ISSN 0078-2017

NOTAS DE LÓGICA MATEMÁTICA

42

Marta Sagastume y Hernán Javier San Martín

ÁLGEBRA DEL CÁLCULO PROPOSICIONAL

2019

INSTITUTO DE MATEMÁTICA (INMABB)
CONICET / UNIVERSIDAD NACIONAL DEL SUR
BAHÍA BLANCA - ARGENTINA

A la memoria de
Alberto Sagastume Berra, mi padre, y
Roberto Cignoli, mi maestro y querido amigo.

MARTA SAGASTUME[1]

[1]Roberto Cignoli falleció el 27 de junio de 2018. Al enviarle en 2016 la primera versión del libro, dedicado a la memoria de mi padre y a él, agradeció el envío considerando "inmerecida" la dedicatoria...

Índice general

Introducción

A book should have either intelligibility or correctness; to combine the two is impossible.
Bertrand Russell

Con el propósito de dar una base para el estudio de temas en el área de Álgebra de la Lógica, fue propuesto y dictado por Marta Sagastume el curso "Álgebra del Cálculo Proposicional" en la Facultad de Ciencias Exactas de la Universidad Nacional de La Plata, Argentina, durante cinco años a partir del año 2002. Estaba destinado a licenciados y a alumnos avanzados en matemática e informática, y era un curso de postgrado u optativo de grado, según el caso. El Dr. Hernán San Martín fue uno de esos sufridos alumnos. Como prerrequisito se pedían los cursos con contenidos de Álgebra, Lógica y Teoría de Conjuntos que se dictaban en ambas carreras.

Los apuntes escritos en esos años fueron el germen de este libro. Estos versaban sobre los cálculos proposicionales Clásico, Intuicionista e Infinito-valente de Łukasiewicz y sus correspondientes contrapartes algebraicas: las álgebras de Boole, las álgebras de Heyting y las MV-álgebras.

Al empezar a escribir el texto, creímos conveniente agregar temas que nos parecieron útiles para la formación en el área, como dualidades en la teoría de retículos, retículos residuados, ℓ-grupos y sus lógicas.

Pretendemos reunir, en castellano y en un nivel accesible, varios temas que usualmente se encuentran dispersos en la literatura. Tratamos de que el texto sea autocontenido y de que se desarrollen los tópicos más abstractos a partir de ejemplos concretos, permitiendo así que la intuición ayude a la comprensión cabal de los conceptos y de su interrelación. Se muestran figuras, diagramas, ejemplos motivadores. Sacrificamos a veces la elegancia de la exposición en aras de hacerla más accesible al estudiante medio. Por ejemplo, se dan elementos de Álgebra Universal en tres etapas de dificultad creciente, en los capítulos 1, 7 y 10, a medida que se van necesitando los contenidos. Asimismo, se suprimen demostraciones muy técnicas y poco conceptuales.

Como el libro apunta más al aspecto algebraico de los temas tratados, daremos en cada caso las herramientas y resultados algebraicos antes que los lógicos, obteniendo estos, en algunos casos, como consecuencia de aquellos. Esto sucede, por ejemplo, con el Teorema de Glivenko.

El núcleo inicial del texto contiene resultados "repetidos" —como las distintas versiones del Teorema de la Deducción— que hacen sospechar al lector la existencia de un marco general del cual podrían derivarse esos resultados como casos particulares. Esa intuición se ve confirmada en el Capítulo 10 con la introducción de la teoría de algebrización de la lógica de Blok y Pigozzi, la llamada "Lógica Algebraica Abstracta". Este tema ha sido desarrollado por el Prof. Renato Lewin, de la Universidad Católica de Chile, especialista en el tema, gran colega y amigo, a quien mucho agradecemos su colaboración.

Hemos incluido una breve exposición de algunos temas a modo de "punta del iceberg", con la intención de que el lector los conozca y (esperamos) desee profundizarlos. Por ejemplo, el tema de los conectivos en el Capítulo 5, de la teoría de categorías y las dualidades en el Capítulo 6, de los retículos residuados en el Capítulo 12, etc.

Al final de cada capítulo se da una bibliografía para quien quiera ampliar sus contenidos. Las referencias del texto corresponden a la bibliografía general que aparece al final del libro. Los ejercicios presentados son, en su mayoría, extraídos de textos de la bibliografía.

En el Capítulo 1 introduciremos las herramientas indispensables para desarrollar los contenidos de los capítulos hasta el 5 inclusive.

En el Capítulo 2 desarrollaremos la teoría básica de los retículos y las álgebras de Boole. En el Capítulo 3 veremos el Cálculo Proposicional Clásico y su correspondiente relación lógica-álgebra con las álgebras de Boole vía la construcción del álgebra de Lindenbaum. Generalizaremos estos resultados en dos sentidos: las álgebras de Heyting y el Cálculo Intuicionista por una parte, en los capítulos 4 y 5, y las MV-álgebras y el Cálculo Infinitovalente de Łukasiewicz por otra, en los capítulos 8 y 9. En el primer sentido, la generalización consiste en admitir un pseudocomplemento que cumple una sola de las propiedades del complemento: $x \wedge \overline{x} = 0$. Esto lleva a que en la lógica intuicionista por una parte siga valiendo el principio clásico de no contradicción y por otra a la no validez del principio del tercero excluido. En el segundo sentido, el de la lógica de Łukasiewicz y sus MV-álgebras asociadas, el supremo se transforma en una suma, el ínfimo en un producto y se acepta cierto grado de contradicción, admitiendo infinitos valores de verdad.

El objetivo del Capítulo 6 es mostrar una conexión —que es una equivalencia categorial— entre los retículos distributivos acotados y ciertos espacios topológicos ordenados. Se dan también casos particulares de esta conexión restringiendo los retículos a las álgebras de Heyting y de Boole. Se expresa así una relación álgebra-topología que completa la relación álgebra-lógica vista en capítulos anteriores. Se usa una notación que no es en todos los casos la que se usaba hasta aquí, pero que es más adecuada para describir los resultados de este capítulo.

Otros resultados y definiciones de Álgebra Universal son incorporados en el Capítulo 7. Estos son básicos para desarrollar el Capítulo 8 de MV-álgebras y el Capítulo 9 sobre el Cálculo Infinitovalente de Łukasiewicz.

En el Capítulo 10, como dijimos, se expone lo esencial de la Lógica Algebraica Abstracta. Hemos conservado la nomenclatura original del texto del Prof. Lewin, aunque la notación tiene algunas diferencias con la usada en el resto del libro.

Los ℓ-grupos, las BCK-álgebras cónicas y sus lógicas asociadas se tratan en el Capítulo 11, a modo de aplicación de lo visto en el Capítulo 10.

Por último, una nueva generalización de lo visto en los primeros capítulos se da en el Capítulo 12, en el que se muestran resultados referentes al vasto campo de los retículos residuados y las lógicas subestructurales. Se tratan también brevemente las BL-álgebras y la Lógica Básica de Hájek y se menciona su relación con las MV-álgebras, dada por un resultado análogo al Teorema de Glivenko visto en los capítulos 4 y 5.

Cada teorema, lema, definición, etc. lleva tres números separados por puntos: el primero indica el capítulo, el segundo la sección y el tercero el número de orden dentro de la sección. Por ejemplo, Teorema 3.4.6 indica que el teorema lleva el número 6 y está en la Sección 4 del Capítulo 3.

Agradecemos especialmente la colaboración del Prof. Lewin, quien no solo proporcionó el texto para el Capítulo 10 sino que aportó importantes observaciones de forma y de fondo que fueron tenidas en cuenta en la redacción del libro. También agradecemos al Prof. Rodolfo Ertola por algunas observaciones sobre lógica.

Capítulo 1

Nociones preliminares

En este capítulo veremos en primer lugar una síntesis de definiciones y resultados de teoría de conjuntos. Luego trataremos los conjuntos ordenados y sus propiedades. En la Sección 3 expondremos ciertos contenidos de Álgebra Universal, que serán reforzados en los capítulos 7 y 10. Por último, expondremos algunas nociones de Lógica en las que se basarán principalmente los capítulos 3, 5 y 9. En este punto haremos de cuenta que es la primera vez que el alumno oye hablar formalmente de Lógica, en particular del Cálculo Proposicional.

1.1. Definiciones básicas

El contenido de esta sección será, posiblemente, conocido para muchos lectores. Sin embargo, hemos querido incluirla para fijar ideas sobre definiciones y notación. Daremos por conocida la teoría de conjuntos elemental.

Una *relación de equivalencia* R en un conjunto A es una relación binaria que cumple las siguientes condiciones:

- Para todo $a \in A$, aRa (reflexividad).

