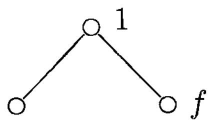


A_2

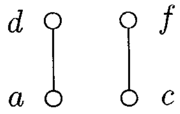


Por lo tanto $N[RB(A_2)] = 6$. Consideremos el elemento $e \in A_1$, entonces $A_{11} = A_1 \setminus (e]$ y $A_{12} = A_1 \setminus [e)$ tienen los siguientes diagramas:

A_{11}

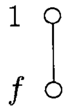


A_{12}



Entonces $N[RB(A_{12})] = 3 \times 3 = 9$. Consideremos el elemento $d \in A_{11}$. Entonces los conjuntos
$A_{111} = A_{11} \setminus (d]$ y $A_{112} = A_{11} \setminus [d)$ tienen los siguientes diagramas:

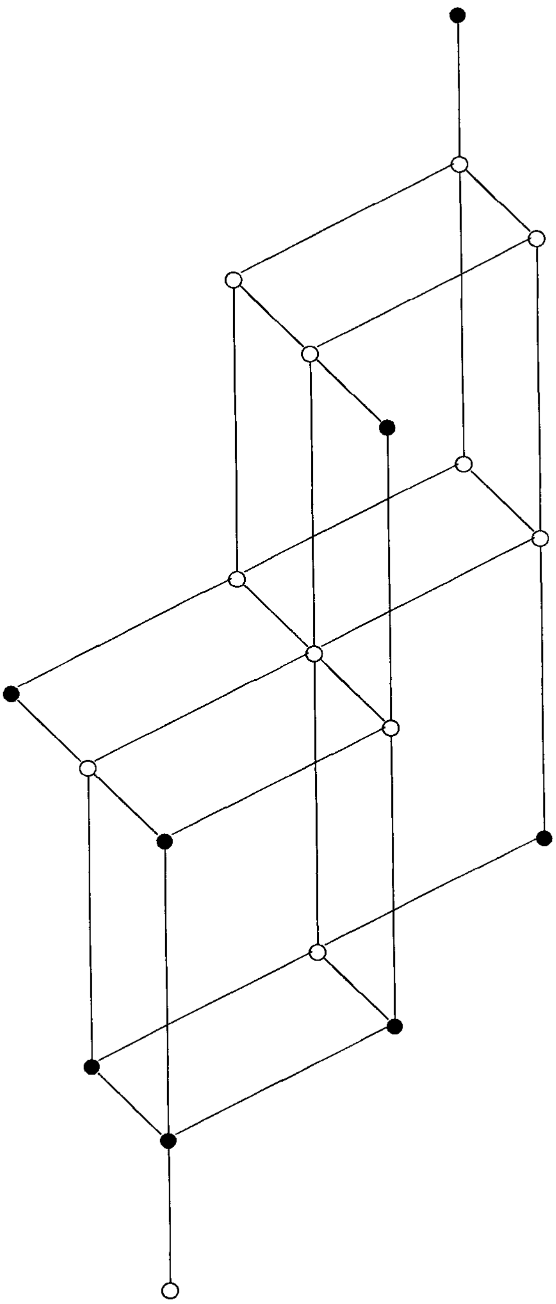
A_{111}



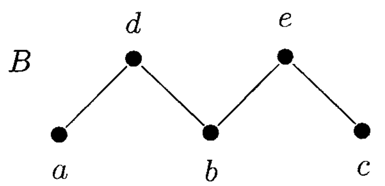
A_{112}

Por lo tanto:
$N[RB(A_{11})] = N[RB(A_{111})] + N[RB(A_{112})] = 3 + 2 = 5$. En consecuencia $N[RB(A)] = 6 + 9 + 5 = 20$, su diagrama de Hasse se indica a continuación:

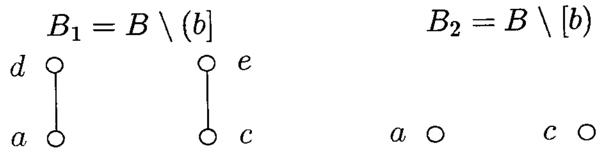
$RB(A)$



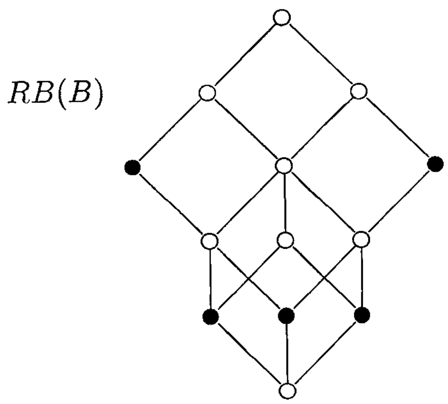
Consideremos el conjunto ordenado B indicado a continuación:



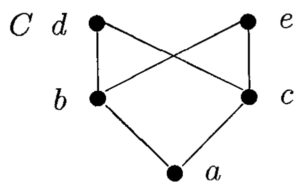
entonces los conjuntos $B_1 = B \setminus (b]$ y $B_2 = B \setminus [b)$ tienen los siguientes diagramas:



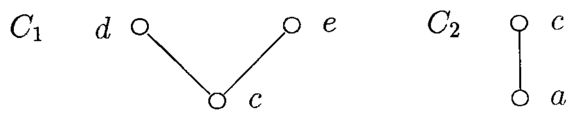
luego $N[RB(B)] = N[RB(B_1)] + N[RB(B_2)] = (3 \times 3) + (2 \times 2) = 13$, y su diagrama es:



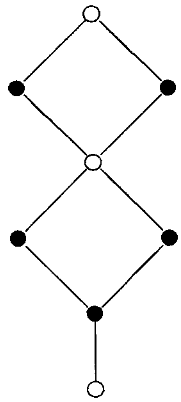
Consideremos ahora el siguiente conjunto ordenado:



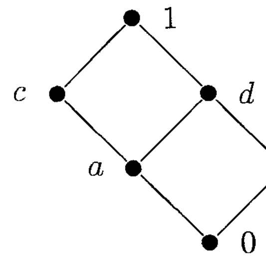
entonces los conjuntos $C_1 = C \setminus (b]$ y $C_2 = C \setminus [b)$ tienen los siguientes diagramas:



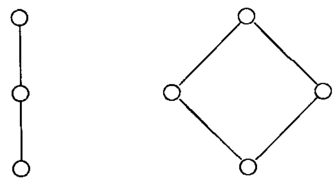
entonces, ya vimos que $N[RB(C_1)] = 5$ y $N[RB(C_2)] = 3$, por lo tanto $N[RB(C)] = 8$. Su diagrama se indica a continuación:



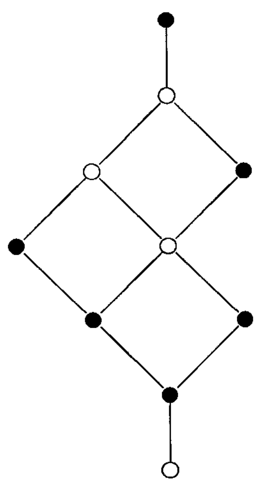
Consideremos el siguiente conjunto ordenado D:



entonces los conjuntos $D_1 = D \setminus (c]$ y $D_2 = D \setminus [c)$ tienen los siguientes diagramas:



entonces, ya vimos que $N[RB(D_1)] = 4$ y $N[RB(D_2)] = 6$, por lo tanto $N[RB(C)] = 10$. Su diagrama se indica a continuación:



Sabemos que si un conjunto ordenado finito X es la suma cardinal de conjuntos ordenados, $X = \sum_{i=1}^{n} X_i$ y R_i, $1 \leq i \leq n$ son reticulados distributivos tales que $\Pi(R_i) \cong X_i$ $1 \leq i \leq n$ entonces $R = \prod_{i=1}^{n} R_i$ verifica $\Pi(R) \cong X$.
Si el conjunto X es conexo la construcción de $RB(X)$ puede ser mas o menos complicada dependiendo la misma de lo *"complicado"* que sea el diagrama de X.
Indiquemos una simplificación para un caso particular de ciertos conjuntos ordenados conexos (M. Abad y L. Monteiro, Notas de Lógica Matemática 35, INMABB-CONICET-UNS (1987)). Sea X un conjunto ordenado finito, no trivial con primer elemento p_0, luego X es conexo. Sean $p_1, p_2, \ldots, p_t$ los elementos que cubren a p_0 y supongamos que se verifica:

$$[p_i) \cap [p_j) = \emptyset, \quad 1 \leq i, j \leq t, \quad i \neq j.$$

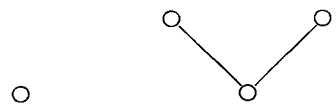
Sean R_i, $1 \leq i \leq t$ reticulados distributivos tales que $\Pi(R_i) \cong [p_i)$, $1 \leq i \leq t$ entonces

$$R = \{0\} \oplus \prod_{i=1}^{t} R_i,$$

es un reticulado distributivo tal que $\Pi(R) \cong X$.

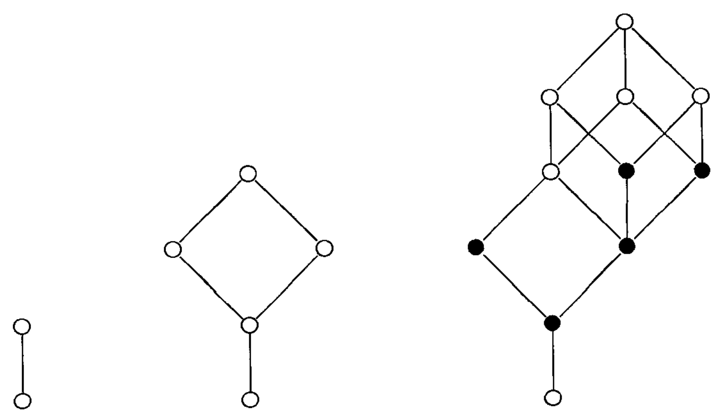
Ejemplo 3.5.4

1) Consideremos el conjunto ordenado indicado en el Ejemplo 3.5.3, 2), entonces $p_0 = a$, $p_1 = b$, $p_2 = c$ y $[b) \cap [c) = \emptyset$. Luego $[c)$ y $[b)$ tienen los siguientes diagramas:

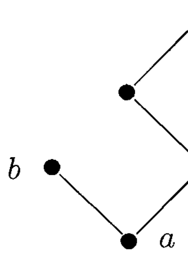


y R_1, R_2 y R los diagramas:

R_1 $\qquad$ R_2 $\qquad$ $R = \{0\} \oplus R_1 \times R_2$

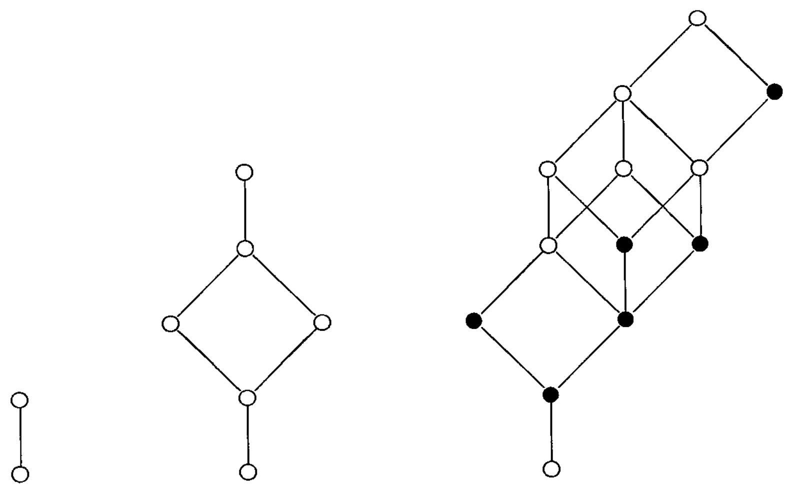


2) Consideremos el conjunto ordenado indicado a continuación:



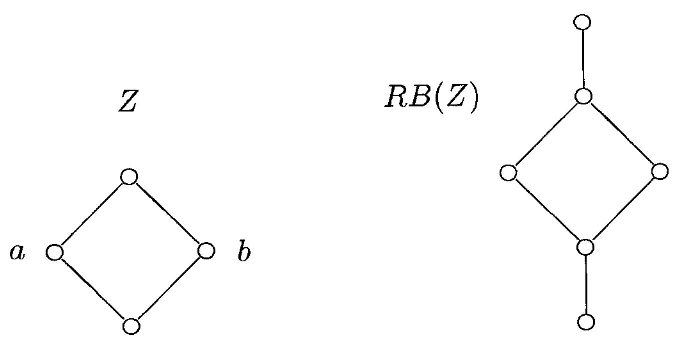
entonces $p_0 = a$, $p_1 = b$, $p_2 = c$ y los reticulados R_1 y R_2 tales que: $R_1 \cong [b)$, $R_2 \cong [c)$ y $R = \{0\} \oplus R_1 \times R_2$ tienen los siguientes diagramas:

R_1 $\qquad$ R_2 $\qquad$ $R = \{0\} \oplus R_1 \times R_2$

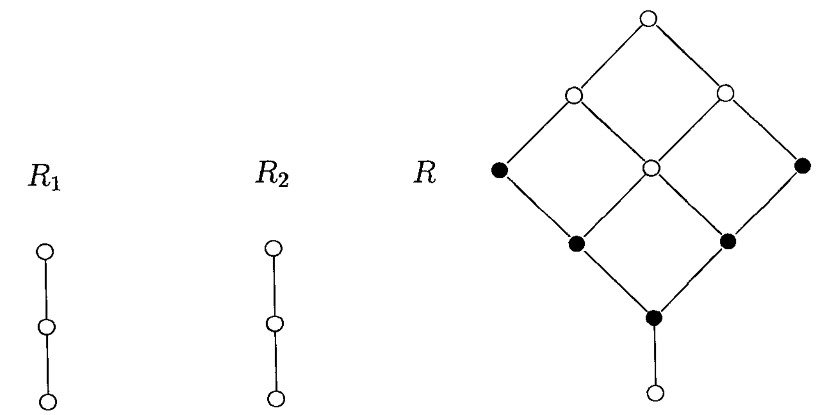


Observemos que esta construcción no vale para cualquier conjunto ordenado finito con primer elemento: Sea Z el conjunto ordenado indicado a continuación, vimos que $RB(Z)$ tiene el siguiente diagrama:

Z $\qquad$ $RB(Z)$

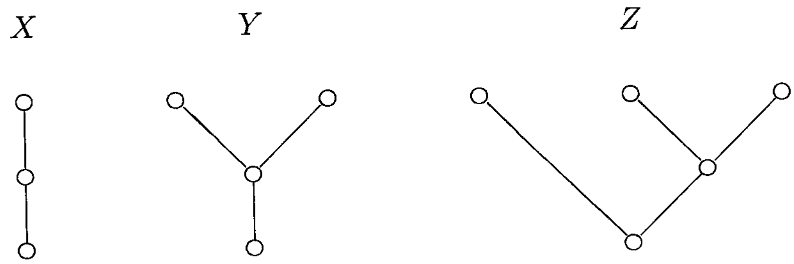


En este caso $R_1 = RB([a))$, $R_2 = RB([b))$ y $R = \{0\} \oplus R_1 \times R_2$ tienen los siguientes diagramas:

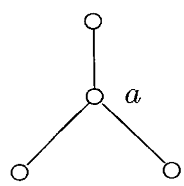


Definición 3.5.1 *Un conjunto ordenado* <u>*conexo*</u> X *se dice un* **árbol** *si* $(x]$ *es una cadena, cualquiera que sea* $x \in X$.

Los siguientes conjuntos ordenados son árboles:



y el conjunto ordenado indicado a continuación, no es un árbol dado que $(a]$ no es una cadena.



Lema 3.5.3 *Un conjunto ordenado* X *es un árbol* $\iff$ $[a) \cap [b) = \emptyset$ *para todo par de elementos incomparables* $a, b \in X$, (L. Monteiro, 1990).

Dem.

$\Longrightarrow$) Supongamos que existen elementos incomparables $a, b \in X$ tales que $[a) \cap [b) \neq \emptyset$, luego existe $x \in [a) \cap [b)$ esto es $a \leq x$, $b \leq x$ y por lo tanto $a, b \in (x]$ de donde resulta por ser $(x]$ una cadena que $a \leq b$ ó $b \leq a$, absurdo.

$\Longleftarrow$) Supongamos que existe $z \in X$ tal que $(z]$ no es una cadena, entonces existen (1) $a, b \in (z]$ incomparables en $(z]$ (y en X). De (1) resulta que $a \leq z$, $b \leq z$ y por lo tanto $z \in [a) \cap [b)$, absurdo.

■

Si consideramos el conjunto ordenado $A = X + Y$, donde X e Y son los conjuntos ordenados indicados precedentemente, entonces A verifica el Lema 3.5.3, pero no es un árbol dado que no es conexo.

Lema 3.5.4 *Todo árbol finito tiene primer elemento.* (L. Monteiro, 1990)

Dem. Sea X un árbol finito, luego, por definición, es un conjunto conexo finito. Como X es un conjunto ordenado finito, sabemos que tiene por lo menos un elemento mínimo, y sabemos además que si un conjunto ordenado finito tiene un único elemento mínimo él es el primer elemento del conjunto ordenado.
Supongamos que X tiene más de un elemento mínimo y sean $m_1, m_2, \ldots, m_n$, donde $n > 1$ los elementos mínimos de X, luego ellos son incomparables dos a dos, en consecuencia por el lema anterior $[m_i) \cap [m_j) = \emptyset$, para todo par de índices i, j, $i \neq j$. Además es claro que $\bigcup_{i=1}^{n} [m_i) = X$. Probemos que $X = \sum_{i=1}^{n} [m_i)$. Supongamos que existen (1) $z \in [m_i)$, (2) $w \in [m_j)$, donde $i \neq j$, que son comparables, por ejemplo (3) $z \leq w$. De (1) resulta (4) $m_i \leq z$, y por lo tanto de (3) y (4) obtenemos (5) $w \in [m_i)$. Finalmente de (2) y (5): $w \in [m_i) \cap [m_j) = \emptyset$, absurdo. Luego X es la suma cardinal de conjuntos ordenados, lo que contradice que X es conexo, por lo tanto X tiene primer elemento. ■

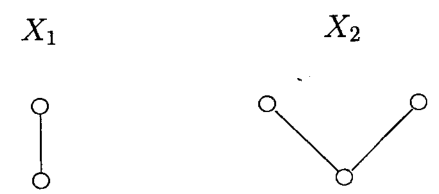
Si X es un árbol finito se puede aplicar la construcción de Abad-Monteiro para obtener $RB(X)$. Observemos que el conjunto ordenado indicado en el Ejemplo 3.5.4, 2), no es un árbol pero a él se le puede aplicar la citada construcción.

Definición 3.5.2 *Un conjunto ordenado X se dice una* **floresta** *o un* **bosque** *si es la suma cardinal de árboles.*

Si X es un bosque finito y $X = \sum_{i=1}^{n} X_i$ entonces:

$$RB(X) = \prod_{i=1}^{n} RB(X_i) = \prod_{i=1}^{n} (\{0\} \oplus \prod_{j=1}^{n_i} RB([m_j)),$$

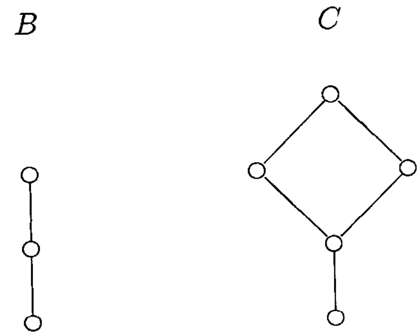
donde n_i indica el número de elementos de X_i que cubren al primer elemento de X_i, y m_j, $1 \leq j \leq n_i$ son tales elementos. Por ejemplo, si $X = X_1 + X_2$ tiene el siguiente diagrama:



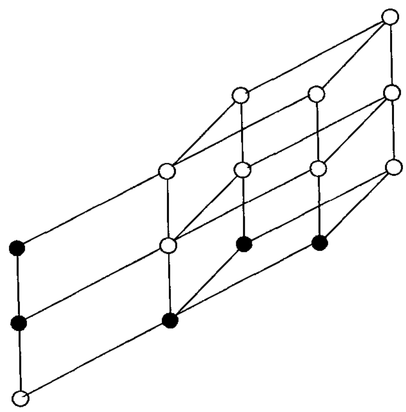
entonces:

$$RB(X) = (\{0\} \oplus X_1) \times (\{0\} \oplus A) = B \times C$$

donde A es el producto cartesiano de dos cadenas con dos elementos cada una y por lo tanto B y C tienen los siguientes diagramas:



y el diagrama de $RB(X)$ es:



3.6 Producto subdirecto de reticulados distributivos

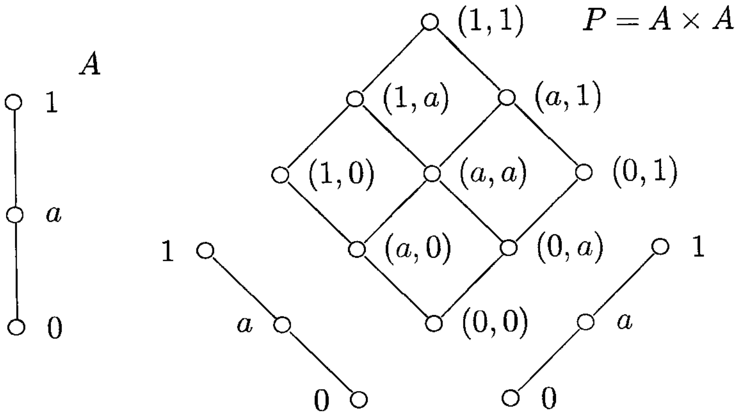
Dada una familia $\{A_i\}_{i \in I}$ no vacía de reticulados distributivos, sabemos que el conjunto $P = \prod_{i \in I} A_i$ es un reticulado distributivo. A los reticulados A_i se los denomina **ejes** del reticulado P. El siguiente resultado se prueba fácilmente.

Lema 3.6.1 *Para que P tenga primer (último) elemento es necesario y suficiente que todos los reticulados A_i, $i \in I$ tengan primer (último) elemento.*

Consideremos la proyección (proyección i-ésima) Π_i de P sobre A_i definida por $\Pi_i(a) = a_i \in A_i$. Probemos que Π_i es un homomorfismo de P sobre A_i. Claramente cada Π_i es una función suryectiva. Sean $a, b \in P$ entonces $\Pi_i(a \wedge b) = \Pi_i((a_i)_{i \in I} \wedge (b_i)_{i \in I}) = \Pi_i(a_i \wedge b_i)_{i \in I} = a_i \wedge b_i = \Pi_i(a) \wedge \Pi_i(b)$. En forma análoga se prueba que $\Pi_i(a \vee b) = \Pi_i(a) \vee \Pi_i(b)$. Si P tiene primer elemento $0 = (0_i)_{i \in I}$ y último elemento $1 = (1_i)_{i \in I}$ entonces $\Pi_i(0) = 0_i$ y $\Pi_i(1) = 1_i$ para todo $i \in I$.
En esta sección sólo consideraremos reticulados distributivos con primer y último elemento.

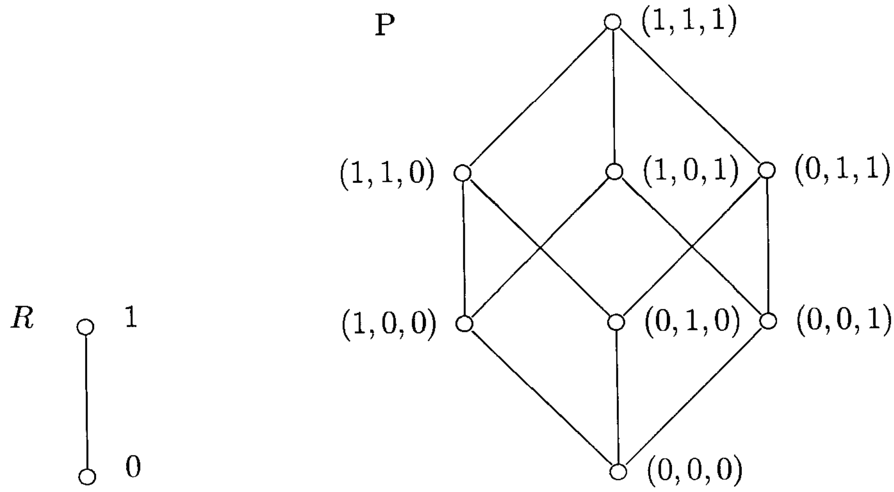
Definición 3.6.1 *Si S es un $(0,1)$-subreticulado del reticulado $P = \prod_{i \in I} A_i$ tal que $\Pi_i(S) = A_i$, para todo $i \in I$, entonces diremos que S es un* **producto subdirecto** *de los reticulados distributivos A_i.*

Ejemplo 3.6.1 *Sean $A_1 = A_2 = A$ y $P = A \times A$ los reticulados distributivos indicados en la figura:*



El subconjunto $S = \{(0,0),(1,0),(0,1),(1,1)\}$ es un $(0,1)$-subreticulado de P y $\Pi_1(S) = \{0,1\} \neq A_1$ y $\Pi_2(S) = \{0,1\} \neq A_2$, luego S no es subproducto directo de los reticulados A_1 y A_2. Observemos que ninguno de los homomorfismos Π_i, $i = 1,2$ es un isomorfismo. Claramente el propio reticulado P es un producto subdirecto de A_1 y A_2, mas precisamente es producto directo de los reticulados A_1 y A_2. El subconjunto $T = \{(0,0),(a,a),(1,1)\}$ de R es un $(0,1)$-subreticulado de P y $\Pi_1(T) = \{0,a,1\} = A_1$ y $\Pi_2(T) = \{0,a,1\} = A_2$. Por lo tanto T es producto subdirecto de los reticulados A_1 y A_2. En este caso los homomorfismos Π_i, $i = 1,2$ son isomorfismos.

Ejemplo 3.6.2 *Dado el reticulado R indicado en la figura consideremos el reticulado $P = R \times R \times R$, que tiene el siguiente diagrama:*



Consideremos el siguiente $(0,1)$-subreticulado de P,

$$S = \{(0,0,0),(0,1,0),(1,0,1),(1,1,1)\}.$$

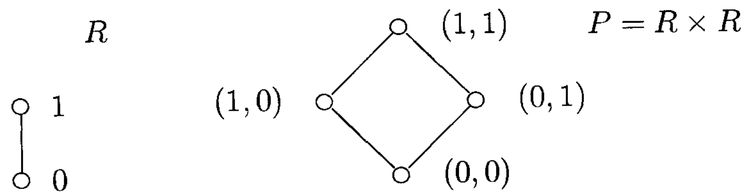
Luego las proyecciones sobre los ejes verifican: $\Pi_1(S) = \Pi_2(S) = \Pi_3(S) = R$, y en consecuencia S es un $(0,1)$-subreticulado propio de P, que es producto subdirecto de tres reticulados iguales a R.

Lema 3.6.2 *Todo $(0,1)$-subreticulado S del producto cartesiano $P = \prod_{i \in I} A_i$ de reticulados distributivos es subproducto directo de reticulados distributivos.*

Dem. Para cada $i \in I$ sea $A_i' = \Pi_i(S)$. Dado que las proyecciones son homomorfismos de P en A_i entonces A_i' es un $(0,1)$-subreticulado de A_i. Sea $P' = \prod\limits_{i \in I} A_i'$ y Π_i' la proyección i-ésima de P' en A_i'. Probemos que S es producto subdirecto de P', esto es que 1) S un $(0,1)$-subreticulado de P' y 2) $\Pi_i'(S) = A_i'$ cualquiera que sea $i \in I$. Por la definición de P' es obvio que se verifica 2). Dado $s = (s_i)_{i \in I} \in S$, como $s_i = \Pi_i(s) \in A_i'$, entonces $s = (a_i)_{i \in I} \in P' = \prod\limits_{i \in I} A_i'$. Por lo tanto S es un subconjunto de P', y en consecuencia S es un $(0,1)$-subreticulado de P'. ■

La condición $\Pi_i(S) = A_i$ indicada en la Definición 3.6.1 significa que sobre el eje A_i ninguna de las coordenadas es *"inútil"*. Pero esto no significa que no existan ejes en *"exceso"*. Cuando S es producto subdirecto de un reticulado $P = \prod\limits_{i \in I} A_i$ puede ocurrir que alguna de las proyecciones Π_i sea un isomorfismo. En el Ejemplo 3.6.1 ambas proyecciones del $(0,1)$-subreticulado T son isomorfismos.

Ejemplo 3.6.3 *Sea R el reticulado indicado y $P = R \times R$.*



entonces P es producto subdirecto de A_1 y A_2. En el Ejemplo 3.6.2 vimos que el $(0,1)$-subreticulado S es producto subdirecto de tres reticulados iguales a R y acabamos de ver que P también es producto subdirecto de dos reticulados iguales a R. Luego la representación de un reticulado como producto subdirecto de reticulados no está en general unívocamente determinada.

Se plantea el problema de la economía en el número de ejes coordenados. Observemos también que un reticulado A puede representarse como producto subdirecto de un número arbitrario de reticulados todos iguales a A. En efecto, sea $\{A_i\}_{i \in I}$, con $A_i = A$, y $P = \prod\limits_{i \in I} A_i = A^I$. Consideremos la diagonal A' de P, esto es, el conjunto de todos los elementos $(a_i)_{i \in I}$ de P tales que $a_i = a$ para todo $i \in I$.
Es evidente que:

1. A es isomorfo a A'. El isomorfismo es la transformación β que a cada elemento $a \in A$ le hace corresponder el elemento $\beta(a) = (a_i)_{i \in I}$, con $a_i = a$ para todo $i \in I$.

2. $\Pi_i(A') = A_i = A$, y por lo tanto A es isomorfa a un producto subdirecto de P.

3. En este caso todas las proyecciones son isomorfismos. Esto indica que sería suficiente tomar un solo eje.

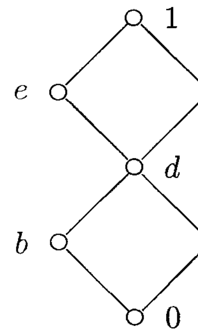
Definición 3.6.2 *Se dice que un reticulado A es* **subdirectamente reducible** *si A es isomorfo a un $(0,1)$-subreticulado A' de un producto directo $P = \prod_{i\in I} A_i$, en forma tal que:*

1. $\Pi_i(A') = A_i$, *cualquiera que sea $i \in I$.*

2. *Ninguna de las proyecciones es un isomorfismo.*

Un reticulado se dice **subdirectamente irreducible** *si no es subdirectamente reducible.*

Ejemplo 3.6.4 *Sea R' el reticulado indicado a continuación:*



El reticulado R' es isomorfo al subreticulado

$$S = \{(0,0),(a,0),(0,a),(a,a),(1,a),(a,1),(1,1)\}$$

del reticulado P indicado en el Ejemplo 3.6.1. S es claramente producto subdirecto de los reticulados $A_1 = A_2$ indicados en el mismo ejemplo y ninguna de las proyecciones (que son funciones suryectivas) de S sobre los ejes son isomorfismos. Por lo tanto R' es subdirectamente reducible.

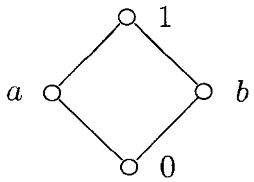
Veremos mas adelante que el único $(0,1)$-reticulado distributivo subdirectamente irreducible es el reticulado $\mathbf{B} = \{0,1\}$. Por tal motivo tiene especial interés considerar los $(0,1)$-subreticulados de productos cartesianos $P = \prod_{i\in I} B_i$ donde $B_i = \mathbf{B}$ para todo $i \in I$.

4 ALGEBRAS DE BOOLE

4.1 Definición, ejemplos.

Se denomina **álgebra de Boole** a todo reticulado distributivo con primer y último elemento, en el cual todo elemento tiene complemento booleano.

Ejemplo 4.1.1 *1) Consideremos el reticulado distributivo cuyo diagrama se indica a continuación:*



entonces $-0 = 1,\ -a = b,\ -b = a,\ -1 = 0.$

2) Sea E *un conjunto no vacío y* $A = \mathcal{P}(E)$. *Sabemos que* $(A, \cap, \cup, \emptyset, E)$ *es un reticulado distributivo con primer y último elemento. Además si* $X \subseteq E$ *entonces* $X \cup (E \setminus X) = E$ *y* $X \cap (E \setminus X) = \emptyset$, *luego* A *es un álgebra de Boole.*

Podemos definir un álgebra de Boole del siguiente modo:

Definición 4.1.1 *Un sistema* $(A, \wedge, \vee, -, 0, 1)$ *formado por un conjunto no vacío* A, *dos operaciones binarias* $\wedge$, $\vee$ *definidas sobre* A, *una operación unaria* $-$ *definida sobre* A *y dos elementos* $0, 1 \in A$ *se dice un álgebra de Boole si se verifican los siguientes axiomas, cualesquiera que sean los elementos* $x, y, z \in A$:

I1)	$x \wedge (y \wedge z) = (x \wedge y) \wedge z$	*S1)*	$x \vee (y \vee z) = (x \vee y) \vee z$
I2)	$x \wedge y = y \wedge x$	*S2)*	$x \vee y = y \vee x$,
I3)	$x \wedge x = x$	*S3)*	$x \vee x = x$
I4)	$x \wedge (x \vee y) = x$	*S4)*	$x \vee (x \wedge y) = x$
D1)	$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$	*D2)*	$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$
I5)	$0 \wedge x = 0$	*S5)*	$0 \vee x = x$
I6)	$1 \wedge x = x$	*S6)*	$1 \vee x = 1$
I7)	$x \wedge -x = 0$	*S7)*	$x \vee -x = 1$

De I1), I2), I3), I4), S1), S2), S3), S4) y D1) resulta que A es un reticulado distributivo. Por I5) e I6) resulta que tiene primer y último elemento. Por I7) y S7) cada elemento tiene complemento.
Es claro que en la definición anterior *sobran* condiciones, pero es habitual encontrar esta definición en la literatura existente.
Vimos anteriormente que si R es un reticulado entonces 1) Todo átomo de R es un elemento irreducible, 2) Todo elemento primo de R es un elemento irreducible, y que si R es distributivo 3) Todo elemento irreducible de R es primo.
Por lo indicado en el Lema 3.4.9 tenemos:

Lema 4.1.1 *Si* A *es un álgebra de Boole y* p *es un elemento primo de* A *entonces* p *es un átomo de* A.

Tenemos así que en las álgebras de Boole las nociones de elemento irreducible, primo y átomo son equivalentes.

Si B es un álgebra de Boole finita, no trivial vamos a notar con $\mathcal{A}(B)$ el conjunto de todos los átomos de B. Por un resultado indicado en el párrafo 3, tenemos que:

$$1 = \bigvee\{a : a \in \mathcal{A}(B)\},$$

ya que $\mathcal{A}(B) = \Pi(B)$, y el supremo de todos los elementos primos es igual a 1.
Es claro que $B = \{0\}$ es un álgebra de Boole, pero ella no tiene átomos. Luego si B es un álgebra de Boole no trivial sin átomos entonces ella debe ser infinita, pués si fuese finita ella tendría elementos primos, luego átomos. Para ver ejemplos de álgebras de Boole sin átomos recomendamos consultar: [48], pag. 90 y [10], pero para entender estos ejemplos hay que tener mas conocimientos sobre las álgebras de Boole.

De acuerdo con el resultado indicado en el Lema 3.4.11 tenemos que:

Lema 4.1.2 *Si R es un reticulado distributivo, finito no trivial, en el cual todo elemento primo es átomo, entonces R es un álgebra de Boole.*

Definición 4.1.2 *Sean A y A' álgebras de Boole. A toda función $h : A \to A'$ tal que:*

H0) $h(0) = 0$,

H1) $h(1) = 1$,

H2) $h(a \wedge b) = h(a) \wedge h(b)$,

H3) $h(a \vee b) = h(a) \vee h(b)$,

H4) $h(-a) = -h(a)$,

cualesquiera que sean $a, b \in A$, se denomina **homomorfismo** *(booleano) de A en A'. Si h es suryectiva, se denomina* **epimorfismo** *(booleano) y si h es biyectiva se denomina* **isomorfismo** *(booleano).*

Observemos que de H0) - H3) resulta H(4). En efecto, $0 = h(0) = h(x \wedge -x) = h(x) \wedge h(-x)$ y $1 = h(1) = h(x \vee -x) = h(x) \vee h(-x)$, luego $h(-x) = -h(x)$. Tambien de H2) y H4) resulta H3). En efecto, $h(x \vee y) = h(-(-x \wedge -y)) = -h(-x \wedge -y) = -(h(-x) \wedge h(-y)) = -h(-x) \vee -h(-y) = h(x) \vee h(y)$.

Lema 4.1.3 *Si h es un isomorfismo de orden de un álgebra de Boole A en un álgebra de Boole A', entonces h es un isomorfismo booleano.*

Dem. Como h es un isomorfismo de orden, sabemos que h es un isomorfismo de reticulado. Además, como $0 \leq x$ para todo $x \in A$, resulta por ser h isótona que $h(0) \leq h(x)$, para todo $x \in A$, y como h es suryectiva tenemos que $h(0) = 0$. En forma análoga de $x \leq 1$, para todo $x \in A$, se deduce que $h(1) = 1$. Luego, h es un isomorfismo booleano. ■

Si A es un álgebra de Boole finita, no trivial en particular A es un reticulado distributivo finito no trivial. Sea $\Pi = \Pi(A)$ el conjunto de todos los elementos primos (átomos) de A.

Por un resultado anterior sabemos que si definimos $\varphi(a) = \{p \in \Pi : p \leq a\}$ entonces φ es un isomorfismo (de reticulado) de A sobre $\mathcal{A} = \{\varphi(a) : a \in A\}$ que verifica $\varphi(0) = \emptyset$ y $\varphi(1) = \Pi$. Además, $\mathcal{A} \subseteq \mathcal{P}(\Pi)$. Vamos a probar que en este caso φ es suryectiva esto es $\varphi(A) = \mathcal{P}(\Pi)$. Sea $X \in \mathcal{P}(\Pi)$, esto es $X \subseteq \Pi$. Si $X = \emptyset$ entonces $\varphi(0) = \emptyset$. Si $X \neq \emptyset$, como Π es finito $X = \{a_1, a_2, \ldots, a_t\}$. Sea $a = \bigvee_{i=1}^{t} a_i$. Veamos que $\varphi(a) = X$. En efecto como $a_i \leq \bigvee_{i=1}^{t} a_i = a$, y $a_i \in \Pi$ entonces $a_i \in \varphi(a)$, para $1 \leq i \leq t$ y en consecuencia $X = \bigcup_{i=1}^{t} \{a_i\} \subseteq \varphi(a)$. Recíprocamente, sea $p \in \varphi(a)$, esto es $p \leq a = \bigvee_{i=1}^{t} a_i$, entonces como p es primo resulta que existe un índice i tal que $p \leq a_i$. Como $0 < p \leq a_i$ y a_i es un átomo entonces $p = a_i$ y en consecuencia $p \in X$.
Tenemos asi que $\varphi : A \to \mathcal{P}(\Pi)$ es una función suryectiva que verifica H0) - H3), y por lo tanto φ es un isomorfismo booleano.

Acabamos así de probar:

Lema 4.1.4 *Toda álgebra de Boole, finita no trivial, A es isomorfa al conjunto de todas las partes del conjunto $\Pi(A)$ de sus átomos.*

Por lo tanto, si A tiene t átomos, A tiene 2^t elementos. Observemos que si A no tiene átomos, esto es $A = \{0\}$ entonces $A \cong \{\emptyset\}$, y su número de elementos es $2^0 = 1$.

Definición 4.1.3 *Sea E un conjunto, no vacío. Una parte, no vacía $\mathcal{A}$ de $\mathcal{P}(E)$ se denomina un* **cuerpo de conjuntos** *si verifica:*

C1) Si $X, Y \in \mathcal{A}$ entonces $X \cap Y \in \mathcal{A}$

C2) Si $X \in \mathcal{A}$ entonces $E \setminus X \in \mathcal{A}$.

Observemos que si $\mathcal{A}$ es un cuerpo de conjuntos entonces se verifica:
Si $X, Y \in \mathcal{A}$ entonces $X \cup Y \in \mathcal{A}$, y $\emptyset, E \in \mathcal{A}$.
Es claro que $\mathcal{A} = \{\emptyset, E\}$ y $\mathcal{A} = \{\emptyset, X, E \setminus X, E\}$ donde $\emptyset \subset X \subset E$ son cuerpos de conjuntos.
Vamos a probar que si E es un conjunto infinito y $\mathcal{A}$ está formado por las partes finitas de E y los complementarios de las partes finitas de E, entonces $\mathcal{A}$ es un cuerpo de conjuntos, y que además $\mathcal{A} \neq \mathcal{P}(E)$.
En efecto sean $X, Y \in \mathcal{A}$, entonces tenemos las siguientes posibilidades: (1) X e Y son partes finitas de E, (2) $X = E \setminus X_1$, $Y = E \setminus Y_1$, donde X_1, Y_1 son partes finitas de E, (3) X es una parte finita de E e $Y = E \setminus Y_1$, donde Y_1 es una parte finita de E. En los casos (1) y (3) tenemos que como $X \cap Y \subseteq X$ y X es finita entonces $X \cap Y$ es una parte finita de E. En el caso (2) $X \cap Y = (E \setminus X_1) \cap (E \setminus Y_1) = E \setminus (X_1 \cup Y_1)$ y como $X_1 \cup Y_1$ es una parte finita de E, tenemos que $X \cap Y \in \mathcal{A}$.
Si $X \in \mathcal{A}$ y X es una parte finita entonces $E \setminus X$ es complementario de una parte finita y si X es complementario de una parte finita su complemento es un conjunto finito. Luego, $\mathcal{A}$ es un cuerpo de conjuntos. Como E es infinito entonces $E = E_1 \cup E_2$ y $\emptyset = E_1 \cap E_2$ donde E_1 y E_2 son infinitos, luego $E_1 = E \setminus E_2$ y $E_1 \notin \mathcal{A}$.

4.2 Algebras de Boole atómicas

Dijimos que existen álgebras de Boole no triviales que no contienen átomos y que tales álgebras son infinitas.
Un álgebra de Boole B se dice **atómica** si dado $x \in B$, $x \neq 0$ existe un átomo a tal que $a \leq x$. Obviamente las álgebras de Boole finitas, no triviales, son atómicas.

Lema 4.2.1 *En un álgebra de Boole* $z \leq w \iff z \wedge -w = 0$.

Dem. $\Longrightarrow$) De $z \leq w$ resulta que $z \wedge -w \leq w \wedge -w = 0$.
$\Longleftarrow$) De $z \wedge -w = 0$ resulta $(z \wedge -w) \vee w = 0 \vee w = w$, esto es $w = (z \vee w) \wedge (-w \vee w) = (z \vee w) \wedge 1 = z \vee w$, esto es $z \leq w$. ∎

Teorema 4.2.1 *Toda álgebra de Boole atómica B es isomorfa a un cuerpo de conjuntos, del conjunto E de todos los átomos del álgebra B* (A. Tarski).

Dem. Dado $b \in B$, pongamos $\varphi(b) = \{a \in E : a \leq b\}$, luego $\varphi(b) \subseteq E$, y por lo tanto, $\mathcal{A} = \{\varphi(b) : b \in B\} \subseteq \mathcal{P}(E)$. En forma análoga a la indicada en el Teorema de Birkhoff se prueba que:

$$\varphi(x \wedge y) = \varphi(x) \cap \varphi(y), \quad \varphi(x \vee y) = \varphi(x) \cup \varphi(y), \quad \varphi(0) = \emptyset, \quad \varphi(1) = E,$$

dado que todo átomo es un elemento primo. Para demostrar que φ es inyectiva, no podemos hacer la misma demostración que en el teorema de Birkhoff, pues en ella utilizamos el hecho de que todo elemento diferente del primer elemento es supremo de los primos que lo preceden.
Supongamos que $x \neq y$. Luego (1) $x \not\leq y$ ó (2) $y \not\leq x$. Si ocurre (1) entonces por el Lema precedente $x \wedge -y \neq 0$, luego como B es atómica existe un átomo a tal que $a \leq x \wedge -y$ y como $x \wedge -y \leq x$ tenemos que $a \in \varphi(x)$. Como $x \wedge -y \leq -y$, resulta que $a \leq -y$ y por lo tanto $a \in \varphi(-y) = E \setminus \varphi(y)$, luego $a \notin \varphi(y)$. En consecuencia $\varphi(x) \neq \varphi(y)$. Por lo tanto $\mathcal{A}$ es un cuerpo de conjuntos isomorfo a B. ∎

En el caso en que B es finita, no trivial, vimos que $\varphi(B) = \mathcal{P}(E)$, donde E es el conjunto de todos los átomos de B, pero este resultado es mas general pues si B es finita no trivial, B es atómica.

4.3 Anillos booleanos

Sea $(A, +, ., 0)$ un anillo, no necesariamente con unidad ni conmutativo. Un anillo se dice **booleano** si:

$$\text{(B)} \quad x.x = x \ \text{ para todo } x \in A.$$

Lema 4.3.1 *Todo anillo booleano A es conmutativo, y se verifica $x + x = 0$, cualquiera que sea $x \in A$, (esto es el simétrico de x es el propio elemento x.)*

Dem. $x+y =$ (*por hip.*) $= (x+y).(x+y) = (x+y).x + (x+y).y = x.x + y.x + x.y + y.y =$ (*por hip*) $= x + y.x + x.y + y$ Luego (i) $y.x + x.y = 0$ En particular si $x = y$ tenemos que $x.x + x.x = 0$ y como A es booleano (ii) $x + x = 0$.
De (i) deducimos $y.x + y.x + x.y = y.x + 0 = y.x$ y por (ii) $x.y = y.x$. ∎

Si B es un anillo booleano con unidad, 1 entonces se verifican:

$$\text{(i)}\ x.x = x,\quad \text{(ii)}\ x + x = 0,\quad \text{(iii)}\ x.y = y.x\quad \text{(iv)}\ 1.x = x.$$

Definamos sobre B la siguiente relación binaria:

$$x \leq y \iff x = x.y$$

Veamos que es una relación de orden:
O1) Como $x = x.x$ entonces $x \leq x$. O2) Supongamos que $x \leq y$ e $y \leq x$ esto es $x = x.y$ e $y = y.x$ luego como el anillo es conmutativo $x = y$. O3) Supongamos que $x \leq y$ e $y \leq z$ esto es $x = x.y$ e $y = y.z$ luego $x.z = (x.y).z = x.(y.z) = x.y = x$ esto es $x \leq z$.
Además como $x = x.1$ tenemos que $x \leq 1$ para todo $x \in B$, y como $0.x = (x + x).x = x.x + x.x = x + x = 0$ resulta que $0 \leq x$ para todo $x \in B$.
Por lo tanto B es un conjunto ordenado con primer elemento 0 y último elemento 1. Vamos a demostrar que B es un reticulado inferior. Mas precisamente vamos a demostar que el ínfimo de 2 elementos $x, y \in B$ es el elemento $x.y$. En efecto:

I1) $\underline{x.y \leq x,\ \ x.y \leq y.}$
Como $(x.y).x = (y.x).x = y.(x.x) = y.x = x.y$ entonces $x.y \leq x$. Análogamente se prueba que $x.y \leq y$.

I2) Sea $z \in B$ tal que $z \leq x$ y $z \leq y$ y probemos que $z \leq x.y$
Por hipótesis $z = z.x$ y $z = z.y$ entonces $z.(x.y) = (z.x).y = z.y = z$ esto es $z \leq x.y$.

Vamos a demostar ahora que B es un reticulado superior. Para ello vamos a probar que el elemento $s = x + y - x.y$ es el supremo de x e y, y dado que el simétrico de a es el propio elemento a entonces $s = x + y + x.y$

S1) $\underline{x \leq s,\ \ y \leq s.}$
$x.s = x.(x + y + x.y) = x.x + x.y + x.y = x + 0 = x$, y por lo tanto $x \leq s$. La otra condición se prueba en forma análoga.

S2) Sea $z \in B$ tal que $x \leq z$ e $y \leq z$ y probemos que $s = x + y + x.y \leq z$
$s.z = (x+y+x.y).z = x.z+y.z+x.(y.z) = \text{(por hip.)} = x+y+x.(y.z) = \text{(por hip.)} = x + y + x.y = s$.
Acabamos así de probar que B es un reticulado con primer (0) y último (1) elemento, donde:

$$x \wedge y = x.y \qquad \text{y} \qquad x \vee y = x + y + x.y.$$

<u>B es un reticulado distributivo</u>.
$x \wedge (y \vee z) = x.(y \vee z) = x.(y + z + y.z) = x.y + x.z + x.(y.z)$, y $(x \wedge y) \vee (x \wedge z) = (x.y) \vee (x.z) = x.y + x.z + (x.y).(x.z) = x.y + x.z + (x.x).(y.z) = x.y + x.z + x.(y.z)$.

Definamos ahora la siguiente operación unaria : $x' = 1 - x = 1 + x$. Entonces $x \wedge x' = x.(1 + x) = x + x.x = x + x = 0$ y $x \vee x' = x + (1 + x) + x.(1 + x) = x + 1 + x + x + x.x = x + x + 1 + x + x = 0 + 1 + 0 = 1$.
Por lo tanto B es un reticulado distributivo con primer (0) y último (1) elemento, donde cada elemento tiene un complemento, esto es B es un álgebra de Boole.
Observemos que $\underline{x + y = (x \wedge y') \vee (x' \wedge y)}$. En efecto, $(x \wedge y') \vee (x' \wedge y) = (x.y') \vee (x'.y) =$

$x.y' + x'.y + (x.y').(x'.y) = x.(1+y) + (1+x).y + x.x' + y.y' = x + x.y + y + x.y + 0 + 0 = x + y + x.y + x.y = x + y + 0 = x + y$.
Por lo tanto la operación de suma $(+)$ se puede expresar en función del ínfimo, el supremo y el complemento booleano.

Dada un álgebra de Boole $(B, \wedge, \vee, ', 0, 1)$ definamos sobre B las siguientes operaciones:

$$\begin{cases} x.y = x \wedge y, \\ x + y = (x \wedge y') \vee (x' \wedge y). \end{cases}$$

Vamos a demostrar que $(B, +, .)$ es un anillo booleano con unidad 1 y elemento neutro 0.
Para ello observemos en primer lugar que:
(1) $\underline{x + y + x.y = x \vee y}$. En efecto $(x+y)' = [(x \wedge y') \vee (x' \wedge y)]' = (x' \vee y) \wedge (x \vee y') = (x' \wedge x) \vee (x' \wedge y') \vee (y \wedge x) \vee (y \wedge y') = 0 \vee (x' \wedge y') \vee (y \wedge x) \vee 0 = (x' \wedge y') \vee (y \wedge x)$.
Entonces:

$$x + y + x.y = (\text{por def.}) = [(x+y) \wedge (x.y)'] \vee [(x+y)' \wedge (x.y)] = (\text{por}(1)) =$$
$$[((x \wedge y') \vee (x' \wedge y)) \wedge (x \wedge y)'] \vee [((x' \wedge y') \vee (x \wedge y)) \wedge x \wedge y],$$

y como $(x' \wedge y') \vee (x \wedge y) \geq x \wedge y$ tenemos que

$$x + y + x.y = [((x \wedge y') \vee (x' \wedge y)) \wedge (x \wedge y)'] \vee (x \wedge y) =$$
$$(x \wedge y' \wedge (x' \vee y')) \vee (x' \wedge y \wedge (x' \vee y')) \vee (x \wedge y)$$

y como $y' \leq x' \vee y'$ y $x' \leq x' \vee y'$ tenemos que

$$x + y + x.y = (x \wedge y') \vee (x' \wedge y) \vee (x \wedge y) = [x \wedge (y' \vee y)] \vee (x' \wedge y) =$$
$$(x \wedge 1) \vee (x' \wedge y) = x \vee (x' \wedge y) = (x \vee x') \wedge (x \vee y) = x \vee y.$$

Veamos ahora que se verifican los axiomas de grupo:

G1)
$$x + (y+z) = [x \wedge (y+z)'] \vee [x' \wedge (y+z)] = (\text{por}(1)) =$$
$$[x \wedge ((y' \wedge z') \vee (y \wedge z))] \vee [x' \wedge ((y' \wedge z) \vee (y \wedge z'))] =$$
$$(x \wedge y' \wedge z') \vee (x \wedge y \wedge z) \vee (x' \wedge y' \wedge z) \vee (x' \wedge y \wedge z').$$

Desarrollando $(x+y)+z$ se llega a la misma expresión.

