

# Sobre el número minimal de generadores de reticulados distributivos finitos \* y álgebras de Boole finitas

António Monteiro

Instituto de Matemática - Universidad Nacional del Sur  
Bahía Blanca - Argentina

## 1. Generadores de reticulados distributivos finitos

### 1.1. Introducción

Vamos a comenzar por recordar algunos resultados conocidos [4], que nos serán necesarios y por fijar notaciones.

Si  $X$  e  $Y$  son conjuntos ordenados isomorfos notaremos  $X \cong Y$ , y si  $X$  es finito con  $n$  elementos notaremos  $N[X] = n$ .

Sea  $(R, \wedge, \vee)$  un reticulado distributivo. Como es habitual diremos que  $R$  es un reticulado distributivo. Si  $G$  es un subconjunto no vacío de  $R$ , notaremos con  $i(G)$  el conjunto de todos los elementos de  $R$  que son ínfimo de un número finito de elementos de  $G$  y con  $s(G)$  el conjunto de todos los elementos de  $R$  que son supremo de un número finito de elementos de  $G$ . Si  $R$  tiene primer (0) y último (1) elemento entonces el ínfimo de una familia vacía de elementos de  $G$  es 1 y el supremo de una familia vacía de elementos de  $G$  es 0.

A todo subconjunto  $S$  de  $R$  que verifica: “Si  $x, y \in S$  entonces  $x \wedge y, x \vee y \in S$ ” se denomina subreticulado de  $R$ . Si  $G \subseteq R$  notaremos con  $SR(G)$  al subreticulado de  $R$  generado por  $G$ . Es bien conocido que  $SR(G) = i(s(G)) = s(i(G))$ . Por ejemplo si  $R$  es el reticulado indicado en la Figura 1.1, y  $G = \{d, e\}$  entonces  $SR(G) = \{b, d, e, g\}$ , y si  $G = \{f, g\}$  entonces  $SR(G) = \{d, f, g, 1\}$ .

---

\*Trabajo presentado en 1968 al Simposio Panamericano de Matemática Aplicada, Buenos Aires, Argentina, [5]

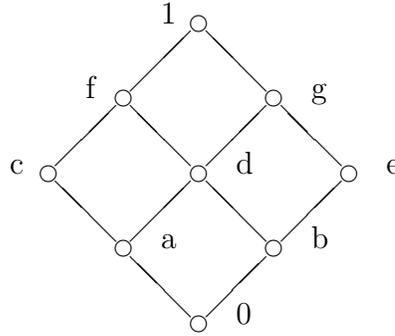


Figura 1.1

Diremos que  $G \subseteq R$  es un conjunto de generadores de  $R$  si  $SR(G) = R$ . En el ejemplo precedente  $G = \{c, d, e\}$  es un conjunto de generadores de  $R$ .

Sea  $R$  es un reticulado distributivo,  $G$  un subconjunto de  $R$  tal que  $SR(G) = R$  y cualquiera que sea el subconjunto propio  $G'$  de  $G$ , esto es  $G' \subset G$ , entonces  $SR(G')$  es un subreticulado propio de  $R$ , ( $SR(G') \subset R$ ). En este caso diremos que  $G$  es un conjunto minimal de generadores de  $R$ .

Sea  $R$  un reticulado distributivo finito, no trivial, luego tiene primer (0) y último (1) elemento. Un elemento  $p \in R$  se dice primo si  $p \neq 0$  y si  $p = a \vee b$  donde  $a, b \in R$  entonces  $p = a$  ó  $p = b$ , lo que es equivalente a decir que  $p \neq 0$  y si  $p \leq a \vee b$  donde  $a, b \in R$  entonces  $p \leq a$  ó  $p \leq b$ . Sea  $\Pi = \Pi(R)$  el conjunto de todos los elementos primos de  $R$ . Es claro que  $\Pi(R)$  es un conjunto ordenado con la relación de orden " $\leq$ " inducida por  $\wedge$  (ó por  $\vee$ ).

Si  $R$  es un reticulado distributivo, no trivial, es bien conocido que  $SR(\Pi(R)) = R$ .

Si  $R$  es finito entonces  $\Pi(R)$  es un conjunto ordenado finito. Es bien conocido que si  $\Pi$  es un conjunto ordenado finito, entonces existe un reticulado distributivo finito  $R$  tal que  $\Pi(R) \cong \Pi$ .

Sea  $\Pi_0 = \Pi_0(R)$  un subconjunto no vacío de  $\Pi(R)$ , luego  $\Pi_0$  también es un conjunto ordenado. Si  $r \in R$  notaremos  $\Pi(r) = \{p \in \Pi : p \leq r\}$  y  $\Pi_0(r) = \{p \in \Pi_0 : p \leq r\}$ , luego  $\Pi_0(r) = \Pi(r) \cap \Pi_0$ .

Sobre  $R$  definamos la siguiente relación binaria: Si  $a, b \in R$  notaremos  $a \equiv b$  (mód.  $\Pi_0$ ) ó  $a \equiv b$  si y sólo si  $\Pi_0(a) = \Pi_0(b)$ . Se prueba sin dificultad que  $\equiv$  es una relación de congruencia. Notaremos con  $C(a) = \{x \in R : x \equiv a \text{ (mód. } \Pi_0)\}$  la clase de equivalencia, módulo  $\Pi_0$ , que contiene al elemento  $a$ . Sea  $R' = R/\Pi_0$  el reticulado cociente donde las operaciones están definidas por  $C(a) \wedge C(b) = C(a \wedge b)$  y  $C(a) \vee C(b) = C(a \vee b)$ . La transformación  $h : R \rightarrow R'$  definida por  $h(a) = C(a)$  es un epimorfismo de reticulados, denominado epimorfismo natural. Observemos que  $C(0)$  es el primer elemento de  $R'$  y  $C(1)$  el último elemento de  $R'$ .

**Ejemplo 1.1** Sea  $R$  el reticulado indicado en la siguiente figura:

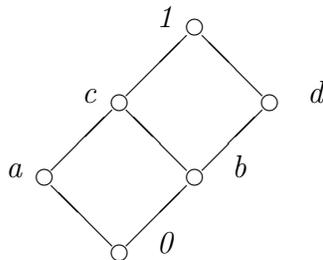


Figura 1.2

luego  $\Pi = \Pi(R) = \{a, b, d\}$ . Si  $\Pi_0 = \{a, d\}$  entonces  $\Pi_0(0) = \emptyset = \Pi_0(b)$ ,  $\Pi_0(a) = \{a\} = \Pi_0(c)$ ,  $\Pi_0(1) = \{a, d\}$ , y por lo tanto  $C(0) = \{0, b\}$ ,  $C(a) = \{a, c\}$ ,  $C(d) = \{d\}$ ,  $C(1) = \{1\}$ . Luego  $R/\Pi_0$  tiene el diagrama indicado en la Figura 1.3 y si  $\Pi_0 = \{a\}$  entonces  $R/\Pi_0$  tiene el diagrama indicado en la Figura 1.4

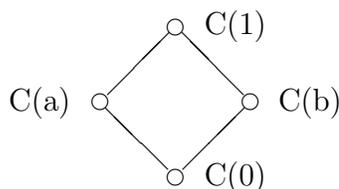


Figura 1.3

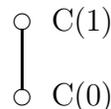


Figura 1.4

**Observación 1.1** Si  $R$  y  $R'$  son reticulados distributivos finitos,  $h : R \rightarrow R'$  un epimorfismo y  $p \in \Pi(R)$  entonces  $h(p)$  no necesariamente es un elemento de  $\Pi(R')$ . Además puede que no exista ningún epimorfismo de orden de  $\Pi(R)$  en  $\Pi(R')$ . En efecto consideremos los reticulados  $R$  y  $R'$  indicados en la siguiente figura:

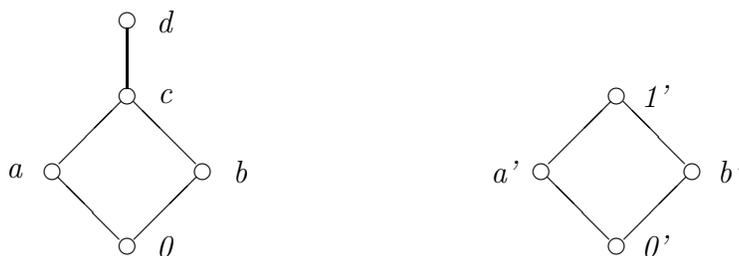


Figura 1.5

entonces definiendo  $h : R \rightarrow R'$  por  $h(0) = 0'$ ,  $h(a) = a'$ ,  $h(b) = b'$ ,  $h(c) = 0'$ ,  $h(1) = 1'$  se verifica sin dificultad que  $h$  es un epimorfismo de  $R$  en  $R'$ . Además  $c \in \Pi(R)$  y  $h(c) = 0' \notin \Pi(R')$ . Es claro que  $\Pi(R)$  y  $\Pi(R')$  son conjuntos ordenados no isomorfos.