- Si aRa' entonces $a'Ra$ (simetría).

- Si aRa' y $a'Ra''$ entonces aRa'' (transitividad).

Dada una relación de equivalencia R, el conjunto $|a|_R = \{x \in A : \ aRx\}$ es la *clase de equivalencia* de a. Suele suprimirse el subíndice R.

Denotaremos A/R al *conjunto cociente*, que es el conjunto de las clases de equivalencia de A por R. La *aplicación canónica* $p_R : A \longrightarrow A/R$, que es suryectiva, se define por $p_R(a) = |a|_R$.

Sea $h : A \longrightarrow B$ una aplicación. La *relación R_h asociada a h* definida por xR_hy si $h(x) = h(y)$ es una relación de equivalencia.

La aplicación $\widetilde{h} : A/R_h \longrightarrow B$ definida por: $\widetilde{h}(|x|) = h(x)$ se llama el *pasaje al cociente* o *aplicación cociente* de h.

Indicaremos con $\circ$ la composición de funciones. Observemos que la expresión $\widetilde{h}(|x|)$ es en realidad el resultado de aplicar a x la composición de las funciones p_{R_h} y $\widetilde{h}$, y esto es igual a $h(x)$. Es decir, la composición $\widetilde{h} \circ p_{R_h}$ es igual a h. Lo anterior se expresa por medio del siguiente diagrama (donde hemos llamado p a p_{R_h}) diciendo que "el diagrama conmuta":

$$\begin{tikzcd} A \arrow[r, "h"'] \arrow[d, "p"] & B \\ A/R_h \arrow[ur, "\widetilde{h}"'] & \end{tikzcd}$$

Esto significa que las dos formas de llegar de A hasta B coinciden.

Dado un conjunto I (los *índices*), una *familia* de conjuntos indicada por I y denotada por $(A_i)_{i\in I}$ es una función que a cada índice $i \in I$ hace corresponder el conjunto A_i. Si I es finito, la familia se denotará $(A_i)_{i=1}^n$.

Supongamos que existe un conjunto X tal que para cada $i \in I$, $A_i \subseteq X$. La unión de la familia de conjuntos $(A_i)_{i\in I}$, se define por:

$$\bigcup_{i\in I} A_i = \{a \in X : \text{existe } i \in I \text{ }, a \in A_i\}.$$

Análogamente, la intersección de la familia queda definida por:

$$\bigcap_{i\in I} A_i = \{a \in X : \text{para todo } i \in I \text{ }, a \in A_i\}.$$

El *producto directo* (o simplemente *producto*) $\prod_{i=1}^n A_i$ de una familia finita $(A_i)_{i=1}^n$ es el conjunto de las n-uplas de elementos $(a_1, a_2, \ldots, a_n)$, donde $a_i \in A_i$. En general, el *producto* $\prod_{i\in I} A_i$ de una familia $(A_i)_{i\in I}$ es el conjunto de las funciones $f : I \longrightarrow \bigcup_{i\in I} A_i$ tales que $f(i) \in A_i$.

También podemos considerar a las funciones como familias de elementos $(a_i)_{i\in I}$, siendo $a_i = f(i)$.

Las *funciones proyecciones* o simplemente *proyecciones* p_k son funciones $p_k : \prod_{i\in I} A_i \longrightarrow A_k$ definidas por $p_k(f) = f(k)$. Cuando I es finito, $p_k((a_1, a_2, \ldots, a_n)) = a_k$.

Cuando existe un conjunto A tal que $A_i = A$ para todo i se denota por A^I al producto $\prod_{i\in I} A_i$. Para I finito, $\prod_{i=1}^n A_i$ se denota A^n; se tiene entonces que $A^1 = A$, $A^2 = A \times A, \ldots$ y se conviene en definir $A^0 = \{\emptyset\}$.

Observemos que A^I es el conjunto de funciones de I en A. Se usará en general la notación X^Y para indicar el conjunto de funciones de un conjunto Y en otro X.

Observación 1.1.1. Supongamos que $A = \{0, 1\}$, $I = \{i_1, \ldots, i_n\}$. ¿Cuántos elementos tiene A^I? Como para cada i_j tenemos dos posibilidades, habrá $2 \times 2 \times \cdots \times 2 = 2^n$ funciones.

Además, cada función f se identifica con un subconjunto J de I: es el conjunto de índices i_j para los cuales $f(i_j) = 1$. Se dice que dicha f es la *función característica* de J. Tenemos así una correspondencia biyectiva entre las $f : I \longrightarrow \{0, 1\}$ y los subconjuntos de I. Trataremos esta biyección en el Ejercicio 14 del Capítulo 2 y con más detalle en el Lema 4.5.6 del Capítulo 4.

En particular, tenemos entonces que hay 2^n subconjuntos de un conjunto de n elementos.

1.2. Conjuntos ordenados

En esta sección nos referiremos a aquellos conjuntos en los que está definida una relación que establece, de alguna manera, un orden entre sus elementos.

Definición 1.2.1. Un *conjunto ordenado* es un par $(P, \leq)$, donde $\leq$ es una relación binaria en el conjunto P, llamada *relación de orden* (o simplemente *orden*), que cumple las siguientes condiciones:

- Para todo $x \in P$, $x \leq x$ (reflexividad).

- Si $x \leq y$ e $y \leq x$ entonces $x = y$ (antisimetría).

- Si $x \leq y$ e $y \leq z$ entonces $x \leq z$ (transitividad).

Si $\leq$ cumple además la siguiente condición:

- Para todo $x, y \in P$: $x \leq y$ o bien $y \leq x$,

entonces se dice que el orden es *total* o que $(P, \leq)$ es un *conjunto totalmente ordenado* o que es una *cadena*.

Dado un conjunto ordenado $(P, \leq)$ podemos considerar en él la relación $\leq^o$ definida por:

$$x \leq^o y \text{ si y solo si } y \leq x.$$

Se prueba que $\leq^o$ es un orden, llamado *orden opuesto* u *orden dual* del dado.

Dado un conjunto ordenado $(P, \leq)$ puede definirse en el producto $P \times P$ el siguiente orden, llamado *orden producto*:

$$(x, y) \preceq (u, v) \text{ si y solo si } x \leq u,\ y \leq v.$$

También podemos definir en el producto el siguiente orden, llamado *orden lexicográfico*:

$$(x, y) \preceq (u, v) \text{ si y solo si } \begin{cases} x = u,\ y \leq v, \text{ o bien} \\ x \neq u,\ x \leq u \end{cases}$$

Ejemplos 1.2.2.

1. El orden usual entre los números reales (respectivamente racionales, naturales, etc.) es una relación de orden. En ese caso, el orden es total.

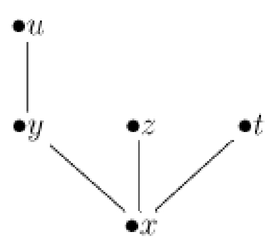
2. En los números naturales se tiene también el orden usual. Pero podemos considerar otra relación de orden que es la dada por la divisibilidad: un número m precede a otro n si m es divisor de n, lo indicaremos: $m \preceq n$. Tenemos entonces dos conjuntos ordenados: $(\mathbb{N}, \leq)$ y $(\mathbb{N}, \preceq)$. Este segundo orden no es total. Por ejemplo, 24 no divide a 14 ni viceversa.

3. Otro ejemplo importante de orden es la relación de inclusión $\subseteq$ entre conjuntos. Dado un conjunto cualquiera X, llamemos $\mathcal{P}(X)$ a la clase de los subconjuntos de X. Entonces, $(\mathcal{P}(X), \subseteq)$ es un conjunto ordenado.

Los *diagramas de Hasse* son un instrumento útil para representar gráficamente los conjuntos ordenados finitos y hasta para visualizar algunos infinitos. No daremos formalmente la definición sino que describiremos la construcción.

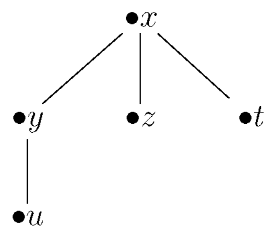
Sea $(P, \leq)$ el conjunto en cuestión. Se dibuja un gráfico donde los puntos representan los elementos de P. Decimos que x *precede inmediatamente* a y si $x \leq y$ y no hay otros elementos entre x e y. En ese caso x está debajo de y y se traza un segmento de x hacia y.

Analicemos el siguiente ejemplo.



El conjunto $P = \{x, y, z, t, u\}$ está ordenado por la relación dada por los pares que aparecen en el gráfico: (x, y), (x, z), (x, t) y (y, u) a los que se agregan todos los pares de la forma (r, r) y los pares que se obtienen por transitividad (en este caso solamente el par (x, u)).