G2) $0 + x = (0 \wedge x') \vee (0' \wedge x) = 0 \vee (1 \wedge x) = 0 \vee x = x$.

G3) $x + x = (x \wedge x') \vee (x' \wedge x) = 0 \vee 0 = 0$.

G4) $x + y = (x \wedge y') \vee (x' \wedge y) = (y \wedge x') \vee (y' \wedge x) = y + x$.

Probemos que se verifican los axiomas de anillo.

A1) $x.(y.z) = (x.y).z$ (es claramente verificada)

A2) $x.(y+z) = x \wedge ((y \wedge z') \vee (y' \wedge z)) = (x \wedge y \wedge z') \vee (x \wedge y' \wedge z)$ y $x.y + x.z = (x \wedge y) + (x \wedge z) = [(x \wedge y) \wedge (x \wedge z)'] \vee [(x \wedge y)' \wedge (x \wedge z)] = (x \wedge y \wedge (x' \vee z')) \vee ((x' \vee y') \wedge (x \wedge z)) = (x \wedge y \wedge x') \vee (x \wedge y \wedge z') \vee (x' \wedge x \wedge z) \vee (y' \wedge x \wedge z) = 0 \vee (x \wedge y \wedge z') \vee 0 \vee (y' \wedge x \wedge z) = (x \wedge y \wedge z') \vee (y' \wedge x \wedge z)$.

Como $x.y = x \wedge y = y \wedge x = y.x$ entonces también se verifica la ley distributiva a derecha esto es:

A3) $(x + y).z = x.z + y.z$.

A4) $x.1 = x \wedge 1 = x$.

Además B es un anillo booleano ya que $x.x = x \wedge x = x$.
Observemos que: $x + 1 = (x \wedge 1') \vee (x' \wedge 1) = 0 \vee x' = x'$, y que si en un anillo booleano B definimos $x \leq y \iff x.y = y$, entonces B es un conjunto ordenado y $x \vee y = x.y$, $x \wedge y = x + y + x.y$, 0 es el último elemento de B y 1 es el primer elemento de B. Por lo tanto se obtiene un orden dual del indicado precedentemente.

4.4 Subálgebras booleanas

Sea B un álgebra de Boole, una parte, no vacía, S de B se dice una **subálgebra (booleana)** de B si:

S1) Si $a, b \in S$ entonces $a \wedge b \in S$.

S2) Si $a \in S$ entonces $-a \in S$.

Es claro que si S es una subálgebra, entonces

S3) Si $a, b \in S$ entonces $a \vee b \in S$.

S4) $0, 1 \in S$.

Por lo tanto, si S es una subálgebra de B tenemos:

$$\{0, 1\} \subseteq S \subseteq B.$$

Es claro que la intersección de subálgebras de B es una subálgebra de B. La noción de subálgebra generada por una parte G de B, que notaremos $SB(G)$, se define en la forma habitual y se prueba que $SB(G)$ es la menor subálgebra de B que contiene a G. Es claro que $SB(\emptyset) = \{0, 1\}$. Si $SB(G) = B$, se dice que G es **un conjunto de generadores de** B.
Si $G \subseteq B$, notaremos con $\mathcal{PF}(G)$ la familia de todas las partes finitas de G, entonces:

Lema 4.4.1 $SB(G) = \bigcup\{SB(F) : F \in \mathcal{PF}(G)\}$.

Dem. Sea $X = \bigcup\{SB(F) : F \in \mathcal{PF}(G)\}$. Si $F \subseteq G$ como $G \subseteq SB(G)$ entonces $F \subseteq SB(G)$ y por lo tanto $SB(F) \subseteq SB(G)$ para todo subconjunto de G , en particular para todo $F \in \mathcal{PF}(G)$, luego: (i) $X \subseteq SB(G)$. Probemos que (ii) $SB(G) \subseteq X$. Para ello probaremos que (iia) $G \subseteq X$ e (iib) X es una subálgebra de B.
(iia) Sea $g \in G$, luego $\{g\} \subseteq SB(\{g\}) \subseteq X$, y por lo tanto $G = \bigcup_{g \in G} \{g\} \subseteq X$.
(iib) Como $0, 1 \in SB(F)$ cualquiera que sea $F \in \mathcal{PF}(G)$, entonces $0, 1 \in X$. Sean $x, y \in X$ entonces $x \in SB(F_1)$, $y \in SB(F_2)$ donde $F_1, F_2 \in \mathcal{PF}(G)$, por lo tanto $F_1 \cup F_2 \in \mathcal{PF}(G)$. De $F_1 \subseteq F_1 \cup F_2$ y $F_2 \subseteq F_1 \cup F_2$ resulta que $SB(F_1) \subseteq SB(F_1 \cup F_2)$ y $SB(F_2) \subseteq SB(F_1 \cup F_2)$, luego $x, y \in SB(F_1 \cup F_2)$ y por lo tanto $x \wedge y, x \vee y \in SB(F_1 \cup F_2) \subseteq X$. Es claro que si $x \in X$ entonces $-x \in X$. ■

Vamos a ver como se determina $SB(G)$ en el caso en que G es un conjunto finito, no vacío, de un álgebra de Boole B.
Recordemos que si $x, y \in B$ y definimos $x + y = (-x \wedge y) \vee (x \wedge -y)$, entonces $x + 0 = x$ y $x + 1 = -x$.
Sea $\{A_i\}_{i\in I}$ una familia de álgebras de Boole y $P = \prod_{i\in I} A_i$ el producto cartesiano de la familia de conjuntos $\{A_i\}_{i\in I}$, esto es conjunto, el de todas las funciones $x : I \rightarrow \bigcup_{i\in I} A_i$ tales que $x(i) = x_i \in A_i$ para cada $i \in I$. Notaremos con $x = (x_i)_{i\in I}$ ó $x = (x_i)$ a los elementos de P. Sean $a = (a_i)_{i\in I}$, $b = (b_i)_{i\in I} \in P$. Definamos sobre P las siguientes operaciones:

$$a \wedge b = (a_i) \wedge (b_i) = (a_i \wedge b_i), \quad a \vee b = (a_i) \vee (b_i) = (a_i \vee b_i), \quad -a = -(a_i) = (-a_i)$$

Sean $\mathbf{0} = (0_i)$ y $\mathbf{1} = (1_i)$, donde $0_i, 1_i$ representan el primer y último elemento de A_i, para $i \in I$. Entonces es claro que $(P, \wedge, \vee, -, \mathbf{0}, \mathbf{1})$ es un álgebra de Boole. P se denomina el **producto cartesiano** o **producto directo** de la familia de álgebras de Boole $\{A_i\}_{i\in I}$.
En el caso particular en que $A_i = A$ para todo $i \in I$, P es simplemente el conjunto de todas las funciones definidas sobre I y que toman sus valores en A. En este caso se suele notar $P = A^I$, y si $f, g \in A^I$, entonces de acuerdo a la definición anterior tenemos que $(f \wedge g)(x) = (f(x)) \wedge (g(x)) = (f(x) \wedge g(x))$, por lo tanto $(f \wedge g)(x) = f(x) \wedge g(x)$. Análogamente $(f \vee g)(x) = f(x) \vee g(x)$, $(-f)(x) = -(f(x))$, $\mathbf{1}(x) = 1$, y $\mathbf{0}(x) = 0$.

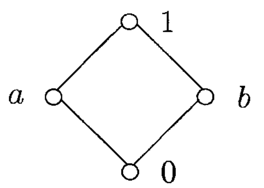
Dada un álgebra de Boole B sea $\mathbf{P}(B, n) = \{p = (p_1, p_2, \ldots, p_n) : p_i \in \{0, 1\} \subseteq B, 1 \leq i \leq n\}$, esto es, el conjunto $\mathbf{P}(B, n)$ está formado por todas las n-uplas de elementos $0, 1 \in B$. $\mathbf{P}(B, n)$ es el producto cartesiano de n álgebras de Boole iguales a $\{0, 1\} \subseteq B$, luego es un álgebra de Boole con n átomos, que son precisamente las n-uplas que tienen una única coordenada igual a 1 y las restantes iguales a 0.

Si $G = \{g_1, g_2, \ldots, g_n\} \subseteq B$ y $p \in \mathbf{P}(B, n)$, notaremos con $m_p(G)$ o mas sencillamente m_p al elemento:

$$\bigwedge_{i=1}^{n} (g_i + p_i).$$

Estos elementos se denominan **combinaciones algebraicas elementales** de G. Observemos que de acuerdo con la definición precedente $g_i + p_i = g_i$ ó $g_i + p_i = -g_i$.
Sea $m(G) = \{m_p : p \in \mathbf{P}(B, n)\}$, como $N[\mathbf{P}(B, n)] = 2^n$ entonces $N[m(G)] \leq 2^n$.

Ejemplo 4.4.1 *Consideremos el álgebra de Boole, cuyo diagrama se indica a continuación:*



y sea $G = \{a, b\}$. *Determinemos* $m(G)$. *Como* $\mathbf{P}(B, 2) = \{(0,0), (0,1), (1,0), (1,1)\}$ *entonces:* $m_{(0,0)} = (a+0) \wedge (b+0) = a \wedge b = 0$, $m_{(0,1)} = (a+0) \wedge (b+1) = a \wedge -b = a \wedge a = a$, $m_{(1,0)} = (a+1) \wedge (b+0) = -a \wedge b = b \wedge b = b$, $m_{(1,1)} = (a+1) \wedge (b+1) = -a \wedge -b = b \wedge a = 0$. *Observemos que la primera y la cuarta combinación algebraica elemental se forman de modo diferente, pero el resultado es el mismo. Acabamos así de ver que* $m(G) = \{0, a, b\}$.

Lema 4.4.2 *Si B es un álgebra de Boole, $G = \{g_1, g_2, \dots, g_n\}$ entonces:*

1) Si $p, q \in \mathbf{P}(B,n)$ y $p \neq q$ entonces $m_p \wedge m_q = 0$.

2) $\bigvee\{m_p : p \in \mathbf{P}(B,n)\} = 1$.

3) Si $p, q \in \mathbf{P}(B,n)$, $p \neq q$ y $m_p \leq m_q$ entonces $m_p = 0$.

4) $g_i = \bigvee\{m_p : p \in \mathbf{P}(B,n),\ p_i = 0\}$, $1 \leq i \leq n$.

Dem.

1) Como $p \neq q$ entonces existe por lo menos una coordenada $i, 1 \leq i \leq n$, tal que $p_i \neq q_i$, y como $p_i, q_i \in \{0,1\} \subseteq B$, entonces "$p_i = 0$ y $q_i = 1$" ó "$p_i = 1$ y $q_i = 0$". En el primero de los casos tenemos: $m_p \wedge m_q = (\cdots \wedge g_i \wedge \cdots) \wedge (\cdots \wedge -g_i \wedge \cdots) = 0$. Análogamente en el segundo caso.

2) Por inducción sobre n. Si $n = 1$, entonces : $m(G) = \{m_0 = g_1 + 0, m_1 = g_1 + 1\} = \{g_1, -g_1\}$, luego $\bigvee\{m_p : p \in \mathbf{P}(B,1)\} = g_1 \vee -g_1 = 1$.
Supongamos que la propiedad enunciada vale para todo conjunto G con $(n-1)$ elementos, y probemos que vale para todo conjunto G con n elementos. Observemos que $\bigvee\{m_p : p \in \mathbf{P}(B,n)\} =$

$$\bigvee\{m_p : p \in \mathbf{P}(B,n),\ p_n = 0\} \ \vee \ \bigvee\{m_p : p \in \mathbf{P}(B,n),\ p_n = 1\} = s_1 \vee s_2.$$

Como los elementos que aparecen en el primer supremo verifican $p_n = 0$, entonces $m_p = \bigwedge_{i=1}^{n-1}(g_i + p_i) \ \wedge \ (g_n + 0) = m_{p'} \wedge g_n$, donde $p' = (p_1, p_2, \dots, p_{n-1}) \in \mathbf{P}(B, n-1)$.
Además $p = (p_1, p_2, \dots, p_n) \in \mathbf{P}(B,n) \iff p' = (p_1, p_2, \dots, p_{n-1}) \in \mathbf{P}(B, n-1)$ y $p_n \in \{0,1\}$, luego $s_1 = g_n \wedge \bigvee\{m_{p'} : p' \in \mathbf{P}(B, n-1)\}$, y por lo tanto teniendo en cuenta la hipótesis de inducción $s_1 = g_n \wedge 1 = g_n$.
Análogamente se prueba que $s_2 = -g_n$, y por lo tanto $s_1 \vee s_2 = 1$.

3) Por hipótesis $m_p = m_p \wedge m_q = [por\ 1)] = 0$.

4) $g_i = g_i \wedge 1 = [por\ 2)] = g_i \wedge \bigvee\{m_p : p \in \mathbf{P}(B,n)\} =$
$(g_i \wedge \bigvee\{m_p : p \in \mathbf{P}(B,n),\ p_i = 0\}) \vee (g_i \wedge \bigvee\{m_p : p \in \mathbf{P}(B,n), p_i = 1\}) =$
$(\bigvee\{g_i \wedge m_p : p \in \mathbf{P}(B,n), p_i = 0\}) \vee (\bigvee\{g_i \wedge m_p : p \in \mathbf{P}(B,n), p_i = 1\})$.
Si $p_i = 0$ entonces $m_p = g_i \ \wedge \ (\bigwedge_{j=1, j=i}^{n} (g_j + p_j))$, luego $g_i \wedge m_p = m_p$ y si $p_i = 1$ entonces $m_p = -g_i \ \wedge \ (\bigwedge_{j=1, j=i}^{n} (g_j + p_j))$, luego $g_i \wedge m_p = 0$. Por lo tanto $g_i = \bigvee\{m_p : p \in \mathbf{P}(B,n),\ p_i = 0\}$.

■

Sea $(R, \wedge, \vee, 0)$ un reticulado con primer elemento 0, $X \subseteq R$, $N[X] = t$, notaremos:

$$S_0(X) = \{0\} \qquad ; \qquad S_1(X) = X,$$

$$S_j(X) = \{\bigvee y : y \in Y, \ \ Y \subseteq X, N[Y] = j\}, \ \ 1 < j \leq t,$$

$$S(X) = \bigcup_{j=0}^{t} S_j(X).$$

Si no ponemos $S_0(X) = \{0\}$ puede ocurrir que $S(m(G)) \neq SB(G)$. En efecto, si consideramos el subconjunto $G = \{a\}$ del álgebra de Boole B indicada precedentemente entonces $m(G) = \{a, b\}$ y $S(m(G)) = \{a, b, 1\}$. Como las únicas subálgebras de B son la propia B y $\{0, 1\}$ entonces $SB(\{a\}) = B$.

Lema 4.4.3 *Si G es un subconjunto finito, con n elementos del álgebra de Boole B, entonces:*

1) $SB(G) = S(m(G))$.

2) $\mathcal{A}(SB(G)) = \{m_p : m_p \in m(G), m_p \neq 0\}$.

Dem.

1) Sea $G = \{g_1, g_2, \ldots, g_n\} \subseteq B$, y $t = N[m(G)] \leq 2^n$.
Probemos que (*) $m(G) \subseteq SB(G)$.
En efecto si $y \in m(G)$, entonces: $y = m_p = \bigwedge_{i=1}^{n} (g_i + p_i)$ donde $g_i + p_i = g_i$ ó $g_i + p_i = -g_i$, para algún $p \in \mathbf{P}(B, n)$. Como $G \subseteq SB(G)$ y $g_i \in G$ entonces $-g_i \in SB(G)$, por lo tanto $m_p \in SB(G)$ cualquiera que sea $p \in \mathbf{P}(B, n)$ luego $y \in SB(G)$.
Dado $y \in S(m(G)) = \bigcup_{j=0}^{t} S_j(m(G))$ si $y \in S_0(m(G)) = \{0\}$ entonces $y = 0 \in SB(G)$. Si $y \in S_1(m(G)) = m(G)$ entonces por (*) $y \in SB(G)$. Si $y \in S_j(m(G))$, con $2 \leq j \leq t$ entonces: $y = m_{p_1} \vee m_{p_2} \vee \ldots \vee m_{p_j}$, donde $p_h \in \mathbf{P}(B, n)$, para $1 \leq h \leq j$ y como por (*) $m_{p_h} \in SB(G)$ para $1 \leq h \leq j$ tenemos que $y \in SB(G)$.
Probemos ahora que $G \subseteq S(m(G))$ y que $S(m(G))$ es una subálgebra del álgebra de Boole B. Sea $g \in G$, luego $g = g_t$, donde $1 \leq t \leq n$. Por el Lema 4.4.2

$$g_t = \bigvee \{m_p : p \in \mathbf{P}(B, n), p_t = 0\}$$

luego $g_t \in S(m(G))$.
$S(m(G))$ es una subálgebra:
(i) $0 \in S(m(G))$. En efecto $\{0\} = S_0(m(G)) \subseteq S(m(G))$.
(ii) Sea $y_1, y_2 \in S(m(G))$. Si alguno de estos elementos pertenece a $S_0(m(G)) = \{0\}$, entonces $y_1 \vee y_2 \in S(m(G))$.
Supongamos que $y_1 \in S_j(m(G))$, $j \geq 1$ e $y_2 \in S_k(m(G))$, $k \geq 1$, luego:
$y_1 \vee y_2 =$

$$\bigvee \{m_p : p \in X_1 \subseteq \mathbf{P}(B, n), \ N[X_1] = j\} \vee \bigvee \{m_p : p \in X_2 \subseteq \mathbf{P}(B, n), \ N[X_2] = k\} =$$

$$\bigvee\{m_p : p \in X_1 \cup X_2 \subseteq \mathbf{P}(B,n),\ N[X_1 \cup X_2] \leq j+k\}$$

por lo tanto $y_1 \vee y_2 \in S(m(G))$.
(iii) Sea $y \in S(m(G))$, si $y \in S_0(m(G)) = \{0\}$ entonces $-y = 1 = \bigvee\{m_p : p \in \mathbf{P}(B,n)\} \in S(m(G))$. Si $y \in S_j(m(G))$, con $j \geq 1$ entonces $y = \bigvee\{m_p : p \in X \subseteq \mathbf{P}(B,n),\ N[X] = j\}$ donde $1 \leq j \leq N[m(G)]$. Si $j = N[m(G)]$ entonces $y = 1$ y por lo tanto $-y = -1 = 0 \in S(m(G))$. Supongamos que $1 \leq j < N[m(G)]$, y sea $x = \bigvee\{m_q : q \in \mathbf{P}(B,n) \setminus X\}$, luego $y \vee x = 1$, e $y \wedge x = y \wedge (\bigvee\{m_q : q \in \mathbf{P}(B,n) \setminus X\}9 = \bigvee\{y \wedge m_q : q \in \mathbf{P}(B,n) \setminus X\}$.
Pero si $q \in \mathbf{P}(B,n) \setminus X$, entonces $y \wedge m_q = \bigvee\{m_p : p \in X \subseteq \mathbf{P}(B,n)\} \wedge m_q = \bigvee\{m_p \wedge m_q : p \in X \subseteq \mathbf{P}(B,n)\}$. Como $q \in \mathbf{P}(B,n) \setminus X$ y $p \in X$ entonces $p \neq q$ luego por lo visto en el Lema 4.4.2, 1) $m_p \wedge m_q = 0$ y en consecuencia $y \wedge m_q = 0$ para todo $q \in \mathbf{P}(B,n) \setminus X$, y por lo tanto $y \wedge x = 0$. Acabamos así de probar que $-y = x$ y como $x \in S(m(G))$ resulta que $-y \in S(m(G))$.

2) En efecto sea $m_p \in m(G) \subseteq S(m(G)) = SB(G)$, $m_p \neq 0$ y supongamos que $0 \leq t \leq m_p$ donde $t \in SB(G)$. De $t \in SB(G)$ resulta que $t = 0$ ó $t \neq 0$, luego en este caso $t \in S_j(m(G))$ con $j \geq 1$, y por lo tanto $t = \bigvee\{m_q : q \in X \subseteq \mathbf{P}(B,n),\ N[X] = j\}$ entonces $m_q \leq t \leq m_p$ para todo $q \in X$. Si $q \neq p$ para todo $q \in X$ entonces por el Lema 4.4.2, 3), resulta que $m_q = 0$ para todo $q \in X$ y por lo tanto $t = 0$, absurdo. Luego $q = p$ para algún $q \in X$, entonces tenemos $m_p \leq t \leq m_p$ y por lo tanto $t = m_p$.
Supongamos ahora que a es un átomo de $SB(G)$ entonces $a \neq 0$ y $a \in SB(G) = S(m(G))$, luego $a \in S_j(m(G))$ con $j \geq 1$, esto es

$$a = \bigvee\{m_p : p \in X \subseteq \mathbf{P}(B,n), N[X] = j\}$$

entonces como a es irreducible tenemos que $a = m_p$ para algún $p \in X$. Observemos que no puede ocurrir que $m_p = 0$ para todo $p \in X$, pues en este caso tendríamos $a = 0$. Contradicción. Observemos aún que p es único, pués si $a = m_p = m_q$ donde $p, q \in X$ y $p \neq q$, $m_p \neq 0$, $m_q \neq 0$, entonces $a = m_p \wedge m_q = 0$ (ver Lema 4.4.2, 1)).

■

Como $N[m(G)] \leq 2^n$ por el Lema precedente, tenemos que $N[\mathcal{A}(SB(G))] \leq 2^n$ y en consecuencia $N[SB(G)] \leq 2^{(2^n)}$.

Lema 4.4.4 *Si B es un álgebra de Boole y $G = \{g_1, g_2, \ldots, g_n\} \subseteq B$ entonces $SB(G) = SB(m(G))$.*

Dem. Como $m(G) = S_1(m(G)) \subseteq \bigcup_{j=0}^{2^n} S_j(m(G)) = S(m(G)) = SB(G)$, entonces $SB(m(G)) \subseteq SB(G)$.
Sea $y \in SB(G) = S(m(G))$ entonces $y \in S_j(m(G))$, para algún j, $0 \leq j \leq 2^n$.
Si $j = 0$, ello equivale a $y = 0$, y por lo tanto $y \in SB(m(G))$.
Si $j = 1$, ello equivale a $y = m_b$, $m_b \in m(G)$. Si $2 \leq j \leq 2^n$, entonces $y = \bigvee\{z : z \in Z,\ Z \subseteq m(G),\ N[Z] = j\}$. Como $m(G) \subseteq SB(m(G))$, entonces en ambos casos $y \in SB(m(G))$. ■

Definición 4.4.1 *Un subconjunto* $G = \{g_1, g_2, \ldots, g_t\}$ *de un álgebra de Boole* B *se dice una partición del elemento* $1 \in B$*, si:*

P1) $g_i \wedge g_j = 0, \;\; i \neq j, \;\; 1 \leq i, j \leq t.$

P2) $\bigvee_{i=1}^{t} g_i = 1.$

(H. Bass, *Finite monadic algebras*, Proc. Amer. Math. Soc. 9 (1958), 258-268)

Observación 4.4.1 *1) Los átomos de un álgebra de Boole finita no trivial* B *forman una partición de* 1.

2) Si $\mathcal{A}(B) = \{a_1, a_2, a_3\}$ *entonces* $\{a_1, a_2 \vee a_3\}$ *es una partición de* 1 *y* $\{0, a_1, a_2 \vee a_3\}$ *también es una partición de* 1*.*
Si $\mathcal{A}(B) = \{a_1, a_2, a_3, a_4\}$ *entonces* $\{a_1 \vee a_2, a_3 \vee a_4\}$ *es una partición de* 1 *y ninguno de sus elementos es un átomo.*

Si G es un subconjunto finito no vacío de B, entonces de acuerdo con los Lemas 4.4.2, 4.4.3 el conjunto $m(G)$ forma una partición de 1, que contiene a los átomos de $SB(G)$.
Si $G = \{g_1, g_2, \ldots, g_t\}$ es una partición de 1, sea $G_0 = \{g \in G : g \neq 0\}$. Si $g_i, g_j \in G_0, \;\; i \neq j$ entonces $g_i \neq g_j$. En efecto, si $g_i = g_j$ entonces $g_i = g_i \wedge g_j = 0$. Absurdo. Por lo tanto G_0 es una partición de 1, cuyos elementos son diferentes dos a dos.

Si G es una partición de 1 tal que $\mathcal{A}(B) \subset G$ entonces $G \setminus \mathcal{A}(B) = \{0\}$. En efecto, por hipótesis existe $x \in G \setminus \mathcal{A}(B)$. Si $x \neq 0$ entonces $x = \bigvee\{a : a \in \mathcal{A}(x)\}$ entonces cualquiera que sea $a \in \mathcal{A}(x)$ tenemos $a \wedge x = a \neq 0$, pero $a, x \in G$, G es una partición y $a \neq x$, dado que $x \in G \setminus \mathcal{A}(B)$, entonces $a = a \wedge x = 0$, absurdo.

Lema 4.4.5 *Si* B *es un álgebra de Boole finita, no trivial, y* $G = \{g_1, g_2, \ldots, g_n\}$ *es una partición de* 1, *entonces* $G_0 = \mathcal{A}(SB(G))$.

Dem. Observemos en primer lugar que $G_0 \neq \emptyset$, pues si $G_0 = \emptyset$, entonces $G = \{0\}$ y este conjunto obviamente no es una partición de 1.
Sabemos que $\mathcal{A}(SB(G)) = \{m_p : m_p \in m(G), m_p \neq 0\}$. Sea $g \in G_0$, esto es $g \neq 0$ y $g = g_j, \;\; 1 \leq j \leq n$. Como $g_i \wedge g_j = 0, \; \forall\, i \neq j, \; 1 \leq i \leq n$, lo que es equivalente a decir que $g_j \leq -g_i, \; \forall i \neq j, \; 1 \leq i \leq n$, entonces $g_j \leq \bigwedge_{i=1}^{n}\{-g_i : i \neq j\}$, luego

$$g_j = g_j \wedge \bigwedge_{i=1}^{n}\{-g_i : i \neq j\} = \bigwedge_{i=1}^{n}(g_i + p_i)$$

donde $p_j = 0$ y $p_i = 1 \; \forall\, i \neq j$, en consecuencia $g_j = m_p$ con $p = (p_1, p_2, \ldots, p_n)$ verificando las condiciones anteriores. Acabamos así de probar que $G_0 \subseteq \mathcal{A}(SB(G))$.
Sea $m_p \in \mathcal{A}(SB(G))$, luego $m_p \neq 0$ y $m_p = \bigwedge_{i=1}^{n} (g_i + p_i)$. Si $p_i = p_j = 0$ con $i \neq j$ entonces $m_p = g_i \wedge g_j \wedge \bigwedge_{h=1}^{n} \{g_h + p_h : h \neq i, h \neq j\} = 0$. Absurdo.
Por lo tanto, si $m_p \neq 0$ no puede existir mas de un $p_i = 0$. Luego tenemos los siguientes casos:

1) $p = (1, 1, \ldots, 1)$

2) $p = (p_1, p_2, \ldots, p_n)$, verifica $p_{i_0} = 0$ donde $1 \leq i_0 \leq n$ y $p_i = 1$, $\forall i$, $1 \leq i \leq n$, $i \neq i_0$.

En el caso 1) tenemos $m_p = \bigwedge\limits_{i=1}^{n} -g_i = -\bigvee\limits_{i=1}^{n} g_i = -1 = 0$. Absurdo. Por lo tanto, se debe verificar el caso 2), y tendremos:

$$m_p = -g_1 \wedge -g_2 \wedge \ldots \wedge g_{i_0} \wedge \ldots \wedge -g_n$$

donde $g_{i_0} \neq 0$ pues si $g_{i_0} = 0$ entonces $m_p = 0$. Absurdo. Como $g_{i_0} \wedge g_j = 0$, $\forall\, j \neq i_0$ entonces $g_{i_0} \leq -g_j$ $\forall\, j \neq i_0$ y en consecuencia

$$-g_1 \wedge -g_2 \wedge \ldots \wedge g_{i_0} \wedge \ldots \wedge -g_n = g_{i_0}$$

esto es $m_p = g_{i_0}$, con $g_{i_0} \neq 0$, y por lo tanto $m_p \in G_0$. ■

Observación 4.4.2 *1) Si G es un subconjunto finito de un álgebra de Boole B, $G_0 = \{g \in G : g \neq 0\}$ entonces $SB(G) = SB(G_0)$. Por definición $G_0 \subseteq G$. Si $G = G_0$ es obvio. Si $G_0 \subset G$ entonces como $G \subseteq SB(G)$ tenemos $G_0 \subseteq SB(G)$ y en consecuencia $SB(G_0) \subseteq SB(G)$. Por otro lado como $G_0 \subseteq SB(G_0)$ y $\{0\} \subseteq SB(G_0)$ entonces $G_0 \cup \{0\} = G \subseteq SB(G_0)$, y por lo tanto $SB(G) \subseteq SB(G_0)$.*

2) Sabemos que $G \subseteq SB(G$, luego si $g \in G$ entonces $g \in SB(G)$ y por lo tanto $-g \in SB(G)$. Representemos por $-G$ al conjunto $\{-g : g \in G\}$, tenemos entonces que $-G \subseteq SB(G)$, y en consecuencia $G \cup -G \subseteq SB(G)$.
Probar que $SB(G) = s(i(G \cup -G))$. (ver 3.3).

4.5 Relación entre subálgebras y particiones de los átomos

Sea B un álgebra de Boole con n átomos: $\mathcal{A}(B) = \{a_1, a_2, \ldots, a_n\}$ y

$$\mathcal{P} = \{X_1, X_2, \ldots, X_t\}, \quad \text{donde } 1 \leq t \leq n \text{ una partición de } \mathcal{A}(B).$$

Sean $g_i = \bigvee\{x : x \in X_i\}$, $\quad 1 \leq i \leq t$. Veamos que: $G_{\mathcal{P}} = \{g_1, g_2, \ldots, g_t\}$ es una partición de 1, donde $g_i \neq 0$, $\;1 \leq i \leq t$.
En efecto

1) Por la definición de los g_i, cada uno de ellos es supremo de átomos, luego $g_i \neq 0$, para $1 \leq i \leq t$.

2) $\bigvee\limits_{i=1}^{t} g_i = \bigvee\{x : x \in \bigcup\limits_{i=1}^{t} X_i\} = \bigvee\{x : x \in \mathcal{A}(B)\} = 1$.

3) Si $1 \leq i, j \leq t$ son tales que $i \neq j$ entonces

$$g_i \wedge g_j = (\bigvee\{x : x \in X_i\}) \wedge (\bigvee\{y : y \in X_j\}).$$

Como $X_i, X_j \subseteq \mathcal{A}(B)$ y $Xi \cap Xj = \emptyset$ entonces $x \neq y$, $\;\forall\, x \in X_i$, $\forall\, y \in X_j$ y por lo tanto $g_i \wedge g_j = 0$ (ver Lema 3.4.10,(IV)).

Sabemos por el Lema 4.4.5 que la subálgebra $B' = SB(G_{\mathcal{P}})$ de B verifica $\mathcal{A}(B') = G_{\mathcal{P}}$. Pongamos por definición:

$$\Psi(\mathcal{P}) = SB(G_{\mathcal{P}})$$

Tenemos así que a cada partición $\mathcal{P}$ de los átomos de B le hacemos corresponder una subálgebra de B.
Dada una subálgebra S de B, como S es finita, si $t = N[\mathcal{A}(S)]$ entonces $N[S] = 2^t \leq N[B] = 2^n$ luego, $1 \leq N[\mathcal{A}(S)] = t \leq n$.
Sea $\mathcal{A}(S) = \{s_1, s_2, \ldots, s_t\}$ entonces como $s_i \in B$, $\forall i$ tenemos:

$$s_1 = \bigvee_{j=1}^{i_1} \{a_{1j} \leq s_1 : a_{1j} \in \mathcal{A}(B)\}$$

$$s_2 = \bigvee_{j=1}^{i_2} \{a_{2j} \leq s_2 : a_{2j} \in \mathcal{A}(B)\}$$

....

$$s_t = \bigvee_{j=1}^{i_t} \{a_{tj} \leq s_t : a_{tj} \in \mathcal{A}(B)\}$$

Como $s_i \wedge s_j = 0, \ \forall\, i \neq j$ y $\bigvee_{i=1}^{t} s_i = 1$, entonces:

$$X_1 = \{a_{11}, a_{12}, \ldots, a_{1i_1}\}$$

$$X_2 = \{a_{21}, a_{22}, \ldots, a_{2i_2}\}$$

....

$$X_t = \{a_{t1}, a_{t2}, \ldots, a_{ti_t}\}$$

es una partición de $\mathcal{A}(B)$. En efecto:

1) Es claro que $X_i \neq \emptyset, \ \ 1 \leq i \leq t$.

2) $X_h \cap X_k = \emptyset$, si $\ h \neq k, \ \ 1 \leq h, k \leq t$. Si $z \in X_h \cap X_k$, entonces $z = a_{hs} = a_{kr} \leq \bigvee_{j=1}^{i_k} \{a_{kj} : a_{kj} \in \mathcal{A}(B)\} = s_k$, y por lo tanto $a_{hs} = a_{hs} \wedge s_h \leq s_k \wedge s_h = 0$, luego $a_{hs} = 0$. Absurdo.

3) $\bigcup_{i=1}^{t} X_i = \mathcal{A}(B)$. En efecto, es claro que $\bigcup_{i=1}^{t} X_i \subseteq \mathcal{A}(B)$. Sea $a \in \mathcal{A}(B)$, entonces $a \leq 1 = \bigvee_{r=1}^{t} s_r$. Como a es primo entonces $a \leq s_r$ para algún r, $1 \leq r \leq t$ luego:

$$a \leq a_{r1} \vee a_{r2} \vee \ldots \vee a_{ri_r}$$

y como a es primo $a \leq a_{rh}$, con $1 \leq h \leq i_r$. Como ambos elementos son átomos tenemos que $a = a_{rh}$ y en consecuencia $a \in \bigcup_{i=1}^{t} X_i$.

Luego $\mathcal{P} = \{X_1, X_2, \ldots, X_t\}$ es una partición de $\mathcal{A}(B)$ y se verifica que:

$$\Psi(\mathcal{P}) = SB(G_{\mathcal{P}}) = SB(\{s_1, s_2, \ldots, s_t\}) = S.$$

Acabamos así de probar que Ψ es una función suryectiva.
Probemos finalmente que Ψ es inyectiva. Sean $\mathcal{P}_1, \mathcal{P}_2$ dos particiones de $\mathcal{A}(B)$ tales que $\Psi(\mathcal{P}_1) = \Psi(\mathcal{P}_2)$, esto es $S_1 = SB(G_{\mathcal{P}_1}) = SB(G_{\mathcal{P}_2}) = S_2$. Probemos que $\mathcal{P}_1 = \mathcal{P}_2$. Sabemos que si $\mathcal{P}_1 = \{X_1, X_2, \ldots, X_s\}$ y $\mathcal{P}_2 = \{Y_1, Y_2, \ldots, Y_t\}$ son particiones de $\mathcal{A}(B)$ entonces:

$$g_i = \bigvee\{x : x \in X_i\}, \ \ 1 \leq i \leq s, \quad \text{son átomos de } S_1,$$

$$h_i = \bigvee\{y : y \in Y_i\}, \ \ 1 \leq i \leq t, \quad \text{son átomos de } S_2.$$

De $S_1 = S_2$ resulta que $\mathcal{A}(S_1) = \mathcal{A}(S_2)$, luego $\{g_1, g_2, \ldots, g_s\} = \{h_1, h_2, \ldots, h_t\}$, y como $g_i \neq g_j$, $\forall\, i \neq j$, $h_i \neq h_j$, $\forall\, i \neq j$, tenemos que $s = t$.
Reordenemos el conjunto $\mathcal{A}(S_2)$ de forma tal que $g_i = h_i$, para todo i, $1 \leq i \leq s$. Tenemos entonces que:

$$g_i = \bigvee\{x : x \in X_i\} \text{ donde } X_i = \{a_{i1}, a_{i2}, \ldots, a_{ij_i}\}, \text{ y } a_{is} \in \mathcal{A}(B), \ 1 \leq s \leq j_i$$

$$h_i = \bigvee\{y : y \in Y_i\} \text{ donde } Y_i = \{b_{i1}, b_{i2}, \ldots, b_{ik_i}\}, \text{ y } b_{iv} \in \mathcal{A}(B), \ 1 \leq v \leq k_i$$

esto es

$$g_i = a_{i1} \vee a_{i2} \vee \ldots \vee a_{ij_i} = b_{i1} \vee b_{i2} \vee \ldots \vee b_{ik_i} = h_i.$$

Cada una de estas representaciones de $g_i = h_i$ es una *representación irredundante*, ellas están formadas por los primos maximales que preceden a g_i y a h_i respectivamente luego $X_i = Y_i$, $1 \leq i \leq s$, y por lo tanto $\mathcal{P}_1 = \mathcal{P}_2$.

Acabamos así de probar que si B es un álgebra de Boole con n átomos, existen tantas subálgebras de B como particiones tiene el conjunto de los átomos de B.

Observación 4.5.1 *Denotemos con p_i el número de particiones de un conjunto con i elementos y pongamos $p_0 = 1$ entonces :*

$$p_{n+1} = \sum_{i=0}^{n} \binom{n}{i} p_i, \quad n \geq 0.$$

O. Ore, *Theory of equivalence relations,* Duke Math. Journal 9 (1942), 573-627.
Si X es un conjunto con un sólo elemento entonces existe una sola partición de X y $p_{0+1} = \sum_{i=0}^{0} \binom{0}{i} p_i = \binom{0}{0} p_0 = 1.$
Supongamos ahora que la fórmula vale para todo conjunto con un número de elementos $t \leq n$ y probemos que vale para todo conjunto con $n+1$ elementos.
Sea $X = \{x_1, x_2, \ldots, x_n, x_{n+1}\}$, y $\mathcal{P}$ una partición de X. Si Z es un conjunto de la partición que contiene al elemento x_{n+1} entonces Z puede contener desde 1 hasta $n+1$ elementos, esto es $Z = \{x_{n+1}, \ldots\}$. Si Z tiene un solo elemento, esto es si $Z = \{x_{n+1}\}$, existen tantas particiones de este tipo como particiones tiene un conjunto con n elementos. Si Z tiene dos elementos $Z = \{x_{n+1}, x\}$ existen $\binom{n}{1}$ conjuntos con 2 elementos que contienen a x_{n+1}, luego para cada uno de estos conjuntos hay tantas particiones de este

tipo como particiones tiene un conjunto con $n-1$ elementos. En general si Z tiene j elementos $Z = \{x_{n+1}, y_1, y_2, \ldots, y_{j-1}\}$ existen $\binom{n}{j-1}$ subconjuntos de X que contienen a x_{n+1} y j elementos, y por lo tanto para cada uno de estos conjuntos hay tantas particiones de este tipo como particiones tiene un conjunto con $n+1-j = n-(j-1)$ elementos. Tenemos así:

$$p_{n+1} = \binom{n}{0}p_n + \binom{n}{1}p_{n-1} + \ldots + \binom{n}{n}p_0 =$$

$$\sum_{j=0}^{n}\binom{n}{j}p_{n-j} = \sum_{j=0}^{n}\binom{n}{n-j}p_{n-j} = \sum_{i=n}^{0}\binom{n}{i}p_i = \sum_{i=0}^{n}\binom{n}{i}p_i.$$

Luego $p_0 = 1$, $p_1 = 1$, $p_2 = 2$, $p_3 = 5$, $p_4 = 15, \ldots$

Dada una partición $\mathcal{P} = \{C_1, C_2, \ldots, C_t\}$ del conjunto de los átomos de un álgebra de Boole B con n átomos, vimos que los átomos de la subálgebra determinada por la partición son los elementos

$$a_i = \bigvee\{x : x \in C_i\}, \quad 1 \leq i \leq t.$$

Por lo tanto una tal subálgebra tiene 2^t elementos.
Se denomina <u>t-partición</u> de un conjunto A a toda partición de A formada por t subconjuntos de A. Entonces es claro, por la construcción indicada que las subálgebras de B con 2^t elementos provienen de las t-particiones de $\mathcal{A}(B)$.
<u>¿ Cuántas subálgebras con 2^t elementos, $1 \leq t \leq n$, existen?</u>
Para ello vamos a indicar previamente como se determina el número de funciones suryectivas de un conjunto $X = \{1, 2, \ldots, m\}$ con m elementos en un conjunto $Y = \{y_1, y_2, \ldots, y_n\}$ con n elementos. Representemos, como es habitual, por Y^X el conjunto de todas las funciones de X en Y, y por $FS(Y^X)$ el conjunto de todas las funciones suryectivas de X en Y, queremos determinar $N[FS(Y^X)]$. Es claro que si $m < n$ entonces $N[FS(Y^X)] = 0$. Supongamos que $m \geq n$, entonces es claro que si $n = 1$, $N[FS(Y^X)] = 1$, cualquiera que sea $m \geq 1$. Supongamos que $n \geq 2$, entonces es evidente que $N[FS(Y^X)] = n^m - n_0$, donde n_0 indica el número de funciones de X en Y que no son suryectivas. Si $f \in Y^X$ y f no es suryectiva, esto es $f \notin FS(Y^X)$ entonces existe $y \in Y$ tal que $f(x) \neq y$, cualquiera que sea $x \in X$. Sea $F_i = \{f \in Y^X : y_i \notin Im\,(f)\}$, $1 \leq i \leq n$, luego $N[F_i] = (n-1)^m$. Tenemos así una familia $\{F_i : 1 \leq i \leq n\}$ de subconjuntos de Y^X, cada uno de los cuales tiene $(n-1)^m$ elementos.

Lema 4.5.1 $f \in Y^X \setminus FS(Y^X) \iff f \in \bigcup_{i=1}^{n} F_i$.

Dem. Es evidente que la condición es suficiente. Sea $f \in Y^X \setminus FS(Y^X)$, entonces $Im\,(f) \neq Y$, mas precisamente $Im\,(f) \subset Y$, luego $f \in F_i$ para algún i, $1 \leq i \leq n$. ■

Lema 4.5.2 $\bigcap_{i=1}^{n} F_i = \emptyset$.

Dem. $f \in \bigcap_{i=1}^{n} F_i \iff f \in F_i$, para $1 \leq i \leq n \iff y_i \notin Im\,(f)$, para $1 \leq i \leq n \iff Im\,(f) = \emptyset$, absurdo. ■

Lema 4.5.3 *Si T es un subconjunto de $\{1, 2, \ldots, n\}$ con t elementos, $1 \leq t \leq n$ entonces el conjunto $Z = \bigcap\{F_i : i \in T\}$ tiene $(n-t)^m$ elementos.*

Dem. $f \in \bigcap\{F_i : i \in T\} \iff f \in F_i$, cualquiera que sea $i \in T$, y esto equivale a decir que $Im\ (f) \subseteq Y \setminus \{y_i\}_{i\in T}$. Por lo tanto el conjunto Z tiene tantos elementos como funciones existen de X en $Y \setminus \{y_i\}_{i\in T}$, esto es $(n-t)^m$ elementos. ■

Es bien conocido que:

$$N[\bigcup_{i=1}^{n} F_i] = \sum_{i=1}^{n} N[F_i] - \sum_{i=j} N[F_i \cap F_j] + \sum_{i=j,i=k,j=k} N[F_i \cap F_j \cap F_k] - \ldots \pm \sum_{i=1}^{n} N[\bigcap_{i=1}^{n} F_i]$$

Luego

$$N[\bigcup_{i=1}^{n} F_i] = n\ (n-1)^m - \binom{n}{2}(n-2)^m + \binom{n}{3}(n-3)^m - \ldots \pm \binom{n}{n}(n-n)^m,$$

esto es el número de funciones de X en Y que no son suryectivas está dado por:

$$N[\bigcup_{i=1}^{n} F_i] = \sum_{i=1}^{n-1}(-1)^{(i+1)}\binom{n}{i}(n-i)^m,$$

por lo tanto

$$N[FS(Y^X)] = n^m - \sum_{i=1}^{n-1}(-1)^{(i+1)}\binom{n}{i}(n-i)^m = \sum_{i=0}^{n-1}(-1)^i\binom{n}{i}(n-i)^m.$$

Observemos que esta fórmula también es válida para el caso en que $n = 1$.

Toda función suryectiva de X en Y dá origen a una n-partición, del conjunto X. Recíprocamente dada una n-partición del conjunto X ella dá origen a una suryección de X en Y, mas precisamente ella dá origen a $n!$ funciones suryectivas de X en Y. Por lo tanto podemos afirmar que

$$\frac{N[FS(Y^X)]}{n!}$$

es el número de n-particiones del conjunto X luego el número de relaciones de equivalencia (esto es el número de particiones) que se pueden definir sobre X es :

$$\sum_{n=1}^{m}\Big(\frac{1}{n!}\sum_{i=0}^{n-1}(-1)^i\binom{n}{i}(n-i)^m\Big).$$

Retornemos a nuestro problema: Dada un álgebra de Boole con n átomos ¿Cuántas subálgebras con 2^t elementos, $1 \leq t \leq n$, existen? Tantas como el número de t-particiones, $1 \leq t \leq n$ de un conjunto con n elementos y este número está dado por:

$$\frac{\sum_{i=0}^{t-1}(-1)^i\binom{t}{i}(t-i)^n}{t!}.$$

donde el numerador de esta fracción indica, como vimos, el número de funciones suryectivas de un conjunto con n elementos en un conjunto con t elementos $(1 \leq t \leq n.)$

En un álgebra B_n las posibles subálgebras son isomorfas a $B_1, B_2, \ldots, B_{n-1}, B_n$. En B_3 existen 1 subálgebra isomorfa a B_1, 3 subálgebras isomorfas a B_2 y 1 subálgebra isomorfa a B_3. En B_4, existen 1 subálgebra isomorfa a B_1, 7 subálgebras isomorfas a B_2, 6 subálgebras isomorfas a B_3 y 1 subálgebra isomorfa a B_4.

Vamos a indicar otro método para calcular $SB(G)$ donde G es un conjunto finito. Si G tiene un sólo elemento $G = \{g\}$, notaremos $SB(g)$ en vez de $SB(\{g\})$ y si $G = Y \cup \{x\}$ notaremos $SB(Y, x)$ en vez de $SB(Y \cup \{x\})$.
Observemos que si $G = \{g\}$ entonces $SB(g) = S(m(G)) = S(\{g, -g\}) = \{0, g, -g, 1\}$ y si $g = 0$ ó $g = 1$ entonces $SB(g) = \{0, 1\}$. Sea $G = \{g_1, g_2, \ldots, g_n\}$, consideremos:

- $S_1 = SB(g_1)$
- $S_2 = SB(S_1, g_2)$
- ....
- $S_n = SB(S_{n-1}, g_n)$

Demostremos que $S_n = SB(G)$. En efecto de la construción anterior resulta que:

$$\{g_1\} \subseteq S_1 \subseteq S_1 \cup \{g_2\} \subseteq SB(S_1, g_2) = S_2 \subseteq \ldots \subseteq S_n,$$

por lo tanto (1) $G \subseteq S_n$ y como por construcción (2) S_n es una subálgebra, de (1) y (2) resulta $SB(G) \subseteq S_n$. De $g_1 \in G$ resulta que $S_1 \subseteq SB(G)$, luego $S_1 \cup \{g_2\} \subseteq SB(G)$, por lo tanto $S_2 = SB(S_1, g_2) \subseteq SB(G), \ldots, S_n = SB(S_{n-1}, g_n) \subseteq SB(G)$.

Lema 4.5.4 *Si B es un álgebra de Boole, S una subálgebra booleana de B y $b \in B$, entonces:*

$$SB(S, b) = \{(s_1 \wedge b) \vee (s_2 \wedge -b) : s_1, s_2 \in S\}.$$

(R. Sikorski, *A theorem on extensions of homomorphisms,* Annales de la Soc. Polonaise de Math. 21 (1948), 332-335).

Dem. Sea $T = \{(s_1 \wedge b) \vee (s_2 \wedge -b) : s_1, s_2 \in S\}$.

1) $T \subseteq SB(S, b)$
Sea $t \in T$ entonces $t = (s_1 \wedge b) \vee (s_2 \wedge -b)$ donde $s_1, s_2 \in S$. Como $b \in SB(S, b)$ entonces $-b \in SB(S, b)$. Además $s_1, s_2 \in S \cup \{b\} \subseteq SB(S, b)$, luego como $SB(S, B)$ es una subálgebra tenemos que $t \in SB(S, b)$.

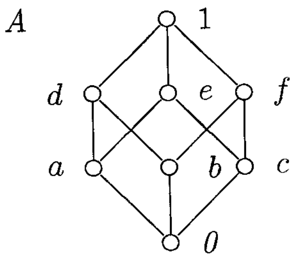
2) $S \cup \{b\} \subseteq T$
Si $s \in S$ entonces $s = s \wedge 1 = s \wedge (b \vee -b) = (s \wedge b) \vee (s \wedge -b) \in T$.
Además $b = b \vee 0 = (1 \wedge b) \vee (0 \wedge -b) \in T$.

3) T es una subálgebra.
De 2) resulta inmediatamente que $T \neq \emptyset$. Sean $u, v \in T$ luego $u \vee v = (s_1 \wedge b) \vee (s_2 \wedge -b) \vee (s_3 \wedge b) \vee (s_4 \wedge -b)$ donde $s_1, s_2, s_3, s_4 \in S$ y por lo tanto $u \vee v = ((s_1 \vee s_3) \wedge b) \vee ((s_2 \vee s_4) \wedge -b)$ donde $(s_1 \vee s_3), (s_2 \vee s_4) \in S$ dado que S es una subálgebra.
Además $-u = (-s_1 \vee -b) \wedge (-s_2 \vee b) =$
$(-s_1 \wedge -s_2) \vee (-s_1 \wedge b) \vee (-b \wedge -s_2) \vee (-b \wedge b) =$

$(-s_1 \wedge -s_2) \vee (-s_1 \wedge b) \vee (-b \wedge -s_2) \vee 0 =$
$(-s_1 \wedge -s_2 \wedge b) \vee (-s_1 \wedge -s_2 \wedge -b) \vee (-s_1 \wedge b) \vee (-s_2 \wedge -b) =$
$(((-s_1 \wedge -s_2) \vee -s_1) \wedge b) \vee (((-s_1 \wedge -s_2) \vee -s_2) \wedge -b) =$
$(-s_1 \wedge b) \vee (-s_2 \wedge -b)$
y como $-s_1, s_2 \in S$ tenemos que $-u \in T$.
De 2) y 3) resulta que $SB(S,b) \subseteq T$.

■

Observación 4.5.2 *1) Si* $S = \{0,1\}$ *y* $b \notin S$ *entonces* $SB(\{0,1\},b) = \{0,1,b,-b\} = SB(b)$.
2) Sea B *el álgebra de Boole indicada en la figura.*



$S = \{0,1,a,f\}$ *es una subálgebra. Entonces* $d \in SB(S,b) = B$ *y* $d = (f \wedge b) \vee (a \wedge -b)$ *y* $d = (1 \wedge b) \vee (a \wedge -b)$*. Esto nos muestra que la expresión de los elementos de* $SB(S,b)$ *no es única.*

Sea B un álgebra de Boole, finita no trivial, $N[\mathcal{A}(B)] = n$, S una subálgebra de B y $g \in B$.
¿Cómo se determinan los átomos de $SB(S,g)$? Si $N[\mathcal{A}(B)] = n = 1$, la única subálgebra de B es la propia B y cualquier elemento de B pertenece a esa subálgebra, luego $SB(S,g) = B$ y por lo tanto $\mathcal{A}(SB(S,g)) = \mathcal{A}(B) = \{1\}$. Supongamos que $N[\mathcal{A}(B)] = n > 1$. Si $g \in S$ entonces $SB(S,g) = S$ y por lo tanto $\mathcal{A}(SB(S,g)) = \mathcal{A}(S)$.
Luego el caso que interesa determinar es cuando $g \notin S$. La siguiente demostración fue indicada por L. Monteiro (1990):

1) *Si* $s \in S$ *entonces* $s \wedge g,\ s \wedge -g \in SB(S,g)$.
   En efecto como $S \subseteq SB(S,g)$ y $g, -g \in SB(S,g)$ entonces $s \wedge g \in SB(S,g)$, $s \wedge -g \in SB(S,g)$.