**Teorema 1.1** Si  $\Pi_0$  es un subconjunto no vacío de  $R$ ,  $R' = R/\Pi_0$ ,  $\Pi' = \Pi(R')$  es el conjunto ordenado de los elementos primos de  $R'$ , y  $h$  es el epimorfismo natural de  $R \rightarrow R'$  definido anteriormente, entonces la función  $h$  restringida a  $\Pi_0$  establece un isomorfismo de orden entre los conjuntos  $\Pi_0$  y  $\Pi'$ , esto es  $\Pi(R/\Pi_0) \cong \Pi_0$ .

**Demostración.**

- 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  $\Pi_0$ , es una función suryectiva de  $\Pi_0$  en  $\Pi'$ .  
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  $X = \{x_1, x_2, \dots, x_n\}$  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  $p' = h(p_0) = h(0) = 0'$ , 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.  $\Pi_0$ ) y en consecuencia  $h(p_0) = h(0) = C(0) = 0'$ , contradicción, luego  $\Pi_0(p_0) = \{q_1, q_2, \dots, q_s\}$ .  
Sea  $x = \bigvee_{i=1}^s q_i$ . Es claro que  $x \equiv p_0$  (mód.  $\Pi_0$ ), 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 que  $p_0 \leq q_i$ . 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.  $\Pi_0$ ), 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  $p_1 = p_2$ .

□

**Lema 1.1** Sean  $R, R'$  reticulados distributivos,  $h : R \rightarrow R'$  un homomorfismo. Si  $G \subseteq R$  es tal que  $SR(G) = R$  entonces  $SR(h(G)) = h(R)$ , (esto es si  $G$  genera  $R$ , entonces  $h(G)$  genera al reticulado  $h(R)$ .) Si  $N[G] = n$  y  $h$  es suryectivo entonces  $R' = SR(h(G))$  y  $N[h(G)] \leq n$ .

**Teorema 1.2** Si  $R$  y  $R'$  son reticulados distributivos finitos, no triviales, tales los conjuntos ordenados  $\Pi$  y  $\Pi'$  de sus elementos primos son isomorfos entonces  $R$  y  $R'$  son reticulados isomorfos.

**Teorema 1.3** Si  $R$  y  $R'$  son reticulados distributivos finitos, no triviales,  $\Pi$  y  $\Pi'$  los conjuntos ordenados de sus elementos primos, y  $\alpha : R \rightarrow R'$  un epimorfismo de reticulados, entonces existe un isomorfismo de orden  $\beta : \Pi' \rightarrow \Pi$ , esto es el conjunto ordenado  $\Pi'$  isomorfo al subconjunto  $\beta(\Pi')$  del conjunto ordenado  $\Pi$ . Además  $R'$  es isomorfo al reticulado  $R/\beta(\Pi')$ .

**Demostración.** Dado (1)  $p' \in \Pi'$ , como  $\alpha$  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 Teorema 1.1 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 el Teorema 1.2 resulta que  $R(\beta(\Pi'))$  y  $R'$  son reticulados isomorfos. □

**Definición 1.1** Un subconjunto  $G$  de un reticulado distributivo  $L$  se dice un conjunto de generadores libres de  $L$  si:

L1)  $SR(G) = L$ , (esto es  $G$  es un conjunto de generadores de  $L$ .)

L2) Dada una función  $f$  de  $G$  en un reticulado distributivo arbitrario  $R$ , existe un homomorfismo  $h_f : L \rightarrow R$  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 reticulado distributivo libre o que  $L$  es un reticulado distributivo con un conjunto  $G$  de generadores libres.

**Teorema 1.4** Para toda “álgebra” definida por igualdades existe siempre el “álgebra” libre con un conjunto de generadores de cardinal prefijado. [1]

Sea  $\mathbf{B} = \{0, 1\}$  un álgebra de Boole con 2 elementos y  $\mathbf{B}^n$  el producto cartesiano de  $n$  álgebras de Boole iguales a  $\mathbf{B}$ . El último elemento de  $\mathbf{B}^n$  es la  $n$ -upla cuyas componentes son todas iguales a 1, esto es  $\mathbf{1} = (1, 1, \dots, 1)$  es el último elemento de  $\mathbf{B}^n$ . Análogamente  $\mathbf{0} = (0, 0, \dots, 0)$  es el primer elemento de  $\mathbf{B}^n$ . Sea  $FD(n)$  el reticulado distributivo con  $n$  generadores libres, es bien conocido que  $\Pi(FD(n))$  es isomorfo al conjunto ordenado  $\mathbf{Q}(n) = \mathbf{B}^n - \{\mathbf{0}, \mathbf{1}\}$ .

**Lema 1.2** Si  $R$  es un reticulado distributivo, y  $G \subseteq R$  verifica  $N[G] = n$  y  $SR(G) = R$  entonces el conjunto ordenado  $\Pi(R)$  es isomorfo a un subconjunto del conjunto ordenado  $\Pi(FD(n))$ .

**Demostración.** Sea  $G'$  un conjunto de generadores libres de  $FD(n)$  como  $N[G'] = n$  entonces existe una biyección  $f : G' \rightarrow G \subseteq R$ , luego  $f$  se puede extender a un único homomorfismo  $h : FD(n) \rightarrow R$ . Entonces por el Lema 1.1,  $h(FD(n)) = SR(SR(G')) = SR(h(G')) = SR(G) = R$  y en consecuencia por el Teorema 1.3,  $\Pi(R)$  es isomorfo a un subconjunto de  $\Pi(FD(n))$ .  $\square$

**Teorema 1.5** Sea  $R$  un reticulado distributivo finito y  $\Pi = \Pi(R)$ . Si el conjunto ordenado  $\Pi$  es isomorfo a una parte  $\Pi_0$  de  $\Pi(FD(n))$  entonces  $R$  tiene un conjunto de generadores con  $n$  elementos.

**Demostración.** Consideremos en  $FD(n)$  la congruencia módulo  $\Pi_0$ . Por el Teorema 1.1 el conjunto ordenado  $\Pi(FD(n)/\Pi_0)$  es isomorfo a  $\Pi_0$  y como por hipótesis  $\Pi_0$  y  $\Pi$  son conjuntos ordenados finitos isomorfos entonces los conjuntos ordenados  $\Pi(FD(n)/\Pi_0)$  y  $\Pi$  son isomorfos, luego por el Teorema 1.2  $FD(n)/\Pi_0$  es un reticulado distributivo isomorfo a  $R$ .  $FD(n)$  entonces  $R$  es una imagen homomórfica de  $FD(n)$ . Sea  $\alpha : FD(n) \rightarrow R$  un isomorfismo y  $G$  un conjunto de generadores libres de  $FD(n)$  luego por el Lema 1.1  $G' = \alpha(G) \subseteq R$  verifica  $SR(G') = R$  y como  $\alpha$  es biyectiva  $N[G'] = N[\alpha(G)] = n$ .  $\square$

**Corolario 1.1** Si  $R$  es un reticulado distributivo finito,  $\Pi = \Pi(R)$  y  $n$  el menor entero positivo tal que el conjunto ordenado  $\Pi$  es isomorfo a una parte  $\Pi_0$  de  $\Pi(FD(n))$  entonces  $n$  es el número minimal de generadores de  $R$ .

**Demostración.** Por el Teorema 1.5 sabemos que  $R$  tiene un conjunto de generadores con  $n$  elementos. Si  $G' \subseteq R$  verifica  $SR(G') = R$ , donde  $m < n$ , entonces por el Lema 1.2,  $\Pi$  es isomorfo a un subconjunto de  $\Pi(FD(m))$  con  $m < n$ , lo que contradice la hipótesis sobre  $n$ .  $\square$

Vamos a indicar una construcción de un conjunto minimal de generadores de un reticulado distributivo finito  $R$ , no trivial.