Veamos el correspondiente diagrama de Hasse del orden dual del ejemplo dado.



Definición 1.2.3. Sean $(P, \leq)$, $(Q, \leq)$ conjuntos ordenados y $f : P \to Q$ una función. Diremos que f *preserva el orden* o que es un *morfismo de orden* si para cada $x, y \in P$, si $x \leq y$ entonces $f(x) \leq f(y)$.

Definición 1.2.4. Dos conjuntos ordenados $(P_1, \leq_1)$ y $(P_2, \leq_2)$ se dicen *isomorfos* si existe entre ellos una función biyectiva $f : P_1 \longrightarrow P_2$ tal que $x \leq_1 y$ en P_1 si y solo si $f(x) \leq_2 f(y)$ en P_2. Dicha función se llama *isomorfismo de orden*. En este caso es fácil ver que P_1 y P_2 tienen el mismo diagrama de Hasse.

Definición 1.2.5. Sean P y Q dos conjuntos tales que $Q \subseteq P$. Diremos que un elemento x de P es *cota superior* de Q si para todo y perteneciente a Q se cumple: $y \leq x$. Si una cota superior de Q pertenece a Q, entonces se prueba que es la única y se llama *máximo* de Q. En particular, el máximo de P, si existe, se llama *último elemento* y se denota con 1. En forma dual se definen los conceptos de *cota inferior* de Q, *mínimo* de Q y *primer elemento* de P, denotado 0.

Si en un conjunto ordenado $(P, \leq)$ todo subconjunto no vacío Q tiene primer elemento entonces se dice que P está *bien ordenado* o que $\leq$ es un *buen orden*.

Los números naturales con el orden usual son un conjunto bien ordenado.

Consideremos el conjunto ordenado $(\mathbb{R}, \leq)$ (orden usual). Tomando como subconjunto un intervalo semiabierto $[a, b)$ vemos que a y todos los reales menores que a son cotas inferiores y que a es el máximo. Además, b y todos los mayores que b son cotas superiores, pero no existe mínimo. Sin embargo, hay una cota superior "distinguida", que es b, que es la menor de todas. Esto motiva la siguiente definición.

Definición 1.2.6. Dado un conjunto ordenado P y un subconjunto Q de P llamaremos *supremo* de Q a la menor cota superior (si existe), es decir, al mínimo del conjunto de las cotas superiores de Q. En forma dual se define el *ínfimo* como el máximo del conjunto de las cotas inferiores.

Interesa en particular, como veremos en la siguiente sección, el caso en el que el conjunto Q tiene dos elementos: $Q = \{x, y\}$. Si existen el supremo y el ínfimo de Q se denotan, respectivamente, $x \vee y$ y $x \wedge y$.

Observación 1.2.7. Una relación binaria R sobre un conjunto X que es reflexiva y transitiva (pero no necesariamente antisimétrica) se denomina *preorden*. Veremos que a partir de R se pueden definir dos cosas: una relación de equivalencia $\widehat{R}$ en X, y una relación de orden $\preccurlyeq$ en el conjunto cociente $X/\widehat{R}$.

Definamos a $\widehat{R}$ por: $x\widehat{R}y$ si y solo si xRy e yRx. Se puede probar que $\widehat{R}$ es una relación de equivalencia (se deja como ejercicio).

Definamos ahora en $X/\widehat{R}$ la siguiente relación binaria: $|x| \preccurlyeq |y|$ si y solo si xRy. La primer pregunta que surge naturalmente es si la relación $\preccurlyeq$ está bien definida. Es decir, si elegimos otros representantes, digamos x', y' tales que $x\widehat{R}x'$ y $y\widehat{R}y'$, ¿se cumplirá también que $x'Ry'$? A continuación probaremos que sí.

Sea xRy y sean $x' \in |x|$ e $y' \in |y|$, i.e.[1], $x'\widehat{R}x$ e $y'\widehat{R}y$. De esta manera tenemos que $x'Rx$, xRx', $y'Ry$, yRy'. Luego, por transitividad de R se obtiene que $x'Ry'$. Lo que nos falta probar es que $\preccurlyeq$ es una relación de orden. Se puede probar que esta relación "hereda" la reflexividad y la transitividad de R. Para probar la antisimetría, sean $|x| \preccurlyeq |y|$ e $|y| \preccurlyeq |x|$. Por lo tanto xRy e yRx, de donde $|x| = |y|$.

1.3. Nociones de Álgebra Universal

Daremos aquí algunos conceptos básicos de la llamada Álgebra Universal: definiremos álgebras en general, en abstracto. Este grado de abstracción permite encontrar propiedades comunes a casos conocidos como los retículos, grupos, anillos, álgebras de Boole, etc., demostrarlas con la mayor generalidad y, además, aplicar los resultados a situaciones nuevas e interesantes.

El Álgebra Universal es, según lo expresara A. N. Whitehead en 1898, el estudio de las estructuras (algebraicas) en general. La célebre algebrista Emmy Noether sintió asimismo la necesidad de crear un marco general dentro del cual se encuadraran resultados conocidos. Fue Garrett Birkhoff quien

[1]'i.e.' es la abreviatura de la expresión latina *id est*, que en español significa "es decir".

contribuyó principalmente a su fundación en 1933. Aunque originalmente Birkhoff permitía operaciones infinitarias, sus principales resultados fueron relativos a operaciones finitarias, y esas son las que se consideran en general en la definición de álgebra actualmente.

Álgebras

Una *operación n-aria* en un conjunto A es una función $f : A^n \longrightarrow A$. Si $n = 0$ la función asigna al elemento $\emptyset$ un elemento de A; podemos considerar entonces que lo que hace es elegir un elemento de A, o sea, dar una función 0-aria es equivalente a distinguir un elemento de A.

Esencialmente, un álgebra está compuesta de un conjunto y algunas operaciones de *aridad* finita (0-arias, unarias, binarias, ..., n-arias, ...). Si consideramos la operación de tomar límite (de una sucesión de números reales, por ejemplo) ella **no es** de aridad finita. Operaciones como tomar límite no entran en el dominio del álgebra sino del análisis. Observemos que un conjunto ordenado tampoco es un álgebra, ya que el orden no es una operación sino una relación.

Definición 1.3.1. Llamaremos *tipo* de álgebras a un conjunto $\mathcal{F}$ de símbolos de función, donde cada símbolo f de $\mathcal{F}$ tiene asociado un número natural n, la *aridad* de f.

Definición 1.3.2. Dado un tipo $\mathcal{F}$ de álgebras, un *álgebra de tipo* $\mathcal{F}$ es un par $\mathbf{A} = \langle A, F\rangle$, donde A es un conjunto no vacío y $F = (f_i^A)_{i\in I}$ una familia de operaciones sobre A, de manera que a cada símbolo de $\mathcal{F}$ de aridad n corresponde una operación n-aria f_i^A. El conjunto A es el *universo* del álgebra. Frecuentemente (por abuso de notación) se habla del álgebra $\mathbf{A}$ mencionando solo su universo A, cuando las operaciones sobre él están sobreentendidas. También frecuentemente se denota f_i^A por f_i cuando no hay lugar a confusión.

Diremos que un álgebra es *finita* si A es finita y *trivial* si A tiene un único elemento.

Si F es finito (como en los casos que trataremos aquí), se escribe $\mathbf{A} = \langle A, f_1, f_2, \ldots, f_k\rangle$, siendo $F = \{f_1, f_2, \ldots, f_k\}$. Normalmente se ordenan las aridades en forma decreciente: aridad de $f_1 \geq$ aridad de f_2,...

Es frecuente referirse al tipo de un álgebra indicando solo las aridades de las operaciones. Por ejemplo, un álgebra de tipo $\langle 2, 2, 1, 0\rangle$ tiene dos operaciones binarias, una unaria y una ceroaria.

Se dice que un álgebra $\mathbf{B} = \langle B, G\rangle$ es *reducto* de otra $\mathbf{A} = \langle A, F\rangle$ si es $B = A$ y $G \subseteq F$.

Observación 1.3.3 (Notación). Como hemos dicho, un álgebra se denota $\mathbf{A} = \langle A, F\rangle$. A veces nos referiremos a un álgebra solo con la letra **negrita** (por ejemplo $\mathbf{A}$) o bien como par en el que se ponen como datos el conjunto subyacente y las operaciones (por ejemplo $\langle A, F\rangle$). Además, a lo largo del libro, al trabajar con las distintas clases de álgebras, cometeremos a menudo el abuso de lenguaje de denotar un álgebra por su conjunto subyacente (por ejemplo, A).

Ejemplos 1.3.4.