2) *Existe* $s \in \mathcal{A}(S)$ *tal que* $s \wedge g \neq 0$.
   Si $s \wedge g = 0,\ \forall\ s \in \mathcal{A}(S)$ entonces $\bigvee\{s \wedge g :\ s \in \mathcal{A}(S)\} = 0$, esto es $(\bigvee\{s :\ s \in \mathcal{A}(S)\}) \wedge g = 0$, y por lo tanto $g = 1 \wedge g = 0$. Absurdo dado que $g \notin S$.

3) *Existe* $s' \in \mathcal{A}(S)$ *tal que* $s' \wedge -g \neq 0$.
   Demostración análoga a la anterior.

4) *Si* $s_1 \wedge g \neq 0,\ s_2 \wedge -g \neq 0$ *donde* $s_1, s_2 \in \mathcal{A}(S)$ *entonces* $s_1 \wedge g \neq s_2 \wedge -g$.
   Si $s_1 \wedge g = s_2 \wedge -g$ entonces $s_1 \wedge g \wedge g = s_2 \wedge -g \wedge g = 0$, absurdo.

5) *Si* $\{b_1, b_2, \ldots, b_r\}$ *es una partición de* 1 , $h \in B$ *y* $b'_i = b_i \wedge h$, $b'_{r+i} = b_i \wedge -h$, $1 \leq i \leq r$ *entonces* $\{b'_1, b'_2, \ldots, b'_r, b'_{r+1}, \ldots b'_{2r}\}$ *es una partición de* 1.

En efecto, $\bigvee_{j=1}^{2r} b'_j = \bigvee_{i=1}^{r}(b_i \wedge h) \vee \bigvee_{i=1}^{r}(b_i \wedge -h) =$

$[(\bigvee_{i=1}^{r} b_i) \wedge h] \vee [(\bigvee_{i=1}^{r} b_i) \wedge -h] = (1 \wedge h) \vee (1 \wedge -h) = h \vee -h = 1.$

Probemos que $b'_u \wedge b'_v = 0$, para $u \neq v$, $1 \leq u, v \leq 2r$. En efecto podemos tener los siguientes casos:

i) Si $1 \leq u, v \leq r$, entonces $b'_u \wedge b'_v = b_u \wedge h \wedge b_v \wedge h = b_u \wedge b_v \wedge h = 0 \wedge h = 0$.

ii) Si $r+1 \leq u, v \leq 2r$, entonces $u = r+i$, $v = r+j$ donde $i \neq j$ y entonces $b'_u \wedge b'_v = b_i \wedge -h \wedge b_j \wedge -h = b_i \wedge b_j \wedge -h = 0 \wedge -h = 0$.

iii) Si $1 \leq u \leq r$, $r+1 \leq v \leq 2r$, entonces: $b'_u \wedge b'_v = b_u \wedge h \wedge b_v \wedge -h = 0$.

6) $\mathcal{A}(SB(S,g)) = \{s \wedge g : s \wedge g \neq 0, s \in \mathcal{A}(S)\} \cup \{s \wedge -g : s \wedge -g \neq 0, s \in \mathcal{A}(S)\}$. Sea $\mathcal{A}(S) = \{s_1, s_2, \ldots, s_t\}$, y consideremos los elementos $s'_i = s_i \wedge g$, $s'_{t+i} = s_i \wedge -g$, $1 \leq i \leq t$. Por lo visto en el punto 5) $\mathcal{P} = \{s'_1, s'_2, \ldots, s'_t, s'_{t+1}, \ldots, s'_{2t}\}$ es una partición de 1. Luego, por el Lema 4.4.5 $\mathcal{A}(SB(\mathcal{P})) = \{s'_i \in \mathcal{P} : s'_i \neq 0\}$. Veamos que $SB(\mathcal{P}) = SB(S,g)$.

En efecto, probemos que $S \cup \{g\} \subseteq SB(\mathcal{P})$ de donde resultará (i) $SB(S,g) \subseteq SB(\mathcal{P})$. Sea $r \in S \cup \{g\}$, luego $r \in S$ ó $r = g$. En este último caso tenemos que $r = g = g \wedge 1 = g \wedge (\bigvee_{i=1}^{t} s_i) = \bigvee_{i=1}^{t}(s_i \wedge g) = \bigvee_{i=1}^{t} s'_i \in SB(\mathcal{P})$. Si $r \in S$ entonces $r = 0$, y en este caso $r \in SB(\mathcal{P})$ ó $r \neq 0$ y entonces $r = \bigvee_{j=1}^{j_r}\{s_{i_j} : s_{i_j} \in \mathcal{A}(S)\}$, luego

$r \wedge g = \bigvee_{j=1}^{j_r}\{s_{i_j} \wedge g : s_{i_j} \in \mathcal{A}(S)\} = \bigvee_{j=1}^{j_r}\{s'_{i_j}\} \in SB(\mathcal{P})$ y también

$r \wedge -g = \bigvee_{j=1}^{j_r}\{s_{i_j} \wedge -g : s_{i_j} \in \mathcal{A}(S)\} = \bigvee_{j=1}^{j_r}\{s'_{i_j}\} \in SB(\mathcal{P})$. Por lo tanto

$$r = r \wedge (g \vee -g) = (r \wedge g) \vee (r \wedge -g) \in SB(\mathcal{P}).$$

Probemos que (ii) $\mathcal{P} \subseteq SB(S,g)$. En efecto, si $p \in \mathcal{P}$ entonces $p = s'_i$, $1 \leq i \leq 2t$ y por lo tanto $p = s_i \wedge g$ ó $p = s_i \wedge -g$ donde $s_i \in \mathcal{A}(S)$ y por lo visto en 1) en ambos casos $p \in SB(S,g)$.

Por lo tanto, dada una subálgebra S de un álgebra de Boole B, finita no trivial, y $g \notin S$ para obtener $SB(S,g)$ basta calcular $s \wedge g$, $s \wedge -g$ donde $s \in \mathcal{A}(S)$ y luego hacer supremos de todos aquellos elementos de esta forma que son diferentes de 0.

Observación 4.5.3 *A la subálgebra* S *le corresponde una partición* $\mathcal{P} = \{X_1, X_2, \ldots, X_t\}$ *de* $\mathcal{A}(B)$ *y a* $SB(S,g)$ *le corresponde una partición* $\mathcal{Q}$ *de* $\mathcal{A}(B)$.
¿Cómo se obtiene $\mathcal{Q}$ *a partir del conocimiento de la partición* $\mathcal{P}$ *y el elemento* $g \notin S$?

La siguiente demostración fue indicada por L. Monteiro (1990).
Si $g = \bigvee_{i \in I}\{a_i : I \text{ finito}\}$ sea $Y = \{a_i\}_{i \in I}$ y $W = \mathcal{A}(B) \setminus Y$. Si $W = \emptyset$ esto es $\mathcal{A}(B) \setminus Y = \emptyset$, y por lo tanto $\mathcal{A}(B) \subseteq Y$ luego $1 = \bigvee\{a : a \in \mathcal{A}(B)\} \leq \bigvee\{a_i : i \in I\} = g$ y en consecuencia

$g = 1$ de donde resulta $g \in S$, absurdo. Luego $W \neq \emptyset$. Entonces $-g = \bigvee\{a \in \mathcal{A}(B) : a \in W\}$.
Pongamos $Y_i = X_i \cap Y$, $1 \leq i \leq t$, $W_i = X_i \cap W$, $1 \leq i \leq t$. Vamos a probar que los conjuntos de la partición $\mathcal{Q}$ son precisamente los $Y_i \neq \emptyset$ y los $W_i \neq \emptyset$.
Por 6) sabemos que:
$\mathcal{A}(SB(S,g)) = \{s \wedge g : s \wedge g \neq 0, s \in \mathcal{A}(S)\} \cup \{s \wedge -g : s \wedge -g \neq 0, s \in \mathcal{A}(S)\}$.
Si $s \wedge g \neq 0$, entonces existe $a \in \mathcal{A}(B)$ tal que $a \leq s \wedge g$, entonces como $a \leq s \wedge g \leq s$ tendremos que $a \in X_i$ para algún i y como $a \leq s \wedge g \leq g$ entonces $a \in Y$, luego $a \in X_i \cap Y = Y_i$. Si $X_i \cap Y \neq \emptyset$ entonces existe $a \in \mathcal{A}(B)$ tal que $a \in X_i \cap Y$ y por lo tanto $a \in X_i$ esto es $a \leq s$, $s \in \mathcal{A}(S)$ y $a \in Y$, esto es $a \leq g$, por lo tanto $a \leq s \wedge g$, y en consecuencia $s \wedge g \neq 0$. En forma análoga se demuestra para los W_i.

4.6 Teoría de homomorfismos

Los resultados mas importantes de la teoría de las álgebras de Boole se obtienen utilizando la teoría de homomorfismos.
Si A y A' son álgebras de Boole y $h : A \to A'$ es un epimorfismo de A sobre A', (esto es $h(A) = A'$) entonces se dice que A' es una imagen homomórfica de A.

Lema 4.6.1 *Si h es un homomorfismo de A en A' entonces $h(A)$ es una subálgebra de A', que es una imagen homomórfica de A.*

Lema 4.6.2 *Sea $(A, \wedge, \vee, -, 0, 1)$ un álgebra de Boole. A' un conjunto no vacío donde están definidas dos operaciones binarias " $\wedge$ ", " $\vee$ " y una operación unaria " $-$ ". Sean $0', 1' \in A'$. Si existe una función h de A sobre A' que verifica: H0) $h(0) = 0'$, H1) $h(1) = 1'$, H2) $h(x \wedge y) = h(x) \wedge h(y)$ H3) $h(x \vee y) = h(x) \vee h(y)$, H4) $h(-x) = -h(x)$, entonces $(A', \wedge, \vee, -, 0', 1')$ es un álgebra de Boole que es una imagen homomórfica de A.*

Dem. Elegida una axiomática para las álgebras de Boole debemos probar que se verifican todos los axiomas sobre A'. Aquí puede tener importancia disponer de una axiomática "breve" y con axiomas independientes. Indiquemos solo la demostración de un axioma: $x' \wedge y' = h(x) \wedge h(y) = h(x \wedge y) = h(y \wedge x) = h(y) \wedge h(x) = y' \wedge x'$. ■

Queremos resolver el siguiente problema: *Dada un álgebra de Boole A como se pueden obtener todas las imágenes homomórficas de A, por intermedio de una construcción efectuada sobre A.*
Para resolver este problema vamos a comenzar por resolver un problema análogo de la teoría de conjuntos.
Dado un conjunto no vacío E diremos que un conjunto E' es una imagen de E si existe una transformación f de E sobre E', esto es $f(E) = E'$. Se suele decir que E' es una imagen de E por intermedio de f.
Es bien conocido que la transformación f induce una partición, que notaremos $\mathcal{P}_f$, sobre E a saber :

$$\mathcal{P}_f = \{f^{-1}(x')\}_{x' \in E'}.$$

Esta partición se denomina **partición de E inducida por f.**
También sabemos que toda partición de E induce una relación de equivalencia sobre E,

por lo tanto a la partición $\mathcal{P}_f$ le corresponde una relación de equivalencia R_f.
Recordemos que R_f se define del siguiente modo:

$$a, b \in E, \quad a\, R_f\, b \;\; sss \;\; existe \;\; x' \in E' \;\; tal\; que \; a, b \in f^{-1}(x')$$

luego

$$a\, R_f\, b \;\; sss \;\; f(a) = f(b)$$

Representemos por $C(a)$ la clase de equivalencia con respecto a R_f que contiene al elemento $a \in E$, esto es:

$$C(a) = \{b \in E : b \;\; R_f \;\; a\} = \{b \in E : f(b) = f(a)\}.$$

Recordemos aun que si R es una relación de equivalencia sobre un conjunto E se denomina **conjunto cociente** de E por R al conjunto de todas las clases de equivalencia con respecto a R. Este conjunto se representa por la notación E/R.

Consideremos la transformación $\varphi : E \rightarrow E/R$ definida por $\varphi(x) = C(x)$. Es bien conocido que φ está bien definida ya que si $x = y$ entonces $\varphi(x) = C(x) = C(y) = \varphi(y)$. Ademas φ es suryectiva, ya que dado $x' \in E/R$ esto es, $x' = C(x)$ con $x \in E$ y entonces $\varphi(x) = C(x) = x'$. Por lo tanto E/R es *una imagen de E por intermedio de φ*.
φ se denomina la **transformación canónica** ("conforme a las reglas") o **natural** de E sobre E/R.
Vamos a demostrar que toda imagen de E se puede obtener de este modo, esto es considerando una relación de equivalencia R sobre E y construyendo el conjunto cociente E/R. Para ello vamos a demostrar una serie de lemas.

Lema 4.6.3 *Si $f_1(E) = E_1$, $f_2(E) = E_2$, y $R_{f_1} \subseteq R_{f_2}$, (esto es, $a \;\; R_{f_1} \;\; b \Rightarrow a \;\; R_{f_2} \;\; b$) entonces existe una única función h de E_1 sobre E_2 tal que $h \circ f_1 = f_2$.*

Dem.

$$\begin{tikzcd} E \arrow[r, "f_1"] \arrow[d, "f_2"'] & E_1 \arrow[dl, "h"] \\ E_2 & \end{tikzcd}$$

Sea $a_1 \in E_1 = f_1(E)$, luego $a_1 = f_1(a)$ con $a \in E$ y por lo tanto $f_2(a) = a_2 \in E_2$.
Pongamos por definición:

$$h(a_1) = a_2 = f_2(a).$$

Probemos que h está bien definida, esto es que si $b \in E$ es tal que $f_1(b) = a_1$ entonces $f_2(b) = f_2(a)$.
En efecto, si $b \in E$ es tal que $f_1(b) = a_1$ entonces $f_1(b) = f_1(a)$ luego $a \;\; R_{f_1} \;\; b$ de donde resulta por la hipótesis que $a\, R_{f_2}\, b$ esto es, $f_2(b) = f_2(a)$. Luego h es una función de E_1 en E_2.
Sea $a \in E$, como $f_1(a) = a_1 \in E_1$, entonces por la definición de h tenemos $h(a_1) = f_2(a)$, esto es $h(f_1(a)) = f_2(a)$, y por lo tanto $(h \circ f_1)(a) = f_2(a)$.
De aquí resulta que h es suryectiva, ya que si $e_2 \in E_2$ entonces $e_2 = f_2(e)$, con $e \in E$, y por lo tanto $f_1(e) = e_1$, luego $h(e_1) = (h(f_1(e)) = f_2(e) = e_2$.
Probemos finalmente que h es única. Supongamos que $h_1 : E_1 \rightarrow E_2$ verifica $h_1 \circ f_1 = f_2$, y probemos que $h(a_1) = h_1(a_1)$, para todo $a_1 \in E_1$. En efecto $a_1 = f_1(a)$ con $a \in E$ entonces $h_1(a_1) = h_1(f_1(a)) =$ (por hipótesis) $f_2(a) = h(f_1(a)) = h(a_1)$, luego $h = h_1$. ■

Lema 4.6.4 *Si $f_1(E) = E_1$, $f_2(E) = E_2$, y $R_{f_1} = R_{f_2}$, entonces E_1 y E_2 son coordinables.*

Dem. Para ello nos basta demostrar que la transformación h definida anteriormente es inyectiva. Sean $a_1, b_1 \in E_1$ tales que $h(a_1) = h(b_1)$. Como $a_1 = f_1(a)$, $b_1 = f_1(b)$ donde $a, b \in E$, entonces $h(f_1(a)) = h(f_1(b))$, esto es $f_2(a) = f_2(b)$, por lo tanto $a\ R_{f_2}\ b$ y como por hipótesis $R_{f_2} = R_{f_1}$, entonces $a\ R_{f_1}\ b$, esto es $f_1(a) = f_1(b)$, y por lo tanto $a_1 = b_1$. ■

Lema 4.6.5 *Si $f(E) = E_1$ entonces $E' = E/R_f$ es coordinable con E_1.*

Dem. Sea φ la transformación canónica de E sobre $E' = E/R_f$, luego $\varphi(E) = E'$.

$$\begin{tikzcd} E \arrow[r, "f"] \arrow[d, "\varphi"'] & E_1 \\ E/R_f & \end{tikzcd}$$

Por el Lema 4.6.4 si probamos que $R_\varphi = R_f$ resulta que E_1 y E/R_f son coordinables, lo que es evidente pués: $a\ R_\varphi\ b \iff \varphi(a) = \varphi(b) \iff C(a) = C(b) \iff a\ R_f\ b$. ■

Por lo tanto, todas las imágenes de un conjunto, no vacío, E se obtienen (a menos de una biyección) considerando relaciones de equivalencia R sobre E y construyendo E/R, dado que: 1) si R es una relacion de equivalencia definida sobre E entonces $E' = E/R$ es una imagen de E y 2) si E' es una imagen de E existe una relación de equivalencia R definida sobre E tal que E' es equipotente con E/R.

Lema 4.6.6 *Sean $f_1(E) = E_1$, $f_2(E) = E_2$, y que existe una función $h : E_1 \to E_2$ tal que $h \circ f_1 = f_2$.*

a) Entonces necesariamente h es suryectiva y $R_{f_1} \subseteq R_{f_2}$.

b) Si la función h es además inyectiva, entonces $R_{f_1} = R_{f_2}$.

Dem.

a) Ya sabemos que de $h \circ f_1 = f_2$ resulta que h es suryectiva. Si $a\ R_{f_1}\ b \Longrightarrow f_1(a) = f_1(b) \Longrightarrow h(f_1(a)) = h(f_1(b)) \Longrightarrow f_2(a) = f_2(b) \Longrightarrow a\ R_{f_2}\ b$.

b) Por a) $R_{f_1} \subseteq R_{f_2}$. Supongamos que $a\ R_{f_2}\ b \Longrightarrow f_2(a) = f_2(b) \Longrightarrow$ (por hipótesis) $h(f_1(a)) = h(f_1(b))$, luego como h es inyectiva $f_1(a) = f_1(b) \Longrightarrow a\ R_{f_1}\ b$.

■

Retornemos al problema de determinar todas las imágenes homomórficas de un álgebra de Boole A. Sea $h : A \to A'$ un epimorfismo, luego en particular el conjunto A' es una imagen del conjunto A por intermedio de la función h. Vimos que toda función de A sobre A' determina una relación de equivalencia sobre A, luego h determina una relación de equivalencia R_h sobre A, definida del siguiente modo:

$$a\ R_h\ b \iff h(a) = h(b).$$

Lema 4.6.7 *En toda álgebra de Boole,* $x \leq y \iff -x \vee y = 1$.

Dem. $\Longrightarrow$) De $x \leq y \implies 1 = -x \vee x \leq -x \vee y$.
$\Longleftarrow$) De $-x \vee y = 1$, resulta $x \wedge (-x \vee y) = x \wedge 1$, esto es $(x \wedge -x) \vee (x \wedge y) = x \implies 0 \vee (x \wedge y) = x \implies x \wedge y = x$, esto es $x \leq y$. ■

Corolario 4.6.1 $x = y \iff -x \vee y = 1$ y $-y \vee x = 1$.

Observación 4.6.1

$$a\, R_h\, b \iff h(a) = h(b) \iff$$
$$-h(a) \vee h(b) = 1 \text{ y } -h(b) \vee h(a) = 1 \iff h(-a \vee b) = 1 \text{ y } h(-b \vee a) = 1 \iff$$
$$-a \vee b \in h^{-1}(1) \text{ y } -b \vee a \in h^{-1}(1).$$

Esto significa que: el conocimiento de la clase de equivalencia $h^{-1}(1)$ es suficiente para conocer las restantes clases de equivalencia.

Lema 4.6.8 *Si* $a\ R_h\ b$ *y* $a'\ R_h\ b'$, *entonces:*

1) $a \vee a'\ R_h\ b \vee b'$

2) $a \wedge a'\ R_h\ b \wedge b'$

3) $-a\ R_h\ -b$

Dem. En efecto, $h(a \vee a') = h(a) \vee h(a') = h(b) \vee h(b') = h(b \vee b')$. Las propiedades 2) y 3) se demuestran en forma análoga. ■

Las propiedades 1), 2) y 3) se expresan abreviadamente diciendo que *la relación de equivalencia* R_h *es* **compatible** *con las operaciones de* $\vee$, $\wedge$ *y* $-$, *o que* R_h *es una* **relación de congruencia.**

Si h es un homomorfismo de A en A' se denomina **núcleo** de h al conjunto:

$$F = Nuc(h) = h^{-1}(1) = \{x \in A : h(x) = 1\}$$

y **antinúcleo** al conjunto $I = ANuc(h) = h^{-1}(0) = \{x \in A : h(x) = 0\}$.

Lema 4.6.9 $F = -I = (def) = \{-i : i \in I\}$.

Dem. $-I \subseteq F$. Sea $j \in -I \implies j = -i$ con $i \in I \implies h(j) = h(-i) = -h(i) = -0 = 1 \implies j \in F$.
$F \subseteq -I$. Sea $j \in F \implies h(j) = 1 \implies -h(j) = 0 \implies h(-j) = 0 \implies -j \in I \implies j = -(-j) \in -I$. ■

Lema 4.6.10 *El núcleo* $F = Nuc(h)$ *de un homomorfismo* $h : A \to A'$ *tiene las siguientes propiedades:*

F1) $1 \in F$.

F2) Si $x, y \in F$, *entonces* $x \wedge y \in F$.

F3) Si $x \in F$ *e* $y \in A$ *verifica* $x \leq y$ *entonces* $y \in F$.

Dem.

F1) Resulta de $h(1) = 1$.

F2) $h(x \wedge y) = h(x) \wedge h(y) = 1 \wedge 1 = 1$.

F3) $1 = h(x) = h(x \wedge y) = h(x) \wedge h(y) = 1 \wedge h(y) = h(y)$.

■

Definición 4.6.1 *Una parte F de un álgebra de Boole A se dice un* **filtro** *si verifica las propiedades F1), F2) y F3).*

Por lo tanto, de acuerdo con esta definición, el núcleo de un homomorfismo es un filtro.

Lema 4.6.11 *Si $h : A \to A'$ es un homomorfismo entonces $h(a) = h(b)$ sss existe $n \in Nuc(h)$ tal que $a \wedge n = b \wedge n$.*

Dem. Vimos en la Observación 4.6.1 que $h(a) = h(b)$ sss $-a \vee b \in Nuc(h)$ y $-b \vee a \in Nuc(h)$. Como $Nuc(h)$ es un filtro, entonces por la propiedad F2) podemos afirmar que:

$$n = (-a \vee b) \wedge (-b \vee a) \in Nuc(h).$$

Luego

$$a \wedge n = a \wedge (-a \vee b) \wedge (-b \vee a) = a \wedge (-a \vee b) = a \wedge b,$$

y

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

Supongamos que existe $n \in Nuc(h)$ tal que $a \wedge n = b \wedge n$, luego:

$$h(a) = h(a) \wedge 1 = h(a) \wedge h(n) = h(a \wedge n) = h(b \wedge n) = h(b) \wedge h(n) = h(b) \wedge 1 = h(b).$$

■

Lema 4.6.12 *Si R es una relación de congruencia definida sobre un álgebra de Boole A entonces:*

I) $C(1) = \{x \in A : x \, R \, 1\}$ *es un filtro.*

II) Las siguientes condiciones son equivalentes:

1) $a \, R \, b$.

2) $-a \vee b, \ -b \vee a \in C(1)$.

3) Existe $n \in C(1)$ *tal que* $a \wedge n = b \wedge n$.

III) $C(1) = -C(0) = \{-x : x \in C(0)\}$.

Dem.

I) Como $1 \; R \; 1$ entonces F1) $1 \in C(1)$.
F2) Sean $x, y \in C(1)$, luego $x \;\; R \;\; 1$, $y \;\; R \;\; 1$, y como R es compatible con $\wedge$ tenemos que $x \wedge y \;\; R \;\; 1 \wedge 1 = 1$, por lo tanto $x \wedge y \in C(1)$.
F3) Si $x \in C(1)$, entonces $x \; R \; 1$ y como $y \;\; R \;\; y$ y R es compatible con $\wedge$ tenemos que $x \wedge y \;\; R \;\; 1 \wedge y = y$. Por lo tanto si $x \leq y$ donde $y \in A$ tendremos que $x \wedge y = x$ y por lo tanto $x \;\; R \;\; y$ y como $x \;\; R \;\; 1$ tendremos, dado que R es una relación de equivalencia, que $y \;\; R \;\; 1$, esto es $y \in C(1)$.

Observemos que basta que R sea compatible con $\wedge$ para que $C(1)$ sea un filtro.

II) Probemos que $1 \rightarrow 2$; $2 \rightarrow 3$; $3 \rightarrow 1$.

$1 \rightarrow 2)$ De $a \; R \; b$ resulta por ser R compatible con $\vee$ que $1 = -a \vee a \; R \; -a \vee b$ por lo tanto $-a \vee b \in C(1)$. Análogamente se prueba que $-b \vee a \in C(1)$.

$2 \rightarrow 3)$ De $-a \vee b \in C(1)$ y $-b \vee a \in C(1)$, resulta por ser $C(1)$ un filtro que $n = (-a \vee b) \wedge (-b \vee a) \in C(1)$, y se prueba en forma análoga a lo indicado en el Lema 4.6.11 la propiedad 3).

$3 \rightarrow 1)$ Supongamos que existe $n \in C(1)$ tal que $a \wedge n = b \wedge n$. De $n \in C(1)$ resulta $n \;\; R \;\; 1$, luego como R es compatible con $\wedge$ tenemos que $a \wedge n \;\; R \;\; a \wedge 1 = a$ y $b \wedge n \;\; R \;\; b \wedge 1 = b$, y como por hipótesis $a \wedge n = b \wedge n$ resulta que $a \; R \; b$.

III) $x \in C(1) \iff x \; R \; 1 \iff$ (por ser R compatible con " $-$ ") $-x \; R \; -1 = 0 \iff -x \in C(0) \iff x \in -C(0)$.

■

Definición 4.6.2 *En un álgebra de Boole A se denomina* **implicación clásica** *a la operación binaria " $\rightarrow$ " definida sobre A del siguiente modo:*

$$x \rightarrow y = -x \vee y, \quad \text{donde} \quad x, y \in A$$

que se lee " x implica clasicamente a y*" ó mas sencilamente "* x implica y*".*

De acuerdo con esta definición el Lema 4.6.7 se puede enunciar del siguiente modo:

Lema 4.6.13 $a \leq b \iff a \rightarrow b = 1$.

y el Corolario 4.6.1 se enuncia

Corolario 4.6.2 $a = b \iff a \rightarrow b = 1$ *y* $b \rightarrow a = 1$.

Lema 4.6.14 *La implicación tiene las siguientes propiedades:*

I1) $a \rightarrow a = 1$.

I2) $a \rightarrow (b \rightarrow a) = 1$.

I3) $a \rightarrow (a \wedge b) = a \rightarrow b$.

- *Leyes distributivas a izquierda [I4) e I5)]*

I4) $a \to (b \vee c) = (a \to b) \vee (a \to c)$.

I5) $a \to (b \wedge c) = (a \to b) \wedge (a \to c)$.

- *Leyes antidistributivas a derecha [I6) e I7)]*

I6) $(a \vee b) \to c = (a \to c) \wedge (b \to c)$.

I7) $(a \wedge b) \to c = (a \to c) \vee (b \to c)$.

I8) $a \to (b \to c) = (a \wedge b) \to c$.

I9) $a \to (b \to c) = (a \to b) \to (a \to c)$.

- *Ley de Peirce*

I10) $(a \to b) \to a = a$.

Lema 4.6.15 *Si h es un homomorfismo booleano entonces $h(x \to y) = h(x) \to h(y)$.*

Corolario 4.6.3 $h(a) = h(b) \iff a \to b \in h^{-1}(1)$ y $b \to a \in h^{-1}(1)$.

Lema 4.6.16 *El núcleo F de un homomorfismo booleano h tiene las siguientes propiedades:*

D1) $1 \in F$.

D2) Si $a \in F$ y $a \to b \in F$ entonces $b \in F$ (**modus ponens**).

Definición 4.6.3 *Una parte D de un álgebra de Boole A se dice un sistema deductivo si verifica las condiciones D1) y D2).*

Lema 4.6.17 *D sistema deductivo $\iff$ D filtro.*

Dem. Necesaria) La propiedad F1) coincide con D1). Sean $a, b \in D$ si probamos que $d \to (a \wedge b) \in D$, con $d \in D$ entonces por la propiedad D2) resultará que $a \wedge b \in D$.
Por hipótesis $b \in D$ y por I2) $b \to (a \to b) = 1 \in D$ luego por D2) deducimos que $a \to b \in D$.
Por la propiedad I3) $a \to (a \wedge b) = a \to b$, de donde resulta por lo que acabamos de probar que $a \to (a \wedge b) \in D$, luego como por hipótesis $a \in D$ resulta $a \wedge b \in D$.
Supongamos que $a \in D$ y $a \leq b$, donde b es un elemento del álgebra. De $a \leq b$ resulta $a \to b = 1 \in D$, luego como por hipótesis $a \in D$ resulta por D2) que $b \in D$.
Suficiente) D1) coincide con F1). Supongamos que a, $a \to b \in D$, luego como D es un filtro resulta por la propiedad F2) que $a \wedge (a \to b) \in D$. Pero $a \wedge (a \to b) = a \wedge b$, entonces como $a \wedge b \leq b$, $a \wedge b \in D$ resulta por F3) que $b \in D$. ■

Definición 4.6.4 *Dado un filtro F de un álgebra de Boole A diremos que el elemento $a \in A$ está relacionado con el elemento $b \in A$, módulo F y escribiremos $a \equiv b$ (mód.F), $a \equiv b$ (F) ó $a \equiv b$, si existe $f \in F$ tal que $a \wedge f = b \wedge f$.*

Lema 4.6.18 *La relación binaria " $\equiv$ " es una congruencia.*

Dem.

I) $\equiv$ es una relación de equivalencia.

1) Como $a \wedge 1 = a \wedge 1$ y $1 \in F$ entonces $a \equiv a$.
2) Si $a \equiv b$ entonces existe $f \in F$ tal que $a \wedge f = b \wedge f$ y por lo tanto $b \wedge f = a \wedge f$ esto es $b \equiv a$.
3) Si $a \equiv b$ y $b \equiv c$ entonces existen $f_1, f_2 \in F$ tales que (i) $a \wedge f_1 = b \wedge f_1$ y (ii) $b \wedge f_2 = c \wedge f_2$. De (i) se deduce $a \wedge f_1 \wedge f_2 = b \wedge f_1 \wedge f_2$ y de (ii) $b \wedge f_2 \wedge f_1 = c \wedge f_2 \wedge f_1$, luego $a \wedge f_1 \wedge f_2 = c \wedge f_1 \wedge f_2$, y como $f_1, f_2 \in F$ y F es un filtro tenemos que $f_1 \wedge f_2 \in F$ y en consecuencia $a \equiv c$.

II) $\equiv$ es compatible con " $\wedge$ ", " $\vee$ " y " $-$ ".
Supongamos que $a \equiv b$ y $a' \equiv b'$, esto es existen $f_1, f_2 \in F$ tales que (i) $a \wedge f_1 = b \wedge f_1$ y (ii) $a' \wedge f_2 = b' \wedge f_2$.

1) De (i) e (ii) resulta que $a \wedge a' \wedge f_1 \wedge f_2 = b \wedge b' \wedge f_1 \wedge f_2$ y como $f_1 \wedge f_2 \in F$ entonces $a \wedge a' \equiv b \wedge b'$.
2) De (i) se deduce $-a \vee -f_1 = -b \vee -f_1$ y por lo tanto $(-a \vee -f_1) \wedge f_1 = (-b \vee -f_1) \wedge f_1$, luego $-a \wedge f_1 = -b \wedge f_1$, donde $f_1 \in F$ esto es $-a \equiv -b$.
3) De 1) y 2) se deduce utilizando las leyes de De Morgan, que $\equiv$ es compatible con $\vee$.
4) Observemos que también se puede probar que $\equiv$ es compatible con $\vee$ del siguiente modo:
(4a) Si $a \equiv b$ entonces $a \vee c \equiv b \vee c$. En efecto, por hipótesis existe $f \in F$ tal que $a \wedge f = b \wedge f$ luego, $(a \wedge f) \vee c = (b \wedge f) \vee c$ y por lo tanto (i) $(a \vee c) \wedge (f \vee c) = (b \vee c) \wedge (f \vee c)$. Como F es un filtro, $f \in F$ y $f \leq f \vee c$ entonces (ii) $f \vee c \in F$. De (i) e (ii) resulta que $a \vee c \equiv b \vee c$.
(4b) Si (iii) $a \equiv b$ y (iv) $a' \equiv b'$ entonces $a \vee a' \equiv b \vee b'$. En efecto, de (iii) resulta por (4a) que (v) $a \vee a' \equiv b \vee a'$ y de (iv) resulta por (4a) que (vi) $a' \vee b \equiv b' \vee b$. De (v) y (vi) tenemos finalmente que $a \vee a' \equiv b \vee b'$.

■

Notaremos $C(x) = C_F(x) = \{y \in A : y \equiv x\}$ (clase de equivalencia que contiene a $x \in A$.)

Lema 4.6.19 $F = C(1)$ *y* $C(0) = -F$.

Dem. Si $x \in F$ como $x \wedge x = 1 \wedge x$ entonces $x \equiv 1$ y por lo tanto $F \subseteq C(1)$. Recíprocamente si $x \in C(1)$ entonces $x \wedge f = 1 \wedge f = f$, donde $f \in F$, luego $f \leq x$ y como F es un filtro tenemos que $x \in F$, por lo tanto $C(1) \subseteq F$.
Por el lema anterior sabemos que $C(1) = -C(0)$ entonces $-F = -C(1) = C(0)$. ■

Acabamos de probar que un filtro F del álgebra de Boole dá origen a una relación de equivalencia " $\equiv$ ". Al conjunto cociente lo notaremos $A/\equiv$ ó A/F. Sobre este conjunto definamos las siguientes operaciones:

$$-C(x) = C(-x); \quad C(x) \wedge C(y) = C(x \wedge y); \quad C(x) \vee C(y) = C(x \vee y).$$

Como " $\equiv$ " es compatible con las operaciones " $\wedge$ ", " $\vee$ " y " $-$ ", podemos afirmar que estas operaciones estan bien definidas.
Tenemos así un sistema $(A/F, \wedge, \vee, -, C(1), C(0))$. Si $\varphi : A \to A/F$ está definida por $\varphi(x) = C(x)$ para todo $x \in A$ entonces φ es una función suryectiva que verifica $\varphi(1) = C(1)$, $\varphi(0) = C(0)$, $\varphi(x \wedge y) = \varphi(x) \wedge \varphi(y)$, $\varphi(x \vee y) = \varphi(x) \vee \varphi(y), \varphi(-x) = -\varphi(x)$, luego por el Lema 4.6.2, A/F es un álgebra de Boole que es una imagen homomórfica de A. φ se denomina el homomorfismo canónico o natural de A sobre A/F, y A/F el **álgebra cociente** de A por F o el álgebra cociente de A por $\equiv$.
Observemos aún que $Nuc(\varphi) = \{x \in A : \varphi(x) = C(1)\} = \{x \in A : C(x) = C(1)\} = \{x \in A : x \equiv 1\} = C(1) = F$.

Lema 4.6.20 *Sean A, A_1, A_2 álgebras de Boole, $h_1 : A \to A_1$ $h_2 : A \to A_2$ epimorfismos booleanos tales que $Nuc(h_1) = Nuc(h_2)$. Entonces A_1 y A_2 son álgebras de Boole isomorfas.*

Dem. $Nuc(h_1) = Nuc(h_2)$, equivale a decir que $R_{h_1} = R_{h_2}$, luego la transformación $h : A_1 \to A_2$ definida por $h(a_1) = h_2(a)$, donde $h_1(a) = a_1$ es una biyección de A_1 en A_2 (ver Lema 4.6.4) que verifica $h \circ h_1 = h_2$ y además h es única. Probemos que en este caso h es un homomorfismo booleano.

H1) $h(a_1 \vee b_1) = h(a_1) \vee h(b_1)$.
Sean $a, b \in A$ tales que $h_1(a) = a_1$, $h_1(b) = b_1$ entonces $h(a_1) \vee h(b_1) = h(h_1(a)) \vee h(h_1(b)) = h_2(a) \vee h_2(b) = h_2(a \vee b) = (h \circ h_1)(a \vee b) = h(h_1(a \vee b)) = h(h_1(a) \vee h_1(b)) = h(a_1 \vee b_1)$.

H2) $h(-a_1) = h(-h_1(a)) = h(h_1(-a)) = h_2(-a) = -h_2(a) = -((h \circ h_1)(a)) = -(h(h_1(a_1)) = -h(a_1)$.

De H1) y H2) se deduce H3) $h(a_1 \wedge b_1) = h(a_1) \wedge h(b_1)$. De estas tres propiedades se deduce H4) $h(1) = 1$ y $h(0) = 0$. ■

Corolario 4.6.4 *Si A y A' son álgebras de Boole y h es un homomorfismo booleano de A sobre A' entonces A' es isomorfa a $A/Nuc(h)$.*

Dem. Sea $F = Nuc(h)$, luego F es un filtro de A y en consecuencia $A'' = A/Nuc(h)$ es un álgebra de Boole. Además $\varphi(x) = C_{Nuc(h)}(x)$ es un epimorfismo booleano de A en A'' tal que $Nuc(\varphi) = F = Nuc(h)$ y por lo tanto $A'' \cong A/Nuc(h)$. ■

Acabamos así de probar que todas las imagenes homomórficas de un álgebra de Boole A se obtienen (a menos de isomorfismo) considerando filtros F de A y construyendo A/F.

Si A es un álgebra de Boole, y $f \in A$ notaremos con $F(f)$, $[f, 1]$ ó $[f)$ al conjunto

$$\{x \in A : f \leq x\}.$$

Lema 4.6.21 $[f)$ *es un filtro de* A.

Dem. Como $f \leq 1$ entonces F1) $1 \in [f)$. Probemos la propiedad F2) Si $x, y \in [f)$ esto es $f \leq x$, $f \leq y$ entonces $f \leq x \wedge y$ luego $x \wedge y \in [f)$. Demostremos F3) Sea $x \in [f)$ e $y \in A$ tal que $x \leq y$, entonces como $f \leq x$ tenemos que $f \leq y$ esto es $y \in [f)$. ■

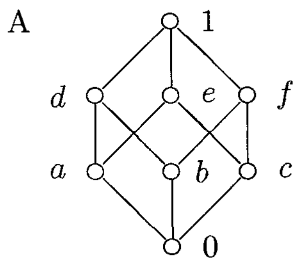
Definición 4.6.5 *Un filtro F de A se dice principal si existe $f \in A$ tal que $F = [f)$.*

Lema 4.6.22 *En un álgebra de Boole finita A, todos los filtros son principales.*

Dem. Sea F un filtro y $f = \bigwedge_{x \in F} x$. Como A es finita entonces F es un conjunto finito y por lo tanto, existe el ínfimo f, y además como F es un filtro (2) $f \in F$.
Por lo tanto si $y \in F$ entonces $f = \bigwedge_{x \in F} x \leq y$, por lo tanto $y \in [f)$. Recíprocamente si $y \in [f)$ esto es $f \leq y$ por lo tanto de (2) y teniendo en cuenta que F es un filtro resulta que $y \in F$. ■

Lema 4.6.23 *Dado un filtro principal $[f)$, entonces $a \equiv b$ (mód. $[f)$) $\iff$ $a \wedge f = b \wedge f$.*

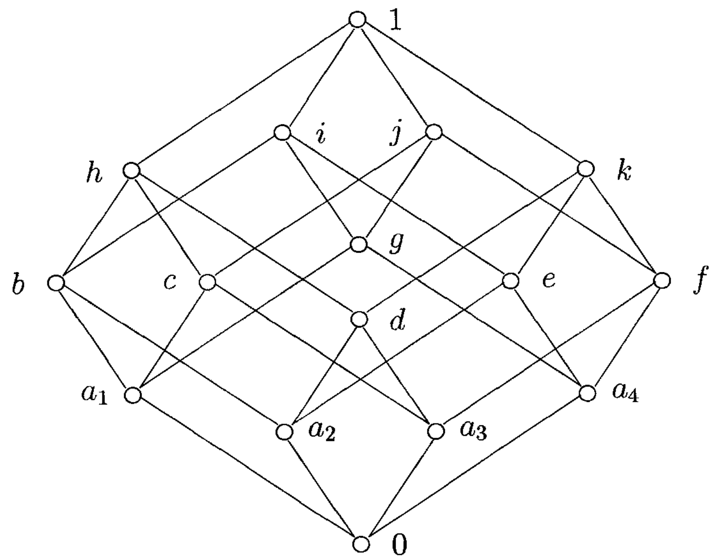
Dem. $\Longrightarrow$) Si $a \equiv b$ (mód. $[f)$) existe $n \in [f)$, esto es $f \leq n$, tal que $a \wedge n = b \wedge n$, luego $a \wedge f \wedge n = b \wedge f \wedge n$, y como $f \wedge n = f$ tenemos $a \wedge f = b \wedge f$.
$\Longleftarrow$) Como $f \in [f)$ es claro que $a \equiv b$ (mód. $[f)$). ■
Sea A el álgebra de Boole indicada en la figura y consideremos el filtro principal $[f)$.



x	0	a	b	c	d	e	f	1
$x \wedge f$	0	0	b	c	b	c	f	f

Luego $C(0) = \{0, a\}$, $C(b) = \{b, d\}$, $C(c) = \{c, e\}$, $C(1) = \{1, f\} = [f)$.

Ejercicio. Dada el álgebra de Boole B_4, con cuatro átomos, indicada en la siguiente figura, y el filtro $[b)$ determinar todas las clase de equivalencia módulo $[b)$.



Sean p, u elementos de un álgebra de Boole tales que $p \leq u$. Sabemos que el segmento $S = [p, u]$ es un reticulado distributivo con primer elemento p y último elemento u.

Lema 4.6.24 *$S = [p, u]$ es un álgebra de Boole.*

Dem. Para ello necesitamos probar que todo elemento de S tiene un complemento en S, esto es que si $s \in S$ existe $s' \in S$ tal que $s \wedge s' = p$ y $s \vee s' = u$.
Pongamos por definición:

$$s' = p \vee (-s \wedge u)$$

luego $p \leq p \vee (-s \wedge u) = (p \vee -s) \wedge (p \vee u) = (p \vee -s) \wedge u \leq u$, y por lo tanto $s' \in S$.
$s \wedge s' = s \wedge [p \vee (-s \wedge u)] = (s \wedge p) \vee (s \wedge -s \wedge u) = p \vee 0 = p$.
$s \vee s' = s \vee p \vee (-s \wedge u) = s \vee (-s \wedge u) = (s \vee -s) \wedge (s \vee u) = 1 \wedge u = u$. ■

Corolario 4.6.5 *$S = [0, u] = (u]$ es un álgebra de Boole donde el complemento de $s \in S$ es $s' = -s \wedge u$, y $T = [u, 1] = [u)$ es un álgebra de Boole donde el complemento de $t \in T$ es $t' = -t \vee u$.*

Lema 4.6.25 *Si A es un álgebra de Boole y $u \in A$ entonces $A' = A/[u)$ es isomorfa a $A'' = (u]$.*

Dem. Dado $a \in A$, sea $h(a) = a \wedge u$, como $0 \leq a \wedge u \leq u$ entonces h es una transformación de A en $(u]$. Además dado $y \in (u]$, esto es $0 \leq y \leq u$, como $y \in A$ entonces $h(y) = y \wedge u = y$. Esto prueba que h es suryectiva y que deja invariantes a los elementos de $(u]$. Además
$h(a \wedge b) = a \wedge b \wedge u = a \wedge u \wedge b \wedge u = h(a) \wedge h(b)$.
$(h(a))' = -h(a) \wedge u = -(a \wedge u) \wedge u = (-a \vee -u) \wedge u = (-a \wedge u) \vee (-u \wedge u) = -a \wedge u = h(-a)$.
Acabamos así de probar que h es un epimorfismo booleano. Sea φ el homomorfismo natural de A sobre $A' = A/[u)$. Si probamos que $Nuc(\varphi) = Nuc(h)$ entonces por el Lema 4.6.20, resultará que $A' = A/[u)$ es isomorfa a $(u]$.
En efecto, $x \in Nuc(\varphi) \iff x \in [u) \iff u = x \wedge u = h(x) \iff x \in Nuc(h)$. ■

Lema 4.6.26 *Si C es una clase de equivalencia módulo $[u)$ entonces el conjunto $C \cap (u]$ contiene un único elemento.*

Dem. 1) $C \cap (u] \neq \emptyset$. Sea $x \in C$, luego $h(x) = x \wedge u \in (u]$ y $h(x) \wedge u = x \wedge u \wedge u = x \wedge u$, por lo tanto $h(x) \equiv x$ (mód. $[u)$) y como $x \in C$ tenemos que $h(x) \in C$ y en consecuencia $h(x) \in C \cap (u]$.
2) El elemento es único. Si $x, y \in C \cap (u]$ entonces tendremos que (i) $x, y \in C$ y (ii) $x, y \in (u]$. De (i) resulta que $x \equiv y$ (mód. $[u)$) esto es (iii) $x \wedge u = y \wedge u$, y como por (ii) tenemos $0 \leq x \leq u$, $0 \leq y \leq u$, de (iii) resulta que $x = y$. ■

Lema 4.6.27 *Si A es un álgebra de Boole y F un filtro de A, entonces toda clase de equivalencia módulo F es coordinable con F.* (A. Monteiro, 1978.)

Dem. Sea C una clase de equivalencia módulo F. Vamos a definir una función g de F en C del siguiente modo:

$$g(f) = (f \to c) \wedge (c \to f) = (-f \vee c) \wedge (-c \vee f)$$

cualquiera que sea $f \in F$, $c \in C$, c fijo.

1) $g(f) \in C$.
$g(f) \wedge f = (-f \vee c) \wedge (-c \vee f) \wedge f = (-f \vee c) \wedge f = (-f \wedge f) \vee (c \wedge f) = c \wedge f$. Por lo tanto como $f \in F$ esto significa que $g(f) \equiv c$ (mód. F) y en consecuencia como $c \in C$ tenemos que $g(f) \in C$.

2) g es suryectiva.
Dado $b \in C$ tenemos que $c \equiv b$ (mód. F), luego $(-c \vee b), (-b \vee c) \in F$ y como F es un filtro tenemos que $f = (-c \vee b) \wedge (-b \vee c) \in F$, entonces $g(f) = (-f \vee c) \wedge (-c \vee f) =$
$[-((-c \vee b) \wedge (-b \vee c)) \vee c] \wedge [-c \vee ((-c \vee b) \wedge (-b \vee c))] =$
$[(c \wedge -b) \vee (b \wedge -c) \vee c] \wedge [-c \vee ((-c \vee b) \wedge (-b \vee c))] =$
$[(b \wedge -c) \vee c] \wedge [(-c \vee b) \wedge (-c \vee -b \vee c)] =$
$[(b \vee c) \wedge (-c \vee c)] \wedge [(-c \vee b) \wedge 1] = (b \vee c) \wedge (-c \vee b) = b \vee (c \wedge -c) = b$.

3) g es inyectiva.
Supongamos que $g(f_1) = g(f_2)$ donde $f_1, f_2 \in F$, esto es

$$(1) \quad (-f_1 \vee c) \wedge (-c \vee f_1) = (-f_2 \vee c) \wedge (-c \vee f_2)$$

luego

$$c \wedge (-f_1 \vee c) \wedge (-c \vee f_1) = c \wedge (-f_2 \vee c) \wedge (-c \vee f_2)$$

y por lo tanto

$$c \wedge (-c \vee f_1) = c \wedge (-c \vee f_2)$$

esto es

$$(2) \quad c \wedge f_1 = c \wedge f_2.$$

Análogamente de (1) se deduce

$$-c \wedge (-f_1 \vee c) \wedge (-c \vee f_1) = -c \wedge (-f_2 \vee c) \wedge (-c \vee f_2)$$

luego

$$-c \wedge (-f_1 \vee c) = -c \wedge (-f_2 \vee c)$$

esto es

$$-c \wedge -f_1 = -c \wedge -f_2.$$

y por lo tanto

$$(3) \quad c \vee f_1 = c \vee f_2.$$

De (2) y (3) resulta por la ley de simplificación que $f_1 = f_2$.

■

Lema 4.6.28 *Si $x \in (u]$ entonces $C_{[u)}(x) = [x, x \vee -u]$.* (L. Monteiro, 1996.)

Dem. Sea $y \in [x, x \vee -u]$, esto es (1) $x \leq y$ e (2) $y \leq x \vee -u$, entonces de (1) resulta $1 = x \vee -x \leq y \vee -x$ por lo tanto (3) $-x \vee y = 1 \in [u)$.
De (2) resulta $-x \wedge u \leq -y$ y por lo tanto $x \vee (-x \wedge u) \leq x \vee -y$, luego (4) $x \vee u = 1 \wedge (x \vee u) = (x \vee -x) \wedge (x \vee u) \leq x \vee -y$. Como (5) $u \leq x \vee u$, entonces de (4) y (5) resulta $u \leq x \vee -y$ y como $u \in [u)$ y $[u)$ es un filtro tenemos (6) $x \vee -y \in [u)$. De (3) y (6) resulta que $y \equiv x$ (mód. $[u)$) y por lo tanto $[x, x \vee -u] \subseteq C(x)$.
Sea $y \in C_{[u)}(x)$ esto es $-x \vee y \in [u)$ y $x \vee -y \in [u)$, luego (7) $u \leq -x \vee y$, y (8) $u \leq x \vee -y$.

De (7) resulta $x \wedge -y \leq -u$ y en consecuencia $x \wedge -y \wedge u \leq -u \wedge u = 0$, por lo tanto $x \wedge -y \wedge u = 0$ y como por hipótesis $x \leq u$, tenemos finalmente $x \wedge -y = 0$, esto es $x \leq y$. De (8) se deduce $y \wedge -x \leq -u$ y por lo tanto $y \leq x \vee y = (x \vee y) \wedge (x \vee -x) = x \vee (y \wedge -x) \leq x \vee -u$. ■

Vimos que dada una relación de congruencia R sobre un álgebra de Boole A, a R le corresponde un filtro de A, a saber $F = C_R(1)$. Pongamos:

$$\Psi(R) = C_R(1).$$

Recíprocamente dado un filtro F de A, él induce una relación de congruencia sobre A , a saber " $a \equiv b$ (mód. F) $\iff a \wedge f = b \wedge f$ donde $f \in F$", y $\Psi(\equiv) = C_{\equiv}(1) = F$. Por lo tanto Ψ es suryectiva.
Supongamos ahora que R_1 y R_2 son dos relaciones de congruencia sobre A tales que $R_1 \neq R_2$, luego existen $a, b \in A$ tales que $a\ R_1\ b$ y $a \not R_2\ b$ (ó $a\ R_2\ b$ y $a \not R_1\ b$). En el primer caso $a\ R_1\ b \iff -a \vee b, -b \vee a \in C_{R_1}(1)$. Si $C_{R_1}(1) = C_{R_2}(1)$, entonces $-a\vee b, -b\vee a \in C_{R_2}(1)$ esto es $a\ R_2\ b$ absurdo. En el otro caso la demostración es análoga. Acabamos así de probar que Ψ es biyectiva, por lo tanto existe una biyección entre relaciones de congruencia sobre un álgebra de Boole A y la familia de todos los filtros de A.

Dada un álgebra de Boole A las siguientes relaciones binarias son relaciones de congruencia sobre A:

1) $x\ I\ y \iff x = y$, (**Relación Identidad**).

2) $x\ U\ y\ \forall\ x, y \in A$, (**Relación Universal**).