Sea  $\Pi = \Pi(R)$  el conjunto ordenado de los elementos primos de  $R$  y  $m = N[R]$ , como  $SR(R) = R$ , sabemos por el Lema 1.2 que  $\Pi(R)$  es isomorfo a un subconjunto de

$\Pi(FD(m))$ . Sea  $n$  el menor entero positivo para el cual  $\Pi$  es isomorfo a un subconjunto de  $\Pi(FD(n))$ ,  $\alpha$  un isomorfismo de orden entre  $\Pi$  y  $\Pi_0 \subseteq \Pi(FD(n))$  y  $M(n) = \{m_1, m_2, \dots, m_n\}$  el conjunto de los elementos maximales del conjunto ordenado  $\Pi(FD(n))$ . En este caso es bien conocido que  $SR(M(n)) = FD(n)$ . Sean:

$$\begin{aligned} P_i &= \{p \in \Pi_0 : p \leq m_i\}, & i = 1, 2, \dots, n \\ \Pi_i &= \{p \in \Pi : \alpha(p) \in P_i\}, & i = 1, 2, \dots, n \\ & \text{y} \\ g_i &= \bigvee \{p : p \in \Pi_i\}, & i = 1, 2, \dots, n. \end{aligned}$$

Observemos que si  $P_i = \emptyset$  entonces  $\Pi_i = \emptyset$  y por lo tanto  $g_i = 0$ .

Probemos que  $G = \{g_1, g_2, \dots, g_n\}$  es un conjunto de generadores de  $R$ . En efecto sea  $f : M(n) \rightarrow R$  definida por  $f(m_i) = g_i$ ,  $i = 1, 2, \dots, n$ . Luego  $f$  se puede extender a un homomorfismo  $h : FD(n) \rightarrow R$ . Por el Lema 1.1 sabemos que  $h(FD(n)) = h(SR(M(n))) = SR(h(M(n))) = SR(G)$  y como  $\Pi_0 \subseteq FD(n)$  resulta que  $\Pi = h(\Pi_0) \subseteq h(FD(n))$ , luego  $R = SR(\Pi) \subseteq h(FD(n))$ , esto es  $SR(G) = R$ .

Acabamos así de probar que el conjunto  $G$  indicado en la construcción anterior genera  $R$ , y por el Teorema 1.5, este conjunto es un conjunto minimal de generadores de  $R$ . Además por el Corolario 1.1 sabemos que  $n$  es el menor número de generadores de  $R$ , luego cualquier conjunto minimal de generadores de  $R$  tiene  $n$  elementos.

Finalmente observemos que para cada representación isomórfica de  $\Pi$  en  $\Pi(FD(n))$  tenemos una solución al problema planteado.

Vamos a indicar algunos ejemplos y para ello comenzaremos por recordar que el conjunto ordenado  $\mathbf{Q}(3)$  de los elementos primos de  $FD(3)$  tiene el siguiente diagrama:

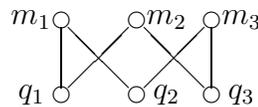


Figura 1.6

**Ejemplos 1.1** 1) Sea  $R$  el reticulado indicado en el siguiente diagrama:

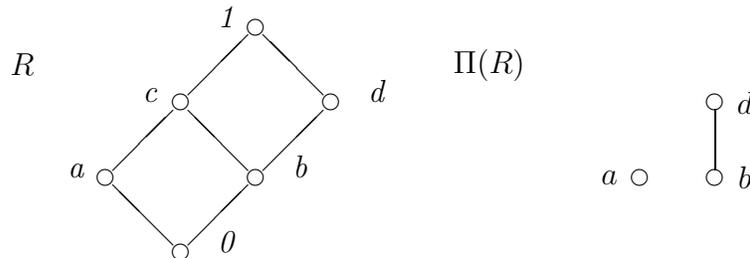


Figura 1.7

Podemos sumergir  $\Pi(R) = \{a, b, d\}$  en  $\mathbf{Q}(3)$  del siguiente modo:  $\alpha(a) = q_1$ ,  $\alpha(b) = q_2$ ,  $\alpha(d) = m_3$ . Luego  $P_1 = \{q_1, q_2\}$ ,  $P_2 = \{q_1\}$ ,  $P_3 = \{q_2, m_3\}$  y por lo tanto  $g_1 = a \vee b = c$ ,  $g_2 = a$ ,  $g_3 = b \vee d = d$ . En consecuencia  $G = \{a, c, d\}$  es un conjunto minimal de generadores de  $R$ .

Si sumergimos  $\Pi(R)$  en  $\mathbf{Q}(3)$  del siguiente modo:  $\beta(a) = m_1$ ,  $\beta(b) = q_3$ ,  $\beta(d) = m_3$ , entonces  $P_1 = \{m_1\}$ ,  $P_2 = \{q_3\}$ ,  $P_3 = \{q_3, m_3\}$  y por lo tanto  $g_1 = a$ ,  $g_2 = b$ ,  $g_3 = d$ . En consecuencia  $G = \{a, b, d\} = \Pi(R)$  es un conjunto minimal de generadores de  $R$ .

2) Sea  $R$  el reticulado indicado en el siguiente diagrama:

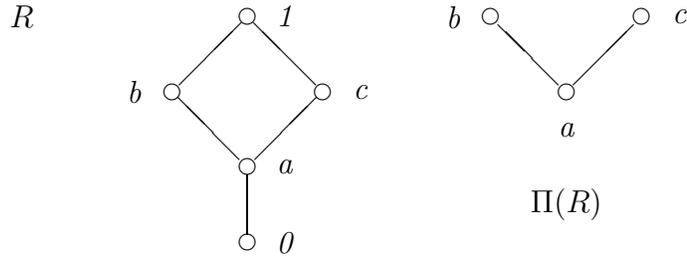


Figura 1.8

Podemos sumergir  $\Pi(R) = \{a, b, c\}$  en  $\mathbf{Q}(3)$  del siguiente modo:  $\alpha(a) = q_2$ ,  $\alpha(b) = m_1$ ,  $\alpha(c) = m_3$ . Luego  $P_1 = \{q_2\}$ ,  $P_2 = \emptyset$ ,  $P_3 = \{q_2, m_3\}$  y por lo tanto  $g_1 = a$ ,  $g_2 = 0$ ,  $g_3 = a \vee c = c$ . En consecuencia  $G = \{0, a, c\}$  es un conjunto minimal de generadores de  $R$ .

3) Sea  $R$  el reticulado distributivo indicado en el siguiente diagrama:

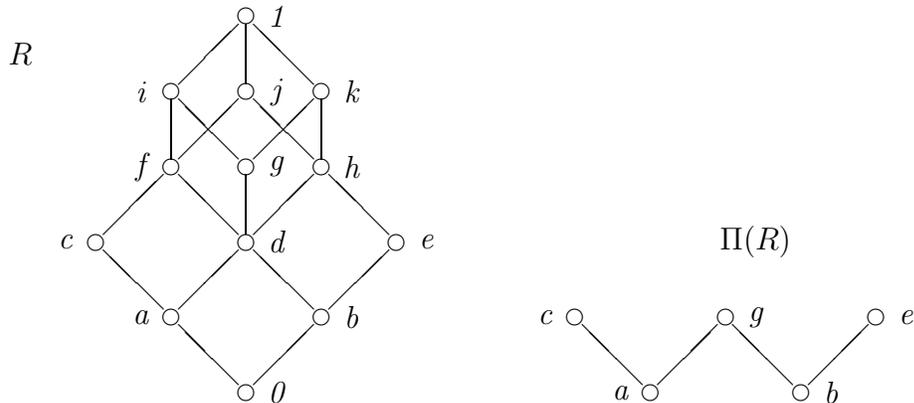


Figura 1.9

El conjunto  $\Pi = \{a, c, g, b, e\}$  puede sumergirse en  $\mathbf{Q}(3)$  del siguiente modo  $\alpha(a) = q_1$ ,  $\alpha(b) = q_3$ ,  $\alpha(c) = m_1$ ,  $\alpha(g) = m_2$ ,  $\alpha(e) = m_3$ , entonces  $g_1 = c \vee a = c$ ,  $g_2 = e \vee a \vee b = e$ ,  $g_3 = d \vee b = d$ , y por lo tanto  $G = \{a, e, g\}$  es un conjunto minimal de generadores de  $R$ . En este caso existe una sola forma de sumergir  $\Pi(R)$  en  $\mathbf{Q}(3)$ .