1. **Monoides**

   Un *monoide* es un álgebra $\langle M, *, \top\rangle$ de tipo $\langle 2, 0\rangle$ tal que $*$ es *asociativa*:

   $$\text{para toda terna } x, y, z, \quad x * (y * z) = (x * y) * z$$

   y además $\top$ es el elemento *neutro* o *unidad*, es decir, se cumple la siguiente propiedad,

   $$\text{para todo } x, \quad x * \top = \top * x = x.$$

   Si se cumple también la *conmutatividad*:

   $$\text{para todo } x, y, \quad x * y = y * x,$$

   entonces decimos que es un *monoide conmutativo*.

   Consideremos el conjunto $\mathbb{N}$ de los números naturales. Podemos dar dos estructuras de monoide tomando a $\mathbb{N}$ como universo: $\langle \mathbb{N}, +, 0\rangle$ y $\langle \mathbb{N}, \cdot, 1\rangle$, siendo $+, \cdot, 0, 1$ las operaciones usuales. Análoga situación se presenta para los enteros $\mathbb{Z}$, los racionales $\mathbb{Q}$ y los reales $\mathbb{R}$. Todos son monoides conmutativos.

   Dado un conjunto A, sea A^A el conjunto de todas las funciones de A en A. Indicaremos con id_A a la función identidad. Entonces $\langle A^A, \circ, id_A\rangle$ es un monoide no conmutativo, donde por $\circ$ se entiende la composición de funciones.

2. **Grupos**

   Un *grupo* es un álgebra $\langle G, *, ^{-1}, \top\rangle$ de tipo $\langle 2, 1, 0\rangle$ tal que

   - El reducto $\langle G, *, \top\rangle$ es un monoide.
   - Se cumple: para todo $x \in G$, $x * x^{-1} = x^{-1} * x = \top$.

Si además tenemos que $*$ es conmutativa, entonces el grupo se llama *conmutativo* o *abeliano*.

Son grupos conmutativos $\langle \mathbb{Z}, +, -, 0\rangle$, $\langle \mathbb{Q}^*, \cdot, ^{-1}, 1\rangle$, $\langle \mathbb{R}^*, \cdot, ^{-1}, 1\rangle$, siendo $\mathbb{Q}^*$ (respectivamente $\mathbb{R}^*$) el conjunto de los racionales no nulos (respectivamente el conjunto de los reales no nulos), $-x$ la operación de tomar el opuesto de un número x y x^{-1} la operación de tomar inverso multiplicativo de un número x.

Dado un conjunto A, sea $Perm(A)$ el conjunto de todas las funciones biyectivas o *permutaciones* de A en A. Entonces $\langle Perm(A), \circ, ^{-1}, id_A\rangle$ es un grupo no conmutativo, siendo $^{-1}$ la operación de tomar la función inversa de una función dada.

Esencialmente, todo grupo es un grupo de permutaciones.

3. **Anillos**

   Un *anillo* es un álgebra $\langle A, +, *, -, 0\rangle$ de tipo $\langle 2, 2, 1, 0\rangle$ tal que

   - El reducto $\langle A, +, -, 0\rangle$ es un grupo abeliano.
   - La operación $*$ es asociativa.
   - Se cumple la siguiente propiedad distributiva:

   $$x * (y + z) = (x * y) + (x * z).$$

   Si la operación $*$ es conmutativa entonces el anillo se llama *conmutativo*. Si el anillo tiene un elemento neutro para la operación $*$, entonces el mismo se llama *con unidad*.

   El ejemplo básico de anillo es $\langle \mathbb{Z}, +, \cdot, -, 0\rangle$ con la suma y el producto usuales. Este es un ejemplo de anillo conmutativo. Si agregamos el 1, entonces $\langle \mathbb{Z}, +, \cdot, -, 0, 1\rangle$ es también un anillo con unidad.

4. En los siguientes capítulos desarrollaremos otros ejemplos de álgebras: retículos, álgebras de Boole y de Heyting, MV-álgebras, ℓ-grupos, etc.

Homomorfismos

Trataremos ahora aquellas funciones entre álgebras del mismo tipo que conservan sus operaciones, es decir, que "pasan bien" de un álgebra a otra. En particular, nos interesarán las que son biyectivas, que se llaman isomorfismos.

Notemos que "isomorfismo" significa "igual forma". Podemos pensar dos álgebras isomorfas como dos maneras de ver una misma realidad, diferenciándose solo en la naturaleza de sus elementos.

Definición 1.3.5. Sean $\mathbf{A} = \langle A, F\rangle$ y $\mathbf{B} = \langle B, G\rangle$ álgebras del mismo tipo, sea $h : A \longrightarrow B$ una función. Diremos que h es un *homomorfismo* de $\mathbf{A}$ en $\mathbf{B}$ si, para cada $f^A \in F$ de aridad n se tiene que, para toda n-upla $(a_1, a_2, \ldots, a_n)$ de elementos de A,

$$h(f^A(a_1, a_2, \ldots, a_n)) = f^B(h(a_1), h(a_2), \ldots, h(a_n)),$$

siendo f^B la operación en B correspondiente a la operación f^A en A.

Si h es inyectiva diremos que es una *inmersión* ("embedding") o *monomorfismo*. Si h es suryectiva entonces se dice que $\mathbf{B}$ es una *imagen homomorfa* de $\mathbf{A}$, y h es llamada un *epimorfismo*. Si h es biyectiva será llamada *isomorfismo*[2].

Notemos que, si $n = 0$, el elemento designado en A por la operación ceroaria debe pasar por h al correspondiente en B.

Observación 1.3.6. Si h es un isomorfismo y h^{-1} es su función inversa, h^{-1} también es un isomorfismo. Para probar esto basta ver que h^{-1} preserva las operaciones.

Sea $(b_1, \ldots, b_n)$ una n-upla de elementos de B. Tenemos que ver que

$$h^{-1}(f^B(b_1, \ldots, b_n)) = f^A(h^{-1}(b_1), \ldots, h^{-1}(b_n)).$$

Por ser h inyectiva, basta probar que la imagen por h del primer miembro es igual a la imagen por h del segundo. En efecto,

$$h(h^{-1}(f^B(b_1, \ldots, b_n))) = f^B(b_1, \ldots, b_n).$$

Además,

$$\begin{aligned} h(f^A(h^{-1}(b_1), \ldots, h^{-1}(b_n))) &= f^B(h(h^{-1}(b_1)), \ldots, h(h^{-1}(b_n))) \\ &= f^B(b_1, \ldots, b_n). \end{aligned}$$

Por lo tanto, $h^{-1}(f^B(b_1, \ldots, b_n)) = f^A(h^{-1}(b_1), \ldots, h^{-1}(b_n))$.

Ejemplo 1.3.7. Sea $\mathbb{R}^+$ el conjunto de los números reales positivos. Sean $\langle \mathbb{R}^+ - \{0\}, \cdot, 1\rangle$ y $\langle \mathbb{R}, +, 0\rangle$ los monoides obtenidos considerando las operaciones usuales en $\mathbb{R}^+ - \{0\}$ y $\mathbb{R}$ respectivamente.

Consideremos la función logaritmo natural,

$$\ln : (\mathbb{R}^+ - \{0\}) \longrightarrow \mathbb{R}.$$

[2]En el Capítulo 6 se introducen los conceptos de monomorfismo, epimorfismo e isomorfismo en el contexto de la teoría de categorías. En dicho capítulo mencionaremos las diferencias y similitudes con la Definición 1.3.5.

Las propiedades de ln nos dicen que es un homomorfismo de monoides: $\ln(1) = 0$, $\ln(a \cdot b) = \ln(a) + \ln(b)$. Más aún, ln es un isomorfismo, ya que tiene por inversa la función exponencial. Los monoides $\langle \mathbb{R}^+ - \{0\}, \cdot, 1\rangle$ y $\langle \mathbb{R}, +, 0\rangle$ son reductos, respectivamente, de los grupos $\langle \mathbb{R}^+ - \{0\}, \cdot, ^{-1}, 1\rangle$ y $\langle \mathbb{R}, +, -, 0\rangle$. Podemos probar que ln es también un isomorfismo entre ambos grupos.

Dados dos grupos $\langle G, \cdot, ^{-1}, 1\rangle$ y $\langle H, \cdot, ^{-1}, 1\rangle$, si se tiene un homomorfismo h del monoide reducto $\langle G, \cdot, 1\rangle$ en el monoide reducto $\langle H, \cdot, 1\rangle$, eso basta para que sea un homomorfismo de grupos. En efecto, $h(x^{-1}) \cdot h(x) = h(x^{-1} \cdot x) = h(1) = 1$ y $h(x) \cdot h(x^{-1}) = h(x \cdot x^{-1}) = h(1) = 1$. Luego, $h(x^{-1})$ es el inverso de $h(x)$, es decir, $h(x^{-1}) = (h(x))^{-1}$.