Estas dos relaciones se denominan **relaciones triviales**. En el primer caso tenemos $C_I(x) = \{x\}$ cualquiera que sea $x \in A$ y en el segundo caso $C_U(x) = A$ cualquiera que sea $x \in A$.
Observemos que si A tiene un sólo elemento entonces $I = U$ y que esta es la única relación de congruencia que se puede definir sobre A, y si A tiene más de un elemento entonces $I \neq U$, y la función Ψ definida precedentemente verifica:

$$\Psi(I) = C_I(1) = \{1\} = [1) \quad \text{y} \quad \Psi(U) = C_U(1) = A = [0).$$

Se plantea en forma natural la siguiente pregunta ¿Cuáles son las álgebras de Boole, con mas de un elemento, en las cuales las únicas relaciones de congruencia son I y U?

Definición 4.6.6 *Un álgebra de Boole A se dice* **simple** *si:*

1) A tiene mas de un elemento (esto es, A no es trivial)

2) Las únicas relaciones de congruencia sobre A son las triviales.

Lema 4.6.29 *Un álgebra de Boole A es simple sss*

1) A no es trivial.

2) Los únicos filtros de A son $[1) = \{1\}$ *y* $[0) = A$.

Dem. Es una consecuencia inmediata de la biyección existente entre las relaciones de congruencia sobre A y la familia de todos los filtros de A. ■

Lema 4.6.30 *Un álgebra de Boole A es simple sss*

1) A no es trivial.

2) Las únicas imágenes homomórficas de A son isomorfas a A ó a un álgebra trivial.

Dem. $\Longrightarrow$) Por hipótesis $[1) = \{1\}$ y $[0) = A$ son los únicos filtros de A y como todas las imágenes homomórficas de A se obtienen (a menos de isomorfismo) haciendo el cociente de A por un filtro de A, las únicas imágenes homomórficas de A son isomorfas a $A/[1) \cong A$ ó a $A/[0) \cong \{0\}$.
$\Longleftarrow$) Supongamos que A no es trivial y que las únicas imágenes homomórficas A' de A son isomorfas a A ó a un álgebra con un sólo elemento $\{0\}$. Sea $h : A \to A'$ el isomorfismo en cuestión. Sabemos que $x \; R_h \; y \iff h(x) = h(y)$ es una relación de congruencia, luego como h es biunívoca $x \; R_h \; y \iff x = y$. En el caso que $A' \cong A$ tendremos que $R_h = I$, y en el caso que $A' \cong \{0\}$ tendremos $x \; R_h \; y, \; \forall \; x, y \in A \iff R_h = U$. ■

Lema 4.6.31 *Las únicas álgebras de Boole simples son isomorfas a* $\{0, 1\}$.

Dem. Es claro que $B = \{0, 1\}$ es un álgebra de Boole simple. Si B tiene más de dos elementos, existe $x \in B$, $x \neq 0$, $x \neq 1$, por lo tanto el filtro $[x)$ verifica $[x) \neq [1)$, $[x) \neq [0) = B$, y en consecuencia B no es simple. ■

4.7 Teoría de filtros

En este párrafo, salvo mención en contrario, vamos a considerar reticulados R con último elemento 1. Entonces:

Lema 4.7.1 *Si $\{F_i\}_{i \in I}$ es una familia de filtros de R entonces $F = \bigcap_{i \in I} F_i$ es un filtro de R.*

Sea $G \subseteq R$ y $\{F_i\}_{i \in I}$ la familia de todos los filtros de R que contienen a G. Esta familia no es vacia ya que R es uno de sus elementos. Por el Lema 4.7.1, $F(G) = \bigcap_{i \in I} F_i$ es un filtro y es claro que $G \subseteq F(G)$, y $F(G)$ es el menor filtro que contiene a G. $F(G)$ se denomina **filtro generado por** G.
Observemos que si $G = \emptyset$ entonces $F(\emptyset) = \{1\}$ y que si $G = \{1\}$ también $F(\{1\}) = \{1\}$.

Lema 4.7.2 *Si G es una parte no vacía de R y*

$$H = \{x \in R : \text{ existen } g_1, g_2, \ldots, g_t \in G \text{ tales que } \bigwedge_{i=1}^{t} g_i \leq x\}$$

entonces $F(G) = H$.

Dem.

1) $H \subseteq F(G)$.
Sea $x \in H$, luego existen (1) $g_1, g_2, \dots, g_t \in G$ tales que (2) $\bigwedge_{i=1}^{t} g_i \leq x$. Como (3) $G \subseteq F(G)$ de (1) y (3) resulta (4) $g_1, g_2, \dots, g_t \in F(G)$, luego como $F(G)$ es un filtro tenemos que (5) $\bigwedge_{i=1}^{t} g_i \in F(G)$. De (5) y (2) resulta por ser $F(G)$ un filtro que $x \in F(G)$.

2) $F(G) \subseteq H$.

2a) $G \subseteq H$.
Sea $g \in G$, entonces como $g \wedge g \leq g$ tenemos que $g \in H$.

2b) H es un filtro.
Como $g \wedge g \leq 1$ cualquiera que sea $g \in G$ entonces $1 \in H$. Si $x, y \in H$ entonces $\bigwedge_{i=1}^{s} g_i \leq x$, donde $g_i \in G$ para $1 \leq i \leq s$ y $\bigwedge_{j=1}^{t} g_j^{'} \leq y$, donde $1 \leq i \leq s$ y $g_j^{'} \in G$ para $1 \leq j \leq t$, luego:

$$\bigwedge_{i=1}^{s} g_i \wedge \bigwedge_{j=1}^{t} g_j^{'} \leq x \wedge y$$

y por lo tanto $x \wedge y \in H$.
Si $x \in H$ e $y \in R$ verifica (1) $x \leq y$ entonces (2) $\bigwedge_{i=1}^{s} g_i \leq x$, donde (3) $g_i \in G$ para $1 \leq i \leq s$. De (1) y (2) resulta $\bigwedge_{i=1}^{s} g_i \leq y$, luego por (3) $y \in H$.

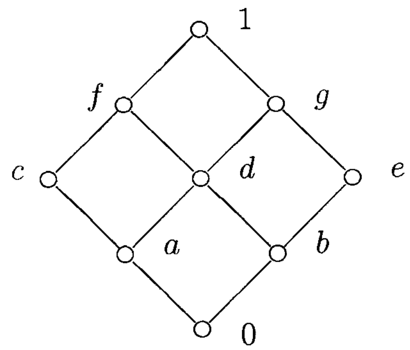
De 2a) y 2b) resulta 2)

■

Lema 4.7.3 *Si G es una parte finita no vacía de R, entonces $F(G)$ es un filtro principal de R y recíprocamente, todo filtro principal de R tiene un conjunto finito de generadores.*

Dem. Sea $G = \{g_1, g_2, \dots, g_t\}$ y $g = \bigwedge_{i=1}^{t} g_i$. Probemos que $[g) = F(G)$. En efecto, si $y \in F(G)$ entonces por el Lema 4.7.2 $\bigwedge_{j=1}^{s} g_j^{'} \leq y$, donde $g_j^{'} \in G$ para $1 \leq j \leq s$, luego como $g = \bigwedge_{i=1}^{t} g_i \leq \bigwedge_{j=1}^{s} g_j^{'} \leq y$, resulta $y \in [g)$. Recíprocamente si $y \in [g)$ entonces $g = \bigwedge_{i=1}^{t} g_i \leq y$, luego por el Lema 4.7.2 $y \in F(G)$. Supongamos ahora que F es un filtro principal, esto es $F = [g)$, donde $g \in R$, luego $y \in [g) \iff g \leq y$ lo que equivale a decir, teniendo en cuenta el Lema 4.7.2 que $y \in F(\{g\})$, por lo tanto $[g) = F(\{g\})$. ■

Ejemplo 4.7.1 *Sea R el reticulado cuyo diagrama se indica, $G = \{f, g\}$ entonces $F(G) = F(\{f \wedge g\}) = [f \wedge g) = [d)$.*



Si R es un reticulado, sin último elemento, un subconjunto, no vacío, F de R se dice un filtro de R si se verifican: F2) Si $x, y \in F$ entonces $x \wedge y \in F$ y F3) Si $x \in F$, e $y \in R$ verifica $x \leq y$ entonces $y \in F$.
Observemos que cualquiera que sea el elemento x del reticulado R entonces $[x)$ es un filtro de R.

Definición 4.7.1 *Un filtro F de un reticulado R, no necesariamente con último elemento, se dice* **propio** *si $F \neq R$.*

Lema 4.7.4 *Si R es un reticulado con primer elemento 0 entonces: F propio $\Longleftrightarrow$ $0 \notin F$*

Dem. $\Longrightarrow$) Si $0 \in F$ entonces como $0 \leq x$ para todo $x \in R$ tendríamos que $x \in F$ para todo $x \in R$ y por lo tanto $F = R$, absurdo.
$\Longleftarrow$) Si $0 \notin F$ entonces $F \neq R$. ■

Definición 4.7.2 *Se dice que una parte no vacía X de un reticulado R con primer elemento 0 tiene la* **propiedad de intersección finita** (PIF) *si el ínfimo de cualquier familia finita, no vacía, de elementos de X es diferente del elemento 0. Esto es si $x_1, x_2, \ldots, x_n \in X$ entonces $\bigwedge_{i=1}^{n} x_i \neq 0$.*

Observemos que si el conjunto X verifica que existe $\bigwedge_{x \in X} x$ y $\bigwedge_{x \in X} x \neq 0$ entonces X tiene la PIF, dado que si $\emptyset \neq Y \subseteq X$, Y finito, entonces $0 \neq \bigwedge_{x \in X} x \leq \bigwedge_{y \in Y} y$.

Lema 4.7.5 *Sea un reticulado R con primer elemento 0, y $\emptyset \neq G \subseteq R$ entonces $F(G)$ es un filtro propio $\Longleftrightarrow$ G tiene la PIF.*

Dem. $\Longrightarrow$) Sean $g_1, g_2, \ldots, g_t \in G$ y supongamos que $\bigwedge_{i=1}^{t} g_i = 0$, entonces como $G \subseteq F(G)$ resulta que $g_1, g_2, \ldots, g_t \in F(G)$, y como $F(G)$ es un filtro entonces $0 \in F(G)$. Absurdo.
$\Longleftarrow$) Si $0 \in F(G)$ entonces existen elementos $g_1, g_2, \ldots, g_t \in G$ tales que $\bigwedge_{i=1}^{t} g_i \leq 0$ y por lo tanto $\bigwedge_{i=1}^{t} g_i = 0$. ■

Representemos con $\mathcal{F}(R)$ el conjunto de todos los filtros de un reticulado no trivial R.

Definición 4.7.3 *Un filtro F de R se dice* **irreducible** *si*

1) F *es propio.*

2) *Si* $F = F_1 \cap F_2$ *donde* $F_1, F_2 \in \mathcal{F}(R)$ *entonces* $F = F_1$ *ó* $F = F_2$.

y se dice **completamente irreducible** *si*

1) F *es propio.*

2) *Si* $F = \bigcap_{i \in I} F_i$ *donde* $F_i \in \mathcal{F}(R)$ $\forall\, i \in I$ *entonces existe* $i_0 \in I$ *tal que* $F = F_{i_0}$.

De acuerdo con este definición es claro que todo filtro completamente irreducible es irreducible.

Observación 4.7.1 *Si R es una cadena y $x \in R$ es tal que $[x)$ es un filtro propio entonces $[x)$ es irreducible. Supongamos que $[x) = F_1 \cap F_2$, donde F_1 y F_2 son filtros de R, y que $[x) \neq F_1$ y $[x) \neq F_2$. Como $[x) = F_1 \cap F_2 \subseteq F_1$ y $[x) = F_1 \cap F_2 \subseteq F_2$ entonces tenemos que $[x) \subset F_1$ y $[x) \subset F_2$. Sean $f_1 \in F_1 \setminus [x)$ y $f_2 \in F_2 \setminus [x)$. De $f_1, f_2 \notin [x)$ resulta por ser R una cadena que f_1, $f_2 < x$ y por lo tanto $f_1 \vee f_2 \leq x$. Como $f_1 \leq f_1 \vee f_2$, $f_2 \leq f_1 \vee f_2$, $f_1 \in F_1$, $f_2 \in F_2$ y F_1 y F_2 son filtros de R resulta que $f_1 \vee f_2 \in F_1$ y $f_1 \vee f_2 \in F_2$. Por lo tanto $f_1 \vee f_2 \in F_1 \cap F_2 = [x)$ y en consecuencia (2) $x \leq f_1 \vee f_2$. De (1) y (2) resulta que $x = f_1 \vee f_2$, y como R es una cadena $f_2 \leq f_1$ ó $f_1 \leq f_2$ luego $x = f_1$ ó $x = f_2$ y por lo tanto $f_1 \in [x)$ ó $f_2 \in [x)$.*

Definición 4.7.4 *Dado un subconjunto $\{x_i\}_{i \in I}$ de elementos de un reticulado R se dice que $s \in R$ es el supremo de dicho subconjunto y se nota $s = \bigvee_{i \in I} x_i$ si se verifican:*

SG1) $x_i \leq s$ *para todo* $i \in I$.

SG2) Si $y \in R$ *verifica* $x_i \leq y$ *para todo* $i \in I$, *entonces* $s \leq y$.

Lema 4.7.6 *Si R es un reticulado y $\{x_i\}_{i \in I} \subseteq R$ es tal que existe $x = \bigvee_{i \in I} x_i$ entonces $[x) = [\bigvee_{i \in I} x_i) = \bigcap_{i \in I} [x_i)$.*

Dem. Sea $y \in [x)$ esto es $x \leq y$. Como $x_i \leq \bigvee_{i \in I} x_i = x$, para todo $i \in I$ entonces $x_i \leq y$ para todo $i \in I$, esto es $y \in [x_i)$ para todo $i \in I$, y por lo tanto $y \in \bigcap_{i \in I} [x_i)$. Recíprocamente si $y \in \bigcap_{i \in I} [x_i)$, entonces $y \in [x_i)$ para todo $i \in I$, esto es $x_i \leq y$ para todo $i \in I$, y por lo tanto $x = \bigvee_{i \in I} x_i \leq y$, esto es $y \in [x)$. ∎

Corolario 4.7.1 *Si R es un reticulado y $a, b \in R$ entonces $[a \vee b) = [a) \cap [b)$.*

Observación 4.7.2 *Sabemos que el conjunto $\mathbb{R}$ de los números reales forman un reticulado distributivo. Sea $x \in \mathbb{R}$ e $Y = \{y \in \mathbb{R} : y < x\}$. Probemos que (i) $x = \bigvee_{y \in Y} y$.*
Por hipótesis $y \leq x$, $\forall\, y \in Y$, luego x es una cota superior de Y. Supongamos que (ii) $y \leq x'$, $\forall\, y \in Y$ y probemos que $x \leq x'$. En efecto caso contrario, como $\mathbb{R}$ es una cadena, tendríamos $x' < x$, luego existe $r \in \mathbb{R}$ tal que $x' < r < x$. De $r < x$ resulta que $r \in Y$ luego por (ii) $r \leq x'$. Tenemos así que $x' < r$ y $r \leq x'$, absurdo.
De (i) resulta que $[x) = \bigcap_{y \in Y} [y)$ y por lo tanto $[x) \neq [y)$ para todo $y \in Y$, esto es $[x)$ no es un filtro completamente irreducible.
Como $[x) \neq \mathbb{R}$ y $\mathbb{R}$ es una cadena, podemos afirmar en virtud de la Observación 4.7.1 que $[x)$ es un filtro irreducible.

Si R es un reticulado, $F \in \mathcal{F}(R)$ y $a \in R$ representaremos con $F(F, a)$ el filtro generado por el conjunto $F \cup \{a\}$.

Lema 4.7.7 *Si $F \in \mathcal{F}(R)$ y $T = \{t \in R :$ existe $f \in F$ tal que $a \wedge f \leq t\}$ entonces $F(F, a) = T$.*

Dem. Sea $t \in F(F, a)$, por el Lema 4.7.2 sabemos que existe $G = \{g_1, g_2, \ldots, g_s\} \subseteq F \cup \{a\}$ tal que $\bigwedge_{i=1}^{s} g_i \leq t$.

1) Si $G \subseteq F$ entonces $h = \bigwedge_{i=1}^{s} g_i \in F$, luego $a \wedge h \leq h \leq t$, donde $h \in F$, de donde resulta que $t \in T$.

2) Si $G \subseteq \{a\}$ entonces $h = \bigwedge_{i=1}^{s} g_i = a$, luego $a \wedge f \leq a = h \leq t$, cualquiera que sea $f \in F$, y por lo tanto $t \in T$.

3) Si $G \cap F \neq \emptyset$ y $G \cap \{a\} \neq \emptyset$, entonces $\bigwedge_{g_i \in G \cap F} g_i \wedge a = \bigwedge_{i=1}^{s} g_i \leq t$, y como $\bigwedge_{g_i \in G \cap F} g_i \in F$, entonces $t \in T$.

Recíprocamente, si $t \in T$ entonces existe $f \in F$ tal que (1) $f \wedge a \leq t$. Como $f, a \in F \cup \{a\} \subseteq F(F, a)$ entonces (2) $f \wedge a \in F(F, a)$. De (1) y (2) resulta $t \in F(F, a)$. ∎

Corolario 4.7.2 *Si R es un reticulado y $a, b \in R$ entonces $F([b), a) = [a \wedge b)$.*

Dem. Sea $t \in F([b), a)$ entonces por el Lema 4.7.7: (1) $f \wedge a \leq t$ donde $f \in [b)$, esto es (2) $b \leq f$.
De (1) resulta $f \wedge a \wedge b \leq b \wedge t \leq t$, luego teniendo en cuenta (2) tenemos $a \wedge b \leq t$ y por lo tanto $t \in [a \wedge b)$.
Sea $t \in [a \wedge b)$, esto es $a \wedge b \leq t$, luego como $b \in [b)$ tenemos por el Lema 4.7.7 que $t \in F([b), a)$. ∎

Lema 4.7.8 *Si R es un reticulado y $a, b \in R$ entonces $F([a) \cup [b)) = F([a), b)$.*

Dem. Sean $F_1 = F([a) \cup [b))$ y $F_2 = F([a), b)$. Como

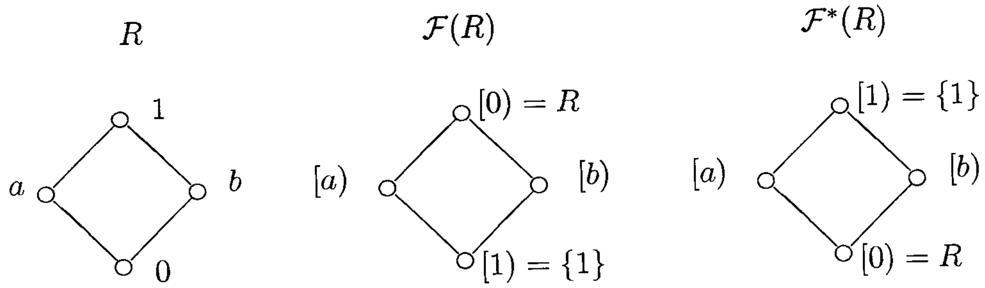
$$[a) \cup \{b\} \subseteq [a) \cup [b) \subseteq F([a) \cup [b)) = F_1$$

entonces $F_2 = F([a), b) \subseteq F_1$. Probemos ahora que $F_1 \subseteq F_2$. En efecto, $[a) \subseteq [a) \cup \{b\} \subseteq F([a), b)$ luego (1) $[a) \subseteq F([a), b)$. Sea $x \in [b)$, esto es $b \leq x$ luego como $b \in F([a), b)$ tenemos que $x \in F([a), b)$, por lo tanto (2) $[b) \subseteq F([a), b)$. De (1) y (2) resulta que $[a) \cup [b) \subseteq F([a), b)$ y en consecuencia $F_1 = F([a) \cup [b)) \subseteq F([a), b) = F_2$. ■

Corolario 4.7.3 *Si R es un reticulado y $a, b \in R$ entonces $F([a) \cup [b)) = [a \wedge b)$.*

Dem. Es una consecuencia inmediata del Lema 4.7.8 y el Corolario 4.7.2. ■

Vamos a indicar algunas propiedades del conjunto $\mathcal{F}(R)$. Es claro que $(\mathcal{F}(R), \subseteq)$ es un conjunto ordenado, que tiene último elemento R, y primer elemento $[1) = \{1\}$. Análogamente $(\mathcal{F}(R), \supseteq)$ es un conjunto ordenado, que tiene primer elemento R y último elemento $[1) = \{1\}$. Además $(\mathcal{F}(R), \subseteq)^* \cong (\mathcal{F}(R), \supseteq)$. De ahora en adelante para referirnos a estos conjuntos ordenados, notaremos mas sencillamente $\mathcal{F}(R)$ y $\mathcal{F}^*(R)$.



Observemos que si R no tiene último elemento entonces $\mathcal{F}(R)$ no tiene primer elemento. En efecto, si $\mathcal{F}(R)$ tuviese primer elemento entonces existiría un filtro P tal que (1) $P \subseteq F$ cualquiera que sea $F \in \mathcal{F}(R)$. Este filtro sólo puede contener un elemento, en efecto, sean $x, y \in P$, luego teniendo en cuenta (1) $y \in P \subseteq [x)$ y $x \in P \subseteq [y)$, entonces $x \leq y$ e $y \leq x$, esto es $x = y$. Por lo tanto $P = \{p\}$, luego por (1) $\{p\} \subseteq [r)$ para todo $r \in R$, esto es $r \leq p$ para todo $r \in R$ y en consecuencia p sería último elemento de R, absurdo.

Si ponemos por definición $h(x) = [x)$, donde $x \in R$ entonces h es una función de R en $\mathcal{F}(R)$ que verifica:

$$x \leq y \iff h(x) = [x) \supseteq [y) = h(y).$$

Observemos que esta función no es necesariamente suryectiva. En efecto, en el conjunto de los números reales $\mathbb{R}$ dado $x_0 \in \mathbb{R}$, el conjunto $F = \{y \in \mathbb{R} : x_0 < y\}$ es un filtro que no es principal.

Representemos con $\mathcal{FP}(R)$ el conjunto de todos los filtros principales de un reticulado distributivo R, entonces h es una función suryectiva de R en $\mathcal{FP}(R)$ y por lo tanto h es un antiisomorfismo de orden de $(R, \leq)$ en $(\mathcal{FP}(R), \subseteq)$ y un isomorfismo de orden de $(R, \leq)$ en $(\mathcal{FP}(R), \supseteq)$. Luego en el caso en que R es finito tenemos:

$$(R, \leq) \cong (\mathcal{FP}(R), \subseteq)^* = (\mathcal{FP}(R), \supseteq).$$

Si $F_1, F_2 \in \mathcal{F}(R)$ pongamos por definición:

$$F_1 \sqcap F_2 = F_1 \cap F_2$$

entonces es claro que $F_1 \sqcap F_2$ es el ínfimo de los elementos F_1 y F_2 del conjunto ordenado $(\mathcal{F}(R), \subseteq)$. Pero no podemos afirmar que $F_1 \cup F_2$ es el supremo de estos elementos pues en general $F_1 \cup F_2$ no es un filtro.

Lema 4.7.9 *El supremo de dos filtros de R es el filtro generado por su unión.*

Dem. En efecto, $F_1 \subseteq F_1 \cup F_2 \subseteq F(F_1 \cup F_2)$ y $F_2 \subseteq F_1 \cup F_2 \subseteq F(F_1 \cup F_2)$, luego $F(F_1 \cup F_2)$ es una cota superior del conjunto $\{F_1, F_2\}$. Supongamos ahora que $F \in \mathcal{F}(R)$ verifica $F_1 \subseteq F$ y $F_2 \subseteq F$, luego $F_1 \cup F_2 \subseteq F$ y por lo tanto $F(F_1 \cup F_2) \subseteq F$. ∎

$$\text{Notaremos } F_1 \sqcup F_2 = F(F_1 \cup F_2).$$

Acabamos así de probar que el conjunto ordenado $(\mathcal{F}(R), \subseteq)$ es un reticulado con primer elemento $[1)$ y último elemento R.

NOTACION: Si X e Y son subconjuntos de un reticulado R pongamos:

$$X \wedge Y = \{x \wedge y : x \in X,\ y \in Y\}.$$

Lema 4.7.10 *Si F_1 y F_2 son filtros de un reticulado distributivo R entonces $F_1 \wedge F_2$ es un filtro de R y $F(F_1 \cup F_2) = F_1 \wedge F_2$.*

Dem.

1) $F_1 \wedge F_2$ es un filtro.
   Como $1 \in F_1, F_2$ entonces F1) $1 = 1 \wedge 1 \in F_1 \wedge F_2$. Sean $x, y \in F_1 \wedge F_2$ entonces $x = f_1 \wedge f_2$, $y = g_1 \wedge g_2$ donde $f_1, g_1 \in F_1$, $f_2, g_2 \in F_2$, y por lo tanto $x \wedge y = (f_1 \wedge g_1) \wedge (f_2 \wedge g_2)$ donde $f_1 \wedge g_1 \in F_1$ y $f_2 \wedge g_2 \in F_2$ luego, $x \wedge y \in F_1 \wedge F_2$. Si $x \in F_1 \wedge F_2$ e $y \in R$ verifica $x \leq y$ entonces $x = f_1 \wedge f_2$, e $y = y \vee x = y \vee (f_1 \wedge f_2) = (y \vee f_1) \wedge (y \vee f_2)$. Como $f_1 \in F_1$ $(f_2 \in F_2)$ entonces $y \vee f_1 \in F_1$ e $y \vee f_2 \in F_2$ y en consecuencia $y \in F_1 \wedge F_2$.

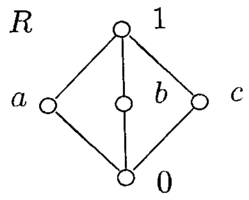
2) $F_1 \wedge F_2 \subseteq F(F_1 \cup F_2)$.
   Sea $f \in F_1 \wedge F_2$ luego $f = f_1 \wedge f_2$ donde $f_1 \in F_1$ y $f_2 \in F_2$. Como $F_1 \subseteq F_1 \cup F_2 \subseteq F(F_1 \cup F_2)$ y $F_2 \subseteq F_1 \cup F_2 \subseteq F(F_1 \cup F_2)$, entonces $f = f_1 \wedge f_2 \in F(F_1 \cup F_2)$.

3) $F_1 \cup F_2 \subseteq F_1 \wedge F_2$.
   $F_1 \subseteq F_1 \wedge F_2$.
   Si $f \in F_1$ entonces $f = f \wedge (f \vee f_2)$ cqs $f_2 \in F_2$ y como $f_2 \in F_2$ tenemos que $f \vee f_2 \in F_2$. Por lo tanto $f \in F_1 \wedge F_2$, luego (i) $F_1 \subseteq F_1 \wedge F_2$. En forma análoga se demuestra (ii) $F_2 \subseteq F_1 \wedge F_2$. De (i) e (ii) resulta (3).

4) $F(F_1 \cup F_2) \subseteq F_1 \wedge F_2$.
   Es una consecuencia inmediata de 1) y 3)

La parte 4) de este lema también se puede demostrar usando el Lema 4.7.2. ∎

El lema anterior no vale si el reticulado no es distributivo. En efecto, consideremos el reticulado R cuyo diagrama se indica:



entonces $[a) = \{a, 1\}$, $[c) = \{c, 1\}$ y $[a) \wedge [c) = \{a \wedge c, a \wedge 1, 1 \wedge c, 1 \wedge 1\} = \{0, a, c, 1\}$ no es un filtro de R. Observemos que $F([a) \cup [c)) = R$.

Lema 4.7.11 *El conjunto $\mathcal{F}(R)$ de todos los filtros de un reticulado distributivo R con último elemento, ordenado por inclusión es un reticulado distributivo con primer y último elemento.*

Dem. Para ello basta probar que:

$$F_1 \sqcap (F_2 \sqcup F_3) = (F_1 \sqcap F_2) \sqcup (F_1 \sqcap F_3).$$

Pero sabemos que en todo reticulado vale

$$(F_1 \sqcap F_2) \sqcup (F_1 \sqcap F_3) \subseteq F_1 \sqcap (F_2 \sqcup F_3).$$

Probemos que

$$F_1 \sqcap (F_2 \sqcup F_3) \subseteq (F_1 \sqcap F_2) \sqcup (F_1 \sqcap F_3)$$

esto es que

$$F_1 \cap (F_2 \sqcup F_3) \subseteq (F_1 \cap F_2) \sqcup (F_1 \cap F_3)$$

y por lo tanto debemos probar

$$F_1 \cap (F_2 \wedge F_3) \subseteq (F_1 \cap F_2) \wedge (F_1 \cap F_3)$$

Sea $f \in F_1 \cap (F_2 \wedge F_3)$, luego $f \in F_1$ y $f = f_2 \wedge f_3$ donde $f_2 \in F_2$ y $f_3 \in F_3$. Como $f \leq f \vee f_2$, $f \in F_1$ y F_1 es un filtro tenemos $f \vee f_2 \in F_1$ y análogamente como $f_2 \leq f \vee f_2$, $f_2 \in F_2$ y F_2 es un filtro resulta que $f \vee f_2 \in F_2$. Por lo tanto $f \vee f_2 \in F_1 \cap F_2$. Análogamente se prueba que $f \vee f_3 \in F_1 \cap F_3$, y por lo tanto

$$(f \vee f_2) \wedge (f \vee f_3) \in (F_1 \cap F_2) \wedge (F_1 \cap F_3),$$

luego como R es distributivo

$$f \vee (f_2 \wedge f_3) \in (F_1 \cap F_2) \wedge (F_1 \cap F_3),$$

y como $f = f_2 \wedge f_3$ entonces $f \vee (f_2 \wedge f_3) = f$ lo que prueba que

$$f \in (F_1 \cap F_2) \wedge (F_1 \cap F_3).$$

■

Vimos que si a, b son elementos de un reticulado R:

$$(1) \quad [a) \sqcap [b) = (\text{por def.}) = [a) \cap [b) = (\text{por Corolario 4.7.1}) = [a \vee b).$$

$$(2) \quad [a) \sqcup [b) = (\text{por def.}) = F([a) \cup [b)) = (\text{por Corolario 4.7.3}) = [a \wedge b).$$

Probemos que si $a, b \in R$, donde R es un reticulado distributivo entonces:

$$(3) \quad [a) \wedge [b) = [a \wedge b).$$

En efecto, $[a) \wedge [b) = (\text{por Lema 4.7.10}) = F([a) \cup [b)] = (\text{por }(1)) = F([a \wedge b)) = [a \wedge b)$.
De aquí resulta que en los reticulados distributivos:

$$[a) \sqcup [b) = [a \wedge b) = [a) \wedge [b).$$

Observación 4.7.3 *Si R no es distributivo, no podemos afirmar que $[a) \wedge [b) = [a \wedge b)$. En efecto consideremos el reticulado R indicado precedentemente. Entonces $[a) \wedge [b) = \{0, a, b, 1\}$ y $[a \wedge b) = R$.*

Teorema 4.7.1 *Sea R un reticulado no trivial tal que el conjunto de todos los filtros de R, ordenado por $\subseteq$ es un reticulado distributivo, entonces R es distributivo.*

Dem. Como

$$[a) \sqcap ([b) \sqcup [c)) = ([a) \sqcap [b)) \sqcup ([a) \sqcap [c)),$$

entonces por el Corolario 4.7.3 $[b) \sqcup [c) = F([b) \cup [c)) = [b \wedge c)$ y por el Corolario 4.7.1 $[a) \sqcap [b) = [a) \cap [b) = [a \vee b)$, y análogamente $[a) \sqcap [c) = [a \vee c)$ luego

$$[a) \sqcap [b \wedge c) = [a \vee b) \sqcup [a \vee c),$$

y por lo tanto teniendo en cuenta nuevamente los Corolarios 4.7.1 y 4.7.3 tenemos

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

luego

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

■

Lema 4.7.12 *Si $\{F_i\}_{i \in I}$ es <u>una cadena de filtros</u> de un reticulado R entonces $F = \bigcup_{i \in I} F_i$ es un filtro de R.*

Sea F un filtro propio de R y $b \notin F$, notaremos

$$\mathcal{F}(F, b) = \{F' \in \mathcal{F}(R) : F \subseteq F', b \notin F'\}$$

Es claro que $F \in \mathcal{F}(F, b)$ y que $(\mathcal{F}(F, b), \subseteq)$ es un conjunto ordenado.
Veamos que este conjunto es **inductivo superiormente**, esto es que toda cadena $\mathcal{K}$ de elementos del conjunto $\mathcal{F}(F, b)$ tiene una cota superior en $\mathcal{F}(F, b)$ (Observación: la recta $\mathbb{R}$ con su orden natural no es un conjunto inductivo superiormente, $\mathbf{R}$ es una cadena de $\mathbb{R}$ y no tiene cota superior en $\mathbb{R}$).

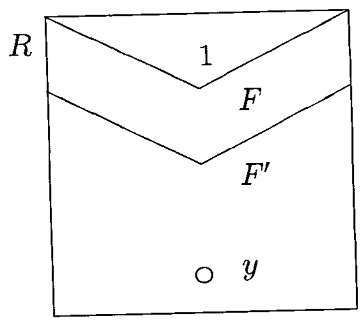
Sea $\mathcal{K} = \{F_i\}_{i\in I}$ una cadena de $\mathcal{F}(F, b)$ y consideremos el conjunto $F' = \bigcup_{i\in I} F_i$, entonces por el Lema 4.7.12 (1) $F' \in \mathcal{F}(R)$, ademas (2) $b \notin F'$, ya que $b \notin F_i$ cualquiera que sea $i \in I$. Como $F \subseteq F_i$ para todo $i \in I$ entonces (3) $F \subseteq \bigcup_{i\in I} F_i = F'$, y por lo tanto de (1) y (2) resulta que (4) $F' \in \mathcal{F}(F, b)$, y de (3) y (4) que F' es una cota superior de $\mathcal{K}$ que pertenece al conjunto $\mathcal{F}(F, b)$. Observemos que F' es un filtro propio de R ya que $b \notin F'$. Como el conjunto $\mathcal{F}(F, b)$ es inductivo superiormente, por el lema de Zorn, podemos afirmar que este conjunto tiene por lo menos un elemento máximo.

Si R es un reticulado no trivial y tiene último elemento 1, sea $y \in R$ tal que $y \neq 1$, entonces $[1) = \{1\}$ es un filtro de R que no contiene al elemento y. Sea $\mathcal{F}(y) = \mathcal{F}([1), y) = \{F' \in \mathcal{F}(R) : [1) \subseteq F', y \notin F'\} = \{F' \in \mathcal{F}(R) : y \notin F'\}$.
A cada elemento máximo de este conjunto ordenado daremos el nombre de **filtro ligado al elemento** y lo notaremos C_y.

Lema 4.7.13 *Sea $F \in \mathcal{F}(R)$ e $y \notin F$, entonces si M es un elemento máximo de $\mathcal{F}(F, y)$, M es un elemento máximo de $\mathcal{F}(y)$.*

Dem.

1) $\mathcal{F}(F, y) \subseteq \mathcal{F}(y)$.
Sea $F' \in \mathcal{F}(F, y)$, luego (i) $F \subseteq F'$ e (ii) $y \notin F'$. De (ii) resulta que (iii) $y \neq 1$, luego $F' \in \mathcal{F}(y)$.



2) Supongamos que M es un elemento máximo de $\mathcal{F}(F, y)$, en particular $M \in \mathcal{F}(F, y)$ entonces por 1) tenemos que $M \in \mathcal{F}(y)$. Si M no fuese un elemento máximo de $\mathcal{F}(y)$ existiría (i) $C \in \mathcal{F}(y)$ tal que (ii) $M \subset C$.
De (i) resulta (iii) $y \notin C$. Por hipótesis (iv) $F \subseteq M$, luego de (ii) y (iv) tenemos (v) $F \subset C$. De (v) y (iii), resulta por ser C un filtro que (vi) $C \in \mathcal{F}(F, y)$. Luego tenemos que $M \in \mathcal{F}(F, y)$, M máximo, $C \in \mathcal{F}(F, y)$ y $M \subset C$. Absurdo !!!

■

Observemos que la recíproca no es verdadera. Para ello consideremos el reticulado R indicado en la figura A. El conjunto ordenado $(\mathcal{F}(R), \subseteq)$ está indicado en la figura B. Los elementos del conjunto $\mathcal{F}(a)$ estan indicados con $\bullet$, por lo tanto $[b)$ y $[d)$ son los elementos máximos de $\mathcal{F}(a)$.
Los elementos del conjunto $\mathcal{F}([c), a)$ estan indicados con $\square$, luego $[d)$ es un elemento máximo de $\mathcal{F}(a)$ y no es máximo de $\mathcal{F}([c), a)$ ya que $[d) \notin \mathcal{F}([c), a)$.

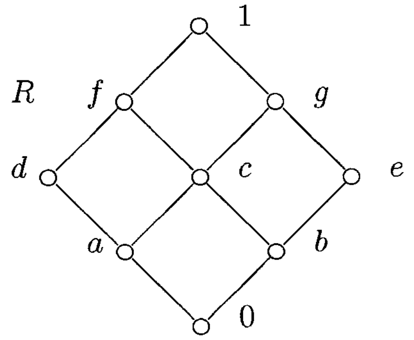


Figura A

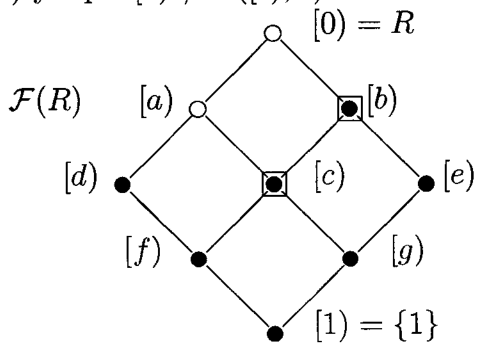


Figura B

Lema 4.7.14 *Si R es un reticulado, con último elemento 1, todo filtro C_y (ligado a un elemento $y \neq 1$) es completamente irreducible.*

Dem. Como $y \notin C_y$ entonces C_y es propio. Supongamos que $C_y = \bigcap_{i \in I} F_i$ donde $\{F_i\}_{i \in I}$ es una familia de filtros de R. Como $y \notin C_y$ existe $i_0 \in I$ tal que $y \notin F_{i_0}$, luego $F_{i_0} \in \mathcal{F}(y)$. Además, $C_y = \bigcap_{i \in I} F_i \subseteq F_{i_0}$ y como C_y es un elemento maximal de $\mathcal{F}(y)$ resulta que $C_y = F_{i_0}$. ■

Lema 4.7.15 *Todo filtro propio de un reticulado R, con último elemento, es intersección de filtros completamente irreducibles.*

Dem. Sea F un filtro propio de R, luego existe $r \in R$ tal que $r \notin F$. Por lo tanto, existe un elemento máximo M de $\mathcal{F}(F, r)$ y en consecuencia M es máximo de $\mathcal{F}(r)$ esto es $M = C_r$. Además $F \subseteq C_r$.
Luego, para cada $r \notin F$ existe un C_r tal que $F \subseteq C_r$ y por lo tanto $F \subseteq \bigcap_{r \notin F} C_r$. Probemos que (1) $\bigcap_{r \notin F} C_r \subseteq F$. Probar (1) es equivalente a probar que $\complement F \subseteq \complement(\bigcap_{r \notin F} C_r) = \bigcup_{r \notin F} \complement C_r$.
Sea $y \in \complement F$ entonces $y \notin F$ luego, $y \notin C_y$ y en consecuencia $y \in \complement C_y \subseteq \bigcup_{r \notin F} \complement C_r$. ■

Corolario 4.7.4 *Todo filtro propio de un reticulado R, con último elemento, es intersección de filtros irreducibles.*

Dem. Basta observar que todo filtro propio completamente irreducible es irreducible. ■

Definición 4.7.5 *Un filtro F de un reticulado R, no necesariamente con último elemento, se dice* **primo** *si :*

P1) F es propio.

P2) Si $x \vee y \in F$ entonces $x \in F$ ó $y \in F$.

Representaremos con $\mathcal{P}(R)$ el conjunto de todos los filtros primos de un reticulado R. El filtro $[c)$ del reticulado indicado precedentemente en la Figura A, no es primo dado que $c = a \vee b \in [c)$ y $a \notin [c)$, $b \notin [c)$.

Lema 4.7.16 *Si F es un filtro primo de un reticulado R, no necesariamente con último elemento, entonces F es un filtro irreducible.*

Dem. Como por hipótesis F es primo, en particular, F es propio. Supongamos que $F = F_1 \cap F_2$ donde $F_1, F_2 \in \mathcal{F}(R)$ y supongamos que (1) $F \neq F_1$, (2) $F \neq F_2$. Como (3) $F = F_1 \cap F_2 \subseteq F_1$, y (4) $F = F_1 \cap F_2 \subseteq F_2$, entonces de (1) y (3) resulta $F \subset F_1$ y de (2) y (4) que $F \subset F_2$. Sean $f_1 \in F_1 \setminus F$, $f_2 \in F_2 \setminus F$. Como $f_1 \leq f_1 \vee f_2$, $f_1 \in F_1$ y F_1 es un filtro resulta que $f_1 \vee f_2 \in F_1$. Análogamente, de $f_2 \leq f_1 \vee f_2$, $f_2 \in F_2$ y F_2 filtro resulta que $f_1 \vee f_2 \in F_2$. Luego $f_1 \vee f_2 \in F_1 \cap F_2 = F$ y como F es primo entonces $f_1 \in F$ ó $f_2 \in F$ absurdo. ■

Lema 4.7.17 *Todo filtro irreducible de un reticulado distributivo R, es un filtro primo.*

Dem. Por hipótesis I es propio. Supongamos que $x \vee y \in I$ y consideremos los filtros $F_1 = F(I, x)$, $F_2 = F(I, y)$, luego $I \subseteq F_1$ e $I \subseteq F_2$ en consecuencia $I \subseteq F_1 \cap F_2$.
Probemos que $F_1 \cap F_2 \subseteq I$. Sea $t \in F_1 \cap F_2$, esto es $t \in F(I, x)$ y $t \in F(I, y)$, luego por el Lema 4.7.7 tenemos que: (1) $i_1 \wedge x \leq t$ donde (2) $i_1 \in I$ y (3) $i_2 \wedge y \leq t$ donde (4) $i_2 \in I$.
Luego de (1) resulta :

$$i_1 \wedge i_2 \wedge x \leq t \wedge i_2 \leq t$$

y de (3):

$$i_1 \wedge i_2 \wedge y \leq t \wedge i_1 \leq t$$

Sea $i = i_1 \wedge i_2 \in I$, entonces (2) y (4) resulta por ser I un filtro que $i \in I$. Tenemos entonces que:

$$i \wedge x \leq t, \qquad i \wedge y \leq t$$

luego

$$(i \wedge x) \vee (i \wedge y) \leq t$$

esto es (5) $i \wedge (x \vee y) \leq t$. Pero como por hipótesis $x \vee y \in I$, y además $i \in I$ e I es un filtro, entonces (6) $i \wedge (x \vee y) \in I$. Luego, de (5) y (6) resulta teniendo en cuenta que I es un filtro que $t \in I$.
Acabamos así de probar que $I = F_1 \cap F_2$, luego como I es irreducible tenemos que $I = F_1$ ó $I = F_2$ y como $x \in F_1$ e $y \in F2$ tenemos que $x \in I$ ó $y \in I$, por lo tanto I es primo. ■

Tenemos así:

$$\begin{tikzcd}[column sep=huge, row sep=huge]
\begin{array}{c}\text{FILTRO}\\ \text{COMPLETAMENTE}\\ \text{IRREDUCIBLE}\end{array} \arrow[r, "\boxed{\textit{En reticulados}}"] & \text{FILTRO IRREDUCIBLE} \arrow[d, shift right, "\boxed{\begin{array}{c}\textit{En reticulados}\\ \textit{distributivos}\end{array}}"'] \\
& \text{FILTRO PRIMO} \arrow[u, shift right, "\boxed{\textit{En reticulados}}"']
\end{tikzcd}$$

Lema 4.7.18 *En un reticulado distributivo R todo filtro propio es intersección de filtros primos.*

Dem. Sabemos que todo filtro propio es intersección de filtros irreducibles (ver Corolario 4.7.4) y por el Lema 4.7.17 todo filtro irreducible es un filtro primo. ∎

Vimos que si R es un reticulado distributivo, entonces el conjunto ordenado $\mathcal{F}(R)$ es un reticulado distributivo donde $F_1 \sqcap F_2 = F_1 \cap F_2$ y $F_1 \sqcup F_2 = F(F_1 \cup F_2)$. Luego el conjunto ordenado $\mathcal{F}^*(R)$ es un reticulado distributivo donde $F_1 \sqcup F_2 = F_1 \cap F_2$ y $F_1 \sqcap F_2 = F(F_1 \cup F_2)$.

Lema 4.7.19 *F filtro primo de R $\Longleftrightarrow$ F es un elemento primo del reticulado $\mathcal{F}^*(R)$.*

Dem. $\Longrightarrow$) Si F es un filtro primo de R, en particular, $F \neq R$, esto es F es diferente del primer elemento del reticulado $\mathcal{F}^*(R)$. Supongamos que $F \supseteq F_1 \sqcup F_2 = F_1 \cap F_2$ y que $F \not\supseteq F_1$ y $F \not\supseteq F_2$, entonces existen (1) $f_1 \in F_1$, (2) $f_2 \in F_2$ tales que $f_1, f_2 \notin F$.
Como (3) $f_1 \leq f_1 \vee f_2$ y (4) $f_2 \leq f_1 \vee f_2$, entonces de (1) y (3) resulta (5) $f_1 \vee f_2 \in F_1$ y de (2) y (4) resulta (6) $f_1 \vee f_2 \in F_2$. Entonces de (5) y (6) tenemos que $f_1 \vee f_2 \in F_1 \cap F_2 \subseteq F$. Esto es, $f_1 \vee f_2 \in F$ y como F es un filtro primo resulta que $f_1 \in F$ ó $f_2 \in F$. Absurdo!!!
$\Longleftarrow$) Supongamos que (1) F es un elemento primo del reticulado $\mathcal{F}^*(R)$, luego en particular $F \neq R$. Si $x \vee y \in F$ entonces $F \supseteq [x \vee y) = [x) \cap [y) = [x) \sqcup [y)$, luego por (1): $F \supseteq [x)$ ó $F \supseteq [y)$ y por lo tanto $x \in F$ ó $y \in F$. ∎

Sabemos que en todo reticulado si un elemento es primo entonces es un elemento irreducible. Acabamos de demostrar que F filtro primo de R $\Longleftrightarrow$ F es un elemento primo del reticulado $\mathcal{F}^*(R)$, por lo tanto, F es un elemento irreducible del reticulado $\mathcal{F}^*(R)$ esto es $F \neq R$ y si $F = F_1 \sqcup F_2 = F_1 \cap F_2$ entonces $F = F_1$ ó $F = F_2$, es decir F es un filtro irreducible de R (resultado que ya hemos demostrado de otro modo, ver Lema 4.7.16).
Vimos que si R es distributivo entonces $\mathcal{F}^*(R)$ es un reticulado distributivo. En este caso, si F es un filtro irreducible de R, esto es $F \neq R$ y si $F = F_1 \cap F_2$ entonces $F = F_1$ ó $F = F_2$, lo que es equivalente a decir que $F \neq R$ y si $F = F_1 \sqcup F_2$ entonces $F = F_1$ ó $F = F_2$, entonces F es un elemento irreducible del reticulado distributivo $\mathcal{F}^*(R)$, luego como en todo reticulado distributivo los conceptos de elemento irreducible y elemento primo son equivalentes, podemos afirmar que F es un elemento primo del reticulado distributivo $\mathcal{F}^*(R)$, luego por el Lema 4.7.19 F es un filtro primo de R. (ésta es otra demostración de un resultado anterior, ver Lema 4.7.17).

Definición 4.7.6 *Una parte I de un reticulado distributivo R, con primer (0) y último elemento (1) se dice un* **ideal** *de R si:*

I1) $0 \in I$.

I2) Si $x, y \in I$ *entonces* $x \vee y \in I$.

I3) Si $x \in I$ *e* $y \leq x$ *donde* $y \in R$ *entonces* $y \in I$.

Un ideal I se dice propio si $I \neq R$ e I se denomina **primo**, *si es propio y si verifica: "Si $x \wedge y \in I$ entonces $x \in I$ ó $y \in I$."*

Lema 4.7.20 *Si P es un filtro primo de R entonces $I = \complement P$ es un ideal primo de R y recíprocamente si I es un ideal primo de R entonces $P = \complement I$ es un filtro primo de R.*

Dem.

$\Rightarrow$) Por hipótesis $P \neq R$, luego $I = \complement P \neq R$. Si $0 \notin I$ entonces $0 \in P$ y por lo tanto $P = R$, absurdo. Sean $a, b \in I$. Si $a \vee b \notin I$ entonces $a \vee b \in P$ y como P es un filtro primo entonces $a \in P$ ó $b \in P$ luego $a \notin I$ ó $b \notin I$, absurdo. Sea $a \in I$ y $b \in R$ tal que (1) $b \leq a$. Si $b \notin I$ entonces $b \in P$, luego por (1) resulta, por ser P un filtro, que $a \in P$, esto es $a \notin I$, absurdo. Sean $a, b \in R$ tales que $a \vee b \in I$, supongamos que $a \notin I$ y $b \notin I$ esto es $a, b \in P$, luego como P es un filtro $a \wedge b \in P$ esto es $a \wedge b \notin I$ absurdo.

$\Leftarrow$) Demostración análoga.

■

Teorema 4.7.2 (Teorema del Filtro Primo). *Dado un filtro F y un ideal I de un reticulado distributivo R tales que $F \cap I = \emptyset$, existe un filtro primo P tal que $F \subseteq P$ e $I \cap P = \emptyset$.* M. Stone (1937)

Dem. Sea Φ el conjunto de todos los filtros de R que contienen a F y son disjuntos de I. Como $F \in \Phi$ entonces $\Phi \neq \emptyset$. Se prueba sin dificultad que el conjunto ordenado $(\Phi, \subseteq)$ es inductivo superiormente, luego en este conjunto existen elementos maximales. Sea P un elemento maximal de Φ. Probemos que P es primo. Sean $a, b \in R$ tales que $a \vee b \in P$ y supongamos que (1) $a, b \notin P$. Consideremos los siguientes filtros $F_1 = F(P, a)$ y $F_2 = F(P, b)$, luego por (1) tenemos que $P \subset F_1$ y $P \subset F_2$ y por lo tanto $I \cap F_1 \neq \emptyset$ e $I \cap F_2 \neq \emptyset$ ya que P es un elemento máximo de Φ. Sean $i_1 \in I \cap F_1$ e $i_2 \in I \cap F_2$, por lo tanto (2) $i_1, i_2 \in I$, (3) $i_1 \in F_1$ e (4) $i_2 \in F_2$. De (3) resulta (ver Lema 4.7.7) que existe $p_1 \in P$ tal que $p_1 \wedge a \leq i_1$ y de (4) resulta que existe $p_2 \in P$ tal que $p_2 \wedge b \leq i_2$. Luego, $p_1 \wedge p_2 \wedge a \leq i_1$ y $p_1 \wedge p_2 \wedge b \leq i_2$ y en consecuencia (5) $z = (p_1 \wedge p_2) \wedge (a \vee b) \leq i_1 \vee i_2$. Por (2) tenemos (6) $i_1 \vee i_2 \in I$. De (5) y (6) resulta por ser I un ideal que (7) $z \in I$. Como $p_1, p_2 \in P$ resulta $p_1 \wedge p_2 \in P$ y como $a \vee b \in P$ entonces (8) $z = (p_1 \wedge p_2) \wedge (a \vee b) \in P$. De (7) y (8) concluímos que $z \in P \cap I$, lo que contradice que $P \cap I = \emptyset$. ■

Corolario 4.7.5 *Si a y b son elementos diferentes de un reticulado distributivo entonces existe un filtro primo que contiene a uno de los dos elementos sin contener al otro.*

Dem. Como $a \neq b$ entonces (1) $a \not\leq b$ ó (2) $b \not\leq a$. Entonces $[a) \cap (b] = \emptyset$, pues si $[a) \cap (b] \neq \emptyset$ entonces existiría $x \in [a) \cap (b]$ y por lo tanto $a \leq x \leq b$, absurdo. Luego por el Teorema 4.7.2 existe un filtro primo P tal que $[a) \subseteq P$ y $(b] \cap P = \emptyset$. Luego como $a \in [a)$ tenemos $a \in P$. Si $b \in P$ entonces $(b] \cap P \neq \emptyset$, absurdo. Luego $b \notin P$.
Otro modo de demostrar este resultado es el siguiente: de (1) resulta que $b \notin [a)$, y por lo tanto $[a)$ es un filtro propio. Por el Lema 4.7.18 todo filtro propio es intersección de filtros primos, luego $[a) = \bigcap_{i \in I} P_i$, donde $\{P_i\}_{i \in I}$ es una familia de filtros primos. Si $b \in P_i, \ \forall\, i \in I$ entonces $b \in [a)$ absurdo, luego existe un filtro primo $P = P_i$ tal que $b \notin P$ y $a \in P$. ■

En forma análoga a la indicada en el Teorema anterior se prueba:

Teorema 4.7.3 *Dado un filtro F y un ideal I de un reticulado distributivo R tales que $F \cap I = \emptyset$, existe un ideal primo P tal que $I \subseteq P$ y $F \cap P = \emptyset$.* M. Stone (1937)

El resultado anterior también es una consecuencia del Teorema 4.7.2, teniendo en cuenta que el complementario de un filtro primo es un ideal primo.