El reticulado  $C$  considerado por C. Cardot ([2], Fig. 9) tiene el diagrama indicado en la Figura 1.10 (ver también [3], pág. 246):

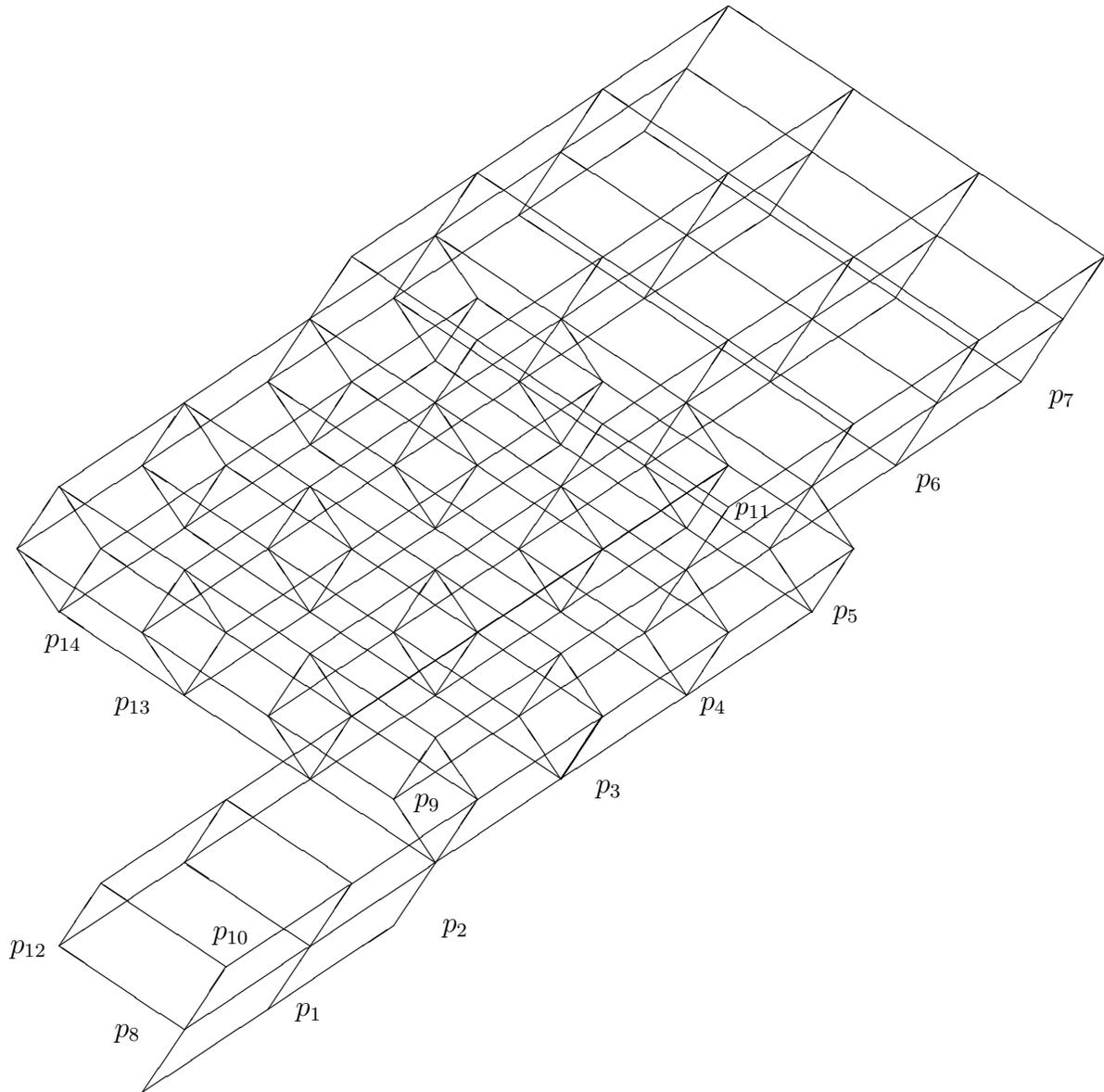


Figura 1.10

C. Cardot prueba que el reticulado  $C$  está generado por los 11 elementos indicados en la Figura 1.11 por los círculos negros.

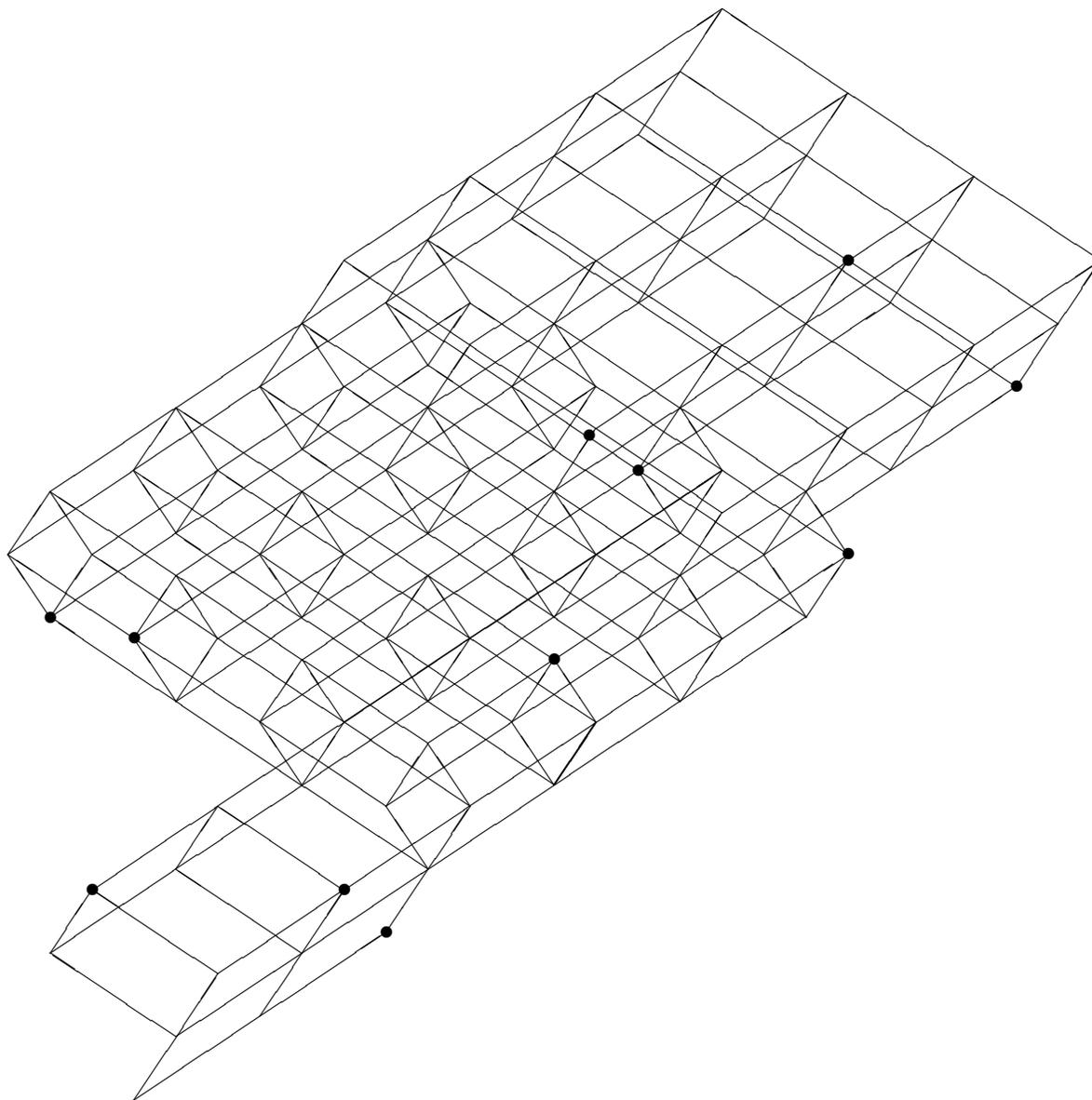


Figura 1.11

El conjunto  $\Pi(C)$  de los elementos primos del reticulado  $C$  tiene 14 elementos, y su diagrama es el siguiente:

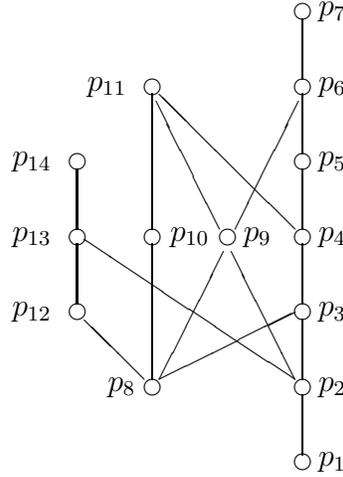


Figura 1.12

**Nota del redactor** En el resumen de este trabajo, A. Monteiro dice que el número mínimo de generadores de  $C$  es 8. No hemos podido encontrar notas del autor donde indica sus cálculos. El número 8 es seguramente un error de tipeado pues si  $A$  es un conjunto con 8 elementos,  $X = \mathcal{P}(A) - \{\emptyset, A\}$  es un conjunto ordenado isomorfo a  $\mathbf{Q}(8)$ . Si  $\Pi(C)$  pudiera sumergirse en  $X$ , entonces existiría un isomorfismo de orden de  $\Pi(C)$  en  $X$  y entonces la cadena  $\{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}$  se transformarían en una cadena  $\{A_1, A_2, A_3, A_4, A_5, A_6, A_7\}$  de  $X$  y por lo tanto debe ser  $N[A_i] = i$ ,  $1 \leq i \leq 7$ . Sea  $A_3 = \{a, b, c\}$ , luego como  $A_2 \subseteq A_3$  tendremos  $A_2 = \{a, b\}$ ,  $A_2 = \{a, c\}$  ó  $A_2 = \{b, c\}$ . Supongamos que (1)  $A_2 = \{a, b\}$  luego  $A_1 = \{a\}$  ó  $A_1 = \{b\}$ . Consideremos el caso en que (2)  $A_1 = \{a\}$ . Como  $A_8 \subseteq A_3$  entonces por la hipótesis (1) tenemos  $A_8 = \{a, c\}$ ,  $A_8 = \{b, c\}$ ,  $A_8 = \{a\}$ ,  $A_8 = \{b\}$  ó  $A_8 = \{c\}$ . Pero si  $A_8 = \{a\}$  tendríamos  $A_8 = A_1$ , contradicción. Si  $A_8 = \{b\}$  entonces  $A_8 \subseteq A_2$ , contradicción. Si  $A_8 = \{a, c\}$  como  $A_8 \subseteq A_9$  y  $A_2 \subseteq A_9$  tendríamos  $\{a, b, c\} \subseteq A_8 \cup A_2 \subseteq A_9$  y por lo tanto  $A_3 \subseteq A_9$ , absurdo. Análogamente si  $A_8 = \{b, c\}$  llegamos a una contradicción, luego la única posibilidad es que  $A_8 = \{c\}$ , luego  $\{a, b, c\} \subseteq A_8 \cup A_2 \subseteq A_9$  y por lo tanto  $A_3 \subseteq A_9$ , absurdo. Analizando todos los otros casos también llegamos a contradicciones. Por lo tanto  $\Pi(C)$  no puede sumergirse en  $\mathbf{Q}(8)$ .

Sea  $A = \{a_i : 1 \leq i \leq 9\}$  y  $\mathcal{P}(A)$  la familia de todos los subconjuntos de  $A$ , es bien conocido que  $X = \mathcal{P}(A) - \{\emptyset, A\}$  es un conjunto ordenado isomorfo a  $\mathbf{Q}(9)$ . Además los elementos maximales de  $X$  son  $M_i = A - \{a_i\}$  para  $i = 1, 2, \dots, 9$ .

Sean:

$$\begin{aligned}
 A_1 &= \{a_1\}, & A_2 &= \{a_1, a_2\}, \\
 A_3 &= \{a_1, a_2, a_3, a_4\}, & A_4 &= \{a_1, a_2, a_3, a_4, a_5\}, \\
 A_5 &= \{a_1, a_2, a_3, a_4, a_5, a_6\}, & A_6 &= \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}, \\
 A_7 &= \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_9\}, & A_8 &= \{a_3\}, \\
 A_9 &= \{a_1, a_2, a_3, a_7\}, & A_{10} &= \{a_3, a_5, a_8\}, \\
 A_{11} &= \{a_1, a_2, a_3, a_4, a_5, a_7, a_8\}, & A_{12} &= \{a_3, a_6, a_8\}, \\
 A_{13} &= \{a_1, a_2, a_3, a_6, a_8\}, & A_{14} &= \{a_1, a_2, a_3, a_6, a_8, a_9\}.
 \end{aligned}$$

Entonces el conjunto  $\{A_i : 1 \leq i \leq 14\}$  ordenado por la relación  $\subseteq$  tiene el siguiente diagrama de Hasse:

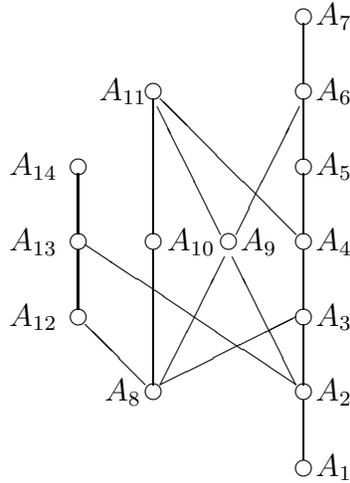


Figura 1.13

Entonces  $\Pi(C)$  se puede sumergir en  $X$  del siguiente modo  $\alpha(p_i) = A_i$ ,  $1 \leq i \leq 14$ . Luego:

$$\begin{aligned}
 P_1 &= \{A_8, A_{10}, A_{12}\}, \\
 P_2 &= \{A_1, A_8, A_{10}, A_{12}\}, \\
 P_3 &= \{A_1, A_2\}, \\
 P_4 &= \{A_1, A_2, A_8, A_{10}, A_{12}, A_{13}, A_{14}\}, \\
 P_5 &= \{A_1, A_2, A_3, A_8, A_9\}, \\
 P_6 &= \{A_1, A_2, A_3, A_4, A_8, A_9, A_{10}, A_{11}\}, \\
 P_7 &= \{A_1, A_2, A_3, A_4, A_5, A_8, A_{10}, A_{12}, A_{13}, A_{14}\},
 \end{aligned}$$

$$P_8 = \{A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8, A_9\},$$

$$P_9 = \{A_1, A_2, A_3, A_4, A_5, A_6, A_8, A_{10}, A_{11}, A_{12}, A_{13}\}.$$

y por lo tanto determinamos el siguiente conjunto de generadores de  $R$ :

$$g_1 = p_8 \vee p_{10} \vee p_{12} = p_{10} \vee p_{12},$$

$$g_2 = p_1 \vee p_8 \vee p_{10} \vee p_{12} = p_1 \vee p_8 \vee g_1,$$

$$g_3 = p_1 \vee p_2 = p_2,$$

$$g_4 = p_1 \vee p_2 \vee p_8 \vee p_{10} \vee p_{12} \vee p_{13} \vee p_{14} = p_2 \vee p_{10} \vee p_{14},$$

$$g_5 = p_1 \vee p_2 \vee p_3 \vee p_8 \vee p_9 = p_3 \vee p_9,$$

$$g_6 = p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_8 \vee p_9 \vee p_{10} \vee p_{11} = p_{11},$$

$$g_7 = p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_5 \vee p_8 \vee p_{10} \vee p_{12} \vee p_{13} \vee p_{14} = p_5 \vee p_{10} \vee p_{14},$$

$$g_8 = p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_5 \vee p_6 \vee p_7 \vee p_8 \vee p_9 = p_7,$$

$$g_9 = p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_5 \vee p_6 \vee p_8 \vee p_{10} \vee p_{11} \vee p_{12} \vee p_{13} = p_6 \vee p_{11} \vee p_{13},$$

Los 9 generadores determinados precedentemente estan indicados, por círculos negros, en la Figura 1.14.