Subálgebras y álgebras libres

Comenzaremos con la siguiente definición.

Definición 1.3.8. Sea $\langle A, F\rangle$ un álgebra y sea $B \subseteq A$. Si para todas las aridades n, para cada n-upla $(b_1, b_2, \ldots, b_n)$ de elementos de B y para cada operación n-aria f^A de A se cumple que $f^A(b_1, b_2, \ldots, b_n) \in B$ entonces se dice que B es un *subuniverso* de A.

En otras palabras, B es subuniverso de A si es *cerrado* con respecto a las operaciones de A, en el sentido de que B contiene los resultados de todas ellas.

Ejemplo 1.3.9. Dado el anillo de los enteros $\langle \mathbb{Z}, +, \cdot, -, 0\rangle$, un subuniverso de $\mathbb{Z}$ es, por ejemplo, el conjunto de los números pares. En general puede probarse que todo subuniverso de $\mathbb{Z}$ es el conjunto de múltiplos de k, para algún k natural.

Definición 1.3.10. Sean $\langle A, F\rangle$ un álgebra de tipo $\mathcal{F}$ y B un subuniverso no vacío de A. Sea f un símbolo de operación n-aria de $\mathcal{F}$. Si llamamos f^B a la restricción de la operación n-aria f^A al conjunto B^n entonces el álgebra $\langle B, G\rangle$ se llama una *subálgebra* de $\langle A, F\rangle$, siendo G la familia de las operaciones f^B.

Sea $X \subseteq A$. Se puede probar que la intersección de subuniversos es un subuniverso. El mínimo subuniverso que contiene a X es la intersección de todos los subuniversos que contienen a X y se llama el *subuniverso generado por* X; lo denotaremos $Sg(X)$. Si A mismo es el subuniverso generado por X, o sea si $A = Sg(X)$, se dice simplemente que A es *generado por* X o que X *genera* A. En particular, si X es finito, A se dice finitamente generado.

Ejemplos 1.3.11.

1. Dado el monoide $\langle \mathbb{Q}, +, 0 \rangle$, si tomamos $X = \{\frac{1}{5}\}$ entonces $Sg(X)$ es el conjunto de todas las fracciones de la forma $\frac{m}{5}$, con $m \in \mathbb{N}$.

2. Sea el grupo $\mathbb{Z}_3 = \langle \{0, 1, 2\}, +, -, 0 \rangle$ (*grupo de enteros módulo 3*), donde las operaciones $+$ y $-$ son dadas por las siguientes tablas:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

x	-x
0	0
1	2
2	1

Si $X = \{1\}$, entonces $Sg(X) = \{0, 1, 2\}$, ya que sumando unos se obtienen 0, 1 y 2.

3. Asimismo, el grupo de los enteros $\langle \mathbb{Z}, +, -, 0 \rangle$ también es generado por $X = \{1\}$.

Definición 1.3.12. Sea $\mathcal{K}$ una clase de álgebras del mismo tipo, $\langle A, F \rangle$ un álgebra de $\mathcal{K}$, $X \subseteq A$ un conjunto de generadores de A. Diremos que A es *libremente generada por X en $\mathcal{K}$*, o que *X es un conjunto de generadores libres de A en $\mathcal{K}$* si se cumple la siguiente condición (*Propiedad universal de extensión de homomorfismos*):

Dadas un álgebra B de la clase $\mathcal{K}$ y una función $f : X \longrightarrow B$, existe un homomorfismo $g : A \longrightarrow B$ tal que $g(x) = f(x)$, para todo $x \in X$.

Según vimos en la Sección 1, esto se expresa diciendo que el siguiente diagrama conmuta, donde *inc* indica la inclusión de X en A.

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "inc"'] & B \\ A \arrow[ur, "g"'] & \end{tikzcd}$$

Observación 1.3.13. Supongamos que son X e Y dos conjuntos que se corresponden biyectivamente. Si A y B verifican la propiedad de extensión de homomorfismos con respecto a X e Y respectivamente puede probarse intercambiando los roles de A y de B que hay un isomorfismo entre ellas. Por eso podemos hablar de "el" álgebra libre con un conjunto de generadores, porque es única salvo isomorfismo.

Veamos en los ejemplos anteriores que si consideramos la clase $\mathcal{K}$ de los grupos entonces $X = \{1\}$ es libre en $\mathbb{Z}$ pero no en $\mathbb{Z}_3$.

Comenzaremos mostrando que $X = \{1\}$ no es libre en $\mathbb{Z}_3$. Tomemos la aplicación $f : \{1\} \longrightarrow \mathbb{Z}$ definida por $f(1) = 1$ y veamos que no se puede extender a $\mathbb{Z}_3$. Si $g : \mathbb{Z}_3 \longrightarrow \mathbb{Z}$ fuera un homomorfismo, debe ser $g(0) = 0$. También debe ser $g(1) = f(1) = 1$ y por lo tanto $g(2) = g(1+1) = g(1) + g(1) = 1 + 1 = 2$. Luego $g(1 + 2) = g(1) + g(2) = 1 + 2 = 3$. Pero $g(1 + 2) = g(0) = 0$. Luego, no puede existir tal g.

Ahora veremos que $X = \{1\}$ genera libremente $\mathbb{Z}$ en la clase de los grupos. En efecto, sea B un grupo, $f : \{1\} \longrightarrow B$. En B definiremos $z.b$ para z entero y $b \in B$, por:

$$z.b = \begin{cases} b + b + \cdots + b \ (z \text{ veces}) & \text{si } z \geq 0, \\ (-b) + (-b) + \cdots + (-b) \ (z \text{ veces}) & \text{si } z < 0. \end{cases}$$

Se prueba que, por ser B un grupo, $0.b = 0$, $(u + v).b = u.b + v.b$ y $(-w).b = -(w.b)$ (hacerlo como ejercicio).

Definimos $g : \mathbb{Z} \longrightarrow B$ por: $g(z) = z.f(1)$, y veamos que g cumple la propiedad universal de extensión de homomorfismos.

En primer lugar, $g(1) = 1.f(1) = f(1)$.

Veamos ahora que g es un homomorfismo de grupos. Debe cumplirse que $g(0) = 0$, $g(u + v) = g(u) + g(v)$ y $g(-w) = -g(w)$, para $u, v, w \in \mathbb{Z}$.

Se tiene $g(0) = 0.f(1) = 0$; además,

$$\begin{aligned} g(u + v) &= (u + v).f(1) \\ &= u.f(1) + v.f(1) \\ &= g(u) + g(v) \end{aligned}$$

y también

$$\begin{aligned} g(-w) &= (-w).f(1) \\ &= -(w.f(1)) \\ &= -g(w). \end{aligned}$$

Por lo tanto, $\mathbb{Z}$ es libremente generado por $X = \{1\}$ en la clase de los grupos.

Productos

Definimos al principio el producto $\prod_{i \in I} A_i$ de una familia de conjuntos $(A_i)_{i \in I}$. Supongamos que tenemos ahora una familia de álgebras de tipo $\mathcal{G}$ (el mismo para todas las álgebras de la familia) $(\langle A_i, G_i \rangle)_{i \in I}$. Vamos a definir una estructura de álgebra en el conjunto $\prod_{i \in I} A_i$.

Las operaciones en el producto se hacen “componente a componente”. Por ejemplo, si $I = \{1, 2, 3\}$ y $g \in \mathcal{G}$ es un símbolo de función binaria, en el producto $A = A_1 \times A_2 \times A_3$ definimos la operación binaria g^A correspondiente del siguiente modo.