Vimos que *"Todo filtro propio de un reticulado distributivo, no trivial, R es intersección de filtros primos"*.

Teorema 4.7.4 *Si en un reticulado, no trivial, R se verifica que todo filtro propio es intersección de filtros primos entonces R es distributivo.*

Dem. Sabemos que en cualquier reticulado se verifica:

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

Supongamos que

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

luego $p \notin [a \wedge (b \vee c)) = F$, por lo tanto F es un filtro propio y en consecuencia $F = \bigcap\{P_i : i \in I\}$ donde los P_i, $i \in I$ son filtros primos. Luego $a \wedge (b \vee c) \in P_i$ para todo $i \in I$. Como $a \wedge (b \vee c) \leq a$ y $a \wedge (b \vee c) \leq b \vee c$ entonces (1) $a \in P_i$ para todo $i \in I$ y (2) $b \vee c \in P_i$, para todo $i \in I$. Dado que los P_i son filtros primos de (2) resulta que para cada $i \in I$ (3) $b \in P_i$ ó (4) $c \in P_i$, luego para cada $i \in I$ tenemos que $a \wedge b \in P_i$ ó $a \wedge c \in P_i$ y por lo tanto $p = (a \wedge b) \vee (a \wedge c) \in P_i$ para cada $i \in I$ y en consecuencia $p \in \bigcap\{P_i : i \in I\} = F$, absurdo. ■

Lema 4.7.21 *Si R es un reticulado con primer y último elemento* (0 y 1) *entonces $[a)$ es un filtro primo de $R \iff a$ es un elemento primo de R.*

Dem. $\Longrightarrow$) Si $[a)$ es un filtro primo de R, en particular $[a) \neq R$, luego $a \neq 0$. Supongamos que $a \leq b \vee c$ donde $b, c \in R$, luego $b \vee c \in [a)$ y como $[a)$ es un filtro primo, tenemos que $b \in [a)$ ó $c \in [a)$ esto es $a \leq b$ ó $a \leq c$.
$\Longleftarrow$) Si a es un elemento primo de R en particular $a \neq 0$ y por lo tanto $[a) \neq R$. Si $b \vee c \in [a)$, donde $b, c \in R$, esto es $a \leq b \vee c$ entonces como a es un elemento primo de R tenemos que $a \leq b$ ó $a \leq c$, esto es $b \in [a)$ ó $c \in [a)$. ■

Corolario 4.7.6 *Si R es un reticulado distributivo con primer y último elemento* (0 y 1) *entonces $[a)$ es un filtro irreducible de $R \iff a$ es un elemento irreducible de R.*

Dem. Sabemos que decir que $[a)$ es un filtro irreducible es equivalente, en reticulados distributivos, a decir que $[a)$ es un filtro primo y esto equivale a decir, por el lema anterior, en cualquier reticulado, que a es un elemento primo, lo que equivale a decir, en reticulados distributivos que a es un elemento irreducible. ■

Corolario 4.7.7 *En un álgebra de Boole B, $[a)$ es un filtro primo de $B \iff a$ es un átomo.*

Dem. $[a)$ filtro primo, equivale a decir (en reticulados) que a es un elemento primo, y en las álgebras de Boole ello equivale a decir que a es un átomo. ■

En los reticulados distributivos, existen filtros primos principales que no son generados por átomos. En el reticulado R indicado precedentemente en la Figura A, $[d)$ es un filtro primo y d no es átomo de R.

Lema 4.7.22 *Para que en un reticulado las nociones de filtro primo y filtro irreducible sean equivalentes en necesario y suficiente que el reticulado sea distributivo.*

Dem. $\Longleftarrow$) Ya vimos que si el reticulado es distributivo entonces las nociones de filtro primo y filtro irreducible son equivalentes.
$\Longrightarrow$) Sabemos que en cualquier reticulado se verifica:

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

Supongamos que

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

luego, $p \notin [a \wedge (b \vee c)) = F$, entonces existe un elemento máximo $M \in \mathcal{F}(F, p)$ y por lo tanto $F \subseteq M$ y $p \notin M$.
Sabemos que M es completamente irreducible, luego irreducible y por la hipótesis hecha M es un filtro primo. Como $a \wedge (b \vee c) \in F \subseteq M$, $a \wedge (b \vee c) \leq a$, $a \wedge (b \vee c) \leq b \vee c$ entonces (1) $a \in M$ y (2) $b \vee c \in M$. De (2) resulta por ser M un filtro primo que (3) $b \in M$ ó (4) $c \in M$. Luego $a \wedge b \in M$ ó $a \wedge c \in M$ y por lo tanto $p = (a \wedge b) \vee (a \wedge c) \in M$. Absurdo !!! ■

Definición 4.7.7 *Si F es un filtro propio de un reticulado distributivo R, se dice que un filtro primo P es un* **filtro primo mínimo** *de F si:*

1) $F \subseteq P$,

2) Si P_1 es un filtro primo tal que $F \subseteq P_1 \subseteq P$ entonces $P_1 = P$.

Esto equivale a decir que si $\mathcal{F}$ es el conjunto de los filtros primos que contienen a F, entonces P es un elemento minimal del conjunto ordenado $(\mathcal{F}, \subseteq)$.

Lema 4.7.23 *Sea R un reticulado distributivo y F un filtro de R. Para que un filtro primo P sea un filtro primo mínimo de F es necesario y suficiente que el ideal primo $I = \complement P$ sea un elemento maximal del conjunto ordenado $(\mathcal{I}, \subseteq)$ donde $\mathcal{I}$ es la familia de todos los ideales de R que son disjuntos de F.*

Dem. $\Rightarrow$) Si P es un filtro primo mínimo de F, en particular $F \subseteq P$ y en consecuencia $F \cap I = F \cap \complement P \subseteq P \cap \complement P = \emptyset$ y por lo tanto $F \cap I = \emptyset$. Luego $I = \complement P \in \mathcal{I}$. Sea $Y \in \mathcal{I}$ tal que (1) $I = \complement P \subseteq Y$. Como $Y \in \mathcal{I}$ entonces (2) $Y \cap F = \emptyset$, luego por el Teorema 4.7.3 existe un ideal primo I_1 tal que (3) $Y \subseteq I_1$ y (4) $F \cap I_1 = \emptyset$. De (4) resulta que (5) $F \subseteq \complement I_1 = P_1$, donde P_1 es un filtro primo. De (1) y (3) tenemos que (6) $I \subseteq I_1$. De (3) resulta que (7) $P_1 = \complement I_1 \subseteq \complement Y$. De (1) deducimos que (8) $\complement Y \subseteq P$. De (5), (7) y (8) resulta $F \subseteq P_1 \subseteq P$ y como P es un filtro primo mínimo de F entonces $P_1 = P$ esto es $\complement I_1 = \complement I$, por lo tanto $I_1 = I$ y como por (7) $Y \subseteq I_1$ entonces (9) $Y \subseteq I$. De (9) y (1) resulta que $I = Y$.
$\Leftarrow$) Sea $I = \complement P$ un elemento maximal del conjunto ordenado $(\mathcal{I}, \subseteq)$, luego I es un ideal primo tal que $I \cap F = \emptyset$ luego $F \subseteq \complement I = P$ y P es un filtro primo. Supongamos que P_1 es un filtro primo tal que $F \subseteq P_1 \subseteq P$ luego $\complement P = I \subseteq \complement P_1 = I_1$ donde I_1 es un ideal primo y como I es un elemento maximal tenemos que $I = I_1$ y por lo tanto $P = \complement P_1 = \complement I_1 = P_1$. ■

Lema 4.7.24 *Dado un filtro propio F de un reticulado distributivo R y un filtro primo P tal que $F \subseteq P$, existe un filtro primo mínimo P_1 de F tal que $F \subseteq P_1 \subseteq P$.*

Dem. $I = \complement P$ es un ideal primo. Por hipótesis $F \subseteq P$, luego $I \cap F = \emptyset$ entonces por el Teorema 4.7.2 existe un filtro primo P_1 tal que $F \subseteq P_1$ y (*) $I \cap P_1 = \emptyset$. De (*) resulta que $P_1 \subseteq \complement I = P$. ■

Corolario 4.7.8 *Todo filtro propio F es intersección de filtros primos mínimos de F.*

Dem. Como F es un filtro propio entonces por el Lema 4.7.18 $F = \bigcap_{i \in I} P_i$ donde $\{P_i\}_{i \in I}$ es una familia de filtros primos. Luego $F \subseteq P_i$, $\forall\, i \in I$. Por el lema anterior, para cada $i \in I$ existe un filtro primo mínimo P'_i tal que $F \subseteq P'_i \subseteq P_i$, luego

$$F \subseteq \bigcap_{i \in I} P'_i \subseteq \bigcap_{i \in I} P_i = F.$$

■

Observación 4.7.4 En un reticulado distributivo finito R, no trivial, todo elemento $x \in R$, $x \neq 0$ es supremo de elementos primos. *En efecto, como $x \neq 0$ entonces $[x)$ es propio, luego por el Lema 4.7.18 todo filtro propio es intersección de filtros primos, luego $[x) = \bigcap_{i \in I} P_i$, donde $\{P_i\}_{i \in I}$ es una familia de filtros primos. Como R es finito, sabemos que para todo $i \in I$, $P_i = [p_i)$ donde $p_i \in \Pi(R)$. Luego $[x) = \bigcap_{i \in I} [p_i) = [\bigvee_{i \in I} p_i)$ y por lo tanto $x = \bigvee_{i \in I} p_i$. Pero como $[x) \subseteq [p_i)$ cualquiera que sea $i \in I$ entonces $p_i \leq x$ para todo $i \in I$. Por lo tanto*

$$x = \bigvee \{p \in \Pi(R) : p \leq x\}.$$

Un resultado similar ya fué indicado en el Teorema 2.4.3. Es fácil ver que esta forma de expresar un elemento diferente de 0 como supremo de primos, no es única.
Vimos en el Corolario 4.7.8 que todo filtro propio F es intersección de filtros primos mínimos de F. Luego si $x \neq 0$

$$[x) = \bigcap_{i \in I} P_i,$$

donde los P_i son filtros primos mínimos de F y como $P_i = [p_i)$ con $p_i \in \Pi(R)$ tenemos, en forma análoga a la indicada precedentemente que x es supremo de un conjunto de elementos primos $\{p_i\}_{i\in I}$ tales que cada $[p_i)$ es un filtro primo mínimo de $[x)$. Luego los elementos p_i son elementos primos maximales del conjunto ordenado $(\Pi(x), \leq)$. Esta es la representación irredundante de x.

Definición 4.7.8 *Sea R un reticulado con primer y último elemento* (0 y 1). *Se denomina* **ultrafiltro** *ó* **filtro máximo** *a todo elemento máximo de $\mathcal{F}(0)$.*

Luego en un reticulado con primer y último elemento (0 y 1), todo ultrafiltro es un filtro completamante irreducible ya que es un filtro ligado al elemento 0.
Notaremos con $\mathcal{U}(R)$ la familia de todos los ultrafiltros de un reticulado R.

1) Si R es un reticulado distributivo con primer y último elemento (0 y 1) y F es un filtro propio de R, entonces $0 \notin F$ y por lo tanto $F \in \mathcal{F}(0)$, luego existe $U \in \mathcal{F}(0)$, U maximal tal que $F \subseteq U$, y si F no es maximal entonces U verifica $F \subset U$.

2) Decir que un filtro propio U es un ultrafiltro equivale a cualquiera de las siguientes condiciones:

   A) Si $U' \in \mathcal{F}(R)$ es tal que $U \subseteq U'$ entonces $U' = U$ ó $U' = R$.

   B) Si $U' \in \mathcal{F}(R)$ es tal que $U \subset U'$ entonces $U' = R$.

   Es claro que las condiciones A) y B) son equivalentes. Veamos que decir que U es ultrafiltro equivale a la condición A.
   $\Longrightarrow$) Si $U' \in \mathcal{F}(R)$, es tal que $U \subseteq U'$ y $U' \subset R$, entonces $0 \notin U'$ luego $U' \in \mathcal{F}(0)$ y como U es un elemento máximo de $\mathcal{F}(0)$ tenemos que $U = U'$.
   $\Longleftarrow$) Sea U un filtro propio de R que verifica la condición indicada y probemos que U es un ultrafiltro. En efecto si $U^* \in \mathcal{F}(0)$ verifica $U \subseteq U^*$, entonces U^* es propio, esto es $U^* \neq R$ de donde resulta por la hipotesis hecha que $U^* = U$.

Lema 4.7.25 *Sea R un reticulado distributivo, no trivial, con primer y último elemento* (0 y 1). *Para que un filtro propio U de R sea un ultrafiltro es necesario y suficiente que $\forall\, a \notin U$ exista $u \in U$, tal que $a \wedge u = 0$.*

Dem. $\Longrightarrow$) Sea U un filtro propio de R, y supongamos que (1) U es un ultrafiltro y sea $a \notin U$, luego $U \subset U \cup \{a\} \subseteq F(U,a)$ de donde resulta por (1) que $F(U,a) = R$, y por lo tanto $0 \in F(U,a)$, entonces por el Lema 4.7.7 existe $u \in U$ tal que $u \wedge a \leq 0$, esto es $u \wedge a = 0$, donde $u \in U$.
$\Longleftarrow$) Sea U un filtro propio de R que verifica la condición indicada y supongamos que U no es un ultrafiltro, luego existe un ultrafiltro U^* tal que $U \subset U^*$. Sea $a \in U^* \setminus U$, entonces por la hipótesis hecha existe $u \in U$ tal que $a \wedge u = 0$. Pero como $a, u \in U^*$ y U^* es un filtro tenemos que $0 = a \wedge u \in U^*$ y por lo tanto $U^* = R$. Absurdo. ■

Lema 4.7.26 *Sea R un reticulado, no trivial, con primer y último elemento* (0 y 1) *y $a \in R$, entonces $[a)$ es ultrafiltro $\Longleftrightarrow$ a es un átomo de R.*

Dem. $\Longrightarrow$) Si $[a)$ es un ultrafiltro entonces $a \neq 0$. Si a no fuese átomo de R, existe $b \in R$ tal que $0 < b < a$ y por lo tanto $[a) \subset [b) \subset R$, absurdo, dado que $[a)$ es un ultrafiltro.
$\Longleftarrow$) Si a es un átomo de R, en particular $a \neq 0$, luego $[a) \neq R$. Si $[a)$ no fuese un ultrafiltro entonces existiría un ultrafiltro U tal que $[a) \subset U$ y por lo tanto $a \in U$. Como a es un átomo de R sabemos que cualquiera que sea $x \in R$ entonces $a \wedge x = 0$ ó $a \wedge x = a$, por lo tanto si $u \in U \setminus [a)$ tenemos $a \wedge u = 0$ ó $a \wedge u = a$, pero en este último caso tendríamos $a \leq u$ y por lo tanto $u \in [a)$, absurdo, luego $a \wedge u = 0$, y como $a, u \in U$ entonces $0 = a \wedge u \in U$, absurdo. ■

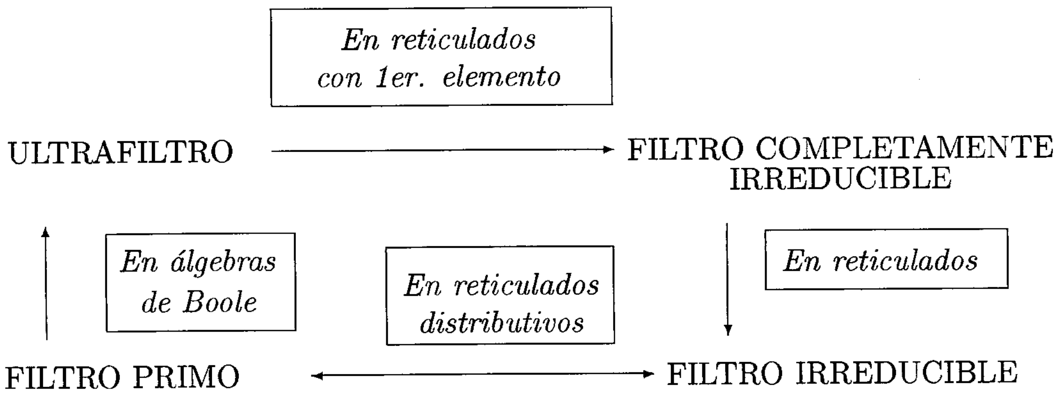
De este lema resulta que si R es un reticulado distributivo finito, no trivial, los únicos ultrafiltros son de la forma $[a)$ donde $a \in \mathcal{A}(R)$, ya que hemos visto que $a \in \mathcal{A}(R)$, equivale a $[a)$ ultrafiltro y si U es un ultrafiltro de R, como R es finito, U es principal, esto es $U = [a)$ con $a \in R$, luego por el Lema 4.7.26 $a \in \mathcal{A}(R)$.

Lema 4.7.27 *En un álgebra de Boole B todo filtro primo es un ultrafiltro.*

Dem. Sea $P \in \mathcal{P}(B)$, luego en particular P es propio. Supongamos que P no es un ultrafiltro, entonces existe un ultrafiltro U tal que $P \subset U$. Sea (1) $u \in U \setminus P$, como $1 = u \vee -u \in P$ y P es primo entonces (2) $u \in P$ ó (3) $-u \in P$. Como (2) se contradice con (1) entonces (4) $-u \in P \subset U$. De (1) y (4) resulta $0 = u \wedge -u \in U$, absurdo.
Otra demostración: Sea $U \in \mathcal{F}(B)$, tal que (1) $P \subseteq U$. Sea (2) $u \in U$, como $1 = u \vee -u \in P$ y P es primo entonces (3) $u \in P$ ó (4) $-u \in P$. Si ocurre (3) entonces $U \subseteq P$ y por lo tanto $P = U$. Si ocurre (4) por (1): $-u \in U$. De (2) y (4) tenemos $0 = u \wedge -u \in U$, y por lo tanto $U = B$. ■

Corolario 4.7.9 *En las álgebras de Boole las nociones de filtro irreducible, filtro completamente irreducible, filtro primo y ultrafiltro son equivalentes.*

Dado que:



Lema 4.7.28 *Para que un filtro propio F de un álgebra de Boole sea un ultrafiltro es necesario y suficiente que dado $a \notin F$ entonces $-a \in F$.*

Dem. $\Longrightarrow$) Sea F un ultrafiltro y $a \notin F$, como $a \vee -a = 1 \in F$, F es un filtro primo y $a \notin F$ tenemos que $-a \in F$.

$\Longleftarrow$) Sea F un filtro propio que verifica la condición indicada y supongamos que F no es un ultrafiltro, luego existe un ultrafiltro U tal que $F \subset U$. Entonces si (1) $a \in U \setminus F$, tenemos en particular que $a \notin F$, luego por la hipótesis hecha $-a \in F \subset U$. Luego (2) $-a \in U$. De (1) y (2) resulta por ser U un filtro que $0 = a \wedge -a \in U$, absurdo!!!
Otra demostración de la condición suficiente: Probemos que F es un filtro primo. Sea (3) $x \vee y \in F$ y supongamos que $x \notin F$ e $y \notin F$, entonces por la hipótesis hecha resulta que $-x, -y \in F$ y por lo tanto $-x \wedge -y \in F$, esto es (4) $-(x \vee y) \in F$. De (3) y (4) $0 = (x \vee y) \wedge -(x \vee y) \in F$, absurdo!!! ■

Corolario 4.7.10 *Un filtro propio F de un álgebra de Boole B es un ultrafiltro* $\Longleftrightarrow$ $\forall\, b \in B,\ b \in F$ *ó* $-b \in F$.

Dem. $\Longrightarrow$) Sea $b \in B$ entonces $b \in F$ ó $b \notin F$. Si $b \notin F$, resulta por el Lema 4.7.28 que $-b \in F$.
$\Longleftarrow$) Si $b \notin F$ resulta por la hipótesis que $-b \in F$, luego por el Lema 4.7.28 F es un ultrafiltro. ■

En el capítulo de reticulados distributivos indicamos el siguiente teorema de Birkhoff: *Todo reticulado distributivo, finito, es isomorfo a un anillo de conjuntos.* Recordemos que si $R = \{0\}$ entonces $R \cong \{\emptyset\}$, y si R tiene más de un elemento, vimos que el conjunto $\Pi = \Pi(R)$ de los elementos primos (irreducibles) de R no es vacío y si definimos $\varphi(a) = \{p \in \Pi : p \leq a\}$ cualquiera que sea $a \in R$ entonces φ establece un isomorfismo entre R y el anillo de conjuntos $\{\varphi(a)\}_{a \in R}$.

Teorema 4.7.5 (de representación de Stone) *Todo reticulado distributivo R es isomorfo a un anillo de conjuntos.*

Dem. 1er. caso) Si R tiene un solo elemento entonces R es isomorfo al anillo de conjuntos $\mathcal{A} = \{\emptyset\}$.
2do. caso) R tiene más de un elemento. Entonces existe por lo menos un elemento $r \in R$ que no es primer elemento de R, luego $[r)$ es propio, y en consecuencia si $x \notin [r)$, en el conjunto ordenado $\mathcal{F}([r), x)$, existen elementos máximos , que son filtros completamente irreducibles y por lo tanto filtros primos. Sea $E = \mathcal{P}(R)$ el conjunto de todos los filtros primos de R, acabamos de probar que $E \neq \emptyset$. Pongamos por definición:

$$S(r) = \{P \in E : r \in P\}, \qquad \text{donde} \qquad r \in R.$$

Luego $S(r) \subseteq E$, y por lo tanto $S : R \to 2^E$ (conjunto de las partes de E). La función S se denomina **transformación de Stone.**
Observemos que si R tiene primer elemento 0 entonces $S(0) = \emptyset$, dado que ningún filtro primo contiene al 0 y si R tiene último elemento 1, $S(1) = E$, dado que todo filtro de R contiene al elemento 1, en particular todos los filtros primos contienen al elemento 1.

1) $S(a \wedge b) = S(a) \cap S(b)$.
$P \in S(a \wedge b) \Longleftrightarrow P \in E$ y $a \wedge b \in P \Longleftrightarrow P \in E$ y $a, b \in P \Longleftrightarrow P \in S(a)$ y $P \in S(b) \Longleftrightarrow P \in S(a) \cap S(b)$.

2) $S(a \vee b) = S(a) \cup S(b)$.
$P \in S(a \vee b) \Longleftrightarrow P \in E$ y $a \vee b \in P \Longleftrightarrow$ (dado que P es un filtro primo) $P \in E$ y $a \in P$ ó $b \in P \Longleftrightarrow P \in S(a)$ ó $P \in S(b) \Longleftrightarrow P \in S(a) \cup S(b)$.

3) S es biunívoca.
Sean $a, b \in R$ tales que $a \neq b$. Vimos en el Corolario 4.7.5 que existe un filtro primo P que contiene a uno de los elementos sin contener al otro. Entonces si $a \in P$ y $b \notin P$ tenemos que $P \in S(a)$ y $P \notin S(b)$, luego $S(a) \neq S(b)$.

Acabamos asi de probar que R es isomorfo al anillo de conjuntos $\mathcal{A} = \{S(r)\}_{r \in R}$.
Observemos que podemos también hacer la demostración del siguiente modo:

1) S es una función del conjunto ordenado $(R, \leq)$ sobre el conjunto ordenado $(\mathcal{A} = \{S(r)\}_{r \in R}, \subseteq)$.

2) Si (1) $x \leq y$ entonces $S(x) \subseteq S(y)$.
En efecto, sea $P \in S(x)$ luego (2) $P \in \mathcal{P}(R)$ y $x \in P$ luego por (1) tenemos que (3) $y \in P$. De (2) y (3) resulta $P \in S(y)$.

3) Si (4) $S(x) \subseteq S(y)$ entonces $x \leq y$.
Supongamos que $x \not\leq y$, luego $y \notin [x)$ y por lo tanto existe (5) $P \in \mathcal{P}(R)$ tal que $y \notin P$ y $[x) \subseteq P$, luego (6) $x \in P$. De (5) y (6) resulta $P \in S(x)$, luego por (4) $P \in S(y)$ esto es $y \in P$, absurdo!!

■

Observación 4.7.5 *Si en vez de considerar el conjunto de todos los filtros primos de R consideramos el conjunto E' de todos los filtros completamente irreducibles de R, toda la demostración anterior es válida. Este es un teorema de representación establecido por Birkhoff. Recordemos que $E' \subseteq E$ (ver Lema 4.7.17), por lo tanto la representación de Birkhoff es "mas económica" que la representación de Stone. Pero en el caso en que R es finito $E' = E$. En efecto sea P un filtro primo de R, luego $P = [p)$ con $p \in \Pi(R)$. Por el Lema 4.7.15 sabemos que todo filtro propio es intersección de filtros completamente irreducibles, y como R es finito P es intersección de un número finito de filtros completamente irreducibles, esto es $P = \bigcap_{i=1}^{r} F_i$. Como el reticulado es finito entonces todos los filtros son principales, luego $F_i = [x_i)$, $1 \leq i \leq r$ luego $[p) = \bigcap_{i=1}^{r} [x_i) = [\bigvee_{i=1}^{r} x_i)$, y por lo tanto $p = \bigvee_{i=1}^{r} x_i$, luego como p es primo tendremos que $p = x_{i_0}$ donde $1 \leq i_0 \leq r$, luego $[p) = [x_{i_0})$ y como $[x_{i_0})$ es completamente irreducible resulta que $E \subseteq E'$.*

Observación 4.7.6 *Sabemos que si R es un reticulado distributivo finito, no trivial, $p \in \Pi(R) \iff [p) \in \mathcal{P}(R)$. Sea $h : \mathcal{P}(R) \to \Pi(R)$ definida por :*

$$h([p)) = p.$$

h es una biyección y un antiisomorfismo de orden ($[p) \subseteq [q) \iff q \leq p$). Veamos que:

$$\varphi(r) = h(S(r)), \quad \forall\, r \in R$$

*En efecto, $h(S(r)) = h(\{P \in \mathcal{P}(R) : r \in P\}) = h(\{[p) : p \in \Pi(R),\ r \in [p)\}) =$
$h(\{[p) : p \in \Pi(R),\ p \leq r\}) = \{h([p)) : p \in \Pi(R),\ p \leq r\} = \{p : p \in \Pi(R),\ p \leq r\} = \varphi(r)$.
Luego en el caso finito $\varphi = h \circ S$. Esto es la transformación de Birkhoff es igual a la composición de la transformación de Stone con la función h, definida precedentemente.*

Teorema 4.7.6 *Toda álgebra de Boole B, no trivial, es isomorfa a un cuerpo de conjuntos.*

Dem. Sea $E = \mathcal{U}(B)$ el conjunto de todos los ultrafiltros (filtros primos) de B. Como B no es trivial entonces $E \neq \emptyset$. Pongamos

$$S(a) = \{P \in E : a \in P\}, \quad \textit{donde} \quad a \in B.$$

Hemos visto que 1) $S(0) = \emptyset$; 2) $S(1) = E$; 3) $S(x \wedge y) = S(x) \cap S(y)$; 4) $S(x \vee y) = S(x) \cup S(y)$ y por lo tanto $S(-x) = \complement S(x)$, luego B es isomorfo al cuerpo de conjuntos $\mathcal{A} = \{S(x)\}_{x \in B}$. ■

Observación 4.7.7 *Vimos anteriormente un teorema análogo para las álgebras de Boole atómicas, pero el teorema precedente es más general puesto que vale para cualquier álgebra de Boole, no trivial. En el caso finito las dos demostraciones coinciden ya que existe correspondencia biunívoca entre átomos de B y ultrafiltros de B.*

Teorema 4.7.7 *En toda álgebra de Boole infinita B existen ultrafiltros que no son principales.*

Dem. Supongamos que todos los ultrafiltros de B son principales, luego, si U es un ultrafiltro de B, $U = [a)$ donde $a \in \mathcal{A}(B)$, por lo tanto $\mathcal{A}(B) \neq \emptyset$.
Probemos que $-\mathcal{A}(B) = \{-a : a \in \mathcal{A}(B)\}$ tiene la PIF. Sean $x_1, x_2, \ldots, x_t \in -\mathcal{A}(B)$ luego $x_i = -a_i$, $1 \leq i \leq t$ donde $a_i \in \mathcal{A}(B)$, $1 \leq i \leq t$. Por lo tanto, $\bigwedge_{i=1}^{t} x_i = \bigwedge_{i=1}^{t} -a_i = -(\bigvee_{i=1}^{t} a_i)$. Supongamos que $\bigwedge_{i=1}^{t} x_i = 0 \iff -(\bigvee_{i=1}^{t} a_i) = 0 \iff \bigvee_{i=1}^{t} a_i = 1$. Luego, dado $a \in \mathcal{A}(B)$, tenemos $a \leq 1 = \bigvee_{i=1}^{t} a_i$ de donde resulta, por ser a un elemento primo, que $a \leq a_{i_0}$ para algún i_0, $1 \leq i_0 \leq t$, luego $a = a_{i_0}$ ya que a y a_{i_0} son átomos. Esto prueba que $\mathcal{A}(B) \subseteq \{a_1, a_2, \ldots, a_t\}$ y por lo tanto $\mathcal{A}(B)$ sería finito. Probemos que B es atómica. En efecto, si $b \in B$, $b \neq 0$ entonces $[b)$ es principal y $[b) \subseteq U$ donde U es un ultrafiltro de B, luego $[b) \subseteq U = [a)$ donde a es un átomo. Entonces $a \leq b$ lo que prueba que B es atómica. Por el Teorema 4.2.1 (de Tarski) B es isomorfa a una subálgebra B' del álgebra de Boole $\mathcal{P}(\mathcal{A}(B))$ y como $\mathcal{A}(B)$ es finito entonces también el álgebra de Boole $\mathcal{P}(\mathcal{A}(B))$ es finita y, en consecuencia, B' y B lo son, absurdo!! Luego, $\bigwedge_{i=1}^{t} x_i \neq 0$. Acabamos así de probar que $-\mathcal{A}(B)$ tiene la PIF, luego, por el Lema 4.7.5 $F = F(-\mathcal{A}(B))$ es un filtro propio. Sea U un ultrafiltro tal que $F \subseteq U = [a)$ con $a \in \mathcal{A}(B)$ entonces $-a \in -\mathcal{A}(B) \subseteq F$ y por lo tanto $a, -a \in U$ de donde resulta que $0 = a \wedge -a \in U$, absurdo. ■
EJERCICIOS.

1) Si E' es una familia de ultrafiltros de un álgebra de Boole B tal que $\{1\} = \bigcap_{U \in E'} U$, pongamos por definición $\varphi(b) = \{U \in E' : b \in U\}$. Entonces $\varphi(b) \subseteq E'$. Probar que φ es un isomorfismo booleano de B sobre $\{\varphi(b)\}_{b \in B} \subseteq 2^{E'}$.
Como E' no es la familia de todos los ultrafiltros (filtros primos) de B, no se puede probar que φ es biunívoca del mismo modo que en el Teorema 4.7.5. Suponer que $\varphi(x) = \varphi(y)$ y probar que $x = y$.

2) Si B un álgebra de Boole atómica y $E' = \{[a) : a \in \mathcal{A}(B)\}$. Probar que $\bigcap\limits_{a\in\mathcal{A}(B)} [a) = \{1\}$.

Lema 4.7.29 *Sea A un álgebra de Boole, no trivial, y U un ultrafiltro de A, entonces $A/U \cong \mathbf{B} = \{0,1\}$.*

Dem. Empezemos por observar que como A es no trivial, existen ultrafiltros en A. Si U es un ultrafiltro de A consideremos la siguiente función:

$$h(x) = \begin{cases} 0 & \text{si } x \notin U \\ 1 & \text{si } x \in U \end{cases} \qquad x \in A.$$

Vamos a demostrar que h es un epimorfismo de A en $\mathbf{B}$.

1) h es suryectiva.
Obvio por la definición de h.

2) $h(1) = 1$.
Como U es un filtro entonces $1 \in U$, luego $h(1) = 1$.

3) $h(0) = 0$.
Como U es un filtro propio $0 \notin U$, luego $h(0) = 0$.

4) $h(x \wedge y) = h(x) \wedge h(y)$.
$h(x \wedge y) = 1 \iff x \wedge y \in U \iff x \in U \; e \; y \in U \iff h(x) = 1$ e $h(y) = 1 \iff h(x) \wedge h(y) = 1$.
Observemos que como $\mathbf{B} = \{0,1\}$ entonces $a \wedge b = 0$ implica que $a = 0$ ó $b = 0$.
$h(x \wedge y) = 0 \iff x \wedge y \notin U \iff x \notin U \; ó \; y \notin U \iff h(x) = 0$ ó $h(y) = 0 \iff h(x) \wedge h(y) = 0$.

5) $h(x \vee y) = h(x) \vee h(y)$.
Observemos que como $\mathbf{B} = \{0,1\}$ entonces $a \vee b = 1$ implica que $a = 1$ ó $b = 1$.
$h(x \vee y) = 1 \iff x \vee y \in U \iff$ (dado que U es un filtro primo) $x \in U$ *ó* $y \in U \iff h(x) = 1 \; ó \; h(y) = 1 \iff h(x) \vee h(y) = 1$.
$h(x \vee y) = 0 \iff x \vee y \notin U \iff$ (dado que U es un filtro primo) $x \notin U \; e \; y \notin U \iff h(x) = 0 = h(y) \iff h(x) \vee h(y) = 0$.

De 1) a 5) resulta que h es un epimorfismo booleano de $A \to \mathbf{B}$, y además por la definición de h , $Nuc(h) = U$.
Sea $\varphi : A \to A/U$ el epimorfismo natural, luego como $Nuc(\varphi) = U = Nuc(h)$ resulta que $\mathbf{B}$ es isomorfa a A/U. ∎

Veamos una nueva demostración del resultado indicado en el Lema 4.6.31.

Lema 4.7.30 *Si A es un álgebra de Boole simple entonces $A \cong \mathbf{B} = \{0,1\}$.*

Dem. Sea A un álgebra de Boole simple, luego, A no es trivial, y por lo tanto, existen ultrafiltros. Sea U un ultrafiltro de A, luego, por el lema anterior tenemos que

$$(1) \qquad A/U \cong \mathbf{B} = \{0,1\}.$$

Como A es simple entonces (2) $A/U \cong \{0\}$ ó (3) $A/U \cong A$.
(2) no puede ocurrir porque $\mathbf{B} \cong A/U \cong \{0\}$, absurdo. Luego,, debe ocurrir (3) y por lo tanto, $A \cong A/U \cong \mathbf{B}$. ∎

Lema 4.7.31 *Si A es un álgebra de Boole y F es un filtro de A tal que A/F es simple, entonces F es un ultrafiltro de A.*

Dem. 1) F es un filtro propio. En efecto, si $F = A$ entonce $A/F = A/A = \{0\} \not\cong \mathbf{B} = \{0,1\}$. Absurdo.
2) Sea M un filtro de A tal que $F \subseteq M$ y sean $\varphi_1 : A \to A/F$, $\varphi_2 : A \to A/M$ los homomorfismos naturales respectivos.

$$\begin{tikzcd} A \arrow[r, "\varphi_1"] \arrow[d, "\varphi_2"'] & A/F \arrow[dl, "g"] \\ A/M & \end{tikzcd}$$

Entonces como $Nuc(\varphi_1) = F \subseteq M = Nuc(\varphi_2)$ existe un epimorfismo $g : A/F \to A/M$ tal que $g \circ \varphi_1 = \varphi_2$. Pero $Nuc(g)$ es un filtro de $A/F \cong \mathbf{B}$ luego $Nuc(g) = \{1\}$ ó $Nuc(g) = \{0,1\}$.
1er. caso) $Nuc(g) = \{1\}$. Sea $x \in M$ luego $\varphi_2(x) = 1$ y como $g(\varphi_1(x)) = \varphi_2(x)$ tenemos $g(\varphi_1(x)) = 1$ y por lo tanto $\varphi_1(x) \in Nuc(g) = \{1\}$ esto es $\varphi_1(x) = 1$ y por lo tanto $x \in Nuc(\varphi_1) = F$ y en consecuencia $M \subseteq F$ de donde resulta $F = M$.
2do. caso) $Nuc(g) = \{0,1\} = A/F$. entonces $g(y) = 1, \forall\ y \in A/F$, luego $g(\varphi_1(x)) = 1,\ \ \forall x \in A$ esto es $\varphi_2(x) = 1\ \forall x \in A$ y entonces $x \in M = Nuc(\varphi_2) = A$. Luego F es un ultrafiltro de A ■

Si $\{A_i\}_{i\in I}$ es una familia de álgebras de Boole tales que $A_i = A$ para todo $i \in I$, entonces sabemos que $P = \prod\limits_{i\in I} A_i$ es simplemente el conjunto de todas las funciones definidas sobre I y que toman sus valores en A. En este caso se suele notar $P = A^I$. A toda subálgebra booleana de A^I se denomina **álgebra de Boole funcional**. En particular, A^I es un álgebra de Boole funcional.

Teorema 4.7.8 (de Stone) *Toda álgebra de Boole, no trivial, A es isomorfa a un álgebra de Boole funcional.*

Dem. Como A no es trivial, entonces el conjunto E de todos los ultrafiltros de A no es vacío. Consideremos el álgebra de Boole funcional $\mathcal{F} = \mathbf{B}^E$, donde $\mathbf{B} = \{0,1\}$.
A cada elemento $f \in A$ le vamos a hacer corresponder un elemento $F \in \mathcal{F}$, esto es una función de E en $\mathbf{B}$, $\varphi(f) = F$, del siguiente modo:

$$F(U) = u(f),$$

donde $U \in E$ y u es el homomorfismo canónico $u : A \to A/U \cong \mathbf{B}$.
Luego como para cada $U \in E$, $F(U) \in \mathbf{B}$ tenemos que $F \in \mathcal{F}$, y por lo tanto φ es una función de A sobre $A' = \{\varphi(f)\}_{f\in A}$. Probemos que:

1) $\varphi(f \wedge g) = \varphi(f) \wedge \varphi(g)$.
Sean $h = f \wedge g$ $\ \varphi(h) = H$, $\ \varphi(f) = F$, $\ \varphi(g) = G$. Queremos probar que $H = F \wedge G$ esto es que $H(U) = (F \wedge G)(U) = F(U) \wedge G(U)$, para todo $U \in E$. En efecto:
$H(U) =$ (def.) $= u(h) = u(f \wedge g) =$ (por ser u un homomorfismo) $= u(f) \wedge u(g) = F(U) \wedge G(U)$.

2) $\varphi(f \vee g) = \varphi(f) \vee \varphi(g)$.
Demostración análoga a la anterior.

3) $\varphi(0) = \mathbf{0}$.
Sea $F = \varphi(0)$ luego, $F(U) = u(0) = 0$ para todo $U \in E$ esto es $F = \mathbf{0}$.

4) $\varphi(1) = \mathbf{1}$.
Demostración análoga.

Como φ es un función de A sobre A' que verifica 1), 2) 3) y 4) entonces A' es una subálgebra booleana de $\mathcal{F}$. Probemos que φ es inyectiva. Sean $f, g \in A$, $f \neq g$ luego, (1) $f \not\leq g$ ó (2) $g \not\leq f$. Supongamos que ocurre (1) entonces, existe $U_0 \in E$ tal que $f \in U_0$ y $g \notin U_0$, y probemos que $F = \varphi(f) \neq \varphi(g) = G$. En efecto como $f \in U_0 = Nuc(u_0)$ y entonces $F(U_0) = u_0(f) = 1$ y como $g \notin U_0$ entonces $G(U_0) = u_0(g) = 0$.
Acabamos así de probar que las funciones F y G toman valores diferentes en el punto U_0, luego $F \neq G$. ∎

Veamos que en el caso en que A es finita, no trivial, la función φ es suryectiva. Sea $\{a_1, a_2, \ldots, a_n\}$ el conjunto de los átomos de A, por lo tanto $E = \{[a_1), [a_2), \ldots, [a_n)\}$ y

$$\mathbf{B}^E = \prod_{i=1}^{n} A/[a_i) = A/[a_1) \times A/[a_2) \times \ldots A/[a_n)$$

donde $A/[a_i) \cong \mathbf{B}$ para $1 \leq i \leq n$.
Sea $y \in \mathbf{B}^E$, luego $y = (y_1, y_2, \ldots, y_n)$ donde $y_i \in A/[a_i)$, $1 \leq i \leq n$.
Sea $u_i : A \to A/[a_i)$ el homomorfismo natural. Luego, para cada $y_i \in A/[a_i)$ existe $x_i \in A$ tal que $u_i(x_i) = y_i$. Sea $x = \bigvee_{i=1}^{n} (x_i \wedge a_i)$ y probemos que $\varphi(x) = y$. Pero $\varphi(x) = (u_1(x), u_2(x), \ldots, u_n(x))$.
Observemos que $u_j(x) = u_j(\bigvee_{i=1}^{n} (x_i \wedge a_i)) = \bigvee_{i=1}^{n} u_j(x_i \wedge a_i) = \bigvee_{i=1}^{n} u_j(x_i) \wedge u_j(a_i)$. Pero como $a_j \in [a_j)$ entonces

$$u_j(a_j) = 1 \quad y \quad u_j(a_i) = 0 \text{ si } i \neq j$$

Luego, $u_j(x) = u_j(x_j) \wedge u_j(a_j) = u_j(x_j) \wedge 1 = u_j(x_j) = y_j$ y para $i \neq j$, $u_j(x) = u_j(x_j) \wedge u_j(a_i) = u_j(x_j) \wedge 0 = 0$, luego $\varphi(x) = y$.

Acabamos así de probar que si A es finita, no trivial, con n átomos entonces

$$A \cong \underbrace{\mathbf{B} \times \mathbf{B} \times \ldots \times \mathbf{B}}_{n \text{ veces}}.$$

Lema 4.7.32 *Si X es un conjunto arbitrario, $\mathbf{B} = \{0, 1\}$, entonces $\mathbf{B}^X$ y $\mathcal{P}(X)$ son álgebras de Boole isomorfas.*

Dem. Dada $f \in \mathbf{B}^X$ consideremos la función $H : \mathbf{B}^X \to \mathcal{P}(X)$ definida por:

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

Dado que $f^{-1}(1) \subseteq X$ es claro que H toma sus valores en $\mathcal{P}(X)$, además claramente se verifican $H(\mathbf{0}) = \mathbf{0}^{-1}(1) = \emptyset$ y $H(\mathbf{1}) = \mathbf{1}^{-1}(1) = X$. También se verifica $H(-f) = \complement H(f)$.

En efecto, $x \in H(-f) = (-f)^{-1}(1) \iff (-f)(x) = 1 \iff -(f(x)) = 1 \iff f(x) = 0 \iff x \notin f^{-1}(1) = H(f) \iff x \in \complement H(f)$. Probemos que $H(f \wedge g) = H(f) \cap H(g)$. En efecto, $x \in H(f \wedge g) = (f \wedge g)^{-1}(1) \iff (f \wedge g)(x) = 1 \iff (1) f(x) \wedge g(x) = 1$ y como $f(x), g(x) \in \mathbf{B} = \{0,1\}$ entonces (1) $\iff f(x) = g(x) = 1 \iff x \in f^{-1}(1)$, $x \in g^{-1}(1) \iff x \in H(f) \cap H(g)$. En forma análoga se prueba que $H(f \vee g) = H(f) \cup H(g)$. H es suryectiva. En efecto, dado $Z \subseteq X$ consideremos la función $f : X \to \mathbf{B}$ defina por:

$$f(x) = \begin{cases} 1 \in \mathbf{B} & \text{si } x \in Z \\ \\ 0 \in \mathbf{B} & \text{si } x \notin Z \end{cases} \qquad x \in X.$$

verifica $H(f) = f^{-1}(1) = Z$.
H es inyectiva. Sean $f, g \in \mathbf{B}^X$, tales que $f \neq g$, luego existe $x \in X$ tal que $f(x) \neq g(x)$. Luego como $f(x), f(y) \in \mathbf{B} = \{0,1\}$, tenemos que $f(x) = 0$, $g(x) = 1$ ó $f(x) = 1$, $g(x) = 0$, esto es, $x \notin f^{-1}(1) = H(f)$, $x \in g^{-1}(1) = H(g)$ ó $x \in f^{-1}(1) = H(f)$, $x \notin g^{-1}(1) = H(g)$ luego $H(f) \neq H(g)$. ■

4.8 Algebras de Boole libres

Definición 4.8.1 *Un subconjunto G de un álgebra de Boole L se dice un* **conjunto de generadores libres** *de L si:*

L1) $SB(G) = L$, (esto es, G es un conjunto de generadores de L.)

L2) Dada una función f de G en un álgebra de Boole arbitraria A, existe un homomorfismo $h_f : L \to A$ que extiende a f, esto es $f(g) = h_f(g)$, $\forall\, g \in G$.

En este caso se suele decir que L es un **álgebra de Boole libre** o que L es un álgebra de Boole con un conjunto G de generadores libres.

Teorema 4.8.1 *(de Birkhoff) Para toda "álgebra" definida por igualdades existe siempre el álgebra libre con un conjunto de generadores de cardinal prefijado.*

Lema 4.8.1 *Sean A, A' álgebras de Boole, $h : A \to A'$ un homomorfismo de A en A'. Si $G \subseteq A$ es tal que $SB(G) = A$ entonces $SB(h(G)) = h(A)$. (esto es, si G genera A entonces $h(G)$ genera al álgebra de Boole $h(A)$.)*

Dem. Sea $A'_1 = SB(h(G))$, luego A'_1 es una subálgebra de A' y en consecuencia $A_1 = h^{-1}(A'_1)$ es una subálgebra de A. Además (1) $G \subseteq A_1$. En efecto, si $g \in G$ entonces $h(g) \in h(G) \subseteq A'_1$ y por lo tanto $g \in h^{-1}(A'_1) = A_1$. De (1) resulta que $A = SB(G) \subseteq A_1$, esto es $A_1 = A$, y en consecuencia como h es una función de A sobre $h(A)$:

$$h(A) = h(A_1) = h(h^{-1}(A'_1)) = A'_1 = SB(h(G)).$$

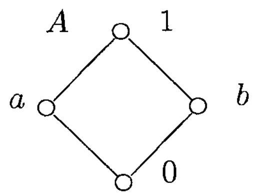
■

Lema 4.8.2 *Si L es un álgebra de Boole con un conjunto de generadores libres G, A un álgebra de Boole con un conjunto G' de generadores y $f : G \to G'$ es una función suryectiva, entonces A es una imagen homomórfica de L.*

Dem. Como L es un álgebra libre la función f se extiende a un homomorfismo $h_f : L \to A$, luego (1) $h_f(g) = f(g)$, $\forall g \in G$. Entonces por el Lema 4.8.1 $SB(h_f(G)) = h_f(L)$, pero por (1) $h_f(G) = f(G) = G'$, luego $SB(G') = h_f(L)$ y como $SB(G') = A$ tenemos finalmente que $h_f(L) = A$. ∎

Observación 4.8.1 *Este lema significa que L es la mayor álgebra entre las que contienen un conjunto de generadores de cardinal igual al cardinal de G.*

Ejemplo 4.8.1 *a) Consideremos el álgebra de Boole A cuyo diagrama se indica a continuación:*



Sea $G = \{a, b\}$*, sabemos que* $SB(G) = A$*. Por lo tanto,* G *es un conjunto de generadores de* A*. Veamos que* G *no es un conjunto de generadores libres. Para ello consideremos la aplicación* $f : G \to \mathbf{B} = \{0, 1\}$*, definida del siguiente modo:* $f(a) = f(b) = 0$*. Supongamos que* h_f *es un homomorfismo que extiende a* f*, entonces* $h_f(a) = h_f(b) = 0$*.* $h_f(a) = h_f(-b) = -h_f(b) = -f(b) = -0 = 1$*. Por lo tanto no existe ningún homomorfismo de* A *en* $\mathbf{B}$ *que extienda a* f*. En consecuencia* G *no es un conjunto de generadores libres.*

b) Consideremos ahora el conjunto $H = \{a\}$*. Como* $m(H) = \{a, -a\}$ *entonces* $SB(H) = S(m(H)) = A$*. Probemos que* H *es un conjunto de generadores libres. Sea* $f : H \to A'$ *donde* A' *es un álgebra de Boole arbitraria, y* $f(a) = a' \in A'$*. Si* h_f *es un homomorfismo de* A *en* A' *que extiende a* f *se debe verificar* $h_f(a) = f(a) = a'$ *y por lo tanto* $h_f(b) = h_f(-a) = -h_f(a) = -f(a) = -a'$*, y además* $h_f(0) = 0'$ *y* $h_f(1) = 1'$*.*
Entonces dada $f : H \to A'$ *pongamos por definición* $h_f(0) = 0$*,* $h_f(1) = 1, h_f(a) = f(a) = a'$ *y* $h_f(b) = h_f(-a) = -f(a) = -a'$*. Luego la función* h_f *extiende a* f*. Probemos que* h_f *es un homomorfismo, para lo cual nos basta probar que* $h_f(-x) = -h_f(x)$*,* $\forall\, x \in A$ *y que* $h_f(x \wedge y) = h_f(x) \wedge h_f(y)$*,* $\forall\, x, y \in A$*. En efecto:*

$$h_f(-0) = h_f(1) = 1 = -0 = -h_f(0); \quad h_f(-1) = h_f(0) = 0 = -1 = -h_f(1)$$

$$h_f(-a) = h_f(b) = -a' = -h_f(a); \quad h_f(-b) = h_f(a) = a' = --a' = -h_f(b)$$

$$h_f(0 \wedge y) = h_f(0) = 0 = 0 \wedge h_f(y) = h_f(0) \wedge h_f(y)$$

$$h_f(1 \wedge y) = h_f(y) = 1 \wedge h_f(y) = h_f(1) \wedge h_f(y)$$

$$h_f(a \wedge b) = h_f(0) = 0 = a' \wedge -a' = h_f(a) \wedge h_f(b).$$

Acabamos así de probar que $H = \{a\}$ *es un conjunto de generadores libres del álgebra* A*.*

c) En forma análoga se demuestra que $I = \{b\}$ *es un conjunto de generadores libres de* A*.*

d) *Consideremos un álgebra de Boole B_3 con tres átomos. Para demostrar que B_3 no tiene ningún subconjunto de generadores libres, deberíamos considerar los $258 = 2^8$ subconjuntos de B_3, ver cuales de ellos generan a B_3. Luego, para cada conjunto $G \subseteq B_3$ tal que $SB(G) = B_3$ verificar que cualquiera que sea el álgebra de Boole A' y cualquiera que sea $f : G \to A'$ no se puede extender a un homomorfismo de B_3 en A'.*
Vamos a indicar una forma mucho mas sencilla de demostrar que B_3 no tiene ningún subconjunto de generadores libres.

e) *Observemos que si A es un álgebra de Boole, $G \subseteq A$ tal que $SB(G) = A$, $g_1, g_2 \in G$ son elementos comparables, pero diferentes, esto es (i) $g_1 < g_2$ ó (ii) $g_2 < g_1$, entonces G no es un conjunto de generadores libres.*
En efecto, en el caso (i) considerando la función $f : G \to \mathbf{B}$ definida por $f(g_1) = 1$, $f(g_2) = 0$, la misma no se puede extender a ningún homomorfismo de A en $\mathbf{B}$.
Vemos así que si G es un conjunto de generadores, y $g_1, g_2 \in G$ donde $g_1 \neq g_2$ ellos deben ser incomparables.