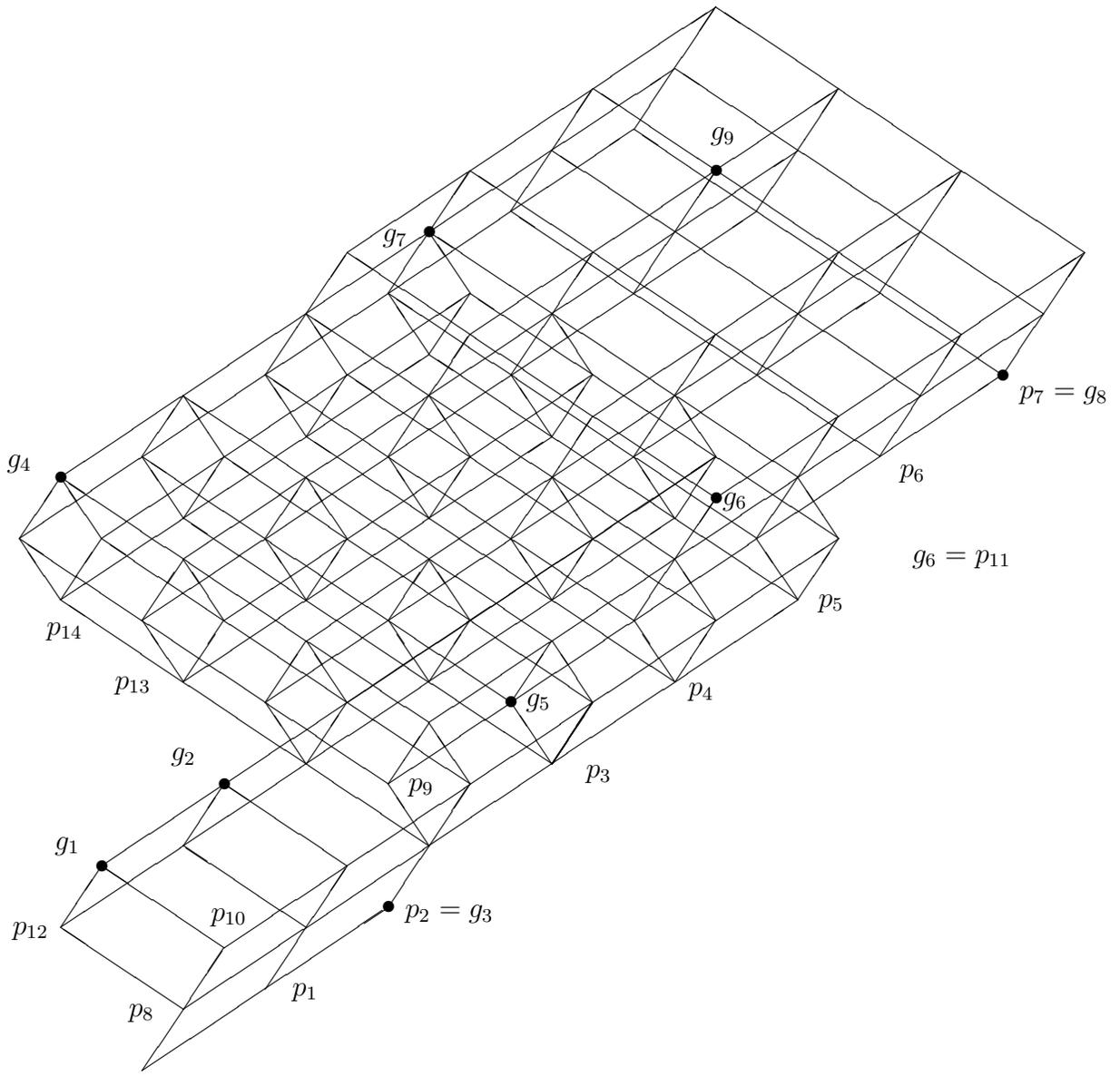


Figura 1.14

## 2. Generadores de álgebras de Boole finitas

### 2.1. Introducción

Sea  $(B, \wedge, \vee, -, 0, 1)$  un álgebra de Boole, si  $X \subseteq B$  notaremos  $-X = \{-x : x \in X\}$ . Si  $B$  es un álgebra de Boole finita con mas de un elemento representaremos con  $\mathcal{A}(B)$  el conjunto de todos los átomos de  $B$ .

Con  $SB(X)$  representaremos la subálgebra booleana de  $B$  generada por  $X$ . Si  $SB(X) = B$  diremos que  $X$  es un conjunto de generadores de  $B$ . Es bien conocido que  $SB(\emptyset) = \{0, 1\}$ , y que si  $B$  tiene un solo elemento entonces  $SB(\emptyset) = \{0\}$ . Luego si  $B$  tiene mas de dos elementos entonces todo conjunto de generadores de  $B$  es no vacío.

Es claro que si  $X \subseteq B$  entonces  $SB(X) = SB(-X)$ . Si  $B$  y  $B'$  son álgebras de Boole y  $h : B \rightarrow B'$  es un homomorfismo de  $B$  en  $B'$ , entonces  $Nuc(h) = \{x \in B : h(x) = 1\}$  es un filtro de  $B$  y si  $h(B) = B'$  entonces el álgebra cociente  $B/Nuc(h)$  es isomorfa a  $B'$ . Si  $z \in B$  entonces  $[z] = \{x \in B : z \leq x\}$  es un filtro de  $B$  y  $(z) = \{x \in B : x \leq z\}$  es un ideal de  $B$ .

Si  $p, u \in B$  son tales que  $p \leq q$ , sea  $[p, u] = \{x \in B : p \leq x \leq u\}$ . Es bien conocido que  $[p, u]$  es un reticulado distributivo con primer elemento  $p$  y último elemento  $u$ . Si  $s \in [p, u]$  definiendo  $s' = p \vee (-s \wedge u)$ , se demuestra que  $s'$  es el complemento booleano de  $s$  en  $[p, u]$  y por lo tanto  $[p, u]$  es un álgebra de Boole. Si  $p = 0$  entonces  $S = [0, u] = (u)$  es un álgebra de Boole donde el complemento de  $s \in S$  es  $s' = -s \wedge u$  y si  $u = 1$  entonces  $S = [p, 1] = (p)$  es un álgebra de Boole donde el complemento de  $s \in S$  es  $s' = p \vee -s$ .

**Lema 2.1** *Si  $B$  es un álgebra de Boole y  $u \in B$  entonces  $B' = A/[u]$  es isomorfa al álgebra de Boole  $A'' = (u)$ .*

Es bien conocido que todas las imágenes homomórficas de un álgebra de Boole  $B$  están determinadas, a menos de isomorfismos, por los filtros de  $B$ .

**Lema 2.2** *Sean  $A, A'$  álgebras de Boole,  $h : A \rightarrow A'$  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  $h(A)$ .)*

**Definición 2.1** *Un subconjunto  $G$  de un álgebra de Boole  $A$  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  $h_f : L \rightarrow A$  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.

## 2.2. Conjuntos minimales de generadores

Si  $B$  es un álgebra de Boole, es importante determinar subconjuntos  $G$  de  $B$  tales que:

- 1)  $SB(G) = B$ .
- 2) Si  $G'$  es un subconjunto propio de  $G$ , esto es  $G' \subset G$ , entonces  $SB(G')$  es una subálgebra propia de  $B$ , esto es  $SB(G') \subset B$ .

Un tal subconjunto  $G$  se denomina un conjunto minimal de generadores del álgebra de Boole  $B$ .

Notaremos con  $B_k$  un álgebra de Boole finita con  $k$  átomos.

Observemos en primer lugar que en un álgebra de Boole finita  $B$  existe *por lo menos* un conjunto minimal de generadores de  $B$ . En efecto, sea  $\mathcal{G}(B)$  la familia de todos los conjuntos de generadores de  $B$ , como  $B$  es un conjunto (maximal) de generadores de  $B$ , entonces  $\mathcal{G}(B) \neq \emptyset$ , por lo tanto el par  $(\mathcal{G}(B), \subseteq)$  es un conjunto ordenado finito, y los elementos minimales de este conjunto ordenado son conjuntos minimales de generadores de  $B$ . Observemos aún que  $\mathcal{G}(B)$  es un reticulado superior con último elemento  $B$ , dado que  $SB(B) = B$  y si  $X, Y \in \mathcal{G}(B)$  entonces  $X \cup Y \in \mathcal{G}(B)$ .

Sea  $B$  un álgebra de Boole con mas de un elemento. Observemos que si  $G$  es un conjunto minimal de generadores de  $B$  entonces  $-g \notin G$  cualquiera que sea  $g \in G$ . En efecto si existiera  $g_0 \in G$  tal que (1)  $-g_0 \in G$  entonces (2)  $G_0 = G \setminus \{g_0\} \subset G$ . Además (3)  $G \subseteq SB(G_0)$ , en efecto si  $g \in G$  y  $g \neq g_0$  tenemos que  $g \in G_0 \subseteq SB(G_0)$  y si  $g = g_0$  entonces por (1)  $-g_0 \in G$ , luego como  $B$  tiene mas de un elemento  $-g_0 \neq g_0$  y por lo tanto  $-g_0 \in G_0 \subseteq SB(G_0)$ , lo que prueba (3). De (2) y (3) resulta  $B = SB(G) \subseteq SB(G_0)$  esto es  $SB(G_0) = B$ . Luego  $G_0$  sería un conjunto de generadores de  $B$  tal que  $G_0 \subset G$ , lo que contradice que  $G$  es un conjunto mínimo de generadores.