Para cada par (a, b) de A, donde $a = (a_1, a_2, a_3)$, $b = (b_1, b_2, b_3)$, es

$$\begin{aligned} (g^A(a,b))_1 &= g^{A_1}(a_1, b_1), \\ (g^A(a,b))_2 &= g^{A_2}(a_2, b_2) \quad \text{y} \\ (g^A(a,b))_3 &= g^{A_3}(a_3, b_3), \end{aligned}$$

es decir:

$$g^A(a,b) = (g^{A_1}(a_1, b_1), g^{A_2}(a_2, b_2), g^{A_3}(a_3, b_3)).$$

Definición 1.3.14. Dada la familia de álgebras $(\mathbf{A_i})_{i\in I}$ de tipo $\mathcal{G}$, siendo $\mathbf{A_i} = \langle A_i, G_i \rangle$, el *álgebra producto* $\mathbf{A} = \langle \prod_{i\in I} A_i, G \rangle$ es el álgebra cuyo universo es $\prod_{i\in I} A_i$ y tal que cada operación n-aria $g^A \in G$ se define, en cada n-upla $(a^1, a^2, \ldots, a^n)$ de elementos de $\mathbf{A}$ (siendo $a^j = (a_i^j)_{i\in I}$ para $j = 1, \ldots, n$) por:

$$(g^A(a^1, a^2, \ldots, a^n))_i = g^{A_i}(a_i^1, a_i^2, \ldots, a_i^n).$$

Por ejemplo, sean $\langle \mathbb{R}, \cdot, 1 \rangle$ y $\langle \mathbb{Z}, +, 0 \rangle$ con las operaciones usuales, que determinan estructuras de monoide en los números reales y en los números enteros, respectivamente. Entonces, en el álgebra producto $\langle \mathbb{R} \times \mathbb{Z}, f, u \rangle$ las operaciones están definidas por: $f((a, b), (r, s)) = (a \cdot r, b + s)$, $u = (1, 0)$.

Definición 1.3.15. Acabamos de definir tres “operaciones” entre álgebras, que consisten en: tomar subálgebras, imágenes homomorfas y productos. Una clase de álgebras que es cerrada bajo esas tres operaciones se llama *variedad*. Dicho de otra manera: una variedad es una clase $\mathcal{K}$ de álgebras del mismo tipo tal que si $A \in \mathcal{K}$ entonces toda subálgebra de A está en $\mathcal{K}$, toda imagen de A por un homomorfismo está en $\mathcal{K}$ y para toda familia de álgebras de $\mathcal{K}$ su producto está en $\mathcal{K}$.

Ejemplos de variedades son la clase de los monoides, la clase de los grupos, la clase de los anillos y la mayoría de las clases de álgebras de las que hablaremos en este libro.

Una propiedad importante de las variedades es la siguiente: si $\mathcal{K}$ es una variedad, entonces para todo conjunto X existe un álgebra de $\mathcal{K}$ que es libremente generada por X.

Posteriormente trataremos más a fondo las variedades.

Congruencias y álgebras cociente

Dada un álgebra $\langle A, F\rangle$ nos interesa conocer cuáles son aquellas relaciones de equivalencia R definidas en A tales que la aplicación canónica

$$p_R : A \longrightarrow A/R$$

es un homomorfismo. En particular, A/R deberá tener una estructura de álgebra del mismo tipo. Veamos cómo se define entonces el *álgebra cociente*, lo que es posible solo en el caso en que la relación R cumple cierta condición de compatibilidad con las operaciones.

Por ejemplo, consideremos $\langle \mathbb{Z}, +, -, 0\rangle$, el grupo aditivo de los enteros con las operaciones habituales. Consideremos además la siguiente relación, llamada *de congruencia módulo* p, para un número natural p:

$$x \equiv_p y \text{ si y solo si la diferencia } x - y \text{ es múltiplo de } p.$$

Es sencillo ver que dos números enteros positivos son equivalentes si al dividir cada uno de ellos por p obtenemos el mismo resto. Sus clases de equivalencia están entonces en correspondencia con los restos: $\{0, 1, 2, \ldots, p-1\}$, donde también los números negativos se ubican adecuadamente.

Ya hemos visto el grupo $\mathbb{Z}_3$, que es justamente el cociente de $\mathbb{Z}$ por la congruencia módulo 3 (¡probarlo!).

El cociente $\mathbb{Z}/\equiv_p$ puede ser dotado de una estructura de grupo. Para sumar dos clases $|z|$ y $|t|$ se toma un representante de cada una: $z \in |z|$, $t \in |t|$, se suman y se calcula la clase de esa suma: $|z + t|$. La relación $\equiv_p$ permite hacer eso. En efecto, si tomáramos $z' \in |z|$, $t' \in |t|$ y sumáramos, $z' + t'$ estaría en la misma clase que $z + t$, pues puede probarse que $z \equiv_p z'$ y $t \equiv_p t'$ implican $(z + t) \equiv_p (z' + t')$. Algo análogo sucede con la operación de opuesto.

Definición 1.3.16. Sea R una relación de equivalencia definida en el universo A de un álgebra $\langle A, F\rangle$. Diremos que R es una *congruencia* si para cada operación n-aria $f^A \in F$ y para cada par de n-uplas $(x_1, \ldots, x_n)$, $(y_1, \ldots, y_n)$ de elementos de A tales que $x_i R y_i$, $i = 1, \ldots, n$ se verifica que

$$f^A(x_1, \ldots, x_n) R f^A(y_1, \ldots, y_n).$$

Ejemplos 1.3.17.

1. Sea $\langle A, +, *, -, 0\rangle$ un anillo. Para que una relación de equivalencia R sea una congruencia debe cumplir:

   - Si sRt entonces $(-s)R(-t)$.

- Si xRy, uRv, entonces $(x+u)R(y+v)$ y también $(x*u)R(y*v)$.

Ambas condiciones se cumplen para la congruencia módulo p definida ahora en el anillo $\langle \mathbb{Z}, +, \cdot, -, 0\rangle$, pues, como puede probarse, xRy, uRv implica $(x \cdot u)R(y \cdot v)$.

2. Sea $\langle A, F\rangle$ un álgebra, $a, b \in A$. Llamaremos *congruencia principal generada por* (a, b), denotada R_{ab}, a la intersección de todas las congruencias R tales que aRb:

$$R_{ab} = \bigcap_{(a,b)\in R} R.$$

¿Es esta relación realmente una congruencia? ¿El par (a, b) está en R_{ab}?

Aplicando la definición de congruencia se ve que podemos responder afirmativamente a las dos preguntas.

Además, se puede probar que R_{ab} se caracteriza por ser la mínima congruencia que contiene al par (a, b), es decir, que cumple:

1 $aR_{ab}b$.

2 Si S es una congruencia y aSb, entonces $R_{ab} \subseteq S$.

Sea R una congruencia en un álgebra $\langle A, F\rangle$ de tipo $\mathcal{F}$. Para cada $f \in \mathcal{F}$ (n-aria) definimos

$$f^{A/R}(|x_1|, \ldots, |x_n|) = |f^A(x_1, \ldots, x_n)|. \tag{1.1}$$

Veamos que tenemos una "buena" definición, en el sentido de que si elegimos otro elemento x'_i de la clase $|x_i|$, para cada $i = 1, \ldots, n$, el resultado de $|f^A(x'_1, \ldots, x'_n)|$ es el mismo que antes. Es decir, debemos probar que si $|x'_i| = |x_i|$ entonces $|f^A(x_1, \ldots, x_n)| = |f^A(x'_1, \ldots, x'_n)|$.

En efecto, por ser R congruencia tenemos que

$$x_1Rx'_1, \ldots, x_nRx'_n \text{ implica } (f^A(x_1, \ldots, x_n))R(f^A(x'_1, \ldots, x'_n)),$$

es decir, $|f^A(x_1, \ldots, x_n)| = |f^A(x'_1, \ldots, x'_n)|$.

Definición 1.3.18. Sea $\langle A, F\rangle$ un álgebra, R una congruencia. El *álgebra cociente* $\langle A/R, |F|\rangle$ es aquella cuyo universo es el conjunto cociente A/R y tal que $|F|$ es la familia de las operaciones $f^{A/R}$, con $f \in \mathcal{F}$, definidas anteriormente.

Teorema 1.3.19. *La aplicación canónica $p_R : A \longrightarrow A/R$ es un homomorfismo suryectivo de $\langle A, F\rangle$ sobre $\langle A/R, |F|\rangle$.*

Demostración. La aplicación p_R, que es suryectiva, está definida por:

$$p_R(x) = |x|.$$

Sea f^A una operación n-aria de A y $f^{A/R}$ la correspondiente operación en A/R. Para que p_R sea un homomorfismo debe cumplirse, para cada n-upla $(x_1, \ldots, x_n)$ de elementos de A, la siguiente condición:

$$p_R(f^A(x_1, \ldots, x_n)) = f^{A/R}(p_R(x_1), \ldots, p_R(x_n)).$$

El primer miembro es igual a $|f(x_1, \ldots, x_n)|$ y el segundo es $f^{A/R}(|x_1|, \ldots, |x_n|)$, que son iguales por definición de $f^{A/R}$ (ver (1.1) antes de la Definición 1.3.18).

$\square$

Sea $h : A \longrightarrow B$ un homomorfismo entre las álgebras $\langle A, F\rangle$ y $\langle B, G\rangle$. Hemos definido en A la relación de equivalencia R_h (ver 1.1 en la Sección 1) por xR_hy si $h(x) = h(y)$. Veamos que es una congruencia.