Teorema 4.8.2 *Sea G un conjunto de generadores de un álgebra de Boole B y $f : G \to A$ una función de G en un álgebra de Boole arbitraria A. Si existe un homomorfismo de $B \to A$ que extiende a f, él es único.*

Dem. Sean h', h'' homomorfismos de B en A que extienden a f, esto es:

$$(i)\ \ h'(g) = f(g)\ \ \forall\, g \in G\,; \qquad\qquad (ii)\ \ h''(g) = f(g)\ \ \forall\, g \in G.$$

Consideremos el conjunto $X = \{x \in B : h'(x) = h''(x)\} \subseteq B$, entonces (1) $G \subseteq X$. En efecto, si $g \in G$ entonces $h'(g) = f(g) = h''(g)$ y por lo tanto $g \in X$.
Sean $x, y \in X$ entonces $h'(x \wedge y) = h'(x) \wedge h'(y) = h''(x) \wedge h''(y) = h''(x \wedge y)$ luego, $x \wedge y \in X$. Análogamente se prueba que $x \vee y, -x \in X$. De estas condiciones resulta que $0, 1 \in X$. Luego (2) X es subálgebra de B. De (1) y (2) resulta $B = SB(G) \subseteq X$ y por lo tanto $B = X$ esto es, $h'(x) = h''(x)$, $\forall\, x \in B$. ■

Teorema 4.8.3 *Si L_1 es un álgebra de Boole con un conjunto de generadores libres G_1, L_2 un álgebra de Boole con un conjunto de generadores libres G_2 y si existe una biyección $f : G_1 \to G_2$, entonces $L_1 \cong L_2$.*

Dem. Como L_1 es libre y $f : G_1 \to L_2$, esta función se puede extender a un homomorfismo $h_f : L_1 \to L_2$.
Como f es una biyección, entonces también $f^{-1} : G_2 \to G_1$ es una biyección.
Entonces como L_2 es libre y $f^{-1} : G_2 \to L_1$, esta función se puede extender a un homomorfismo $h_{f^{-1}} : L_2 \to L_1$.
Consideremos el homomorfismo $h = h_{f^{-1}} \circ h_f : L_1 \to L_1$, y sea:

$$X = \{x \in L_1 : h(x) = x\} \subseteq L_1.$$

a) $G_1 \subseteq X$.
Sea $g \in G_1$ luego $h(g) = h_{f^{-1}}(h_f(g)) = h_{f^{-1}}(f(g))$ y como $f(g) \in G_2$ tenemos finalmente $h(g) = f^{-1}(f(g)) = g$, luego $g \in X$.

b) X es subálgebra de L_1.
Su demostración es obvia.

De a) y b) resulta que $L_1 = SB(G_1) \subseteq X$ y por lo tanto $L_1 = X$, y en consecuencia:

c) $h(x) = x, \quad \forall\, x \in L_1$.

d) h_f es inyectiva.
Si $h_f(x) = h_f(y)$ entonces $h_{f^{-1}}(h_f(x)) = h_{f^{-1}}(h_f(y))$, esto es $h(x) = h(y)$ de donde resulta por c) que $x = y$.

e) h_f es suryectiva.
Como $SB(G_1) = L_1$ y $h_f : L_1 \to L_2$ es un homomorfismo entonces por el Lema 4.8.1: $h_f(L_1) = SB(h_f(G_1)) = SB(f(G_1)) = SB(G_2) = L_2$.

■

Esto nos prueba que *el álgebra de Boole con un conjunto de generadores libres G, es <u>única</u> a menos de isomorfismos.*

Vamos a indicar una construcción del álgebra de Boole $L(n)$ con un conjunto de generadores libres, con n elementos, $n \in \mathbb{N}$.
Claramente $L(n)$ no es un álgebra de Boole trivial. Sea $E = \{U_i\}_{i\in I}$ el conjunto de todos los ultrafiltros de $L(n)$. Por el teorema de Stone sabemos que $L(n)$ es isomorfa a una subálgebra del álgebra de Boole $P = \prod\limits_{i\in I} L(n)/U_i$, y tambien sabemos que cada uno de los cocientes $L(n)/U_i \cong \mathbf{B} = \{0,1\}$.
Por lo tanto, si probamos que el conjunto E es finito tendremos que P es un álgebra finita y por lo tanto $L(n)$ es finita. Si además determinamos el número de elementos de E conoceremos el número de elementos de P y su "estructura".
Para ello vamos a demostrar, utilizando una técnica indicada por L. Monteiro en 1964, para las álgebras de Heyting, que existe una correspondencia biunívoca entre el conjunto $\mathbf{B}^G$ de todas las funciones de G en $\mathbf{B}$ y el conjunto E. Esta técnica fué utilizada posteriormente por R. Cignoli, A. Monteiro, L. Iturrioz, M. Abad y A. Figallo, entre otros.
Dada $f \in \mathbf{B}^G$ como G es un conjunto de generadores libres de $L(n)$, existe un homomorfismo $h_f : L(n) \to \mathbf{B}$ que extiende a f. Ademas sabemos que $SB(h_f(G)) = h_f(L(n))$ y como la única subálgebra de $\mathbf{B}$ es la propia $\mathbf{B}$ entonces $SB(h_f(G)) = \mathbf{B}$ y por lo tanto $h_f(L(n)) = \mathbf{B}$. Probemos que: $Nuc(h_f) \in E$.
Sea φ el homomorfismo natural de $L(n) \to L(n)/Nuc(h_f)$. Como $Nuc(h_f) = Nuc(\varphi)$, entonces $L(n)/Nuc(h_f) \cong \mathbf{B}$, esto es $L(n)/Nuc(h_f)$ es un álgebra simple, luego por un resultado anterior $Nuc(h_f)$ es un ultrafiltro de $L(n)$.

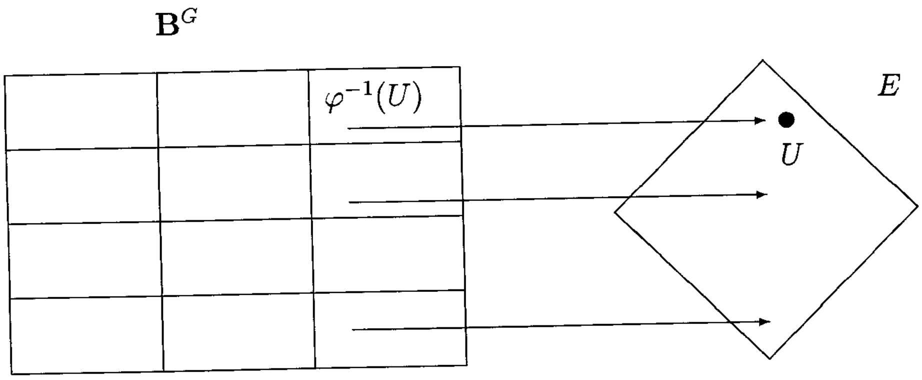
$$\begin{tikzcd} L(n) \arrow[r, "h_f"] \arrow[d, "\varphi"'] & \mathbf{B} \\ L(n)/Nuc(h_f) & \end{tikzcd}$$

Pongamos por definición:

$$\psi(f) = Nuc(h_f), \quad f \in \mathbf{B}^G,$$

luego $\psi : \mathbf{B}^G \to E$.

1) ψ es suryectiva. Sea $U \in E$ y $\varphi : L(n) \to L(n)/U$ el homomorfismo natural. Como $L(n)/U \cong \mathbf{B}$ podemos suponer que $\varphi : L(n) \to \mathbf{B}$. Sea $f = \varphi_{|G}$, luego $f \in \mathbf{B}^G$, y por lo tanto puede extenderse a un homomorfismo $h_f : L(n) \to \mathbf{B}$. Pero como h_f y φ son extensiones de f resulta por el Teorema 4.8.2 que $h_f = \varphi$ y en consecuencia $\psi(f) = Nuc(h_f) = Nuc(\varphi) = U$.
Observemos que de la condición 1) ya resulta que E es finito, pués $N[E] \leq 2^n$.



2) ψ es inyectiva. Sean $f_1, f_2 \in \mathbf{B}^G$, tales que $\psi(f_1) = \psi(f_2)$, esto es $Nuc(h_1) = Nuc(h_2)$. Luego $L(n)/Nuc(h_1) = L(n)/Nuc(h_2) \cong \mathbf{B}$. Entonces si $x \in Nuc(h_1) = Nuc(h_2)$, $h_{f_1}(x) = h_{f_2}(x) = 1$ y si $x \in L(n) \setminus Nuc(h_1) = L(n) \setminus Nuc(h_2)$, $h_{f_1}(x) = h_{f_2}(x) = 0$, por lo tanto $h_{f_1}(x) = h_{f_2}(x) \quad \forall\ x \in L(n)$, en particular $f_1(g) = f_2(g)\ \forall\ g \in G$, esto es $f_1 = f_2$.

Acabamos así de probar que E tiene 2^n elementos y por lo tanto

$$L(n) \cong \prod_{i=1}^{2^n} L(n)/U_i = \prod_{i=1}^{2^n} L(n)/[a_i).$$

Luego, como cada uno de los cocientes tiene 2 elementos tenemos que:

$$N[L(n)] = 2^{2^n}.$$

Si ponemos por convención que $\mathbf{B} = \{0, 1\}$ es un álgebra libre con un conjunto vacío de generadores, entonces las álgebras con $1, 2, 4, \ldots, 2^t, \ldots$ átomos son libres , esto es el número de átomos es una potencia de 2. De aquí resulta que el álgebra de Boole B_3 con 3 átomos no es libre.

4.9 Homomorfismos de un cuerpo de conjuntos en otro, inducidos por una función puntual.

Sean X e Y conjuntos no vacíos y $f : X \to Y$. Pongamos por definición:

$$h_f(Z) = f^{-1}(Z) = \{x \in X : f(x) \in Z\}, \quad \forall\ Z \subseteq Y.$$

Entonces

Lema 4.9.1 *La función* $h_f : \mathcal{P}(Y) \to \mathcal{P}(X)$ *verifica*

(1) $h_f(\emptyset) = \emptyset$.

(2) $h_f(Y) = X$.

(3) $h_f(Z \cap W) = h_f(Z) \cap h_f(W), \quad \forall\, Z, W \subseteq Y$.

(4) $h_f(Z \cup W) = h_f(Z) \cup h_f(W), \quad \forall\, Z, W \subseteq Y$.

(5) $h_f(\complement Z) = \complement h_f(Z) \ \forall\, Z \subseteq Y$.

Por lo tanto, h_f es un homomorfismo del álgebra de Boole $\mathcal{P}(Y)$ en el álgebra de Boole $\mathcal{P}(X)$, que se denomina **homomorfismo inducido por la función** f. (R. Sikorski).

Observación 4.9.1 *Si* $Z \subseteq Y$, *entonces* $h_f(Z) = f^{-1}(Z) = \emptyset \iff Z \subseteq Y - Im\,(f)$.

Lema 4.9.2 h_f *inyectiva* $\iff$ f *suryectiva.*

Dem. $\Longrightarrow$) Dado $y \in Y$ entonces $\{y\} \subseteq Y$ y además $\{y\} \neq \emptyset$, por lo tanto como h_f es inyectiva $h_f(\{y\}) \neq h_f(\emptyset)$, esto es $f^{-1}(\{y\}) \neq f^{-1}(\emptyset) = \emptyset$, luego existe $x \in X$ tal que $x \in f^{-1}(\{y\})$, esto es $f(x) = y$, por lo tanto f es suryectiva.

$\Longleftarrow$) Sean $Z, W \subseteq Y$ tales que $Z \neq W$, esto es (1) $Z \not\subseteq W$ ó (2) $W \not\subseteq Z$. Supongamos que ocurre (1) entonces existe $z \in Z$ tal que $z \notin W$. Como $z \in Y$ y f es suryectiva, existe $x \in X$ tal que $f(x) = z$, por lo tanto $x \in f^{-1}(Z) = h_f(Z)$ y $x \notin f^{-1}(W) = h_f(W)$, esto es $h_f(Z) \neq h_f(W)$. ∎

Lema 4.9.3 h_f *suryectiva* $\iff$ f *inyectiva.*

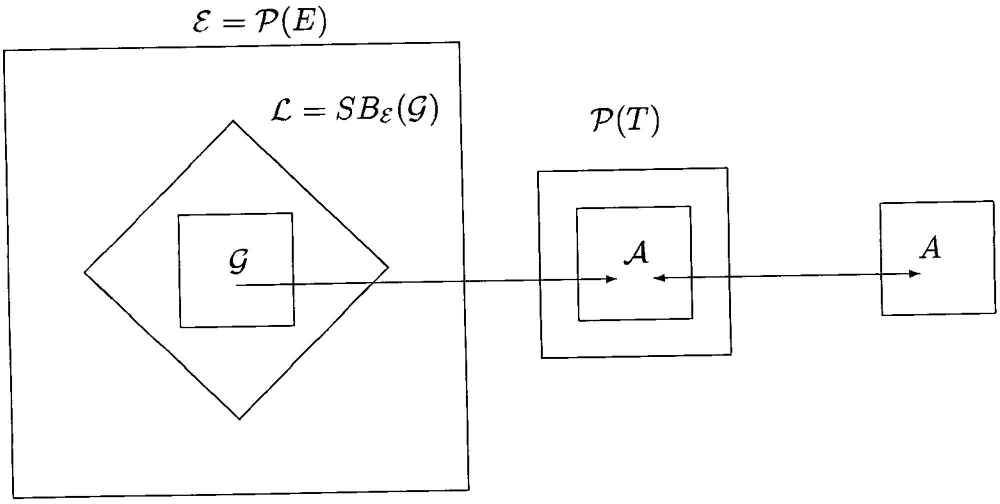
Dem. $\Longrightarrow$) Sean $x_1, x_2 \in X$, tales que $x_1 \neq x_2$, entonces $C_1 = \{x_1\} \subseteq X$, $C_2 = \{x_2\} \subseteq X$ y $C_1 \neq C_2$. Como h_f es suryectiva existen $Z_1, Z_2 \subseteq Y$ tales que $h_f(Z_1) = C_1$ y $h_f(Z_2) = C_2$, esto es $f^{-1}(Z_1) = C_1 = \{x_1\}$ y $f^{-1}(Z_2) = C_2 = \{x_2\}$, luego $f(x_1) \in Z_1$ y $f(x_2) \in Z_2$. Además $f^{-1}(Z_1) \cap f^{-1}(Z_2) = \{x_1\} \cap \{x_2\} = \emptyset$, esto es $f^{-1}(Z_1 \cap Z_2) = \emptyset$ y esto significa que *no existe* $x \in X$ tal que $f(x) \in Z_1 \cap Z_2$. Luego, si $f(x_1) = f(x_2)$ tendremos que $f(x_1) = f(x_2) \in Z_1 \cap Z_2$. Absurdo, luego $f(x_1) \neq f(x_2)$ y por lo tanto f es inyectiva.

$\Longleftarrow$) Si $C \subseteq X$ entonces $Z = f(C) \subseteq Y$, luego $h_f(Z) = f^{-1}(f(C)) =$ (por ser f inyectiva) $= C$. ∎

4.10 Algebras de Boole libres, construcción de A. Monteiro

Dado un número cardinal **c** vamos a indicar una construcción, debida a A. Monteiro, del álgebra de Boole con un conjunto de generadores de cardinal **c**.
Dada el álgebra de Boole $\mathbf{B} = \{0, 1\}$, sea I un conjunto de cardinal **c**, $E = \prod_{i \in I} B_i$ donde $B_i = \mathbf{B}$, para todo $i \in I$ y $\mathcal{E} = \mathcal{P}(E)$ la familia de todos los subconjuntos de E.
Consideremos la siguiente familia de conjuntos $G_i = \{x \in E : x_i = 1\}$, donde $i \in I$. Por lo tanto $G_i \subseteq E, \ \forall\, i \in I$ esto es $G_i \in \mathcal{E}, \ \forall\, i \in I$.
Observemos que el elemento $e \in E$ definido por $e(i) = 1, \ \forall\, i \in I$ pertenece a todos los conjuntos G_i. Luego $G_i \neq \emptyset, \ \forall\, i \in I$.

Tenemos así un subconjunto $\mathcal{G} = \{G_i\}_{i\in I}$ del álgebra de Boole $\mathcal{E}$ que verifica cuyo cardinal es igual a $\mathbf{c}$, lo que equivale a decir que los cardinales de $\mathcal{G}$ y de I son iguales. En efecto si ponemos por definición $\alpha(i) = G_i$, entonces α es una función de I sobre $\mathcal{G}$. Además α es inyectiva, ya que si $i, j \in I$, $i \neq j$, entonce el elemento $x \in E$ definido por $x(j) = 0$ y $x(k) = 1$ para todo $k \neq j$ verifica $x \notin G_j$ y $x \in G_i$, luego $\alpha(i) = G_i \neq G_j = \alpha(j)$.
Sea $\mathcal{L} = SB_{\mathcal{E}}(\mathcal{G})$, esto es $\mathcal{L}$ es la subálgebra booleana generada en $\mathcal{E}$ por $\mathcal{G}$. Vamos a demostrar que $\mathcal{G}$ es un conjunto de generadores libres de $\mathcal{L}$. Para ello debemos demostrar que dada un álgebra de Boole arbitraria A y una función $f : \mathcal{G} \to A$, f se puede extender a un homomorfismo $h_f : \mathcal{L} \to A$.
PRIMER CASO) A tiene un sólo elemento, $A = \{0\}$, entonces si $f : \mathcal{G} \to A$, tendremos que $f(G_i) = 0$, $\forall\, G_i \in \mathcal{G}$ y por lo tanto la función $h_f(x) = 0$, $\forall\, x \in \mathcal{L}$ es un homomorfismo que extiende a f.
SEGUNDO CASO) A tiene más de un elemento. Sea T el conjunto de todos los ultrafiltros de A, entonces por el teorema de Stone A es isomorfa a una subálgebra $\mathcal{A}$ del álgebra funcional $\mathbf{B}^T$ y como el álgebra de Boole $\mathbf{B}^T$ es isomorfa al álgebra de Boole $\mathcal{P}(T)$ de todos los subconjuntos de T, entonces podemos suponer que A es isomorfa a una subálgebra $\mathcal{A}$ de $\mathcal{P}(T)$.
Sí f es una función de $\mathcal{G}$ en $\mathcal{A}$ entonces $f(G_i) = H_i$ donde $H_i \in \mathcal{A}$, esto es $H_i \subseteq T$.



Vamos a definir una función $h_f : \mathcal{P}(E) \to \mathcal{P}(T)$ de forma tal que h_f sea un homomorfismo que extienda a f. Una tal función debe hacer corresponder a cada subconjunto X de E un subconjunto de T, esto es

$$\text{Si } X \subseteq E \text{ entonces } h_f(X) \subseteq T.$$

Para cada $H_i \subseteq T$ consideremos la siguiente función $k_{H_i} : T \to \mathbf{B} = \{0, 1\}$.

$$k_{H_i}(t) = \begin{cases} 1 \in \mathbf{B} & \text{si } t \in H_i \\ 0 \in \mathbf{B} & \text{si } t \notin H_i \end{cases} \qquad t \in T$$

y la función $K : T \to E$ definida por:

$$K(t) = (k_{H_i}(t))_{i\in I} \in \prod_{i\in I} B_i = E, \quad t \in T.$$

Luego
$$h_f(X) = K^{-1}(X), \qquad \text{donde } X \subseteq E$$
es una función de $\mathcal{P}(E)$ en $\mathcal{P}(T)$, que verifica $h_f(\emptyset) = \emptyset$, $h_f(E) = T$, $h_f(X \cap Y) = h_f(X) \cap h_f(Y)$, $h_f(X \cup Y) = h_f(X) \cup h_f(Y)$. Por lo tanto, h_f es un homomorfismo booleano $\mathcal{P}(E)$ en $\mathcal{P}(T)$. Probemos h_f es una extensión de f. Esto es que $h_f(G_j) = f(G_j) = H_j$, $\forall\, j \in I$, lo que equivale a demostrar que $K^{-1}(G_j) = H_j$, $\forall\, j \in I$.
En efecto $t \in K^{-1}(G_j) \iff K(t) \in G_j \iff (k_{H_i}(t))_{i\in I} \in G_j \iff k_{H_j}(t) = 1 \iff t \in H_j$.

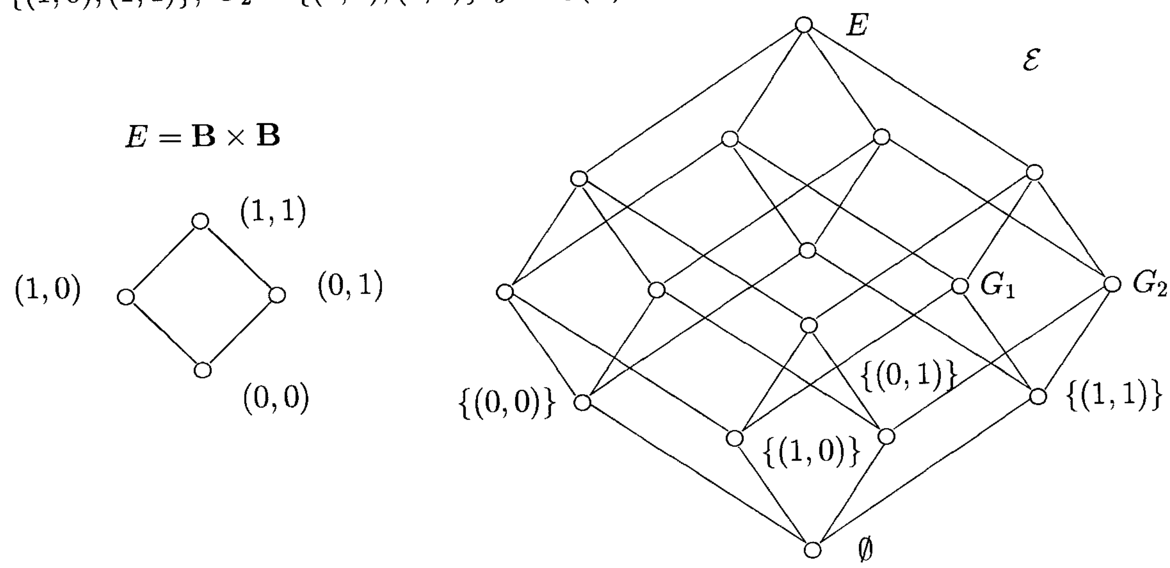
Veamos finalmente que el homomorfismo h_f toma sus valores en $\mathcal{A}$, esto es que $h_f(\mathcal{L}) \subseteq \mathcal{A}$. Sea $\mathcal{L}' = \{X \in \mathcal{P}(E) : h_f(X) \in \mathcal{A}\}$, entonces:

1) $\mathcal{G} \subseteq \mathcal{L}'$.
En efecto si $G_i \in \mathcal{G}$, entonces $h_f(G_i) = f(G_i) = H_i \in \mathcal{A}$, luego $G_i \in \mathcal{L}'$ para todo $i \in I$.

2) $\mathcal{L}'$ es una subálgebra de $\mathcal{P}(E)$.
Como $h_f(\emptyset) = \emptyset \in \mathcal{A}$, $h_f(E) = T \in \mathcal{A}$, entonces $\emptyset, E \in \mathcal{A}$. Si $X, Y \in \mathcal{L}'$ entonces $h_f(X), h_f(Y) \in \mathcal{A}$, y como $\mathcal{A}$ es una subálgebra de $\mathcal{P}(T)$ tenemos que $h_f(X \cap Y) = h_f(X) \cap h_f(Y) \in \mathcal{A}$, $h_f(X \cup Y) = h_f(X) \cup h_f(Y) \in \mathcal{A}$, luego $x \cap Y$, $X \cup Y \in \mathcal{A}$.

De 1) y 2) se deduce que (3) $\mathcal{L} = SB_{\mathcal{E}}(\mathcal{G}) \subseteq \mathcal{L}'$. Por lo tanto si $Y \in h_f(\mathcal{L})$ esto es (4) $Y = h_f(X)$ donde (5) $X \in \mathcal{L}$. De (5) y (3) resulta $X \in \mathcal{L}'$ y por lo tanto $Y = h_f(X) \in \mathcal{A}$.

Ejemplo 4.10.1 *Sea* $\mathbf{c} = 2$, $I = \{1, 2\}$, $E = \mathbf{B} \times \mathbf{B}$. *Luego tenemos que los diagramas de* E *y* $\mathcal{E} = \mathcal{P}(E)$ *son los que se indican a continuación, y* $\mathcal{G} = \{G_1, G_2\}$ *donde* $G_1 = \{(1,0), (1,1)\}$, $G_2 = \{(0,1), (1,1)\}$ *y* $SB_{\mathcal{E}}(\mathcal{G}) = \mathcal{E}$.



Apliquemos la construcción de A. Monteiro para el caso en que $\mathbf{c}$ es un número natural, luego $I = \{1, 2, \ldots, n\}$,
$$E = \underbrace{\mathbf{B} \times \mathbf{B} \times \ldots \times \mathbf{B}}_{n \text{ veces}},$$

$N[E] = 2^n$, $\mathcal{E} = \mathcal{P}(E)$, $N[\mathcal{E}] = 2^{2^n}$, $G_i = \{x \in E : x_i = 1\}, 1 \leq i \leq n$, $\mathcal{G} = \{G_i : 1 \leq i \leq n\}$. Probemos que $SB_{\mathcal{E}}(\mathcal{G}) = \mathcal{E}$.
El conjunto de los átomos de $\mathcal{E}$ es $\mathcal{A}(\mathcal{E}) = \{\{x\}\}_{x\in E}$. Si probamos que $\mathcal{A}(\mathcal{E}) \subseteq m(\mathcal{G})$ entonces $S(m(\mathcal{G})) = SB_{\mathcal{E}}(\mathcal{G}) = \mathcal{E}$. Si $\{x\} \in \mathcal{A}(\mathcal{E})$, entonces $x = (x_1, x_2, \ldots, x_n) \in E$ y por lo tanto $x_i \in \mathbf{B} = \{0,1\}$, $1 \leq i \leq n$.
Pongamos

$$X_i = \begin{cases} \emptyset & si \quad x_i = 1 \\ E & si \quad x_i = 0 \end{cases} \qquad 1 \leq i \leq n$$

Entonces

$$X = (X_1, X_2, \ldots, X_n) \in \underbrace{\{\emptyset, E\} \times \{\emptyset, E\} \times \ldots \times \{\emptyset, E\}}_{n \ veces}.$$

Probemos que $m_X = \{x\}$.

1) $\{x\} \subseteq m_X$.
Sea $I(x,1) = \{i \in I : x_i = 1\}$ e $I(x,0) = I \setminus I(x,1)$.
Si $I(x,1) = I$ esto es $x_i = 1$ para todo $i \in I$ entonces $x \in G_i$ para todo $i \in I$ y por lo tanto si $X = (X_1, X_2, \ldots, X_n) = (\emptyset, \emptyset, \ldots, \emptyset)$ entonces

$$x \in m_X = \bigcap_{i=1}^{n} G_i = \bigcap_{i=1}^{n} (G_i + X_i).$$

Si $I(x,0) = I$ esto es $x_i = 0$ para todo $i \in I$ entonces $x \in \complement G_i$ para todo $i \in I$ y por lo tanto si $X = (X_1, X_2, \ldots, X_n) = (E, E, \ldots, E)$ entonces

$$x \in m_X = \bigcap_{i=1}^{n} \complement G_i = \bigcap_{i=1}^{n} (G_i + X_i).$$

Si $I(x,1) \neq I$ entonces $x_i = 1$ para todo $i \in I(x,1)$ y $x_i = 0$ para todo $i \in I(x,0)$ esto es $x \in G_i$ para todo para todo $i \in I(x,1)$ y $x \in \complement G_i$ para todo para todo $i \in I(x,0)$ y por lo tanto si $X = (X_1, X_2, \ldots, X_n)$ es tal que $X_i = \emptyset$ para todo $i \in I(x,1)$ y $X_i = E$ para todo $i \in I(x,0)$ tenemos que

$$x \in m_X = \bigcap_{i \in I(x,1)} (G_i + X_i) \cap \bigcap_{i \in I(x,0)} (G_i + X_i).$$

2) $m_X \subseteq \{x\}$.
Sea $y \in m_X = \bigcap_{i=1}^{n} (G_i + X_i)$, luego $y \in G_i + X_i$, $1 \leq i \leq n$. Por lo tanto si $X_i = \emptyset \iff x_i = 1$, entonces $y \in G_i + \emptyset = G_i$ luego (1) $y(i) = 1 = x(i)$, y si $X_i = E \iff x_i = 0$, entonces $y \in G_i + E = \complement G_i$ luego $y \notin G_i$ y por lo tanto (2) $y(i) = 0 = x(i)$. De (1) y (2) resulta que $y = x$.

De $\mathcal{A}(\mathcal{E}) \subseteq m(\mathcal{G}) \subseteq S(m(\mathcal{G})) = SB_{\mathcal{E}}(\mathcal{G})$ resulta que $\mathcal{E} = SB_{\mathcal{E}}(\mathcal{A}(\mathcal{E})) \subseteq SB_{\mathcal{E}}(\mathcal{G})$.

4.11 Extensión de homomorfismos

Definición 4.11.1 *Un álgebra de Boole C se dice* **completa** *si para todo subconjunto $\{a_i\}_{i\in I}$ de elementos de C, existe el elemento $\bigvee_{i\in I} a_i$ en C.*

Lema 4.11.1 *Si en un álgebra de Boole A existe el supremo (ínfimo) de un subconjunto $\{a_i\}_{i\in I}$ de A entonces también existe el ínfimo (supremo) del subconjunto $\{-a_i\}_{i\in I}$ y además*

$$\bigwedge_{i\in I} -a_i = -(\bigvee_{i\in I} a_i) \quad \text{y} \quad \bigvee_{i\in I} -a_i = -(\bigwedge_{i\in I} a_i).$$

Lema 4.11.2 *Un álgebra de Boole C es completa si y solamente si para todo subconjunto $\{a_i\}_{i\in I}$ de elementos de C, existe $\bigwedge_{i\in I} a_i$.*

Es obvio que todas las álgebras de Boole finitas son completas. Indiquemos un ejemplo de un álgebra de Boole que no es completa.

Ejemplo 4.11.1 *Sea $\mathbf{N}$ el conjunto de los números naturales, entonces $A = \mathcal{P}(\mathbf{N})$ es un álgebra de Boole. Sea S el subconjunto de A formado por las partes finitas de $\mathbf{N}$ y los complementarios de las partes finitas de $\mathbf{N}$. Como $\emptyset$ es una parte finita de $\mathbf{N}$, entonces $\emptyset \in S$. Como $\mathbf{N} = \complement\emptyset$ entonces $\mathbf{N} \in S$. Dados $X, Y \in S$ entonces (1) X es finita ó (2) $X = \complement F_1$, donde F_1 es una parte finita de $\mathbf{N}$, (3) Y es finita ó (4) $Y = \complement F_2$, donde F_2 es una parte finita de $\mathbf{N}$. Si se verifica (1) entonces $\complement X \in S$, y si se verifica (2) entonces $\complement X = F_1 \in S$. Por lo tanto, S es cerrado con respecto al complemento.*
Como $X \cap Y \subseteq X$, entonces si se verifica (1), $X \cap Y$ es finito esto es $X \cap Y \in S$. Si se verifican (2) y (3) como $X\cap Y \subseteq Y$ entonces $X \cap Y$ es finito y en consecuencia $X\cap Y \in S$. Si se verifican (2) y (4) entonces $X \cap Y = \complement F_1 \cap \complement F_2 = \complement(F_1 \cup F_2)$, por lo tanto $X \cap Y$ es el complementario de la parte finita $F_1 \cup F_2$ de $\mathbf{N}$, luego $X \cap Y \in S$.
Tenemos así un álgebra de Boole S. Para probar que S no es completa basta indicar un subconjunto de elementos de S que no tenga supremo en S.
Sea I el conjunto de los números naturales impares, P el conjunto de los números naturales pares y consideremos el siguiente subconjunto de S : $X = \{\{i\}\}_{i\in I}$. Supongamos que $Y \in S$ es una cota superior de X, esto es :

$$\{i\} \subseteq Y, \quad \forall\, i \in I,$$

entonces $I \subseteq Y$. Por lo tanto Y no puede ser un subconjunto finito de $\mathbf{N}$ y en consecuencia debe ser el complementario de una parte finita de $\mathbf{N}$, esto es $Y = \complement F$ donde F es finita y $F \subseteq \mathbf{N}$. Luego $F = \complement Y \subseteq \complement I = P$, esto es el conjunto finito F es un subconjunto del conjunto de los naturales pares. Sea $F = \{p_1, p_2, \ldots, p_n\}$ donde los p_i son números naturales pares. Tenemos entonces

$$I \subseteq Y = \complement F = \complement\{p_1, p_2, \ldots, p_n\}.$$

Sea p un número natural par tal que $p \neq p_i$, para $1 \leq i \leq n$, esto es $p \in \complement F$. Entonces el conjunto $F_1 = \{p_1, p_2, \ldots, p_n, p\}$ verifica $F \subseteq F_1$ y por lo tanto :

$$\text{(i)} \quad Y_1 = \complement F_1 \subseteq \complement F = Y,$$

y como $I \subseteq I \cup (P \setminus F_1) = \complement F_1 = Y_1$ entonces Y_1 es una cota superior del conjunto X de elementos de S que es "menor ó igual" que Y, (ver (i)) . Esto prueba que el conjunto de las cotas superiores de X no tiene primer elemento.

Lema 4.11.3 *El producto cartesiano de álgebras de Boole completas es un álgebra de Boole completa.*

Dem. Sea $\{A_i\}_{i\in I}$ una familia de álgebras de Boole completas y $P = \prod_{i\in I} A_i$. Dado un conjunto $\{x^{(j)}\}_{j\in J}$ de elementos de P, esto es $x^{(j)} = (x_i^{(j)})_{i\in I}$ $\forall\, j \in J$, vamos a demostrar que existe el supremo de este conjunto.
Para cada i fijo, $i \in I$, $\{x_i^{(j)}\}_{j\in J}$ es un subconjunto de elementos de A_i, y como A_i es completa existe el elemento (1) $s_i = \bigvee_{j\in J} x_i^{(j)}$, para cada $i \in I$. Consideremos el elemento de P definido por $s = (s_i)_{i\in I}$, entonces :

S1) Por (1) $x_i^{(j)} \leq s_i$, $\forall\, j \in J$, $\forall\, i \in I$, luego $x^{(j)} = (x_i^{(j)})_{i\in I} \leq (s_i)_{i\in I} = s$, $\forall\, j \in J$.

S2) Sea $p \in P$ tal que $(x_i^{(j)})_{i\in I} = x^{(j)} \leq p = (p_i)_{i\in I}$, $\forall\, j \in J$, luego $x_i^{(j)} \leq p_i$, $\forall\, j \in J$, $\forall\, i \in I$, luego por (1) tenemos que $s_i \leq p_i$, $\forall\, i \in I$, esto es $s \leq p$.

■

Definición 4.11.2 *Se dice que un álgebra de Boole completa C es* **un completamiento** *de un álgebra de Boole A si C contiene una subálgebra isomorfa a A.*

Lema 4.11.4 *Toda álgebra de Boole A admite un completamiento.*

Dem. Si A es trivial, es claro que es completa. Si A no es trivial, sabemos por el Teorema de Stone que A es isomorfa a una subálgebra de $C = \mathbf{B}^E$, donde E es el conjunto de todos los ultrafiltros de A. Como $\mathbf{B}$ es un álgebra de Boole completa, dado que es finita, entonces por el lema anterior C es completa, luego C es un completamiento de A. ■

Lema 4.11.5 *Si A es un álgebra de Boole, S una subálgebra de A, h un homomorfismo de S en un álgebra de Boole completa C y $b \in A$, entonces h se puede extender a un homomorfismo H de $SB(S,b)$ en C.* (R. Sikorski)

Dem. Sabemos que:

$$SB(S,b) = \{x = (s_1 \wedge b) \vee (s_2 \wedge -b) : s_1, s_2 \in S\}.$$

Sean $X = \{s \in S : s \leq b\}$ $Y = \{s \in S : b \leq s\}$. Estos conjuntos no son vacíos dado que $0 \in X$ y $1 \in Y$.
Como C es completa podemos asegurar la existencia de los siguientes elementos de C:

$$m = \bigvee_{x\in X} h(x); \quad M = \bigwedge_{y\in Y} h(y).$$

Veamos que $m \leq M$. En efecto, sean $x \in X$, $y \in Y$, esto es $x \in S$, $x \leq b$, $y \in S$, $b \leq y$, luego $x \leq y$ cualesquiera que sean $x \in X$, $y \in Y$, y por lo tanto $h(x) \leq h(y)$ cualesquiera que sean $x \in X$, $y \in Y$, por lo tanto $m = \bigvee_{x\in X} h(x) \leq h(y)$ cualquiera que sean $y \in Y$ y $m \leq \bigwedge_{y\in Y} h(y) = M$.

De $x \leq b \leq y$, $\forall\, x \in X$, $\forall\, y \in Y$, resulta que si H es un homomorfismo de $SB(S,b)$ que extiende a h entonces

$$h(x) = H(x) \leq H(b) \leq H(y) = h(y), \quad \forall\, x \in X, \ \ \forall\, y \in Y,$$

por lo tanto

$$m \leq H(b) \leq M.$$

Además, si $x \in SB(S,b)$ entonces $x = (s_1 \wedge b) \vee (s_2 \wedge -b)$ donde $s_1, s_2 \in S$, y por lo tanto $H(x) = (H(s_1) \wedge H(b)) \vee (H(s_2) \wedge H(-b)) = (h(s_1) \wedge H(b)) \vee (h(s_2) \wedge -H(b))$.
Sea $c \in C$ tal que $m \leq c \leq M$, si $x = (s_1 \wedge b) \vee (s_2 \wedge -b)$ donde $s_1, s_2 \in S$ pongamos por definición:

$$H(x) = (h(s_1) \wedge c) \vee (h(s_2) \wedge -c).$$

Sabemos que la "representación" de los elementos de $SB(S,b)$ no es única, entonces para ver que H es una función debemos probar que si:

$$(1) \qquad x = (s_1 \wedge b) \vee (s_2 \wedge -b) = (s_3 \wedge b) \vee (s_4 \wedge -b)$$

donde $s_i \in S$, $1 \leq i \leq 4$, entonces :

$$z = (h(s_1) \wedge c) \vee (h(s_2) \wedge -c) = (h(s_3) \wedge c) \vee (h(s_4) \wedge -c) = w.$$

Recordemos que $z = w \iff z \wedge -w = 0$ y $w \wedge -z = 0$.
En efecto $z \wedge -w = [(h(s_1) \wedge c) \vee (h(s_2) \wedge -c)] \wedge (-h(s_3) \vee -c) \wedge (-h(s_4) \vee c) =$

$$[(h(s_1) \wedge c) \wedge (h(-s_3) \vee -c) \wedge (h(-s_4) \vee c)] \vee [(h(s_2) \wedge -c) \wedge (h(-s_3) \vee -c) \wedge (h(-s_4) \vee c)].$$

Como $h(s_1) \wedge c \leq c \leq h(-s_4) \vee c$ y $h(s_2) \wedge -c \leq -c \leq h(-s_3) \vee -c$, entonces:

$$z \wedge -w = [h(s_1) \wedge c \wedge (h(-s_3) \vee -c)] \vee [h(s_2) \wedge -c \wedge (h(-s_4) \vee c)] =$$

$$[h(s_1) \wedge c \wedge h(-s_3)] \vee [h(s_1) \wedge c \wedge -c)] \vee [h(s_2) \wedge -c \wedge h(-s_4)] \vee [h(s_2) \wedge -c \wedge c] =$$

$$[h(s_1) \wedge c \wedge h(-s_3)] \vee [h(s_2) \wedge -c \wedge h(-s_4)] = [h(s_1 \wedge -s_3) \wedge c] \vee [h(s_2 \wedge -s_4) \wedge -c].$$

Por lo tanto $z \wedge -w = 0$ si y solamente si $h(s_1 \wedge -s_3) \wedge c = 0$ y $h(s_2 \wedge -s_4) \wedge -c = 0$.
De (1) haciendo el ínfimo de ambos miembros con b y luego con $-b$ tenemos

$$(2) \quad s_1 \wedge b = s_3 \wedge b \quad \text{y} \quad (3) \quad s_2 \wedge -b = s_4 \wedge -b.$$

Entonces de (2) resulta

$$s_1 \wedge -s_3 \wedge b = 0 \quad \text{esto es} \quad (4) \quad b \leq -(s_1 \wedge -s_3)$$

y de (3) resulta

$$s_2 \wedge -s_4 \wedge -b = 0, \quad \text{esto es} \quad (5) \quad s_2 \wedge -s_4 \leq b,$$

y como

$$-(s_1 \wedge -s_3) \in S \quad \text{y} \quad s_2 \wedge -s_4 \in S$$

tenemos que

$$(6) \quad s_2 \wedge -s_4 \in X \quad \text{y} \quad (7) \quad -(s_1 \wedge -s_3) \in Y.$$

Por lo tanto de (4) y (7) resulta que

$$c \leq M = \bigwedge_{y \in Y} h(y) \leq h(-(s_1 \wedge -s_3))$$

y de (5) y (6) resulta $h(s_2 \wedge -s_4) \leq \bigvee_{x \in X} h(x) \leq c$. Por lo tanto

$$c \wedge -h(-(s_1 \wedge -s_3)) = 0 \quad \text{y} \quad h(s_2 \wedge -s_4) \wedge -c = 0,$$

esto es

$$c \wedge h(s_1 \wedge -s_3) = 0 \quad \text{y} \quad h(s_2 \wedge -s_4) \wedge -c = 0.$$

Análogamente se prueba que $w \wedge -z = 0$. Acabamos así de probar que H es una función de $SB(S,b)$ en C.

1) H extiende a h.
Si $s \in S$ entonces $s = s \wedge 1 = s \wedge (b \vee -b) = (s \wedge b) \vee (s \wedge -b)$, y por lo tanto$H(s) = (h(s) \wedge c) \vee (h(s) \wedge -c) = h(s) \wedge (c \vee -c) = h(s)$.

2) H es un homomorfismo.
Como H extiende a h entonces $H(0) = h(0) = 0$, y $H(1) = h(1) = 1$. Sean $x, y \in SB(S,b)$ entonces $H(x) \vee H(y) = (h(s_1) \wedge c) \vee (h(s_2) \wedge -c) \vee (h(s_3) \wedge c) \vee (h(s_4) \wedge -c) = [(h(s_1) \vee h(s_3)) \wedge c) \vee [(h(s_2) \vee h(s_4)) \wedge -c) = [h(s_1 \vee s_3) \wedge c)] \vee [h(s_2 \vee s_4) \wedge -c]$.
Como $x \vee y = (s_1 \wedge b) \vee (s_2 \wedge -b) \vee (s_3 \wedge b) \vee (s_4 \wedge -b) = [(s_1 \vee s_3) \wedge b] \vee [(s_2 \vee s_4) \wedge -b]$, entonces $H(x \vee y) = H(x) \vee H(y)$.
Vimos que si $x = (s_1 \wedge b) \vee (s_2 \wedge -b)$ entonces $-x = (-s_1 \wedge b) \vee (-s_2 \wedge -b)$, luego $H(-x) = (h(-s_1) \wedge c) \vee (h(-s_2) \wedge -c)$, y $-H(x) = -[(h(s_1) \wedge c) \vee (h(s_2) \wedge -c)] = (-h(s_1) \wedge c) \vee (-h(s_2) \wedge -c) = (h(-s_1) \wedge c) \vee (h(-s_2) \wedge -c)$.

Observemos que $H(b) = c$. En efecto, como $b = (1 \wedge b) \vee (0 \wedge -b)$ entonces $H(b) = (h(1) \wedge c) \vee (h(0) \wedge -c) = c \vee 0 = c$. ■

¿Cuantas extensiones podemos construir? Tantas como elementos tiene el segmento $[m, M] \subseteq C$. Luego la extensión no es única salvo que $[m, M] = \{x_0\}$.

Teorema 4.11.1 *Si S es una subálgebra de un álgebra de Boole A, h un homomorfismo de S en un álgebra de Boole completa C, entonces existe un homomorfismo $H : A \to C$ que extiende a h.* (R. Sikorski)

Dem. Sea $\mathcal{F}$ el conjunto de todos los pares (B, H) donde B es una subálgebra de A que contiene a S y H un homomorfismo de B en C que extiende a h. Es claro que $(S, h) \in \mathcal{F}$. Pongamos por definición $(B_1, H_1) \leq (B_2, H_2)$ si y solamente si B_2 es una subálgebra que contiene a B_1 y H_2 es una extensión de H_1. Entonces es claro que $(\mathcal{F}, \leq)$ es un conjunto ordenado. Veamos que es inductivo superiormente. Sea $\mathcal{K} = \{(B_j, H_j)\}_{j \in J}$ una cadena de elementos de $\mathcal{F}$ y consideremos el conjunto $B = \bigcup_{j \in J} B_j$. Este conjunto es una subálgebra que contiene a S. En efecto, como $S \subseteq B_j$, $\forall\, j \in J$, entonces $S \subseteq \bigcup_{j \in J} B_j = B$. Como $0, 1 \in B_j$ cualquiera que sea $j \in J$ entonces $0, 1 \in B$. Si $x, y \in B$ entonces $x \in B_{j_1}$ e $y \in B_{j_2}$ y como por hipótesis $B_{j_1} \subseteq B_{j_2}$ ó $B_{j_2} \subseteq B_{j_1}$ entonces $x, y \in B_{j_2}$ ó $x, y \in B_{j_1}$, por lo tanto $x \wedge y, x \vee y \in B_{j_2}$ ó $x \wedge y, x \vee y \in B_{j_1}$ luego en cualquiera de los dos casos

$x \wedge y, x \vee y \in B$.
Probar que $(B, H) \in \mathcal{F}$, para algún homomorfismo $H : B \to C$, es una cota superior de $\mathcal{K}$ equivale a probar que

$$(B_j, H_j) \leq (B, H), \qquad \forall\ j \in J,$$

esto es que B_j es una subálgebra de B, $\forall\ j \in J$, lo cual es obvio y que H es un homomorfismo de B en C que extiende a H_j, $\forall\ j \in J$.
Sea $b \in B = \bigcup_{j \in J} B_j$, entonces existe $j_0 \in J$ tal que $b \in B_{j_0}$. Pongamos por definición:

$$H(b) = H_{j_0}(b).$$

Observemos que si $j \in J$ es tal que $b \in B_j$, como $\mathcal{K}$ es una cadena entonces :

$$(1) \quad (B_{j_0}, H_{j_0}) \leq (B_j, H_j), \qquad ó \quad (2) \quad (B_j, H_j) \leq (B_{j_0}, H_{j_0}),$$

En el caso (1), como H_j es extensión de H_{j_0} y $b \in B_{j_0}$ entonces $H_j(b) = H_{j_0}(b)$ y en el caso (2) como H_{j_0} es extensión de H_j y $b \in B_j$ entonces $H_{j_0}(b) = H_j(b)$, luego $(B, H) \in \mathcal{F}$ y es además cota superior de $\mathcal{K}$.
Por lo tanto dado $(S, h) \in \mathcal{F}$ existe un elemento maximal $(M, H) \in \mathcal{F}$ tal que $(S, h) \leq (M, H)$.
Si $M \neq A$, entonces existe $a \in A - M$ y por lo tanto $M_1 = SB(M, a)$ es una subálgebra tal que (3) $M \neq M_1$, y por el lema de R. Sikorski sabemos que existe un homomorfismo $H_1 : M_1 \to C$ que extiende a H, entonces por (3) tenemos $(M, H) < (M_1, H_1)$, Absurdo.
Por lo tanto $M = A$. ■

Definición 4.11.3 *Un álgebra de Boole I se dice* **inyectiva** *si todo homomorfismo h de una subálgebra S, de un álgebra de Boole A en I se puede extender a un homomorfismo de A en I.*

Lema 4.11.6 *Un álgebra de Boole es inyectiva si y solamente si es completa*

Dem. $\Longleftarrow$) Si A es completa entonces por el Teorema de R. Sikorski A es inyectiva.
$\Longrightarrow$) Sea A un álgebra de Boole inyectiva. Sabemos que A se puede sumergir en un álgebra de Boole completa C. Sea h la función definida en el subconjunto A de C y que toma sus valores en A por $h(x) = x$, $\forall\ x \in A$. Es claro que h es un homomorfismo de la subálgebra A de C en A, luego como A es inyectiva, h se puede extender a un homomorfismo $H : C \to A$. Probemos que A es completa. Sea $F = \{a_j\}_{j \in J} \subseteq A \subseteq C$, luego como C es completa existe el elemento (1) $c = \bigvee_{j \in J} a_j \in C$, por lo tanto $a_j \leq c$, $\forall j \in J$ y en consecuencia $a_j = h(a_j) = H(a_j) \leq H(c)$, $\forall\ j \in J$ esto es $H(c) \in A$ es una cota superior en A del conjunto F. Supongamos que $a_j \leq b$, $\forall j \in J$, donde (2) $b \in A$. Probemos que $H(c) \leq b$. En efecto de (2) y $A \subseteq C$ resulta que (3) $b \in C$. Luego de (3) y (1) tenemos $c \leq b$ y en consecuencia $H(c) \leq H(b)$ y como $b \in A$, y H es una extensión de h tenemos finalmente $H(b) = h(b) = b$, y por lo tanto $H(c) \leq b$. ■

4.12 Número de epimorfismos entre álgebras de Boole finitas

En esta sección, salvo mención en contrario B_1, B_2 representaran álgebras de Boole, finitas no triviales, $A_1 = \mathcal{A}(B_1)$, $A_2 = \mathcal{A}(B_2)$ los conjuntos de sus átomos.

Lema 4.12.1 *Si $h : B_1 \to B_2$ un epimorfismo, entonces:*

(1) Si $b \in A_2$ existe un único $a \in A_1$ tal que $h(a) = b$.
(M. Abad and L. Monteiro, *Number of epimorphisms between finite symmetric Boolean algebras,* Reports on Mathematical Logic, 10 (1978),3-7).

(2) Si $a \in A_1$ entonces $h(a) = 0$ ó $h(a) \in A_2$.
(M. Abad and L. Monteiro, *Monadic symmetric Boolean algebras,* Notas de Lógica Matemática 37, (1989)).

(3) Si h es inyectivo entonces $h(a) \in A_2$, cualquiera que sea $a \in A_1$.
(M. Abad y L. Monteiro, *Monadic symmetric Boolean algebras* (1989)).

Dem.

(1) Como h es suryectiva existe $x \in B_1$ tal que $h(x) = b$. Es claro que $x \neq 0$ por lo tanto $x = \bigvee_{i=1}^{t} a_i$, donde $a_i \in A_1$, $a_i \leq x$, para $1 \leq i \leq t$. En consecuencia $b = h(x) = \bigvee_{i=1}^{t} h(a_i)$, y por lo tanto $0 \leq h(a_i) \leq b$, $\forall\, i$, $1 \leq i \leq t$. Como b es un átomo entonces $h(a_i) = 0$ ó $h(a_i) = b$, $1 \leq i \leq t$. Pero como $b \neq 0$ entonces necesariamente $h(a_i) \neq 0$ para algún i. Si a_i, a_j son átomos de B_1 que preceden a x, $a_i \neq a_j$ y $h(a_i) = h(a_j) = b$ entonces $0 = h(0) = h(a_i \wedge a_j) = h(a_i) \wedge h(a_j) = b \wedge b = b$, absurdo.

(2) Supongamos que $h(a) \neq 0$, luego existen $b_1, b_2, \ldots, b_r \in A_2$ tales que $h(a) = \bigvee_{i=1}^{r} b_i$. Por (1) sabemos que para cada b_i existe un único $a_i \in A_1$, tal que $h(a_i) = b_i$, luego $h(a) = \bigvee_{i=1}^{r} b_i = \bigvee_{i=1}^{r} h(a_i)$. Por lo tanto $h(a \wedge a_i) = h(a) \wedge h(a_i) = (\bigvee_{i=1}^{r} h(a_i)) \wedge h(a_i) = h(a_i) = b_i$, para cada i, $1 \leq i \leq r$. Como $b_i \neq 0$ entonces $a \wedge a_i \neq 0$ luego $0 < a \wedge a_i \leq a$. En consecuencia $a = a \wedge a_i$ y por lo tanto $h(a) = h(a \wedge a_i) = b_i \in A_2$.