Como  $SB(G) = SB(-G)$ , si  $G$  es un conjunto minimal de generadores de  $B$  entonces  $-G$  también es un subconjunto minimal de generadores de  $B$  y por lo visto precedentemente  $G \neq -G$ . Esto prueba que si existe un subconjunto minimal, no vacío, de generadores de  $B$ , entonces existe mas de un conjunto en estas condiciones.

En forma natural se plantea el siguiente problema:

¿dos conjuntos minimales de generadores de un álgebra de Boole finita, tienen el mismo número de elementos? La respuesta al mismo es negativa. Pero antes observemos lo siguiente: si consideramos el álgebra de Boole  $B_2$  cuyo diagrama indicamos en la Figura 2.1 entonces  $\mathcal{G}(B_2)$  tiene el diagrama indicado en la Figura 2.2, lo que muestra que todos los elementos minimales de  $\mathcal{G}(B_2)$  tienen todos 1 elemento.

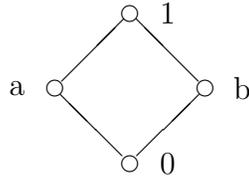


Fig. 2.1

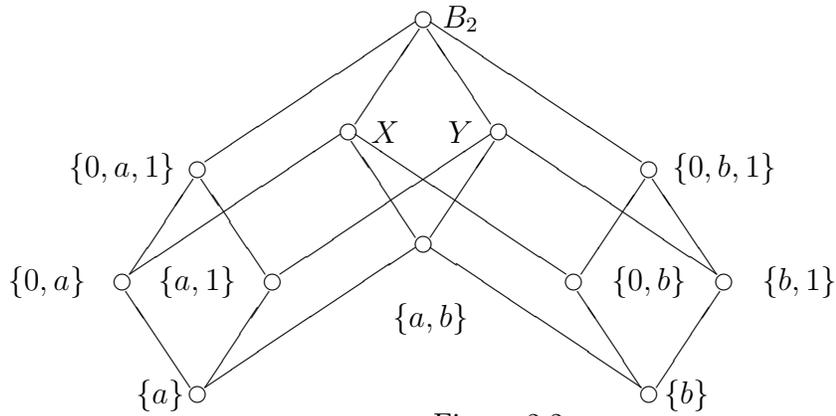


Figura 2.2

donde  $X = \{0, a, b\}$  e  $Y = \{a, b, 1\}$ .

Consideremos ahora el álgebra de Boole  $B_3$  cuyo diagrama se indica en la Figura 2.3.

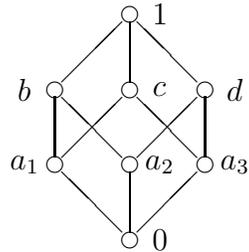


Figura 2.3

Entonces es fácil ver que los conjuntos minimales de generadores de  $B_3$  son  $G_1 = \{a_1, b\}$ ,  $G_2 = \{a_1, c\}$ ,  $G_3 = \{a_2, b\}$ ,  $G_4 = \{a_2, d\}$ ,  $G_5 = \{a_3, c\}$ ,  $G_6 = \{a_3, d\}$ ,  $G_7 = \{a_1, a_3\}$ ,  $G_8 = \{a_1, a_2\}$ ,  $G_9 = \{a_2, a_3\}$ ,  $G_{10} = \{b, d\}$ ,  $G_{11} = \{c, d\}$ ,  $G_{12} = \{b, c\}$ .

Consideremos el álgebra de Boole  $B_4$  cuyo diagrama de Hasse se indica a continuación:

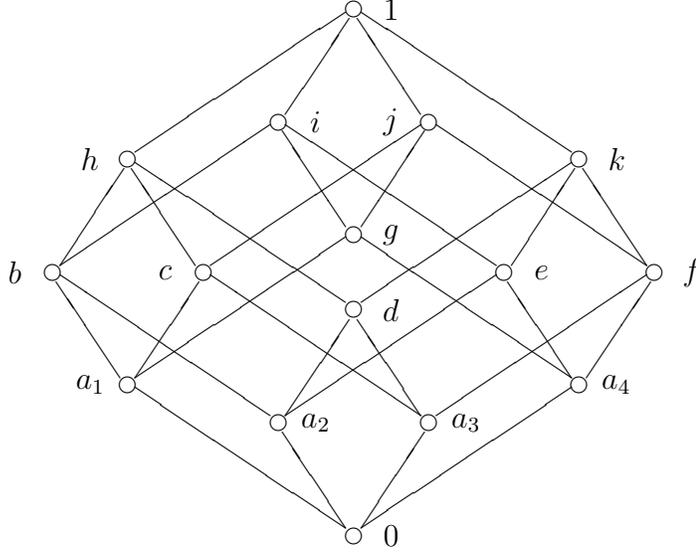


Figura 2.4

En este caso el conjunto  $G = \{a_1, b, h\}$  genera  $B_4$  y cualquier subconjunto propio de  $G$  no genera a  $B_4$ , por lo tanto  $G$  es un conjunto minimal de generadores de  $B_4$ . Por otro lado es bien conocido que  $B_4$  es un álgebra de Boole con dos generadores libres: por ejemplo  $\{e, f\}$  es un conjunto de generadores libres de  $B_4$ . Tenemos así dos conjuntos minimales de generadores que no tienen el mismo número de elementos.

El ejemplo precedente nos sugiere el siguiente problema: Dada un álgebra de Boole finita, determinar un conjunto de generadores de  $B$ , con un número mínimo de elementos.

**Lema 2.3** *El álgebra de Boole  $FB(n)$  con  $n$  generadores libres,  $n \in \mathbf{N}$  no puede ser generada por un conjunto de  $m$  elementos, donde  $m < n$ .*

**Demostración.** Sea  $X = \{b_1, b_2, \dots, b_m\} \subseteq FB(n)$ , donde  $m < n$ , un conjunto tal que  $SB(X) = FB(n)$  y  $G = \{g_1, g_2, \dots, g_m, g_{m+1}, \dots, g_n\}$  un conjunto de generadores libres de  $FB(n)$ .

Consideremos la función  $f : G \rightarrow FB(n)$  definida por:

$$\begin{cases} (1) & f(g_i) = b_i, \quad 1 \leq i \leq m \\ y \\ (2) & f(g_i) = b_m, \quad m+1 \leq i \leq n \end{cases}$$

Entonces como  $FB(n)$  es un álgebra de Boole libre,  $f$  se puede extender a un homomorfismo  $H$  de  $FB(n)$  en  $FB(n)$ . Observemos que  $H$  es suryectiva pues  $H(FB(n)) = SB(H(G)) = SB(X) = FB(n)$ . Es claro que  $H$  no es inyectiva, luego  $Nuc(H) \neq \{1\}$ . Como  $Nuc(H)$  es un filtro principal entonces  $Nuc(H) = [f]$  con  $f \in FB(n)$ ,  $f \neq 1$ . Sea  $\varphi : FB(n) \rightarrow FB(n)/[f]$  el epimorfismo natural, luego  $Nuc(\varphi) = [f]$  y como  $H : FB(n) \rightarrow FB(n)$  es un epimorfismo y  $[f]$  es su núcleo entonces  $FB(n)$  es isomorfa a

$FB(n)/[f]$ . Por el Lema 2.1 sabemos que  $FB(n)/[f]$  es isomorfa al álgebra de Boole  $(f]$ . Como  $f \neq 1$ , entonces el número de átomos del álgebra de Boole  $(f]$  es menor que  $2^n$ , lo que es una contradicción.  $\square$

**Teorema 2.1** *Dada un álgebra de Boole  $B_k$ , sea  $n$  el menor entero tal que  $k \leq 2^n$ , esto es  $2^{n-1} < k \leq 2^n$ . Entonces  $n$  es el menor cardinal de un conjunto de generadores de  $B_k$ .*

**Demostración.** Vamos a probar en primer lugar que  $B_k$  no puede tener un conjunto de generadores  $G$  tal que  $N[G] < n$ .