Sean $(x_1, \ldots, x_n)$ y $(y_1, \ldots, y_n)$ n-uplas de A, f^A una operación n-aria de A y f^B la correspondiente operación en B. Supongamos que para cada $i = 1, \ldots, n$ se verifica que $x_iR_hy_i$ (es decir que $h(x_i) = h(y_i)$). Veamos que $f^A((x_1, \ldots, x_n))R_hf^A((y_1, \ldots, y_n))$.

En efecto, por ser h homomorfismo tenemos que

$$\begin{aligned} h(f^A((x_1, \ldots, x_n))) &= f^B(h(x_1), \ldots, h(x_n)) \\ &= f^B(h(y_1), \ldots, h(y_n)) \\ &= h(f^A((y_1, \ldots, y_n))). \end{aligned}$$

Teorema 1.3.20. *Sea $h : A \longrightarrow B$ un homomorfismo suryectivo. Sea $\langle A/R_h, |F|\rangle$ el álgebra cociente, $\widetilde{h}$ el pasaje al cociente de h, p la aplicación canónica al cociente. Entonces, $\widetilde{h}$ es un isomorfismo de A/R_h en B y se verifica: $h = \widetilde{h} \circ p$. Es decir, el siguiente diagrama conmuta:*

$$\begin{tikzcd} A \arrow[r, "h"'] \arrow[d, "p"] & B \\ A/R_h \arrow[ur, "\widetilde{h}"'] & \end{tikzcd}$$

Demostración. Por la definición de $\widetilde{h}$, para todo $x \in A$, $h(x) = \widetilde{h}(|x|) = \widetilde{h}(p(x))$. Veamos que $\widetilde{h}$ es inyectiva. Sea $\widetilde{h}(|x|) = \widetilde{h}(|y|)$, es decir, $h(x) = h(y)$. Luego obtenemos que xR_hy, de donde $|x| = |y|$.

Por ser h suryectiva resulta $\widetilde{h}$ suryectiva.

Solo resta probar que $\widetilde{h}$ es un homomorfismo, o sea, que

$$\widetilde{h}(|f|^A((|x_1|,\ldots,|x_n|))) = g^B(\widetilde{h}(|x_1|),\ldots,\widetilde{h}(|x_n|)).$$

Aplicando las definiciones se tiene

$$\begin{aligned}\widetilde{h}(|f|^A((|x_1|,\ldots,|x_n|))) &= \widetilde{h}(|f^A((x_1,\ldots,x_n))|)\\ &= h(f^A((x_1,\ldots,x_n)))\\ &= g^B(h(x_1),\ldots,h(x_n))\\ &= g^B(\widetilde{h}(|x_1|),\ldots,\widetilde{h}(|x_n|)).\end{aligned}$$ □

1.4. Lógica

Comenzaremos tratando de responder la siguiente pregunta, desde un punto de vista informal e intuitivo:

¿Qué es la lógica?

La lógica trata de dilucidar cuáles de los razonamientos que hacemos son válidos, ya sea en la vida diaria o en un estudio sistemático, científico. Saber qué se deduce de qué, o qué es consecuencia de qué, válidamente. Queremos progresar en nuestro pensamiento por carriles seguros. Para eso el comienzo es analizar aquellas afirmaciones que usualmente tomamos como indiscutibles. Por ejemplo: "si *me llamo Juan* entonces *me llamo Juan*". Podemos poner (las dos veces) en lugar de *me llamo Juan* otra aserción cualquiera, digamos *el 3 es un número primo*; en este caso obtendríamos: "si *el 3 es un número primo* entonces *el 3 es un número primo*". Vemos que lo verdadero de la frase "Si ...entonces ..." depende de su estructura, que es de la forma "Si x entonces x", y no de cuál sea la aserción por la que reemplacemos los puntos o la x. Esas estructuras seguras, indiscutibles, son las que estudia la lógica. Podemos observar, curiosamente, que las verdades lógicas son las que, a diferencia de los resultados de una investigación científica, no aportan nada nuevo. Son "verdades de perogrullo", pero sin explicitarlas no podemos avanzar por vías confiables en el conocimiento.

El poner claramente de manifiesto los puntos de partida y las reglas para avanzar en los razonamientos es lo que proporciona verosimilitud a las deducciones, en particular las que se usan para obtener resultados en las llamadas ciencias deductivas, especialmente en la matemática. Se deberá usar un lenguaje libre de ambigüedades y explicitar claramente cuáles son los axiomas o datos iniciales y cuáles las reglas de inferencia usadas para obtener conclusiones. Hay que "traducir" proposiciones del lenguaje natural a un lenguaje formal. En este tendremos variables proposicionales y conectivos, a partir de los cuales (y con reglas precisas) construiremos proposiciones compuestas; es el mismo proceso de abstracción de cuando operamos con variables x, y, $\ldots$ y signos operacionales $+$, $-$, $/, \ldots$, para construir expresiones algebraicas como $x/(y-x)$, $(y+x)+(y-x)$, $\ldots$.

Este punto de vista operacional o algebraico (que es el que nos interesa estudiar aquí) es el que G. Boole adoptó a fines del siglo XIX en sus trabajos, cambiando así el enfoque clásico de la lógica, más ligado a la filosofía. También casi por la misma época aporta sus ideas y su simbolización original de enunciados lógicos G. Frege, cuyas investigaciones fueron poco conocidas en su época, pero bien valoradas por Bertrand Russell en sus trabajos. Fue Frege uno de los que iniciaron la lógica formal o "álgebra de la lógica". Asimismo, J. Łukasiewicz y A. Tarski estudiaron, alrededor de 1920, al cálculo proposicional con ese mismo enfoque pero considerando un cálculo proposicional abstracto, más general. El primero en analizar sistemáticamente la lógica como una ciencia que estudia las formas válidas de razonamiento fue sin duda Aristóteles. Son Boole, Frege, Łukasiewicz, Tarski y sus seguidores los primeros en profundizar la lógica en un sentido diferente del dado por los griegos. A partir de estos trabajos comenzó a crecer la llamada *Lógica Matemática*. Estos desarrollos respondieron también a otras motivaciones que surgieron en esa época.

En efecto, a principios del siglo XX aparecieron indicios de que los cimientos de la lógica (y, por extensión, los de las ciencias deductivas) no eran tan sólidos como se creía. Esos indicios fueron, entre otros, las paradojas y el descubrimiento de propiedades no esperadas en sistemas lógico-matemáticos clásicos.

Las paradojas eran conocidas desde la antigüedad. El filósofo Epiménides de Creta afirmaba "Todos los cretenses son mentirosos". Si esta afirmación era verdadera, entonces el mismo Epiménides era un mentiroso, con lo cual su afirmación era falsa. En tiempos más modernos se hizo famosa la paradoja que descubrió Bertrand Russell, que podía derivarse de la naciente teoría de conjuntos de Georg Cantor y ponía en duda sus fundamentos. También era un tropiezo para la construcción formal de la lógica debida a Frege. Esta paradoja consiste en lo siguiente: llamemos $\mathcal{A}$ al conjunto de todos los conjuntos que no pertenecen a sí mismos. Por ejemplo, si es S el conjunto de símbolos escritos en esta página, tenemos que $S \in S$. En cambio, si es P el conjunto de palabras de dos letras, entonces $P \notin P$. Luego: $S \notin \mathcal{A}$ y $P \in \mathcal{A}$. Nos preguntamos ¿Qué ocurre con $\mathcal{A}$? Si $\mathcal{A} \in \mathcal{A}$, entonces, debido a la definición de $\mathcal{A}$, $\mathcal{A} \notin \mathcal{A}$. Pero si suponemos que $\mathcal{A} \notin \mathcal{A}$ entonces resultaría que $\mathcal{A} \in \mathcal{A}$.

Uno de los primeros "sistemas formales" fue el dado por Euclides en sus *Elementos*, donde de un pequeño grupo de axiomas deduce todas las propiedades geométricas más conocidas. Fue preocupación de algunos lógicos y matemáticos durante mucho tiempo el demostrar, a partir de los otros axiomas, el postulado V de Euclides: "por un punto exterior a una recta pasa una y solo una paralela a dicha recta". Se demostró, sin embargo, que si se reemplazaba dicho postulado por otro entonces este otro podía "convivir" con los demás postulados sin producir ninguna contradicción. Esto dio origen a las llamadas *geometrías no euclidianas*. Por ejemplo, Lobachevsky, a principios del siglo XIX, reemplaza el postulado V de Euclides por el siguiente: "por un punto exterior a una recta pasan infinitas paralelas a dicha recta". En la geometría de Riemann, en cambio, se reemplaza por el postulado: "por un punto exterior a una recta no pasa ninguna paralela a dicha recta". La interpretación de "recta" es, en este caso, la de círculo máximo sobre una esfera.