(3) Es una consecuencia inmediata de (2) y de la hipótesis.

■

Lema 4.12.2 *Si B es un álgebra de Boole finita, no trivial, $h : B \to B$ un automorfismo, $x, y \in B$ tales que $h(x) = y$ entonces: $h(\mathcal{A}(x)) = \mathcal{A}(y)$ y $h(\mathcal{A}(-x)) = \mathcal{A}(-y)$.*
(M. Abad and L. Monteiro, *Monadic symmetric Boolean algebras,* Notas de Lógica Matemática 37, (1989)).

Dem. Si $x = 0$ entonces $y = 0$ y por lo tanto $h(\mathcal{A}(0)) = \emptyset = \mathcal{A}(0)$ y $h(\mathcal{A}(-0)) = h(\mathcal{A}(1)) = \mathcal{A}(1) = \mathcal{A}(-0)$.
Supongamos que $x \neq 0$ y sea $a \in h(\mathcal{A}(x))$, esto es, $a = h(b)$ donde $b \in \mathcal{A}(x)$. Como

$b \in \mathcal{A}(B)$ por el Lema 4.12.1,(3) tenemos que $a \in \mathcal{A}(B)$. Como $b \leq x$ entonces $a = h(b) \leq h(x) = y$, esto es $a \in \mathcal{A}(y)$ y por lo tanto $h(\mathcal{A}(x)) \subseteq \mathcal{A}(y)$.
Sea $c \in \mathcal{A}(y)$, entonces por el Lema 4.12.1, (1) existe un único $a \in \mathcal{A}(B)$ tal que $h(a) = c$. Como $a \leq 1 = x \vee -x$ y a es un elemento primo de B tenemos que $a \leq x$ ó $a \leq -x$. Si $a \leq -x$ entonces $c = h(a) \leq h(-x) = -h(x) = -y$, y como $c \leq y$ tendriamos que $c \leq y \wedge -y = 0$, absurdo. Luego $a \leq x$ y por lo tanto $c = h(a) \in h(\mathcal{A}(x))$. Como $h(-x) = -y$, la otra parte del enunciado es obvia dada la demostración anterior. ■

Sabemos por el teorema de Birkhoff que $B_1 \cong \mathcal{P}(A_1)$ y $B_2 \cong \mathcal{P}(A_2)$ donde los isomorfismos $\varphi_1 : B_1 \to \mathcal{P}(A_1)$, $\varphi_2 : B_2 \to \mathcal{P}(A_2)$ estan dados por:

$$\varphi_1(x) = \mathcal{A}(x), \quad x \in B_1 \qquad \text{y} \qquad \varphi_2(y) = \mathcal{A}(y), \quad y \in B_2.$$

Ahora bien, por el Lema 4.9.1 si f es una función de A_2 en A_1 ella induce un homomorfismo $h_f = f^{-1} : \mathcal{P}(A_1) \to \mathcal{P}(A_2)$. Como $\varphi_2 : B_2 \to \mathcal{P}(A_2)$ es un isomorfismo, también ${\varphi_2}^{-1} : \mathcal{P}(A_2) \to B_2$ es un isomorfismo. Además sabemos que $\varphi_2^{-1}(\emptyset) = 0$ y si $X \subseteq A_2$ entonces $\varphi_2^{-1}(X) = \bigvee\limits_{x \in X} x$.
Si $x \in B_1$ pongamos por definición:

$$H_f(x) = (\varphi_2^{-1} \circ h_f \circ \varphi_1)(x).$$

$$\begin{tikzcd}
A_1 & A_2 \arrow[l, "f"'] \\
B_1 \arrow[r, "h_f = f^{-1}"] & B_2 \arrow[d, "\varphi_2^{-1}"] \\
\mathcal{P}(A_1) \arrow[u, "\varphi_1"] \arrow[r, "H_f"] & \mathcal{P}(A_2)
\end{tikzcd}$$

Luego $H_f : B_1 \to B_2$ es un homomorfismo, por ser composición de homomorfismos.

Lema 4.12.3 *Además:*

(1) H_f *inyectiva* $\Longleftrightarrow$ f *suryectiva.*

(2) H_f *suryectiva* $\Longleftrightarrow$ f *inyectiva.*

Dem.

(1) $\Longleftarrow$) Si f es suryectiva entonces por el Lema 4.9.2, h_f es inyectiva, luego H_f es inyectiva, por ser composición de tres funciones inyectivas.

$\Longrightarrow$) Si probamos que h_f es inyectiva entonces por el Lema 4.9.2 resultará que f es suryectiva. Supongamos que (1) $h_f(X_1) = h_f(X_2)$ donde $X_1, X_2 \in \mathcal{P}(A_1)$. Como φ_1 es suryectiva entonces $X_1 = \varphi_1(x_1)$, $X_2 = \varphi_1(x_2)$ donde $x_1, x_2 \in B_1$. Entonces de (1) resulta $h_f(\varphi_1(x_1)) = h_f(X_1) = h_f(X_2) = h_f(\varphi_1(x_2))$ y por lo tanto $H_f(x_1) = H_f(x_2)$, de donde resulta por ser H_f inyectiva que $x_1 = x_2$ y en consecuencia $X_1 = \varphi_1(x_1) = \varphi_1(x_2) = X_2$.

(2) $\Longleftarrow$) Si f es inyectiva entonces por el Lema 4.9.3, h_f es suryectiva y por lo tanto H_f es suryectiva, dado que es composición de tres funciones suryectivas.

$\Longrightarrow$) Supongamos que H_f es suryectiva, esto es $B_2 = H_f(B_1) = \varphi_2^{-1}(h_f(\varphi_1(B_1))$ luego $\varphi_2(B_2) = h_f(\varphi_1(B_1))$, y como φ_1, φ_2 son suryectivas tenemos que $\mathcal{P}(A_2) = h_f(\mathcal{P}(A_1))$, luego h_f es suryectiva, de donde resulta por el Lema 4.9.3 que f es inyectiva.

■

Observación 4.12.1 *Como H_f es un homomorfismo $H_f(0) = 0$ y si $x \in B_1$, $x \neq 0$ entonces $H_f(x) = (\varphi_2^{-1} \circ h_f \circ \varphi_1)(x) = (\varphi_2^{-1} \circ h_f)(\varphi_1(x)) = (\varphi_2^{-1} \circ h_f)(\mathcal{A}(x)) = \varphi_2^{-1}(h_f(\mathcal{A}(x))) = \varphi_2^{-1}(f^{-1}(\mathcal{A}(x))) = \bigvee\{b : b \in f^{-1}(\mathcal{A}(x))\} = \bigvee\{b \in A_2 : f(b) \in \mathcal{A}(x)\} = \bigvee\{b \in A_2 : f(b) \leq x\}$. Además por lo visto en la Observación 4.9.1 $H_f(x) = 0 \iff f(A_2) \subseteq A_1 \setminus \mathcal{A}(x)$.*

De acuerdo con los resultados anteriores tenemos que:

Lema 4.12.4 *Si B_1, B_2 son álgebras de Boole, $A_1 = \mathcal{A}(B_1)$, $A_2 = \mathcal{A}(B_2)$ los conjuntos de sus átomos y $f : A_2 \to A_1$, entonces la función $H_f : B_1 \to B_2$ definida por:*

$$H_f(x) = \begin{cases} 0 & \text{si } x = 0 \\ & \qquad\qquad x \in B_1 \\ \bigvee\{b \in A_2 : f(b) \leq x\} & \text{si } x \neq 0 \end{cases}$$

es un homomorfismo de B_1 en B_2, y si f es inyectiva entonces H_f es un epimorfismo.

Observación 4.12.2 *Si f es inyectiva y $a \in A_1$ entonces $H_f(a) = \bigvee\{b \in A_2 : f(b) \leq a\}$, pero $f(b) \in A_1$, luego de $f(b) \leq a$, y $f(b), a \in A_1$ resulta que $f(b) = a$ y por lo tanto $H_f(a) = \bigvee\{b \in A_2 : f(b) = a\}$. Luego, de acuerdo con el Lema 4.12.1,(2) tenemos los siguientes casos:*

(1) Si $H_f(a) = c \in A_2$ tendremos que $c = H_f(a) = \bigvee\{b \in A_2 : f(b) = a\} \iff \{b \in A_2 : f(b) = a\} = \{c\}, \Longrightarrow f(c) = a$.

(2) Si $H_f(a) = 0 \iff \bigvee\{b \in A_2 : f(b) = a\} = 0 \iff$ no existe b $\in A_2$ tal que *$f(b) = a \iff a \notin Im\,(f)$.*

Además

(3) Si $a \in A_1$, $c \in A_2$ entonces $H_f(a) = c \iff f(c) = a$.
En efecto en (1) vimos que $H_f(a) = c \Longrightarrow f(c) = a$. Recíprocamente si $f(c) = a$ como $H_f(a) = \bigvee\{b \in A_2 : f(b) = a\}$, luego $f(c) = f(b)$ y como f es inyectiva $c = b$, entonces $H_f(a) = c$.

Si B_1 y B_2 son álgebras de Boole y $h : B_1 \to B_2$ es un epimorfismo, $F = Nuc\,(h)$, $\mathcal{F}_2$ el conjunto de todos los filtros de B_2 y $\mathcal{F}_1$ el conjunto de todos los filtros de B_1 que contienen a F. Es claro que $(\mathcal{F}_1, \subseteq)$ y $(\mathcal{F}_2, \subseteq)$ son conjuntos ordenados.

Lema 4.12.5 *Los conjuntos ordenados $\mathcal{F}_2$, $\mathcal{F}_1$ son isomorfos.*

Dem. Si $U \in \mathcal{F}_2$ pongamos por definición $\beta(U) = h^{-1}(U)$. Luego $\beta(U) = h^{-1}(U) \subseteq B_1$. Además si $x \in Nuc\ (h)$, entonces $h(x) = 1 \in U$, luego $x \in h^{-1}(U) = \beta(U)$, por lo tanto $Nuc\ (h) \subseteq \beta\ (U)$.

(A) β es una función de $\mathcal{F}_2$ en $\mathcal{F}_1$.
Probemos que $\beta(U) = h^{-1}(U)$ es un filtro de B_1.

F1) Como $h(1) = 1 \in U$ entonces $1 \in h^{-1}(U)$.

F2) Si $x, y \in h^{-1}(U)$ esto es, $h(x), h(y) \in U$ entonces como U es un filtro $h(x \wedge y) = h(x) \wedge h(y) \in U$ y por lo tanto $x \wedge y \in h^{-1}(U)$.

F3) Si $x \in h^{-1}(U)$ esto es (1) $h(x) \in U$ e $y \in B_1$ verifica $x \leq y$, entonces como h es isótona (2) $h(x) \leq h(y)$. De (1) y (2) resulta por ser U un filtro que $h(y) \in U$, esto es, $y \in h^{-1}(U)$.

(B) $U_1 \subseteq U_2 \iff \beta(U_1) \subseteq \beta(U_2)$ donde $U_1, U_2 \in \mathcal{F}_2$.
$\Longrightarrow$) Sea $y \in \beta(U_1) = h^{-1}(U_1)$, esto es $h(y) \in U_1$, luego como $U_1 \subseteq U_2$ tenemos $h(y) \in U_2$ y por lo tanto $y \in h^{-1}(U_2) = \beta(U_2)$.

$\Longleftarrow$) Sea (1) $y \in U_1$, luego como h es suryectiva existe $x \in B_1$ tal que (2) $h(x) = y$. De (1) y (2) resulta que $x \in h^{-1}(U_1)$ y como por hipótesis $h^{-1}(U_1) = \beta(U_1) \subseteq \beta(U_2) = h^{-1}(U_2)$ tenemos que $x \in h^{-1}(U_2)$ esto es $y = h(x) \in U_2$.

(C) La función β es suryectiva.
Sea M un filtro de B_1 tal que $F = Nuc\ (h) \subseteq M$ y $U = h(M)$. Probemos que $U \in \mathcal{F}_2$ y que $\beta(U) = M$.
$\underline{U \in \mathcal{F}_2.}$

F1) Como $1 \in M$, entonces $1 = h(1) \in h(M) = U$.

F2) Si $a, b \in U = h(M)$ entonces $a = h(m_1)$ y $b = h(m_2)$ donde $m_1, m_2 \in M$, luego (1) $m_1 \wedge m_2 \in M$. Además (2) $a \wedge b = h(m_1) \wedge h(m_2) = h(m_1 \wedge m_2)$. De (1) y (2) resulta $a \wedge b \in h(M) = U$.

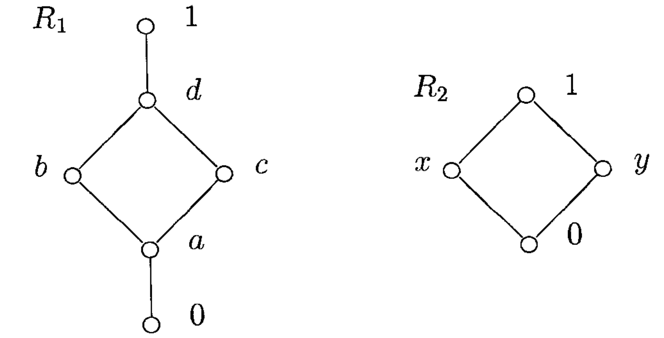
F3) Sean (1) $x \in U = h(M)$, (2) $y \in B_2$ tales que (3) $x \leq y$. De (1) resulta que $x = h(m)$ con $m \in M$, e de (2) resulta por ser h suryectiva que existe $z \in A$ tal que $h(z) = y$. Por (3) $y = y \vee x$ esto es (4) $h(z) = h(m) \vee h(z) = h(m \vee z)$. Como $m \in M$, $m \leq m \vee z$ y M es un filtro tenemos que $m \vee z \in M$ y por lo tanto (5) $h(m \vee z) \in h(M)$. De (4) y (5) resulta que $y = h(z) \in h(M)$.

$\underline{\beta(U) = M.}$ Ya sabemos que $F = Nuc\ (h) \subseteq h^{-1}(U) = M$. Es bien conocido que $\underline{M \subseteq h^{-1}(h(M))}$. Probemos que $h^{-1}(h(M)) \subseteq M$. En efecto, sea $x \in h^{-1}(h(M))$ esto es, $h(x) \in h(M)$ y por lo tanto $h(x) = h(m)$ para algún (1) $m \in M$. Luego existe (2) $f \in Nuc\ (h)$ tal que (3) $x \wedge f = m \wedge f$. Como por hipótesis $Nuc\ (h) \subseteq M$ entonces por (2) resulta (4) $f \in M$. De (1) y (4) tenemos que (5) $m \wedge f \in M$ y de (3) y (5) que (6) $x \wedge f \in M$ y como $x \wedge f \leq x$ y M es un filtro tenemos finalmente que $x \in M$.

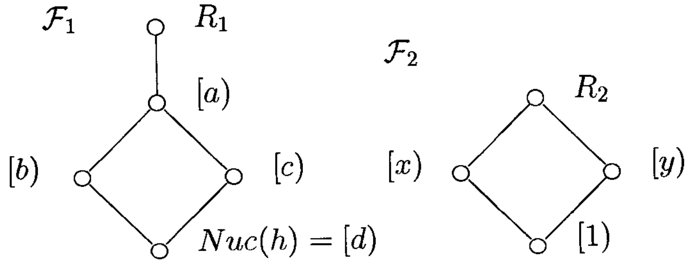
∎

Corolario 4.12.1 *Existe correspondencia biyectiva entre los elementos maximales de los conjuntos ordenados $\mathcal{F}_2$ y $\mathcal{F}_1$.*

Observación 4.12.3 *Sean R_1, R_2 los reticulados distributivos con primer y último elemento, cuyos diagramas se indican:*



Consideremos el epimorfismo (de reticulado) $h : R_1 \to R_2$ definido por $h(0) = h(a) = 0$, $h(b) = x$, $h(c) = y$, $h(d) = h(1) = 1$. Entonces $Nuc\ (h) = \{d, 1\}$. Los diagramas del conjunto $\mathcal{F}_1$ de todos los filtros de R_1 que contienen a $Nuc(h)$ y del conjunto $\mathcal{F}_2$, de todos los filtros de R_2 se indican a continuación. Luego $\mathcal{F}_1$ y $\mathcal{F}_2$ no son conjuntos ordenados isomorfos.



Dadas las álgebras de Boole finitas A, A'. Si A' es un álgebra trivial es claro que existe un único epimorfismo de A en A'. Supongamos que ambas álgebras no son triviales, que A tiene r átomos y A' tiene t átomos. Pongamos $A = B_r$ y $A' = B_t$ entonces $N[B_r] = 2^r$ y $N[B_t] = 2^t$, luego para que existan epimorfismos de B_r en B_t debe ser $2^r \geq 2^t$, y por lo tanto $r = log_2\ 2^r \geq log_2\ 2^t = t$, esto es $r = N[A_r] \geq N[A_t] = t$ donde A_r, A_t son los conjuntos de átomos de B_r, B_t, respectivamente. Vimos en el Lema 4.12.4 que a toda función inyectiva $f : A_t \to A_r$ le corresponde un epimorfismo $H_f : B_r \to B_t$. Sea $FI(A_t, A_r)$ el conjunto de todas las funciones inyectivas de A_t en A_r y $Epi(B_r, B_t)$ el conjunto de todos los epimorfismos de B_r en B_t. Pongamos $\mathbf{\Phi}(f) = H_f$. Es claro, de acuerdo con el Lema 4.12.4 que $\mathbf{\Phi}$ es una función. Tenemos así que:

$$\mathbf{\Phi} : FI(A_t, A_r) \to Epi(B_r, B_t).$$

Lema 4.12.6 $\mathbf{\Phi}$ *es biyectiva.*

Dem.

1) $\mathbf{\Phi}$ es inyectiva.
Sean $f, g \in FI(A_t, A_r)$, $f \neq g$ entonces existe $a \in A_t$ tal que $f(a) \neq g(a)$. Entonces $f(a) = b \in A_r$, $g(a) = c \in A_r$ y $b \neq c$ y por lo visto en la Observación 4.12.2, (3): $f(a) = b \iff H_f(b) = a$ y $g(a) = c \iff H_g(c) = a$, luego (1) $H_f(b) = H_g(c)$. Si $H_g(b) = a$ entonces ello equivale a decir que $g(a) = b$, absurdo. Por lo tanto $H_f(c) \neq H_g(c)$.

2) Φ es suryectiva.
Sea $h \in Epi(B_r, B_t)$, y $a \in A_t$, luego $[a)$ es un ultrafiltro de B_t y en consecuencia por el Corolario 4.12.1, $h^{-1}([a))$ es un ultrafiltro de B_r, en consecuencia $h^{-1}([a)) = [b)$, donde $b \in A_r$, y además $Nuc\ (h) \subseteq h^{-1}([a))$. Pongamos $f(a) = b$. Por el Corolario 4.12.1 existe correspondencia biyectiva entre los ultrafiltros de B_t y los ultrafiltros de B_r que contienen al núcleo de h, por lo tanto f está bien definida. Probemos que $f \in FI(A_t, A_r)$. Sean $a_i, a_j \in A_t$ tales que $a_i \neq a_j$ luego $[a_i) \neq [a_j)$, por lo tanto (1) $[a_i) \not\subseteq [a_j)$ ó (2) $[a_j) \not\subseteq [a_i)$. Supongamos que se verifica (1), luego existe $y \in [a_i)$ tal que $y \notin [a_j)$. Como h es suryectiva entonces $y = h(x)$ con $x \in B_r$. Luego $h(x) \in [a_i)$ y por lo tanto $x \in h^{-1}([a_i))$ y $x \notin h^{-1}([a_j))$ en consecuencia $[b_i) = h^{-1}([a_i)) \neq h^{-1}([a_j)) = [b_j)$ y por lo tanto $b_i \neq b_j$.
Probemos que $\Phi(f) = h$, esto es, que $H_f = h$. Como B_1 es finita para demostrar que estos dos epimorfismos son iguales nos basta demostrar que $H_f(b) = h(b)$, para todo $b \in A_r$. Si $b \in A_r$ entonces por el Lema 4.12.1,(2) sabemos que (1) $H_f(b) = a \in A_t$ ó (2) $H_f(b) = 0$. En la Observación 4.12.2,(3) vimos que $H_f(b) = a \iff f(a) = b$ y de acuerdo con la definición de f : $h^{-1}([a)) = [b)$. Como $b \in [b)$ tenemos $b \in h^{-1}([a))$ entonces $h(b) \in [a)$, esto es, (3) $a \leq h(b)$.Como $b \in A_r$, y h es un epimorfismo por el Lema 4.12.1,(2) tenemos: (4) $h(a) = 0$ ó (5) $h(a) \in A_t$. Como (4) se contradice con (3) entonces de (3) y (5) resulta por ser $h(b), a \in A_t$ que $h(b) = a$ y por lo tanto $H_f(b) = h(b)$.
Si ocurre (2) vimos en la Observación 4.12.2, (2) que $b \notin Im\ (f)$. Como h es un epimorfismo, por el Lema 4.12.1,(2) : (6) $h(b) = a \in A_t$ ó (7) $h(b) = 0$. Si ocurre (6) $h^{-1}([a))$ es un ultrafiltro de B_r y por lo tanto $h^{-1}([a)) = [c)$, donde $c \in A_r$, por lo tanto de acuerdo con la definición de f tenemos que $f(a) = c$. Como $h(b) = a$ entonces $b \in h^{-1}([a)) = [c)$, esto es, $c \leq b$ donde $c, b \in A_r$ y por lo tanto $c = b$, luego $f(a) = c = b$, esto es $b \in Im\ (f)$, absurdo. Luego $h(b) = 0 = H_f(b)$.

■

Pongamos por definición:

$$V_{r,t} = \begin{cases} 0 & si\ r < t, \\ \dfrac{r!}{(r-t)!} & si\ r \geq t. \end{cases}$$

Entonces:

$$N[Epi(B_r, B_t)] = N[FI(A_t, A_r)] = V_{r,t}.$$

Observemos que esta fórmula es válida aún en el caso en que el álgebra A' tenga un solo elemento, luego $A' = A_0$ y por lo tanto $V_{r,0} = \dfrac{r!}{(r-0)!} = 1$.

Si representamos con $Aut(B)$ el número de automorfismos de un álgebra de Boole B con r átomos entonces tenemos en particular que:

$$N[Aut(B)] = V_{r,r} = r!.$$

Sea $h \in Epi(B_r, B_t)$ y $\alpha \in Aut(B_t)$ entonces es claro que $h_1 = \alpha \circ h \in Epi(B_r, B_t)$. Además $Nuc\ (h_1) = \{x \in B_r : h_1(x) = 1\} = \{x \in B_r : \alpha(h_1(x)) = 1\}$, y como α es inyectiva $\alpha(h_1(x)) = 1 = \alpha(1) \iff h(x) = 1$. Por lo tanto $Nuc\ (h_1) = Nuc\ (h)$.

Entonces es natural formularse la siguiente pregunta:

¿Dado $h \in Epi(B_r, B_t)$, cuantos epimorfismos de B_r en B_t tienen el mismo núcleo que h?

Como en B_t existen $t!$ automorfismos entonces existen por lo menos $t!$ epimorfismos de B_r en B_t cuyo núcleo es igual al núcleo de h.
Si $h_1 \in Epi(B_r, B_t)$ es tal que $Nuc\ (h_1) = Nuc\ (h)$, entonces sabemos que existe $\alpha \in Aut\ (B_t)$ tal que $h_1 = \alpha \circ h$.

$$\begin{tikzcd}
B_r \arrow[r, "h"] \arrow[d, "h_1"'] & B_t \arrow[dl, "\alpha"] \\
B_r &
\end{tikzcd}$$

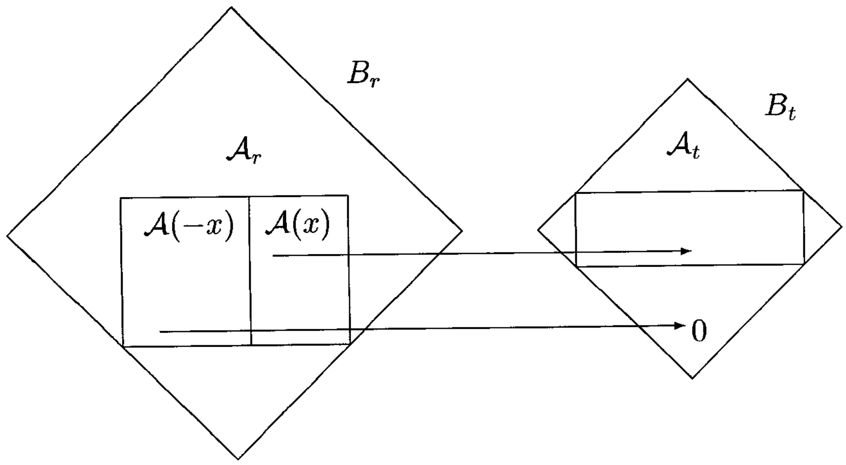
Acabamos así de probar que dado $h \in Epi(B_r, B_t)$ existen $t!$ epimorfismos de B_r en B_t que tienen el mismo núcleo que h.

Dada B_r existen $\binom{r}{t}$, donde $t \leq r$ cocientes B_r con t átomos, esto es isomorfos a B_t y como para cada $h \in EPI(B_r, B_t)$ existen $t!$ epimorfismos que tienen el mismo núcleo que h entonces existen
$$\frac{N[Epi(B_r, B_t)]}{N[Aut(B_t)]} = \binom{r}{t}$$
epimorfismos de B_r en B_t con núcleos diferentes.

Observemos que cada $h_1 \in EPI(B_r, B_t)$ tal que $Nuc\ (h_1) = Nuc\ (h)$, proviene de una función $f_1 \in FI(A_t, A_r)$ tal que $Im\ (f_1) = Im\ (f)$ y recíprocamente si $f_1, f \in FI(A_t, A_r)$ son tales que $Im\ (f_1) = Im\ (f)$ entonces $Nuc(H_{f_1}) = Nuc(H_f)$.
Otro modo de probar lo anterior es el siguiente: Si $h \in EPI(B_r, B_t)$ sabemos que $B_t \cong B_r/Nuc(h)$. Como B_r es finita $Nuc(h) = [x)$, con $x \in B_r$ y también sabemos que $B_r/[x) \cong (x]$, por lo tanto $(x] \cong B_t$, esto es x debe ser supremo de t átomos de B_r. Como $\binom{r}{t}$ es el número de elementos de B_r que son supremo de t átomos, entonces existen: $\binom{r}{t}$ epimorfismos de B_r en B_t con núcleos diferentes.

Si $x \in B_r$ y $h \in Epi(B_r, B_t)$ entonces $h(x) = 0$ ó $h(x) \neq 0$. Si $x = 0$ es claro que todo $h \in Epi(B_r, B_t)$ verifica $h(x) = h(0) = 0$.

Si $x \neq 0$ ¿Cuántos epimorfismos h de B_r en B_t verifican $h(x) = 0$?
Sea $[f) = Nuc(h)$, si $h(x) = 0$ como $h(0) = 0$ entonces $x \equiv 0$ (mód $[f)$), por lo tanto $x \wedge f = 0 \wedge f = 0$ y en consecuencia $f \leq -x$. Como $x \neq 0$ entonces x es supremo de s átomos de B_r, $1 \leq s \leq r$, y por lo tanto $-x$ es supremo de $r - s$ átomos de B_r.
Si $r - s < t$ no existen funciones inyectivas de A_t en $\mathcal{A}(-x)$, por lo tanto ningún homomorfismo verifica $h(x) = 0$, y si $r - s \geq t$ entonces existen $V_{r-s,t} = \dfrac{(r-s)!}{(r-s-t)!}$ epimorfismos h tales que $h(x) = 0$ y $V_{r,t} - V_{r-s,t}$ homomorfismos h tales que $h(x) \neq 0$.



Observación 4.12.4 *Dadas las álgebras de Boole B_r y B_t donde $r \geq t$ y una función inyectiva $f : A_t \to A_r$, podemos definir una función $f^* : A_r \to A_t \cup \{0\}$ del siguiente modo:*

$$f^*(a) = \begin{cases} 0 & si\ a \notin Im\,(f) \\ b & si\ b = f(a) \end{cases}$$

entonces definiendo $H^* : B_r \to B_t$

$$H^*(x) = \begin{cases} 0 & si\ x = 0 \\ \bigvee\{f^*(a) : a \leq x\} & si\ x \neq 0 \end{cases}$$

tenemos que H^* es un epimorfismo.

5 APENDICE

5.1 Reticulados distributivos simples

Definición 5.1.1 *Un reticulado distributivo R con primer y último elemento, esto es acotado, se dice* **simple** *si*

1) R no es trivial.

2) Las únicas imágenes homomórficas de R son isomorfas a R ó a un reticulado trivial, esto es con un sólo elemento.

Definición 5.1.2 *Un reticulado distributivo R acotado se dice* **semisimple** *si es producto subdirecto de reticulados distributivos acotados simples*

Sea R un reticulado distributivo acotado, no trivial, y P un filtro primo de R. Dado el reticulado $\mathbf{B} = \{0, 1\}$ consideremos la tranformación $h : R \to \mathbf{B}$ definida por

$$h(x) = \begin{cases} 0 & si\ x \notin P \\ \\ 1 & si\ x \in P \end{cases} \qquad x \in R.$$

En forma análoga a la indicada en el Lema 4.7.29 se prueba que h es un epimorfismo de R en $\mathbf{B}$.

Supongamos ahora que R es un reticulado distributivo acotado, no trivial, y que existe un epimorfismo de R en $\mathbf{B}$. Sea $P = \{x \in R : h(x) = 1\}$. Por lo indicado en el Lema 4.6.10 P es un filtro. Veamos que es un filtro primo de R. Si $x \vee y \in P$ esto es $h(x) \vee h(y) = h(x \vee y) = 1$ luego como h toma sus valores en $\mathbf{B}$ entonces $h(x) = 1$ ó $h(y) = 1$, esto es $x \in P$ ó $y \in P$, por lo tanto P es primo.

Teorema 5.1.1 *Para que un reticulado distributivo acotado sea simple es necesario y suficiente que contenga sólo dos elementos.*

Dem. $\Rightarrow$) Sea R un reticulado distributivo acotado simple. Luego R no es trivial. Supongamos que existe $a \in R \setminus \{0, 1\}$. Como $a \neq 0$ entonces el filtro principal $[a)$ es propio, por lo tanto (ver Teorema 4.7.5), existe un filtro primo P tal que $[a) \subseteq P$, luego $a \in P$. La transformación $h : R \to \mathbf{B}$ definida por:

$$h(x) = \begin{cases} 0 & si\ x \notin P \\ \\ 1 & si\ x \in P \end{cases} \qquad x \in R,$$

es un epimorfismo de R en $\mathbf{B}$, que no es un isomorfismo dado que $a \neq 1$ y $h(a) = h(1) = 1$. Luego $h(R) = \mathbf{B}$ es una imagen homomórfica de R que no es trivial ni isomorfa a R, lo que contradice la hipótesis de que R es simple.
$\Leftarrow$) El reticulado $\mathbf{B}$ no es trivial, y claramente si A es una imagen homomórfica de $\mathbf{B}$ entonces A es un reticulado trivial ó isomorfo a $\mathbf{B}$. Luego $\mathbf{B}$ es simple. ■

Vamos a demostrar los siguientes resultados:

1. El único (a menos de isomorfismos) reticulado distributivo acotado, subdirectamente irreducible es $\{0,1\}$.

2. Para que un reticulado distributivo acotado no trivial, sea subdirectamente reducible es necesario y suficiente que el no sea simple.

1) Sea R un reticulado distributivo acotado con más de dos elementos y $E = \mathcal{P}(R)$ el conjunto de sus filtros primos. Dado $P \in E$ sea p el epimorfismo de R en $\mathbf{B}$ definido por:

$$p(x) = \begin{cases} 0 & si\ x \notin P \\ 1 & si\ x \in P \end{cases} \qquad x \in R.$$

Consideremos el reticulado distributivo

$$\mathbf{B}^E = \prod_{P \in E} B_P,$$

donde $B_P = \mathbf{B}$ para todo $P \in E$
Dado $P \in E$ sea F la función definida por :

$$F(P) = p(f), \qquad \text{donde} \quad f \in R$$

y donde $p : R \to \mathbf{B}$ es el epimorfismo determinado por P.
Luego como para cada $P \in E$, $F(P) = p(f) \in \mathbf{B}$ tenemos que $F \in \mathbf{B}^E$. Sea $\varphi(f) = F$, luego $\varphi : R \to \mathbf{B}^E$ y por lo tanto φ es una función de R sobre $R' = \{\varphi(f)\}_{f \in R} \subseteq \mathbf{B}^E$. En forma análoga a la indicada en el Teorema 4.7.8 se prueba que, cualesquiera que sean $f, g \in R$: 1) $\varphi(f \wedge g) = \varphi(f) \wedge \varphi(g)$, 2) $\varphi(f \vee g) = \varphi(f) \vee \varphi(g)$, 3) $\varphi(0) = \mathbf{0}$ y 4) $\varphi(1) = \mathbf{1}$. Luego φ es un epimorfismo de R en R' y por lo tanto R' es un subreticulado de $\mathbf{B}^E$. Veamos que φ es inyectiva. En efecto sean $f, g \in R$ tales que $f \neq g$, luego (i) $f \not\leq g$ ó (ii) $g \not\leq f$. Probemos que $F = \varphi(f) \neq \varphi(g) = G$. Supongamos que se verifica (i), luego $g \notin [f)$ y por lo tanto existe un filtro primo P tal que $[f) \subseteq P$, luego $f \in P$ y $g \notin P$. Entonces $F(P) = p(f) = 1$ y $G(P) = p(g) = 0$, por lo tanto $F \neq G$.

Vamos a demostrar que R es producto subdirecto de la familia de reticulados B_P, con $P \in E$. Ya vimos que R es isomorfo al reticulado $R' \subseteq \prod\limits_{P \in E} B_P$. Es claro que $\Pi_P(R') = \Pi_P(\varphi(R)) \subseteq \{0,1\}$. Como $\Pi_P(\mathbf{0}) = \Pi_P(\varphi(0)) = 0$ y $\Pi_P(\mathbf{1}) = \Pi_P(\varphi(1)) = 1$ entonces $\Pi_P(R') = \{0,1\}$.
Además ninguna proyección es un isomorfismo pués $R \cong R'$ tiene más de dos elementos. Acabamos así de probar que todo reticulado distributivo acotado con más de dos elementos es producto subdirecto de reticulados simples por lo tanto es semisimple. Este resultado se debe a M. Stone y G. Birkhoff, pero la demostración indicada precedentemente es diferente y fue dada por A. Monteiro.

Si $\mathbf{B} = \{0,1\}$ fuese subdirectamente reducible entonces $\mathbf{B}$ sería isomorfo a un subreticulado S de un producto directo de reticulados $\prod\limits_{i \in I} A_i$ y más precisamente $\mathbf{B} \cong \{\mathbf{0}, \mathbf{1}\} = S$. Además como estamos suponiendo que $\mathbf{B}$ es subdirectamente reducible tenemos que $\Pi_i(S) = A_i$ para todo $i \in I$, pero $\Pi_i(S) = \Pi_i\{\mathbf{0}, \mathbf{1}\} = \{0,1\}$, entonces tendríamos

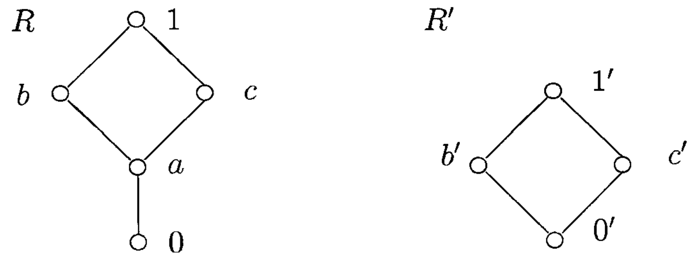
$A_i = \{0, 1\}$ y todas las proyecciones serían isomorfismos, absurdo.
2) Sea R un reticulado distributivo acotado, no trivial, subdirectamente reducible, entonces si R fuese simple por 1) sería subdirectamente irreducible, absurdo. Recíprocamente si R no es simple entonces R tiene más de dos elementos y en consecuencia por 1) R es subdirectamente reducible.

5.2 Imágenes homomórficas de un reticulado distributivo

Vimos (Lema 4.6.18) que si F es un filtro de un reticulado R y definimos

$$(*) \quad x \equiv y \ (\textit{mód. } F) \iff \text{existe } f \in F \ \text{ tal que } \ x \wedge f = y \wedge f$$

entonces $\equiv$ es una relación de congruencia. Observemos que si R no tiene último elemento entonces la *propiedad reflexiva* se demuestra del siguiente modo: Dado $a \in R$ entonces como cualquiera que sea $f \in F$ se verifica $a \wedge f = a \wedge f$ luego $a \equiv a$ cualquiera que sea $a \in R$. Por lo tanto el conjunto cociente, que se nota $R/\equiv$ o R/F, es un reticulado y R/F es una imagen homomórfica de R. Observemos que si $F = R$ entonces R/F tiene un sólo elemento y que si R tiene último elemento 1 y $F = \{1\}$ entonces R/F es isomorfo a R.
En la Observación 3.4.2 indicamos los siguientes reticulados distributivos acotados:



La función $h : R \to R'$ definida por $h(0) = h(a) = 0'$, $h(b) = b'$, $h(c) = c'$, $h(1) = 1'$ es un homomorfismo suryectivo, por lo tanto R' es una imagen homomórfica de R. Sin embargo no existe ningún filtro F de R tal que R/F sea isomorfo a R'.

A. Monteiro indicó una construcción que permite determinar todas las imágenes homomórficas de un reticulado distributivo. Las demostraciones nunca fueron publicadas pero fueron expuestas en dos cursos realizados en la Universidad Nacional del Sur [38], [41] y en el *Simposio Panamericano de Matemática Aplicada* realizado en Buenos Aires en 1968, donde expuso el trabajo *Generadores de reticulados distributivos finitos* [43]. Vamos a indicar a continuación estos resultados.

Recordemos que un homomorfismo de un reticulado distributivo A en un reticulado distributivo A' es una función $\alpha : A \to A'$ que verifica: H1) $\alpha(x \wedge y) = \alpha(x) \wedge \alpha(y)$ y H2) $\alpha(x \vee y) = \alpha(x) \vee \alpha(y)$.

Lema 5.2.1 *Sean A y A' reticulados distributivos, A' no trivial y α un epimorfismo de A en A'. $\mathbf{P}$, $\mathbf{P}'$ las familias de los filtros primos de A y A'. Si $P' \in \mathbf{P}'$ entonces $P = \alpha^{-1}(P') \in \mathbf{P}$.*

Dem. Como A' es no trivial entonces $\mathbf{P}' \neq \emptyset$. Sabemos (ver Lema 4.12.5) que $P = \alpha^{-1}(P')$ es un filtro, veamos que es primo. Si $P = A$ entonces $\alpha(x) \in P'$ para todo $x \in A$ luego $\alpha(A) = P'$, pero α es un epimorfismo $\alpha(A) = A'$, entonces $P' = A'$, absurdo. Por lo tanto P es un filtro propio. Supongamos que $x \vee y \in P$ esto es $\alpha(x) \vee \alpha(y) = \alpha(x \vee y) \in P'$ luego como P' es primo tenemos que $\alpha(x) \in P'$ ó $\alpha(y) \in P'$ esto es $x \in P$ ó $y \in P$. ■

Observemos que si $\mathbf{P}' = \emptyset$ esto es A' tiene un sólo elemento entonces:

$$\mathbf{Q} = \{\alpha^{-1}(P') : P' \in \mathbf{P}'\} = \emptyset.$$

Lema 5.2.2 *Sean A y A' reticulados distributivos, A' no trivial, α un epimorfismo de A en A', $\mathbf{P}'$ la familia de todos los filtros primos de A' y $\mathbf{Q} = \alpha^{-1}(\mathbf{P}')$ entonces: $\alpha(a) = \alpha(b)$ $\iff$ $\{Q \in \mathbf{Q} : a \in Q\} = \{P \in \mathbf{Q} : b \in P\}$*

Dem. $\Rightarrow$) Sea $Q \in \mathbf{Q}$ tal que $a \in Q$, luego $Q = \alpha^{-1}(P')$ donde $P' \in \mathbf{P}'$, luego $\alpha(a) \in P'$ y como por hipótesis $\alpha(a) = \alpha(b)$ tenemos que $\alpha(b) \in P'$ y por lo tanto $b \in Q = \alpha^{-1}(P')$.
$\Leftarrow$) Si $\alpha(a) \neq \alpha(b)$ entonces por el Corolario 4.7.5 existe un filtro primo P' de A' que contiene a uno de los elementos sin contener al otro, lo que contradice la hipótesis. ■

Observemos que si A' tiene un sólo elemento entonces $\mathbf{P}' = \emptyset$ y (*) $\alpha(a) = \alpha(b)\ \forall\ a, b \in A$, y como $\mathbf{Q} = \emptyset$ entonces claramente $\{Q \in \mathbf{Q} : a \in Q\} = \emptyset = \{P \in \mathbf{Q} : b \in P\}$. Como se verifica (*) tambien es claro que la recíproca es verdadera.

Estos resultados nos conducen a la siguiente construcción. Sea $\mathbf{Q}$ un conjunto, no vacío, de filtros primos de un reticulado distributivo A. Notaremos $a \equiv b$, (mód. $\mathbf{Q}$) o mas sencillamente, si fijamos $\mathbf{Q}$, $a \equiv b$, para indicar que la condición del Lema precedente se verifica, entonces se prueba en forma inmediata que: "$\equiv$" es una relación de equivalencia. Veamos que ella es compatible con las operaciones $\wedge$ y $\vee$, esto es "$\equiv$" es una congruencia definida sobre A. En efecto supongamos que $a \equiv b$ y $a' \equiv b'$, esto es $\mathcal{Q}_1 = \{Q \in \mathbf{Q} : a \in Q\} = \{P \in \mathbf{Q} : b \in P\} = \mathcal{Q}_2$ y $\mathcal{Q}_3 = \{Q' \in \mathbf{Q} : a' \in Q'\} = \{P' \in \mathbf{Q} : b' \in P'\} = \mathcal{Q}_4$. Sea $S \in \mathbf{Q}$ tal que $a \wedge a' \in S$ luego como $a \wedge a' \leq a$, $a \wedge a' \leq a'$ y $a \wedge a' \in S$, tenemos que $a, a' \in S$ donde $S \in \mathbf{Q}$ luego $S \in \mathcal{Q}_1 = \mathcal{Q}_2$ y $S \in \mathcal{Q}_3 = \mathcal{Q}_4$, por lo tanto $b, b' \in S$ luego $S \in \mathbf{Q}$ verifica que $b \wedge b' \in S$. Análogamente se demuestra que si $T \in \mathbf{Q}$ es tal que $b \wedge b' \in S$ entonces $a \wedge a' \in S$, luego $a \wedge a' \equiv b \wedge b'$ (mód. $\mathbf{Q}$).
Supongamos ahora que $S \in \mathbf{Q}$ verifica $a \vee a' \in S$, como S es un filtro primo entonces $a \in S$ ó $a' \in S$. Si $a \in S$, esto es $S \in \mathcal{Q}_1 = \mathcal{Q}_2$ entonces $b \in S$ y por lo tanto $b \vee b' \in S$. Análogamente si $a' \in S$ se demuestra que $b \vee b' \in S$, y que si $S \in \mathbf{Q}$ verifica $b \vee b' \in S$, entonces $a \vee a' \in S$, luego $a \vee a' \equiv b \vee b'$ (mód. $\mathbf{Q}$).
Sea $C(a)$ la clase de equivalencia que contiene al elemento $a \in A$, esto es $C(a) = \{x \in A : x \equiv a\}$ y $A' = A/\!\equiv$ el conjunto cociente de A por la relación "$\equiv$". Observemos que si $\mathbf{Q} = \emptyset$ entonces es claro que $\equiv$ es una congruencia, pués $a \equiv b,\ \forall a, b \in A$.
Algebrizemos A' definiendo las operaciones $\wedge$ y $\vee$ sobre A' del siguiente modo:

$$C(a) \wedge C(b) = C(a \wedge b) \quad \text{y} \quad C(a) \vee C(b) = C(a \vee b).$$

Entonces la transformación $h(a) = C(a)$, verifica las condiciones H1 y H1, por lo tanto $(A', \wedge, \vee)$ es un reticulado distributivo, y A' es una imagen homomórfica de A. La transformación h se denomina epimorfismo natural. Notaremos $A/\mathbf{Q}$ para representar el reticulado distributivo obtenido de este modo. Vamos a demostrar que todas las imágenes homomórficas de un reticulado distributivo A pueden obtenerse del modo que acabamos de indicar. Sea A' una imagen homomórfica de A. Si A' tiene un sólo elemento, entonces considerando el conjunto $\mathbf{Q} = \emptyset$ de filtros primos tenemos que $A/\emptyset$ tiene un sólo elemento y por lo tanto A' y $A/\emptyset$ son isomorfos. Supongamos ahora que A' tiene mas de un elemento y sea $\mathbf{P}'$ el conjunto de todos filtros primos de A' y $\mathbf{Q} = \alpha^{-1}(\mathbf{P}')$. Vamos a demostrar que el $A/\mathbf{Q}$ es isomorfo al reticulado A'. Sea $H : A/\mathbf{Q} \to A'$ la función definida por $H(C(a)) = \alpha(a)$ y probemos que H es un isomorfismo. 1) H es suryectiva. En efecto dado $a' \in A'$, como α es suryectiva, existe $a \in A$ tal que $\alpha(a) = a'$, luego $H(C(a)) = \alpha(a) = a'$. 2) $H(C(a) \wedge C(b)) = H(C(a)) \wedge H(C(b))$. En efecto $H(C(a) \wedge C(b)) = H(C(a \wedge b)) = \alpha(a \wedge b) = \alpha(a) \wedge (b) = H(C(a)) \wedge H(C(b))$. En forma análoga se prueba 3) $H(C(a) \vee C(b)) = H(C(a)) \vee H(C(b))$. 4) H es inyectiva. Supongamos que $H(C(a)) = H(C(b))$ esto es $\alpha(a) = \alpha(b)$, luego por el Lema 5.2.2 $\{Q \in \mathbf{Q} : a \in Q\} = \{P \in \mathbf{Q} : b \in P\}$ esto es $a \equiv b$ (mód. $\mathbf{Q}$) y por lo tanto $C(a) = C(b)$.

Puede ocurrir que existan dos conjuntos $\mathbf{Q}_1$ y $\mathbf{Q}_2$ de filtros primos de A tales que $\mathbf{Q}_1 \neq \mathbf{Q}_2$, y que el reticulado $A/\mathbf{Q}_1$ sea isomorfo a $A/\mathbf{Q}_2$. Basta observar que si $\mathbf{Q}_1 = \{P_1\}$ y $\mathbf{Q}_2 = \{P2\}$, donde P_1 y P_2 son dos filtros primos de A tales que $P_1 \neq P_2$, entonces los reticulados $A/\mathbf{Q}_1$, y $A/\mathbf{Q}_2$ son isomorfos al reticulado $\{0,1\}$ donde $0 < 1$.

Si $\mathbf{P}$ es el conjunto de todos los filtros primos del reticulado distributivo A entonces $A/\mathbf{P} \cong A$. En efecto supongamos que $C(x) \neq \{x\}$ para algún $x \in A$ entonces existe (1) $y \in C(x)$ tal que $y \neq x$. Supongamos que $y \not\leq x$ entonces existe $P \in \mathbf{P}$ tal que $x \in P$ e $y \notin P$ y en consecuencia $x \not\equiv y$ lo que contradice (1).

Observemos que en el estudio de los reticulados distributivos con primer y último elemento, para definir un homomorfismo h debemos suponer H1, H2 , H3) $\alpha(0) = 0$, y H4) $\alpha(1) = 1$.

Sea R un reticulado distributivo acotado, no trivial, $\mathbf{Q}$ un conjunto de filtros primos de R, e $\mathbf{I} = \{\complement P : P \in \mathbf{Q}\}$. Como los elementos de $\mathbf{Q}$ son filtros primos entonces los elementos de $\mathbf{I}$ son ideales primos. Sean $F = \bigcap\limits_{P\in\mathbf{Q}} P$, e $Y = \bigcap\limits_{I\in\mathbf{I}} I$.

Lema 5.2.3 $F \cup Y = R \iff \mathbf{Q}$ *tiene un sólo elemento.*

Dem. De $F \cup Y = R$ resulta que

$$\bigcup_{P\in\mathbf{Q}} P = \bigcup_{I\in\mathbf{I}} \complement I = \complement \bigcap_{I\in\mathbf{I}} I = \complement Y \subseteq F = \bigcap_{P\in\mathbf{Q}} P$$

luego tenemos que para todo $P \in \mathbf{Q}$:

$$P \subseteq \bigcup_{P\in\mathbf{Q}} P \subseteq \bigcap_{P\in\mathbf{Q}} P \subseteq P$$

por lo tanto $\bigcap\limits_{P\in\mathbf{Q}} P = P, \quad \forall\ P \in \mathbf{Q}$, y en consecuencia $\mathbf{Q}$ tiene un sólo elemento. Recíprocamente si $\mathbf{Q}$ tiene un sólo elemento P entonces $F = P$ e $Y = \complement P$, luego $F \cup Y = R$. ∎

Si $\mathbf{Q}$ es un conjunto de filtros primos de R e $\mathbf{I} = \{\complement P : P \in \mathbf{Q}\}$, dado $a \in R$ sean $\mathcal{P}(a) = \{P \in \mathbf{Q} : a \in P\}$ e $\mathcal{I}(a) = \{I \in \mathbf{I} : a \in I\}$.
Si $\mathbf{Q}$ tiene un sólo elemento P ya sabemos que $R/\mathbf{Q}$ es isomorfo al reticulado $\{0,1\}$ con $0 < 1$ y que $C(1) = P$ y $C(0) = \complement P$.

Lema 5.2.4 *Si una familia* $\mathbf{Q}$ *de filtros primos de* R *tiene más de un elemento entonces la clase de equivalencia (mód.* $\mathbf{Q}$*) que contiene al elemento* $a \in R$ *es el conjunto:*

$$X(a) = \bigcap_{P \in \mathcal{P}(a)} P \;\cap\; \bigcap_{I \in \mathcal{I}(a)} I.$$

(L. Monteiro, (1966)).

Dem. Como $\mathbf{Q}$ tiene más de un elemento entonces $F \cup Y \neq R$ esto es $\complement(F \cup Y) \neq \emptyset$.

1) Si $a = 1$ entonces $\mathcal{P}(1) = \{P \in \mathbf{Q} : 1 \in P\} = \mathbf{Q}$ y por lo tanto $\bigcap_{P \in \mathcal{P}(1)} P = \bigcap_{P \in \mathbf{Q}} P$ es un filtro e $\mathcal{I}(1) = \emptyset$ luego $\bigcap_{I \in \mathcal{I}(1)} I = R$ y en consecuencia $X(1) = \bigcap_{P \in \mathbf{Q}} P = F$.

2) Si $a = 0$ entonces $\bigcap_{I \in \mathcal{I}(0)} I = \bigcap_{P \in \mathbf{Q}} \complement P = \complement(\bigcup_{P \in \mathbf{Q}} P)$ y $\mathcal{P}(0) = \{P \in \mathbf{Q} : 0 \in P\} = \emptyset$, luego $\bigcap_{P \in \mathcal{P}(0)} P = R$, por lo tanto $X(0) = \bigcap_{I \in \mathbf{I}} I = \bigcap_{P \in \mathbf{Q}} \complement P = \complement(\bigcup_{P \in \mathbf{Q}} P)$.

3) Si $x, y \in X(1) = F$ entonces $x \equiv y$ $(\mathbf{Q})$.
En efecto de $x, y \in F = \bigcap_{P \in \mathbf{Q}} P$ resulta inmediatamente que $\mathcal{P}(x) = \mathbf{Q} = \mathcal{P}(y)$ y por lo tanto $x \equiv y$ $(\mathbf{Q})$.