Si  $k = 2^n$  entonces  $B_k$  es un álgebra de Boole con  $n$  generadores libres y vimos en el Lema 2.3 que esta álgebra no puede tener un conjunto de generadores con menos de  $n$  elementos.

Supongamos ahora que  $k \neq 2^n$  esto es  $2^{n-1} < k < 2^n$  y que  $B_k$  tiene un conjunto de generadores  $G$  tal que  $N[G] = m < n$ . Luego  $B_k$  es una imagen homomórfica del álgebra de Boole  $FB(m)$  con  $m$  generadores libres. Como  $FB(m)$  tiene  $2^m$  átomos entonces el número  $k$  de átomos de  $B_k$  es tal que  $k < 2^m$  lo que contradice la hipótesis sobre  $n$  de que  $m < n$ .

Vamos a demostrar que  $B_k$  tiene un conjunto  $G$  de generadores tal que  $N[G] = n$ .

Para ello vamos a comenzar por recordar una forma de construir  $FB(n)$  que indicaremos en nuestros cursos [4]. Sea  $\mathbf{B} = \{0, 1\}$  un álgebra de Boole con dos elementos, y consideremos el producto cartesiano  $\mathbf{C}(n)$  de  $n$  álgebras de Boole  $\mathbf{B}$ , luego los elementos  $\mathbf{x} \in \mathbf{C}(n)$  son de la forma  $\mathbf{x} = (x_1, x_2, \dots, x_n)$  donde  $x_i \in \mathbf{B}$  para  $i = 1, 2, \dots, n$ .

Sabemos que la familia de todas las partes de  $\mathbf{C}(n)$ , esto es  $\mathcal{P}(\mathbf{C}(n))$  es un álgebra de Boole, que tiene  $2^n$  átomos y por lo tanto ella es isomorfa al álgebra de Boole  $FB(n)$ . Además si para cada  $i = 1, 2, \dots, n$ , consideramos el conjunto

$$G_i = \{\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbf{C}(n) : x_i = 1\}$$

entonces  $G_i \in \mathcal{P}(\mathbf{C}(n))$ ,  $1 \leq i \leq n$  son los generadores libres de  $\mathcal{P}(\mathbf{C}(n)) \cong FB(n)$ .

Observemos que los átomos del álgebra de Boole  $\mathbf{C}(n)$  son los elementos  $\mathbf{a}_i = (x_1, x_2, \dots, x_n)$  donde  $x_i = 1$  y  $x_j = 0$  para  $j \neq i$ ,  $1 \leq i \leq n$ . Luego  $\mathcal{A}(\mathbf{C}(n)) = \{\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n\}$ , y por lo tanto:

$$(1) \mathbf{a}_i \in G_i \text{ y } (2) \mathbf{a}_i \notin G_j, \text{ para } j \neq i, 1 \leq j \leq n.$$

Sea  $\mathbf{K}$  un subconjunto de  $\mathbf{C}(n)$  con  $k$  elementos tal que (3)  $\mathcal{A}(\mathbf{C}(n)) \subseteq \mathbf{K}$ . Observemos que un tal conjunto puede elegirse de  $\binom{2^n - n}{k - n}$  formas diferentes.

Consideremos los siguientes subconjuntos de  $\mathbf{C}(n)$ :  $\mathbf{K}_i = \mathbf{K} \cap G_i$ ,  $1 \leq i \leq n$ . Por (1) y (3)  $\mathbf{a}_i \in \mathbf{K}_i$ , y por (2)  $\mathbf{a}_i \notin \mathbf{K}_j$  para  $j \neq i$ ,  $1 \leq j \leq n$ , en consecuencia estos conjuntos son diferentes dos a dos y por lo tanto tenemos así  $n$  conjuntos.

Sabemos que  $\mathcal{P}(\mathbf{K})$  es un álgebra de Boole isomorfa a  $B_k$ . Vamos a demostrar que  $\mathcal{G}' = \{\mathbf{K}_1, \mathbf{K}_2, \dots, \mathbf{K}_n\}$  es un conjunto de generadores de  $\mathcal{P}(\mathbf{K})$ .

En efecto si  $\mathbf{k} \in \mathbf{K} \subseteq \mathbf{C}(n)$  entonces  $\{k\} \in \mathcal{P}(\mathbf{C}(n))$  y por lo tanto:

$$\{k\} = G_1^* \cap G_2^* \cap \dots \cap G_n^*$$

donde  $G_i^* = G_i$  ó  $G_i^* = \mathcal{C} G_i$ , luego

$$\{k\} = \{k\} \cap \mathbf{K} = (G_1^* \cap \mathbf{K}) \cap (G_2^* \cap \mathbf{K}) \cap \dots \cap (G_n^* \cap \mathbf{K}).$$

Poniendo  $\mathbf{K}_i^* = G_i^* \cap \mathbf{K}$ , tenemos:

$$\{\mathbf{k}\} = \mathbf{K}_1^* \cap \mathbf{K}_2^* \cap \dots \cap \mathbf{K}_n^*,$$

Si  $G_i^* = G_i$  entonces  $G_i^* \cap \mathbf{K} = G_i \cap \mathbf{K} = \mathbf{K}_i$  y si  $G_i^* = \mathcal{C} G_i$  entonces  $G_i^* \cap \mathbf{K} = \mathcal{C} G_i \cap \mathbf{K} = \mathbf{K} - G_i = \mathbf{K} - (\mathbf{K} \cap G_i) = \mathbf{K} - \mathbf{K}_i$ . Por lo tanto  $G_i^* \cap \mathbf{K}$  es el complemento de  $\mathbf{K}_i$  en  $\mathbf{K}$ . lo que significa que todo átomo de  $\mathcal{P}(\mathbf{K})$  es intersección de los elementos  $\mathbf{K}_i^*$  y en consecuencia el conjunto  $\mathcal{G}' = \{\mathbf{K}_1, \mathbf{K}_2, \dots, \mathbf{K}_n\}$  genera  $\mathcal{P}(\mathbf{K})$ .  $\square$

**Ejemplo 2.1** *Vamos a construir un conjunto minimal de generadores del álgebra de Boole  $B_5$ . Es claro que 3 es el menor número  $n$  tal que  $5 \leq 2^n$ . Los átomos de  $\mathbf{C}(3)$  son  $\mathbf{a}_1 = (1, 0, 0)$ ,  $\mathbf{a}_2 = (0, 1, 0)$ ,  $\mathbf{a}_3 = (0, 0, 1)$ . Elijamos dos elementos arbitrarios de  $\mathbf{C}(3)$ , por ejemplo  $\mathbf{a}_4 = (0, 0, 0)$  y  $\mathbf{a}_5 = (1, 1, 1)$ . Entonces  $\mathbf{K} = \{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_4, \mathbf{a}_5\} \subseteq \mathbf{C}(3)$ , y  $\mathbf{K}_1 = \mathbf{K} \cap G_1 = \{\mathbf{a}_1, \mathbf{a}_5\}$ ,  $\mathbf{K}_2 = \mathbf{K} \cap G_2 = \{\mathbf{a}_2, \mathbf{a}_5\}$ ,  $\mathbf{K}_3 = \mathbf{K} \cap G_3 = \{\mathbf{a}_3, \mathbf{a}_5\}$  es un conjunto minimal de generadores de  $\mathcal{P}(\mathbf{K})$  y como  $\mathcal{P}(\mathbf{K}) \cong B_5$ , obtenemos un conjunto minimal de generadores de  $B_5$ .*

## Referencias

- [1] G. Birkhoff, *Lattice Theory*. Amer. Math. Soc. Colloq. Pub. 25, 3<sup>rd</sup> ed., Providence (1967).
- [2] C. Cardot, *Application de la théorie des treillis distributifs à l'étude de la distribution des programmes par télécommande*, Revue générale de l'électricité, 66 (1957), 27-39.
- [3] M. Denis-Papin, A. Kaufmann et R. Faure, *Cours de calcul Booléien appliqué*, Éditions Albin Michel, Paris (1963), Chapitre 10.
- [4] A. Monteiro, *Notas de Cursos sobre Reticulados Distributivos y Algebras de Boole*, Instituto de Matemática, Universidad Nacional del Sur, Bahía Blanca, (1957-1966).
- [5] A. Monteiro, *Générateurs des réticulés distributifs finis*. Actas del Simposium Panamericano de Matemática Aplicada (Panamerican Symposium of Applied Mathematics), Buenos Aires, (1968), 465.