4) Si $x \in F$ e $y \in \complement F$ entonces $x \not\equiv y$ $(\mathbf{Q})$.
Como $x \in F$ entonces $\mathcal{P}(x) = \mathbf{Q}$ y como $y \notin F = \bigcap_{P \in \mathbf{Q}} P$ tenemos que $y \notin P_0$ para algún $P_0 \in \mathbf{Q}$ por lo tanto $\mathcal{P}(y) \neq \mathbf{Q}$ y en consecuencia $x \not\equiv y$ $(\mathbf{Q})$.

5) $C(1) = F = X(1)$.
Consecuencia inmediata de 3) y 4).

6) Si $x, y \in X(0)$ entonces $x \equiv y$ $(\mathbf{Q})$.
De $x \in X(0) = \bigcap_{P \in \mathbf{P}} \complement P$ resulta que $x \notin P$, $\forall\, P \in \mathbf{Q}$ luego $P \notin \mathcal{P}(x)$, $\forall\, P \in \mathbf{Q}$, por lo tanto $\mathcal{P}(x) = \emptyset$. Análogamente $\mathcal{P}(y) = \emptyset$ y en consecuencia $x \equiv y$ $(\mathbf{Q})$.

7) Si $x \in X(0)$ e $y \notin X(0)$ entonces $x \not\equiv y$ $(\mathbf{Q})$.
Como $x \in X(0)$ sabemos que $\mathcal{P}(x) = \emptyset$. De $y \notin X(0) = \bigcap_{I \in \mathbf{I}} I$ resulta que existe $I_0 \in \mathbf{I}$ tal que $y \notin I_0$ y como $I_0 = \complement P_0$ con $P_0 \in \mathbf{P}$ entonces $y \in P_0$ y por lo tanto $\mathcal{P}(y) \neq \emptyset$.

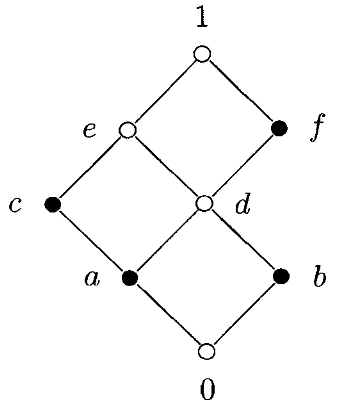
8) $C(0) = X(0)$.
Consecuencia inmediata de 6) y 7).

9) Si $a, b \in \complement(F \cup Y)$ y $b \in X(a)$ entonces $b \equiv a$ $(\mathbf{Q})$.
De (1) $b \in X(a)$ resulta en particular que (2) $b \in P$, $\forall\, P \in \mathcal{P}(a)$ y (3) $b \in I$, $\forall\, I \in \mathcal{I}(a)$. De (2) se deduce que $\mathcal{P}(a) \subseteq \mathcal{P}(b)$. Veamos que $\mathcal{P}(b) \subseteq \mathcal{P}(a)$. En efecto si $P_0 \in \mathcal{P}(b)$ entonces $P_0 \in \mathbf{Q}$ y (4) $b \in P_0$. Si $P_0 \notin \mathcal{P}(a)$ entonces $a \notin P_0$ y por lo tanto $a \in \complement P_0 = I_0$, esto es $I_0 \in \mathcal{I}(a)$ luego por (3) tenemos que $b \in I_0 = \complement P_0$ lo que contradice (4).

10) Si $a, b \in \complement(F \cup Y)$ y $b \notin X(a)$ entonces $b \not\equiv a$ $(\mathbf{Q})$.
De $b \notin X(a)$ resulta que $b \in \bigcup_{P \in \mathcal{P}(a)} \complement P \cup \bigcup_{I \in \mathcal{I}(a)} \complement I$ luego (i) $b \in \complement P_0$ para algún $P_0 \in \mathcal{P}(a)$ o (ii) $b \in \complement I_1$ para algún $I_1 \in \mathcal{I}(a)$. De (i) resulta que $b \notin P_0$ con $P_0 \in \mathcal{P}(a)$ y por lo tanto $P_0 \notin \mathcal{P}(b)$, luego $\mathcal{P}(a) \not\subseteq \mathcal{P}(b)$. De (ii) resulta que $b \in I_1 = \complement P_1$, con $P_1 \in \mathbf{P}$. Por lo tanto $\mathcal{P}(a) \not\subseteq \mathcal{P}(b)$.

De 9) y 10) resulta inmediatamente que si $a \in \complement(F \cup Y)$ entonces $C(a) = X(a)$. Finalmente recordemos que $C(1) = \bigcap_{P \in \mathbf{Q}} P$ es el último elemento de $R/\mathbf{Q}$, y que $C(0) = \complement(\bigcup_{P \in \mathbf{P}} P)$ es el primer elemento de $R/\mathbf{Q}$. ■

Ejemplo 5.2.1 *Sea R el reticulado distributivo cuyo diagrama se indica:*



entonces el conjunto de todos los filtros primos de R es $\mathcal{P}(R) = \{[a), [b), [c), [f)\}$. Luego podemos considerar las siguientes familias de filtros primos:

- $\mathcal{P}_1 = \{[a)\}$, $\mathcal{P}_2 = \{[b)\}$ $\mathcal{P}_3 = \{[c)\}$ $\mathcal{P}_4 = \{[f)\}$.
- $\mathcal{P}_5 = \{[a), [b)\}$, $\mathcal{P}_6 = \{[a), [c)\}$, $\mathcal{P}_7 = \{[a), [f)\}$, $\mathcal{P}_8 = \{[b), [c)\}$, $\mathcal{P}_9 = \{[b), [f)\}$, $\mathcal{P}_{10} = \{[c), [f)\}$.
- $\mathcal{P}_{11} = \{[a), [b), [c)\}$, $\mathcal{P}_{12} = \{[a), [b), [f)\}$, $\mathcal{P}_{13} = \{[a), [c), [f)\}$, $\mathcal{P}_{14} = \{[b), [c), [f)\}$.
- $\mathcal{P}_{15} = \{[a), [b), [c), [f)\} = \mathcal{P}(R)$
- $\mathcal{P}_{16} = \emptyset$.

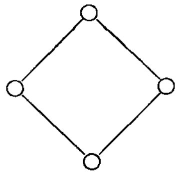
entonces tenemos las siguientes imágenes homomórficas de R:

1) $R/\mathcal{P}_1 \cong R/\mathcal{P}_2 \cong R/\mathcal{P}_3 \cong R/\mathcal{P}_4 \cong R_1$

R_1

2) $R/\mathcal{P}_5 \cong RR/\mathcal{P}_8 \cong R/\mathcal{P}_{10} \cong R_2$

R_2

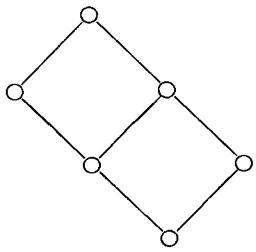


3) $R/\mathcal{P}_6 \cong R/\mathcal{P}_7 \cong R/\mathcal{P}_9 \cong R_3$

R_3

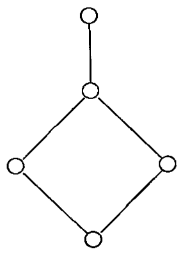
4) $R/\mathcal{P}_{11} \cong R/\mathcal{P}_{14} \cong R_4$

R_4



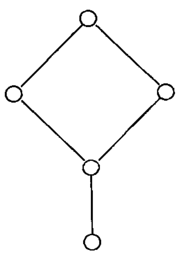
5) $R/\mathcal{P}_{12} \cong R_5$

R_5



6) $R/\mathcal{P}_{13} \cong R_6$

R_6



7) $R/\mathcal{P}_{15} \cong R$

8) $R/\emptyset \cong \{0\}$.

Los resultados precedentes se aplican naturalmente a las álgebras de Boole, pues en este caso los homomorfismos pueden definirse por las condiciones H1, H2, H3 y H4.
Observemos que en las álgebras de Boole es suficiente conocer un filtro F, no necesariamente primo, para determinar el cociente A/F, pero lo mismo no ocurre en los reticulados distributivos. Vemos así que la determinación de las imágenes homomórficas de un reticulado distributivo no es tan simples como en el caso de las álgebras de Boole.

Observemos que la condición de que los filtros de la familia $\mathbf{Q}$ sean primos, se utilizó para demostrar que la relación de equivalencia "$\equiv$" es compatible con la operación de *supremo*. En ejemplo anterior si consideramos la familia de filtros $\mathcal{F} = \{[e), [f)\}$ y definimos, como anteriormente, la relación "$\equiv$" entonces $\equiv$ es una relación de equivalencia, pero no es una congruencia pués $c \equiv d$ (mód. $\mathcal{F}$), $f \equiv f$ (mód. $\mathcal{F}$), y sin embargo $c \vee f = 1$ no es equivalente con $d \vee f = f$.

Sea "$\approx$" una relación de congruencia, diferente de la relación universal, definida sobre un reticulado distributivo acotado R no trivial y $C(a) = \{x \in R : x \approx a\}$. Entonces el conjunto cociente $R' = R/\approx$ algebrizado por $C(a)\wedge C(b) = C(a\wedge b)$ y $C(a)\vee C(b) = C(a\vee b)$ es un reticulado distributivo, no trivial, con primer elemento $C(0)$ y último elemento $C(1)$. Es claro que R' es una imagen homomórfica de R vía la transformación $h(x) = C(x)$, $\forall x \in R$. Sea $\mathbf{P}'$ el conjunto de todos los filtros primos de R' y $\mathbf{Q} = \{h^{-1}(P') : P' \in \mathbf{P}'\}$ luego por el Lema 5.2.1 tenemos que $\mathbf{Q}$ es un conjunto de filtros primos de R.
Probemos que $a \approx b \iff a \equiv b$ (mód. $\mathbf{Q}$). Supongamos que $a \approx b$ luego (1) $h(a) = h(b)$. Sea $Q \in \mathbf{Q}$ tal que $a \in Q$ luego $Q = h^{-1}(P')$ con $P' \in \mathbf{P}$. Por lo tanto $h(a) \in P'$ luego por (1) tenemos $h(b) \in P'$ esto es $b \in h^{-1}(P') = Q$, con $Q \in \mathbf{Q}$. Análogamente se prueba que si $Q \in \mathbf{Q}$ es tal que $b \in Q$ entonces $a \in Q$. Luego $a \equiv b$ (mód. $\mathbf{Q}$).
Supongamos ahora que $a \equiv b$ (mód. $\mathbf{Q}$) y que $h(a) \neq h(b)$ entonces por el Corolario 4.7.5 existe un filtro primo que contiene a uno de ellos sin contener al otro. Sea por ejemplo, $P' \in \mathbf{P}'$ tal que $h(a) \in P'$ y $h(b) \notin P'$, luego $a \in h^{-1}(P')$ y $b \notin h^{-1}(P')$, donde $h^{-1}(P') \in \mathbf{Q}$, absurdo. Luego $h(a) = h(b)$ y como $a \in |a| = h(a) = h(b) = |b|$ entonces $a \in |b|$ y por lo tanto $a \approx b$.

Observación 5.2.1 *Sea A un álgebra de Boole y F un filtro de A. Si $F = A$ entonces sabemos que $A/F \cong \{0\}$ y que si consideramos el conjunto vacío de filtros primos de A entonces el reticulado $A/\emptyset$ es isomorfo a $\{0\}$. Si F es un filtro propio de A, sabemos que todo filtro propio es intersección de filtros primos, luego*

$$F = \bigcap_{Q\in\mathbf{Q}} Q,$$

donde $\mathbf{Q} \subset \mathbf{P}$ y $\mathbf{P}$ es el conjunto de todos los filtros primos de A. Vamos a probar que:

$$a \equiv b \,(\text{mód. F}) \iff a \equiv b \,(\text{mód. } \mathbf{Q}).$$

Supongamos que $a \equiv b$ (mód. F), luego existe (*) $f \in F$ tal que (**) $a \wedge f = b \wedge f$. Si $a \not\equiv b$ (mód. $\mathbf{Q}$) entonces existe $Q \in \mathbf{Q}$ tal que, por ejemplo $a \in Q$ y $b \notin Q$. De (*) resulta que $f \in Q$, $\forall\, Q \in \mathbf{Q}$), luego $a, f \in Q$ y por lo tanto $a \wedge f \in Q$ y por (**) podemos afirmar que $b \wedge f \in Q$ y como $b \wedge f \leq b$ tendríamos $b \in Q$, absurdo.
Supongamos ahora que $a \equiv b$ (mód. $\mathbf{Q}$) esto es que $\mathcal{P}_1 = \{Q \in \mathbf{Q} : a \in Q\} = \{P \in \mathbf{Q} : b \in P\} = \mathcal{P}_2$. Si $a \not\equiv b$ (mód. F) entonces cualquiera que sea $f \in F$ se tiene que $a \wedge f \neq b \wedge f$. Entonces existe, por ejemplo, un filtro primo P tal que $a \wedge f \in P$

y $b \wedge f \notin P$. Como $a \wedge f \leq a$ entonces $a \in P$ y en consecuencia $P \in \mathcal{P}_1$ y por lo tanto $P \in \mathcal{P}_2$. Como $f \in F = \bigcap_{Q \in \mathbf{Q}} Q$, entonces $f \in P$ y por lo tanto $b \wedge f \in P$, absurdo.

Sea R un reticulado distributivo finito, no trivial, $\mathbf{P}$ el conjunto de los filtros primos de R, $\mathbf{P}_0$ un subconjunto de $\mathbf{P}$ tal que $\emptyset \subseteq \mathbf{P}_0 \subseteq \mathbf{P}$. Sea $\Pi = \Pi(R)$ el conjunto de los elementos primos de R. Como R es finito sabemos que $P \in \mathbf{P} \iff P = [p)$, donde $p \in \Pi$. Luego al conjunto $\mathbf{P}_0$ le corresponde un subconjunto Π_0 que verifica $\emptyset \subset \Pi_0 \subseteq \Pi$. Dado $r \in R$ sea $\Pi(r) = \{p \in \Pi : p \leq r\}$ y $\Pi_0(r) = \{p \in \Pi_0 : p \leq r\}$ luego $\Pi_0(r) = \Pi(r) \cap \Pi_0$.
Observemos que si $a, b \in R$ entonces:

$$a \equiv b \text{ (mód. } \mathbf{P}_0) \iff \Pi_0(a) = \Pi_0(b).$$

Notaremos $a \equiv b$ (mód. Π_0) en vez de $a \equiv b$ (mód. $\mathbf{P}_0$) y R/Π_0 en vez de $R/\mathbf{P}_0$.

Lema 5.2.5 *Si R es un reticulado distributivo finito, no trivial, Π el conjunto de los elementos primos de R, Π_0 un subconjunto de Π tal que $\emptyset \subset \Pi_0 \subseteq \Pi$, Π' el conjunto de los elementos primos del reticulado cociente R/Π_0, y h el epimorfismo natural de $R \to R'$ entonces la función h restringida a Π_0 establece un isomorfismo de orden entre los conjuntos ordenados $(\Pi_0, \leq)$ y $(\Pi', \leq)$, esto es $\Pi(R/\Pi_0) \cong \Pi_0$.*
A. Monteiro [43].

Dem. Como $\emptyset \subset \Pi_0 \subseteq \Pi$ entonces R/Π_0 es un reticulado no trivial y en consecuencia $\Pi' \neq \emptyset$.

1) Si $p \in \Pi_0$ entonces $h(p) = C(p) \in \Pi'$.

   1a) $C(p) \neq C(0)$ cualquiera que sea $p \in \Pi_0$.
   Como $p \in \Pi_0$ entonces $p \neq 0$ y $p \in C(p)$,. Si $p \in C(0)$ entonces $\Pi_0(p) = \Pi_0(0) = \emptyset$, absurdo. Luego $C(p) \neq C(0)$.

   1b) Si $p \in \Pi_0$ y $C(p) = C(a) \vee C(b) = C(a \vee b)$ entonces $C(p) = C(a)$ ó $C(p) = C(b)$.
   De $C(p) = C(a \vee b)$ resulta que $p \equiv a \vee b$ esto es $\Pi_0(p) = \Pi_0(a \vee b)$, y como $p \in \Pi_0$ entonces $p \in \Pi_0(p)$ y por lo tanto $p \in \Pi_0(a \vee b)$, esto es $p \leq a \vee b$ y como p es un elemento primo de R tenemos que $p \leq a$ ó $p \leq b$. Si $p \leq a$ entonces $\Pi_0(p) \subseteq \Pi_0(a)$ y como siempre se verifica $\Pi_0(a) \subseteq \Pi_0(a \vee b) = \Pi_0(p)$ tenemos $C(p) = C(a)$. En forma análoga si $p \leq b$ se deduce que $C(p) = C(b)$.

2) La restricción de h al conjunto Π_0, es una función suryectiva de Π_0 en Π'.
En efecto si $p' \in \Pi'$, como h es una suryección existe $y \in R$ tal que $h(y) = C(y) = p'$. Sea $X = \{x \in R : h(x) = p'\}$. Es claro que el conjunto X verifica " Si $x, y \in X$ entonces $x \wedge y \in X$". Sea $X = \{x_1, x_2, \ldots, x_n\}$ y $p_0 = \bigwedge_{i=1}^{n} x_i$, luego $p_0 \in X$. Vamos a demostrar que $p_0 \in \Pi$. Si $p_0 = 0$ entonces $p' = h(p) = h(0) = 0'$, absurdo. Supongamos que $p_0 = a \vee b$, entonces $p' = h(p_0) = C(p_0) = C(a) \vee C(b)$ y como $p' = C(p_0) \in \Pi'$ entonces $p' = C(p) = C(a) = h(a)$ ó $p' = C(p) = C(b) = h(b)$, luego $a \in X$ ó $b \in X$. Si $a \in X$ entonces $p_0 \leq a$ y de $a \leq a \vee b = p_0$ se deduce $p_0 = a$. Del mismo modo si $b \in X$ se concluye que $p_0 = b$. Luego $p_0 \in \Pi$.
Vamos a demostrar mas precisamente que $p_0 \in \Pi_0$.
Sea $\Pi_0(p_0) = \{q \in \Pi_0 : q \leq p_0\}$. Si $\Pi_0(p_0) = \emptyset$ entonces $p_0 \equiv 0$ (mód. Π_0) y en consecuencia $h(p_0) = h(0) = C(0) = 0'$, contradicción, luego $\Pi_0(p_0) = \{q_1, q_2, \ldots, q_s\}$.

Sea $x = \bigvee_{i=1}^{s} q_i$. Es claro que $x \equiv p_0$ (mód. Π_0), luego $x \in X$, de donde resulta por la definición de p_0 que $p_0 \leq x = \bigvee_{i=1}^{s} q_i$, y como p_0 es primo existe un índice i, $1 \leq i \leq s$ tal qu e $p_0 \leq q_i$. Además como $q_i \leq p_0$ tenemos finalmente que $p_0 = q_i \in \Pi_0$.

3) Si $p_1, p_2 \in \Pi_0$ son tales que $p_1 \leq p_2$ entonces $h(p_1) \leq h(p_2)$.
En efecto de $p_1 \leq p_2$ resulta que $p_1 = p_1 \wedge p_2$, luego $C(p_1) = C(p_1) \wedge C(p_2)$ y en consecuencia $h(p_1) = C(p_1) \leq C(p_2) = h(p_2)$.

4) Si $p_1, p_2 \in \Pi_0$ son tales que $h(p_1) = h(p_2)$ entonces $p_1 = p_2$.
Como $h(p_1) = h(p_2)$ esto es $C(p_1) = C(p_2)$, entonces $p_1 \equiv p_2$ (mód. Π_0), esto es $\Pi_0(p_1) = \Pi_0(p_2)$ de donde resulta que $p_1 \leq p_2$ y $p_2 \leq p_1$, luego $p_1 = p_2$.

■

En el capítulo sobre reticulados distributivos demostramos el siguiente resultado: (*) *Si R y R' son reticulados distributivos finitos, no triviales, tales que los conjuntos ordenados Π y Π' de sus elementos primos son isomorfos entonces R y R' son reticulados isomorfos*

Lema 5.2.6 *Si R y R' son reticulados distributivos finitos, no triviales, Π y Π' los conjuntos ordenados de sus elementos primos, y $\alpha : R \longrightarrow R'$ un epimorfimo de reticulados, entonces existe un isomorfismo de orden $\beta : \Pi' \longrightarrow \Pi$, esto es el conjunto ordenado Π' es isomorfo al subconjunto $\beta(\Pi')$ del conjunto ordenado Π. Además R' es isomorfo al reticulado $R/\beta(\Pi')$.*

Dem. Dado (1) $p' \in \Pi'$, como α es una función suryectiva $X = \alpha^{-1}(p') \neq \emptyset$. Sea $p = \bigwedge_{x \in X} x$ luego $\alpha(p) = p'$. Pongamos por definición $\beta(p') = p$. Veamos que $p \in \Pi$. En efecto si $p = 0$ entonces $\alpha(p) = 0'$ lo que contradice (1). Supongamos que (2) $p = a \vee b$ entonces $p' = \alpha(p) = \alpha(a) \vee \alpha(b)$ y como p' es un elemento primo de R' resulta que (3) $p' = \alpha(a)$ ó (4) $p' = \alpha(b)$. Si ocurre (3) entonces $a \in X$ y por lo tanto $p \leq a$. De (3) resulta $a \leq p$, y por lo tanto $p = a$. Análogamente si ocurre (4) se demuestra que $p = b$.
Sean $p', q' \in \Pi'$ tales que $p' \leq q'$ y $\beta(p') = p$, $\beta(q') = q$, entonces $\alpha(p \wedge q) = \alpha(p) \wedge \alpha(q) = p' \wedge q' = p'$ luego $p \wedge q \in \alpha^{-1}(p') = X$ y por lo tanto $p \leq p \wedge q$. Luego como $p \wedge q \leq q$ tenemos $p \leq q$ esto es $\beta(p') \leq \beta(q')$.
Si $\beta(p') = \beta(q')$ esto es $p = q$ entonces $\alpha(p) = \alpha(q)$ y por lo tanto $p' = q'$.
Por el Lema 5.2.5 sabemos que $\Pi(R/\beta(\Pi')) \cong \beta(\Pi')$ y como $\Pi' \cong \beta(\Pi')$ tenemos que $\Pi(R/\beta(\Pi')) \cong \Pi' = \Pi(R')$, luego por resultado (*) tenemos que $R(\beta(\Pi'))$ y R' son reticulados isomorfos. ■

Estos resultados (Lemas 5.2.5 y 5.2.6) fueron generalizados por A. Monteiro [38], [41] para las *álgebras de De Morgan*, y extendidos por M. Tourasse Teixeira, para las *M-álgebras* en su tesis doctoral (1964) realizada bajo la dirección de A. Monteiro.

En virtud del Lema 5.2.5 para determinar imágenes homomórficas de un reticulado distributivo finito, no trivial, R basta considerar subconjuntos X del conjunto ordenado $\Pi = \Pi(R)$ y luego construir $RB(X)$.

Sea R un reticulado distributivo finito, no trivial. $\mathbf{Q}$ una familia, no vacía de filtros primos. Sabemos que $P \in \mathbf{Q} \iff P = [p)$ donde $p \in \Pi = \Pi(R)$. Sea $\mathbf{\Pi_Q} = \{p \in \Pi : [p) \in \mathbf{Q}\}$

y Π^* el conjunto de los elementos primos duales, de R (esto es elementos primos del reticulado R^*, dual de R). Sabemos que si P es un filtro primo de R entonces $I = \complement P$ es un ideal primo de R. Además es fácil ver que $I = (q]$ con $q \in \Pi^*$. Sean $\mathbf{I} = \{I = \complement P : P \in \mathbf{Q}\}$ y $\mathbf{\Pi^*_Q} = \{q \in \Pi^* : (q] \in \mathbf{I}\}$. Sabemos que las clases de equivalencia (mód. $\mathbf{Q}$) son de la forma:

$$C(a) = \bigcap_{P \in \mathcal{P}(a)} P \ \cap \bigcap_{I \in \mathcal{I}(a)} I.$$

Sea $\mathcal{P}(a) = \{P_1, P_2, \dots, P_t\}$ luego $\mathcal{P}(a) = \{[p_1), [p_2), \dots, [p_t)\}$ donde $p_1, p_2, \dots, p_t \in \Pi$. Mas precisamente $\mathcal{P}(a) = \{[p) : p \in \mathbf{\Pi_Q}\ \text{ y }\ p \leq a\}$. Por lo tanto

$$\bigcap_{P \in \mathcal{P}(a)} P = \bigcap_{i=1}^{t} [p_i) = [\bigvee_{i=1}^{t} p_i).$$

Análogamente si $\mathcal{I}(a) = \{I_1, I_2, \dots, I_s\}$ entonces:

$$\mathcal{I}(a) = \{(q_1], (q_2], \dots, (q_s]\} \ \text{ donde } \ q_1, q_2, \dots, q_s \in \Pi^*_{\mathbf{Q}}.$$

Mas precisamente $\mathcal{I}(a) = \{(q] : q \in \mathbf{\Pi^*}\ \text{ y }\ a \leq q\}$. Por lo tanto:

$$\bigcap_{I \in \mathcal{I}(a)} I = \bigcap_{j=1}^{s} (q_j] = (\bigwedge_{j=1}^{s} q_j].$$

Entonces:

$$C(a) = [\bigvee_{i=1}^{t} p_i, \bigwedge_{j=1}^{s} q_j] = \{x \in R : \bigvee_{i=1}^{t} p_i \leq x \leq \bigwedge_{j=1}^{s} q_j\}.$$

Observemos que si $a = 1$ entonces

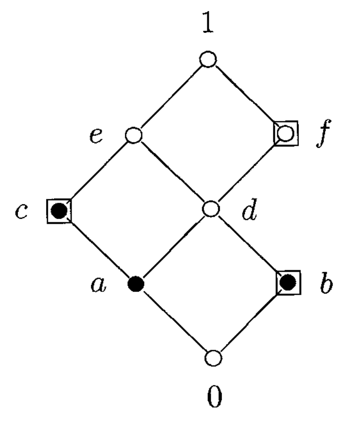
$$\mathcal{P}(1) = \{P \in \mathbf{Q} : 1 \in P\} = \mathbf{Q} \quad \text{e} \quad \mathcal{I}(1) = \{\complement P : P \in \mathbf{Q},\ 1 \in \complement P\} = \emptyset,$$

luego $C(1) = [\bigvee_{p \in \Pi^*_{\mathbf{Q}}} p, 1]$. Análogamente si $a = 0$ entonces

$$\mathcal{P}(0) = \{P \in \mathbf{Q} : 0 \in P\} = \emptyset \quad \text{e} \quad \mathcal{I}(0) = \{\complement P : P \in \mathbf{Q},\ 0 \in \complement P\} = \mathbf{I},$$

luego $C(0) = [0, \bigwedge_{q \in \Pi^*_{\mathbf{Q}}} q]$.

Retornemos al reticulado indicado en el Ejemplo 5.2.1. Consideremos la siguiente familia de filtros primos $\mathbf{Q} = \{[a), [b), [c)\}$ luego $\mathbf{\Pi_Q} = \{a, b, c\}$ y $\mathbf{I} = \{(b], (c], (f]\}$ y por lo tanto $\mathbf{\Pi^*_Q} = \{b, c, f\}$. Indicamos con $\bullet$ los elementos del conjunto $\mathbf{\Pi_Q}$ y con $\square$ los elementos del conjunto $\mathbf{\Pi^*_Q}$.



En consecuencia $C(1) = [a \vee b \vee c, 1] = [e, 1]$, $C(0) = [0, b \wedge c \wedge f] = [0, 0] = \{0\}$, $C(a) = [a, c \wedge f] = [a, a] = \{a\}$, $C(b) = [b, b \wedge f] = [b, b] = \{b\}$, $C(c) = [a \vee c, c] = [c, c] = \{c\}$, $C(d) = [a \vee b, f] = [d, f] = \{d, f\}$.

Sea R un reticulado distributivo finito, no trivial y $\mathbf{Q} = \{P_1, P_2, \ldots, P_n\}$ un conjunto de filtros primos de R, $\mathbf{I} = \{\complement P : P \in \mathbf{Q}\}$. Observemos que $A/\mathbf{Q}$ siempre es un reticulado distributivo no trivial. Vamos a demostrar que $A/\mathbf{Q}$ es un álgebra de Boole, con n átomos sí y solamente sí el conjunto ordenado $(\mathbf{Q}, \subseteq)$ es una anticadena con n elementos.
Si $R/\mathbf{Q}$ es un álgebra de Boole con un átomo entonces $R/\mathbf{Q} = \{C(0), C(1)\}$ y como $C(1) = \bigcap\limits_{P \in \mathbf{Q}} P$, $C(0) = \bigcap\limits_{I \in \mathbf{I}} I$ y $R = C(1) \cup C(0)$ resulta por el Lema 5.2.3 que $\mathbf{Q}$ tiene un sólo elemento. Supongamos ahora que $R/\mathbf{Q}$ es un álgebra de Boole con n átomos, $n \geq 2$. Si existieran $P_i, P_j \in \mathbf{Q}$, $i \neq j$, comparables, supongamos por ejemplo que (1) $P_i \subset P_j$, sean (2) $a \in P_j \setminus P_i$ y $b \notin P_j$ entonces $a \vee b \in P_j \setminus P_i$ y $a \wedge b \notin P_j$. Dado $C(a) \in R/\mathbf{Q}$ como $R/\mathbf{Q}$ es un álgebra de Boole existe $C(d) \in R/\mathbf{Q}$, $d \neq a$ tal que $C(a \vee d) = C(a) \vee C(d) = C(1)$ y $C(a \wedge d) = C(a) \wedge C(d) = C(0)$ por lo tanto $a \vee d \equiv 1$ $(\mathbf{Q})$ y $a \wedge d \equiv 0$ $(\mathbf{Q})$ esto es (3) $a \vee d \in \bigcap\limits_{P \in \mathbf{Q}} P$ y (4) $a \wedge d \notin P$, $\forall\ P \in \mathbf{Q}$. De (3) resulta en particular que $a \vee d \in P_i$ y como P_i es un filtro primo tenemos que $a \in P_i$ o $d \in P_i$, pero como por (2) $a \notin P_i$ entonces $d \in P_i$, luego por (1) tenemos (5) $d \in P_j$. De(5) y (2) resulta $a \wedge d \in P_j$ lo que contradice (4).
Recíprocamente supongamos que la familia de filtros primos $\mathbf{Q}$ es una anticadena con n elementos. Si $n = 1$ entonces $\mathbf{Q}$ es una anticadena (a la vez una cadena) con un sólo elemento y $R/\mathbf{Q}$ es una cadena con dos elementos, luego un álgebra de Boole. Supongamos ahora que $n \geq 2$. Si $a \in F = \bigcap\limits_{P \in \mathbf{Q}} P$ entonces $C(a) = C(1) = F$ y por lo tanto su complemento booleano es $C(0)$. Si $a \in Y = \complement(\bigcup\limits_{P \in \mathbf{Q}} P)$ entonces $C(a) = C(0)$ y por lo tanto $C(1)$ es su complemento booleano. Supongamos ahora que:

$$a \in \complement(F \cup Y) = \complement \bigcap_{P \in \mathbf{Q}} P \ \cap\ \complement \bigcap_{P \in \mathbf{Q}} \complement P = \bigcup_{P \in \mathbf{Q}} \complement P \ \cap\ \bigcup_{P \in \mathbf{Q}} P,$$

entonces $a \in \bigcup\limits_{P \in \mathbf{Q}} \complement P$ y $a \in \bigcup\limits_{P \in \mathbf{Q}} P$ por lo tanto existe $P_a \in \mathbf{Q}$ tal que $a \in P_a$ y existe $P_0 \in \mathbf{Q}$ tal que $a \notin P_0$. Sean (1) $\mathbf{Q}_a = \{P \in \mathbf{Q} : a \in P\}$ y (2) $\mathbf{Q}_0 = \{P \in \mathbf{Q} : a \notin P\}$.

Claramente $\mathbf{Q}_a \neq \mathbf{Q}_0$, $\mathbf{Q}_a \cup \mathbf{Q}_0 = \mathbf{Q}$ y $\mathbf{Q}_a \cap \mathbf{Q}_0 = \emptyset$.

Sabemos que $C(a) = \bigcap\limits_{P \in \mathbf{Q}_a} P \cap \bigcap\limits_{P \in \mathbf{Q}_0} \complement P$. Sea (3) $X = \bigcap\limits_{P \in \mathbf{Q}_0} P \cap \bigcap\limits_{P \in \mathbf{Q}_a} \complement P$.

Si $X = \emptyset$ entonces $\bigcap\limits_{P \in \mathbf{Q}_0} P \subseteq \complement \bigcap\limits_{P \in \mathbf{Q}_a} \complement P = \bigcup\limits_{P \in \mathbf{Q}_a} P$.

Como el reticulado es finito todos los filtros primos son de la forma $[p)$ donde p es un elemento primo de R.

Sean $\mathbf{\Pi}_a = \{p : [p) \in \mathbf{Q}_a\}$, $\mathbf{\Pi}_0 = \{p : [p) \in \mathbf{Q}_0\}$ y $\mathbf{\Pi}_{\mathbf{Q}} = \{p \in \Pi(R) : [p) \in \mathbf{Q}\}$.

Luego $\mathbf{\Pi}_{\mathbf{Q}}$ es una anticadena de R con n elementos y además $\mathbf{\Pi}_a \cap \mathbf{\Pi}_0 = \emptyset$ y $\mathbf{\Pi}_a \cup \mathbf{\Pi}_0 = \mathbf{\Pi}_{\mathbf{Q}}$.
Por (3) tenemos que

$$(4)\quad [\bigvee_{q \in \mathbf{\Pi}_0} q) = \bigcap_{q \in \mathbf{\Pi}_0} [q) \subseteq \bigcup_{p \in \mathbf{\Pi}_a} [p).$$

Como $\bigvee_{q\in\mathbf{\Pi}_0} q \in [\bigvee_{q\in\mathbf{\Pi}_0} q)$ entonces por (4) tenemos que $\bigvee_{q\in\mathbf{\Pi}_0} q \in [p_a)$ con $p_a \in \mathbf{\Pi}_a$, esto es (5) $p_a \leq \bigvee_{q\in\mathbf{\Pi}_0} q$, luego como p_a es un elemento primo de R, de (5) resulta que(iv) $p_a \leq q_0$ con $p_a \in \mathbf{\Pi}_a$ y $q_0 \in \mathbf{\Pi}_0$. Como $\mathbf{\Pi}_\mathbf{Q}$ es una anticadena de (iv) resulta $p_a = q_0$, donde $p_a \in \mathbf{\Pi}_a$ y $q_0 \in \mathbf{\Pi}_0$, absurdo dado que $\mathbf{\Pi}_a \cap \mathbf{\Pi}_0 = \emptyset$.

Acabamos así de probar que $X \neq \emptyset$. Sea $b \in X$. De (3) resulta que (i) $b \in P$ para todo $P \in \mathbf{Q_0}$ y que (ii) $b \notin P$ para todo $P \in \mathbf{Q_a}$. De (1) resulta que $a \in P$ para todo $P \in \mathbf{Q_a}$ luego como $a \leq a \vee b$ tenemos que $a \vee b \in P$ para todo $P \in \mathbf{Q_a}$. Como (iii) $b \leq a \vee b$ de (i) e (iii) se deduce que $a \vee b \in P$ para todo $P \in \mathbf{Q_0}$. Luego tenemos que $a \vee b \in P$ para todo $P \in \mathbf{Q}$ y en consecuencia $a \vee b \equiv 1$ (mód. $\mathbf{Q}$). Luego $C(a) \vee C(b) = C(1)$. Si $a \wedge b \in P$ para algún $P \in \mathbf{Q}$ entonces $a \wedge b \in P$ para algún $P \in \mathbf{Q}_a$ o $a \wedge b \in P$ para algún $P \in \mathbf{Q_0}$. Como $a \wedge b \leq b$ en el primer caso tendríamos que $b \in P$ con $P \in \mathbf{Q}_a$ lo que contradice (ii). Como $a \wedge b \leq a$ en el segundo caso tendríamos que $a \in P$ con $P \in \mathbf{Q}_0$ lo que contradice (2). Luego $a \wedge b \equiv 0$ (mód. $\mathbf{Q}$) y por lo tanto $C(a) \wedge C(b) = C(0)$. En consecuencia $C(b)$ es el complemento booleano de $C(a)$.

5.3 Axiomática de M. Sholander

M. Sholander demostró el siguiente resultado: *Para que un sistema $(R, \wedge, \vee)$ sea un reticulado distributivo es necesario y suficiente que se verifiquen:*

S1) $a \wedge (a \vee b) = a, \quad \forall\, a, b \in R$

S2) $a \wedge (b \vee c) = (c \wedge a) \vee (b \wedge a), \quad \forall\, a, b, c \in R$

Es claro que la condición es suficiente. Probemos que es necesaria.

1) $a = (a \wedge a) \vee (a \wedge a)$.
$a =$ [por S1)] $= a \wedge (a \vee a) =$ [por S2)] $= (a \wedge a) \vee (a \wedge a)$.

2) $a = a \wedge a$.
(i) $a \wedge a =$ [por S1)] $= (a \wedge a) \wedge ((a \wedge a) \vee (a \wedge a)) =$ [por 1)] $= (a \wedge a) \wedge a$.
$a \wedge a =$ [por 1)] $= a \wedge ((a \wedge a) \vee (a \wedge a)) =$ [por S2)] $((a \wedge a) \wedge a) \vee ((a \wedge a) \wedge a) =$ [por (i)] $= (a \wedge a) \vee (a \wedge a) =$ [por 1)] $= a$.

3) $a = a \vee a$.
$a =$ [por 2)] $= (a \wedge a) \vee (a \wedge a) =$ [por 1)] $= a$.

4) $a \wedge b = b \wedge a$.
$a \wedge b =$ [por 3)] $= (a \wedge b) \vee (a \wedge b) =$ [por S2)] $= b \wedge (a \vee a) =$ [por 3)] $= b \wedge a$.

5) $a = (b \wedge a) \vee a$.
$a =$ [por S1)] $= a \wedge (a \vee b) =$ [por S2)] $= (b \wedge a) \vee (a \wedge a) =$ [por 2)] $= (b \wedge a) \vee a$.

6) $a = a \vee ((b \wedge a) \wedge a)$.
$a =$ [por 2)] $= a \wedge a =$ [por 5)] $= a \wedge ((b \wedge a) \vee a) =$ [por S2)] $=$
$(a \wedge a) \vee ((b \wedge a) \wedge a) =$ [por 2)] $= a \vee ((b \wedge a) \wedge a)$.

7) $a \vee b = (b \vee (a \wedge b)) \vee a$.
$a \vee b =$ [por 2)] $= (a \vee b) \wedge (a \vee b) =$ [por S2)] $= (b \wedge (a \vee b)) \vee (a \wedge (a \vee b)) =$ [por S2)] $= ((b \wedge b) \vee (b \wedge a)))) \vee (a \wedge (a \vee b)) =$ [por S1)] $= ((b \wedge b) \vee (b \wedge a)) \vee a =$ [por 2)] $= (b \vee (b \wedge a)) \vee a$.

8) $b = b \vee (a \wedge b)$.
$b =$ [por 5)] $= (a \wedge b) \vee b =$ [por 7)] $= (b \vee ((a \wedge b)) \wedge b)) \vee (a \wedge b) =$ [por 6)] $=$ $b \vee (a \wedge b)$.

9) $a \vee b = b \vee a$.
$a \vee b =$ [por 7)] $= (b \vee (a \wedge b)) \vee a =$ [por 8)] $= b \vee a$.

De las propiedades 2), 3), 4) y 9) resulta que las operaciones "$\wedge$" y "$\vee$" son idempotentes y conmutativas. Además por S1) y 8) se verifican las leyes de absorción y por S2), 4) y 9) se verifica una de las leyes distributivas. Probemos ahora las propiedades asociativas. Sean $p = (a \vee b) \vee c$ y $q = a \vee (a \vee c)$.

10) $a \wedge p = a$.
$a \wedge p = a \wedge ((a \vee b) \vee c) =$ [por S2)] $= (c \wedge a) \vee ((a \vee b) \wedge a) =$ [por 4)] $=$ $(c \wedge a) \vee (a \wedge (a \vee b)) =$ [por S1)] $= (c \wedge a) \vee a =$ [por 9)] $= a \vee (c \wedge a) =$ [por 8)] $= a$.

11) $b \wedge p = b$
$b \wedge p = b \wedge ((a \vee b) \vee c) =$ [por S2)] $= (c \wedge a) \vee ((a \vee b) \wedge a) =$ [por 4)] $=$ $(c \wedge a) \vee (a \wedge (a \vee b)) =$ [por S1)] $= (c \wedge a) \vee a =$ [por 9)] $= a \vee (c \wedge a) =$ [por 8)] $= a$.

12) $c \wedge p = b$.
$c \wedge p = c \wedge ((a \vee b) \vee c) =$ [por 9)] $= c \wedge (c \vee (a \vee b)) =$ [por S1)] $= c$.

13) $q = p \wedge q$.
$q = a \vee (b \vee c) =$ [por 10), 11) y 12)] $= (a \wedge p) \vee ((b \wedge p) \vee (c \wedge p)) =$ [por S2)] $=$ $(a \wedge p) \vee (p \wedge (c \vee b)) =$ [por 4)] $= (a \wedge p) \vee ((c \vee b) \wedge p) =$ [por S2)] $= p \wedge ((c \vee b) \vee a) =$ [por 9)] $= p \wedge (a \vee (c \vee b)) = p \wedge q$.

14) $p = p \wedge q$.
Se demuestra en forma análoga a 12).

15) $(a \vee b) \vee c = a \vee (b \vee c)$.
Consecuencia inmediata de 13) y 14).

16) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.
Se demuestra en forma análoga a 14),

Acabamos así de probar que R es un reticulado distributivo.
Consideremos ahora los siguientes axiomas:

S3) Existe $0 \in R$ tal que $a \vee 0 = a$, $\forall\, a \in R$.

S4) Existe $1 \in R$ tal que $a \wedge 1 = a$, $\forall\, a \in R$.

S5) Existen $0, 1 \in R$ tales que $0 \vee (a \wedge 1) = a$ $\forall\, a \in R$.

S6) Dado $b \in R$ existe $b' \in R$ tal que $a \wedge (b \vee b') = a \vee (b \wedge b')$.

Entonces todo sistema $(R, \wedge, \vee)$ que verifica:

a) S1), S2) y S3) es un reticulado distributivo con primer elemento 0.

b) S1), S2) y S4) es un reticulado distributivo con último elemento 1.

c) S1), S2) y S5) es un reticulado distributivo con primer elemento 0 y último elemento 1.

d) S1), S2) y S6) es un álgebra de Boole.

a) En efecto $a \wedge 0 =$ [por S3)] $= (a \vee 0) \wedge 0 =$ [por 4)] $= 0 \wedge (a \vee 0) =$ [por 9)] $= 0 \wedge (0 \vee a) =$ [por S1)] $= 0$. Probemos que este elemento es único. En efecto si existiera $0' \in R$ tal que (*) $a \vee 0' = a$, $\forall\, a \in R$. entonces $0' =$ [por S3)] $= 0' \vee 0 =$ [por 9)] $= 0 \vee 0' =$ [por (*)] $= 0$.

b) Se demuestra en forma dual de la anterior.

c) $0 \vee a =$ [por S5)] $= 0 \vee (0 \vee (a \wedge 1)) =$ [por 15)] $= (0 \vee 0) \vee (a \wedge 1) =$ [por 3)] $= 0 \vee (a \wedge 1) =$ [por S5)] $= a$.
$a \wedge 1 =$ [por S5)] $= 0 \vee ((a \wedge 1) \wedge 1) =$ [por 16)] $= 0 \vee (a \wedge (1 \wedge 1)) =$ [por 2)] $= 0 \vee (a \wedge 1) =$ [por S5)] $= a$.

d)) Sea (i) $b \vee b' = 1$ y (ii) $b \wedge b' = 0$ entonces (iii) $a \wedge 1 =$ [por (i)] $= a \wedge (b \vee b') =$ [por S6)] $= a \vee (b \wedge b') =$ [por (ii)]) $= a \vee 0$.
$0 \vee (a \wedge 1) =$ [por (iii)] $= 0 \vee (a \vee 0) =$ [por 9)] $= 0 \vee (0 \vee a) =$ [por 15)] $= (0 \vee 0) \vee a =$ [por 3)] $= 0 \vee a =$ [por 9)] $= a \vee 0 =$ [por 3)] $= (a \vee a) \vee 0 =$ [por 15)] $= a \vee (a \vee 0) =$ [por S5)] $= a \vee (a \wedge 1) =$ [por 4)] $= a \vee (1 \wedge a) =$ [por 8)] $= a$, y en consecuencia se verifica S5. Luego R es un reticulado distributivo con primer y último elemento, donde cada elemento tiene un complemento, luego R es un álgebra de Boole.

6 INDICE ALFABETICO

NOTA: Los números indicados entre corchetes corresponden a la numeración del inventario de la Biblioteca *"Dr. Antonio Monteiro"* del Instituto de Matemática, INMABB, C.O.N.I.C.E.T - Universidad Nacional del Sur.

Referencias

[1] Abbott J.C., *Trends in lattice theory*, Van Nostrand, New York, 1970. ...... **[4078]**

[2] Abian A., *Boolean rings*, Branden Press, Boston, 1976. .... **[4496]**

[3] Aigner M., *Combinatorial theory*, Springer-Verlag, Berlín, 1979. .... **[4957]**

[4] *Algorithms and order*, NATO 1989. .... **[6459]**

[5] Balbes R. and Dwinger P., *Distributive lattices*, University of Missouri Press 1974. .... **[6460]**

[6] Barbut M. et Monjardet B., *Ordre et classification, algèbre et combinatoire I*, Hachette, París, 1970. .... **[5304]**

[7] Birkhoff G., *Lattice Theory*, American Mathematical Society, Colloq. Publ. Vol. 25, Providence, 1948. .... **[19]**

[8] Birkhoff G., *Lattice Theory*, American Mathematical Society, Colloq. Publ. Vol. 25, third edition, Providence, 1970. .... **[3629]**

[9] Boulaye G., *Contribution a la théorie des treillis*. .... **[3457]**

[10] Burris S. and Sankappanavar H. P., *A course in universal algebra*, Springer-Verlag, New York, 1981. .... **[6124]**

[11] Carvalho, M., *Principes et applications de l'analyse boolèenne*, Gauthier- Villars, 1965. .... **[2556]**

[12] Carvalho, M., *Monographie des treillis et algèbre de Boole*, Gauthier- Villars, 1966. .... **[2555]**

[13] Casanova G., *L'algèbre de Boole*, Collection "Que sais-je", París, Presse Universitaire, France, 1966.

[14] *Colloquium on lattice theory*, 1980. .... **[5924]**

[15] Davey B. A., Priestley H. A. *Introduction to lattices and order*, Cambridge University Press 1990. .... **[6493]**

[16] Denis-Papin M. et Malgrange Y., *Exercises de calcul booléin avec leurs solutions*, Editions Eyrolles, Paris, 1966. .... **[2294]**

[17] Dubisch R., *Lattices to logic*, Bloisdell Pub., New York, 1964. .... **[2845]**

[18] Dubreil-Jacotin M. L., *Leçons sur la théorie des treillis des structures algèbriques ordonnées et des treillis geométriques*, Gauthier-Villars, 1953. .... **[1935]**

[19] Dwinger Ph., *Introduction to Boolean algebras*, Springer-Verlag, Wurzburg, 1961.

[20] Faure R. et Heurgon E., *Structures ordonnées et algèbres de Boole*, Gauthier-Villars, 1971. .... **[3838]**

[21] Fuchs L., *Partially ordered algebraic systems*, Pergamon Press, 1963. .... **[2886]**

[22] Gericke H., *Lattice theory*, Frederick Ungar, New York, 1966. .... **[4118]**

[23] Gratzer G., *Lattice theory, first concepts and distributive lattices*, W. H. Freeman Co., San Francisco, 1971. .... **[4798]**

[24] Gratzer G., *General lattice theory*, Birkhäuser 1978.......... **[5905]**

[25] Halmos P. R., *Lectures on Boolean algebras*, D. Van Nostrand Co., New York, 1963. .... **[1362]**

[26] Hohn F., *Applied Boolean algebra, an elementary introduction*, Mac Millan Co., New York, 1966.

[27] Hoernes G. E. et Heilweil, *Introduction a l'algèbre de Boole et aux dispositives logiques*, Dunod, París, 1966. .... **[2295]**

[28] Marcus M. P., *Switching circuits for engineers*, Prentice Hall, 1977. .... **[Código Biblioteca Central UNS 621.38, M334]**

[29] Mendelson M., *Boolean algebra and switching circuits*, Schaum's Outline Series, Mc Graw-Hill Book Co.,1970. .... **[4113]**

[30] Monteiro A., *Filtros e Ideais I*, Notas de Matemática 2, Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 1955. .... **[236]**, **[1003]**

[31] Monteiro A., *Filtros e Ideais II*, Notas de Matemática 2, Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 1955. .... **[565]**, **[1004]**

[32] Monteiro A., Notas del curso *Algebra de la Lógica I*, Instituto de Matemática, Universidad Nacional del Sur, Bahía Blanca, 1959.

[33] Monteiro A., Notas del curso *Algebras de Hilbert y de Tarski*, Instituto de Matemática, Universidad Nacional del Sur, Bahía Blanca, 1960.

[34] Monteiro A., Notas del curso *Algebra de la Lógica II*, Instituto de Matemática, Universidad Nacional del Sur, Bahía Blanca, 1960.

[35] Monteiro A., Notas del curso *Algebras de Boole monadicas*, Instituto de Matemática, Universidad Nacional del Sur, Bahía Blanca, 1960.

[36] Monteiro A., Notas del *Seminario de Lógica Matemática I*, Instituto de Matemática, Universidad Nacional del Sur, Bahía Blanca, 1961.

[37] Monteiro A., Notas del *Seminario de Lógica Matemática II*, Instituto de Matemática, Universidad Nacional del Sur, Bahía Blanca, 1962.

[38] Monteiro A., Notas del curso *Algebra de la Lógica III*, Instituto de Matemática, Universidad Nacional del Sur, Bahía Blanca, 1962.

[39] Monteiro A., Notas del curso *Algebras de Lukasiewicz trivalentes*, Instituto de Matemática, Universidad Nacional del Sur, Bahía Blanca, 1963.

[40] Monteiro A., Notas del *Seminario de Lógica de Lukasiewicz*, Instituto de Matemática, Universidad Nacional del Sur, Bahía Blanca, 1963.

[41] Monteiro A., Notas del curso *Algebras de De Morgan*, Instituto de Matemática, Universidad Nacional del Sur, Bahía Blanca, 1966.

[42] Monteiro A., *Generadores de Reticulados distributivos finitos*, Actas del Simposio Panamericano de Matemática Aplicada, Buenos Aires, Argentina (1968), p. 465.

[43] Monteiro A., *Sobre el número minimal de generadores de reticulados distributivos finitos y álgebras de Boole finitas*, Informe Técnico Interno 65, INMABB (1998), 22 págs.

[44] Monteiro L., Notas del curso *Algebras de Boole*, Instituto de Matemática, Universidad Nacional del Sur, Bahía Blanca, 1974.

[45] Morgado J., *Introdução a teoria dos reticulados*, Tomo I, Textos de Matemática 10, Instituto de Física e Matemática, Recife, Brasil, 1962. .... **[1016]**

[46] Morgado J., *Introdução a teoria dos reticulados*, Tomo II, Textos de Matemática 11, Instituto de Física e Matemática, Recife, Brasil, 1962. .... **[1017]**

[47] *Ordered Sets*, Proc. 1982. .... **[5902]**

[48] Rasiowa H. and Sikorski R., *The mathematics of methamathematics*, Warsawa, 1963. .... **[1485]**

[49] Rutheford D. E., *Introduction to lattice theory*, Edinburg, London, Oliver and Boyd, University Math. Monographs, 1965. .... **[2320]**

[50] Sikorski R., *Boolean algebras*, Springer-Verlag, Berlín. .... **[690, 691, 2113, 2789]**

[51] Sikorski R., *Algebras de Boole*, Notas de Lógica Matemática 4, Instituto de Matemática, U.N.S., 1968.

[52] Szasz G., *Introduction to lattice theory*, Academic Press, New York and London, 1963. .... **[3952]**