A partir de las cuestiones que hemos expuesto surgieron no solo nuevas geometrías sino nuevos sistemas lógicos, relativizando la geometría y la lógica clásicas como "una" geometría y "una" lógica, no las únicas. La diferencia esencial es que los postulados ya no se toman como "verdades básicas" sino como puntos de partida.

Para profundizar en el aspecto histórico de la Lógica, ver, por ejemplo, [68].

Vamos a definir, en su lineamiento básico y general, lo que se entiende formalmente por una lógica proposicional.

Lenguaje

En un sentido general, dado un alfabeto o conjunto de símbolos básicos W, tenemos asociado a él el conjunto W^* de todas las cadenas finitas o "palabras" que pueden formarse con los símbolos de W. El conjunto W^* puede ser dotado de una estructura algebraica. En efecto, $\langle W^*, \star, e\rangle$ es un monoide, siendo $\star$ la operación de concatenación de palabras y e la palabra vacía.

Definición 1.4.1. Un *lenguaje sobre* W es cualquier subconjunto L de W^*.

Por ejemplo, si $W = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, un lenguaje sobre W es aquel cuyas palabras son todas las cadenas finitas de elementos de W salvo las que empiezan por 0. Es decir, los números naturales en notación decimal. Otro ejemplo podría ser $W = \{a, b\}$, siendo L el conjunto de cadenas sobre W formadas de la siguiente manera: aa y bb están en L y, si una cadena

x está en L, entonces xx está en L. Con estas reglas obtenemos todas las cadenas de la forma a^{2^n} y las de la forma b^{2^n} (y solo ellas).

Para especificar un lenguaje, que en general será infinito, necesitamos dar un alfabeto y un conjunto finito de reglas de formación, que se definirán usando ciertos símbolos auxiliares llamados *variables*. Una de ellas, el *axioma*, es distinguida: indica el punto de partida de la generación del lenguaje. Estos datos determinarán lo que generalmente se llama *gramática* de dicho lenguaje.

Por ejemplo, para el alfabeto $W = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, los números naturales en notación decimal se generan por la gramática que tiene dos variables S y T, siendo S el axioma, y las reglas siguientes:

1) S se reemplaza por n o bien por nT, siendo $n = 1, 2, 3, \ldots, 9$,

2) T se reemplaza por n o bien por nT, siendo $n = 0, 1, 2, \ldots, 9$.

Lenguaje proposicional

Consideremos ahora que puede haber otros conectivos diferentes de la concatenación que liguen los símbolos básicos para formar expresiones compuestas.

En nuestro contexto, el lenguaje estará dado por el conjunto de las *fórmulas*, que definiremos de manera recursiva. Las fórmulas representarán las proposiciones, y se formarán a partir de las *variables proposicionales* (nuestros símbolos básicos), combinando estas con *conectivos* de la manera que determinen las reglas de formación.

Como veremos, el conjunto de las fórmulas estará determinado por los conectivos, por lo que se suele llamar también *lenguaje* al conjunto de estos.

Definición 1.4.2. Se define el conjunto $\mathcal{L}$ de las *fórmulas bien formadas* dando

1. Los símbolos:

   (a) Símbolos de variables proposicionales: $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n, \ldots$ (consideramos, en general, que hay tantas variables como números naturales, es decir, que el conjunto de variables en *numerable*).

   (b) Símbolos de conectivos: $(\mathrm{c}_i)_{i \in I}$, donde a cada c_i le corresponde un n natural, que es su *aridad*: 0-arios o *constantes*, unarios, binarios, ...

   (c) Símbolos de puntuación: (,).

2. Las reglas de formación:

(i) Cada p_i es una fórmula, para $i = 1, 2, \ldots$

(ii) Si $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n$ son fórmulas y C es un conectivo n-ario, entonces $\mathrm{C}(\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n)$ es una fórmula. Si C es binario, escribiremos $\mathrm{A}_1\mathrm{C}\mathrm{A}_2$ en lugar de $\mathrm{C}(\mathrm{A}_1, \mathrm{A}_2)$.

(iii) Una cadena de símbolos es una fórmula si y solo si se obtiene de (i) y de (ii) en un número finito de pasos.

La definición anterior nos da la *sintaxis* del lenguaje del cálculo proposicional.

Observación 1.4.3. Como dijimos, el conjunto de fórmulas queda definido, en realidad, por el conjunto de los conectivos, ya que se considera siempre un conjunto numerable de variables y los mismos símbolos de puntuación. A cada lenguaje corresponde entonces un *tipo*, de la misma manera que sucede con las álgebras.

Como ejemplo, consideremos el cálculo proposicional llamado *implicativo positivo*. En este cálculo el único conectivo, que es binario, es $\to$. Por lo tanto, toda fórmula que no sea una variable es de la forma $\mathrm{A} \to \mathrm{B}$.

Más adelante trataremos con detalle el Cálculo Proposicional Clásico, en cuyo lenguaje podemos considerar los conectivos: $\neg$ (unario), $\wedge$, $\vee$, $\to$ (binarios).

A los dos ejemplos anteriores se les asocia, respectivamente, el tipo $\langle 2 \rangle$ y $\langle 1, 2, 2, 2 \rangle$.

Aquí empezamos a vislumbrar el vínculo Lógica-Álgebra.

Sistema formal

En lo que sigue definiremos de manera formal un sistema que resulte confiable en el sentido de que no dará lugar a paradojas y describirá las que entendemos como "verdades", desde la óptica de cierta lógica.

Pero antes necesitamos una definición.

Definición 1.4.4. Sea $\mathcal{L}$ el conjunto de las fórmulas de un lenguaje proposicional, $\mathcal{P}$ el conjunto de sus variables proposicionales. Una *sustitución* es una función $s : \mathcal{P} \longrightarrow \mathcal{L}$. Puede extenderse s a $\mathcal{L}$ (llamaremos también s a la extensión) definiendo: $s(\mathrm{C}(\mathrm{A}_1, \ldots, \mathrm{A}_n)) = \mathrm{C}(s(\mathrm{A}_1), \ldots, s(\mathrm{A}_n))$, para cada conectivo n-ario C, para cada n.

Denotaremos $s(\Gamma)$, para un conjunto de fórmulas Γ, al conjunto de las fórmulas $s(\mathrm{B})$, con $\mathrm{B} \in \Gamma$.

Por ejemplo, si el lenguaje tiene $\neg$, $\to$ y $\vee$, sea s tal que $s(\mathrm{p}_1) = \neg\mathrm{p}_3$, $s(\mathrm{p}_2) = \mathrm{p}_1 \vee \mathrm{p}_4$. Sea $\mathrm{A} = \mathrm{p}_2 \to \mathrm{p}_1$. Entonces: $s(\mathrm{A}) = (\mathrm{p}_1 \vee \mathrm{p}_4) \to \neg\mathrm{p}_3$.

Definición 1.4.5. Un sistema formal o *sistema deductivo* **S** se define a partir de tres datos:

1. Un lenguaje proposicional.

2. Un conjunto de fórmulas distinguidas, los *axiomas*; como el conjunto puede ser infinito, ellos se especifican mediante un conjunto finito de "esquemas de axiomas", que muestran la forma general de los axiomas. Los axiomas propiamente dichos se obtienen sustituyendo en los respectivos esquemas sus variables por fórmulas cualesquiera.

3. Un conjunto de *reglas* de deducción, que son de la forma

$$\frac{\Gamma}{\mathrm{A}},$$

donde Γ es un conjunto finito de fórmulas y A es una fórmula. Análogamente, las reglas están dadas por esquemas.

En general, se comete el abuso de hablar de axiomas y no de esquemas. Una *instancia* de un axioma (de un esquema, en realidad) se obtiene sustituyendo sus variables por fórmulas cualesquiera.

Por ejemplo, un sistema formal para el *Cálculo Proposicional Implicativo* está dado por los siguientes esquemas de axiomas:

(A1) $\mathrm{A} \to (\mathrm{B} \to \mathrm{A})$

(A2) $(\mathrm{A} \to (\mathrm{B} \to \mathrm{C})) \to ((\mathrm{A} \to \mathrm{B}) \to (\mathrm{A} \to \mathrm{C}))$

y por la regla de deducción Modus Ponens:

$$(\mathrm{MP})\ \frac{A\,,\ A \to B}{B}.$$

Una *instancia* de (A1) es, por ejemplo: $(\mathrm{p}_1 \to \mathrm{p}_2) \to (\mathrm{p}_1 \to (\mathrm{p}_1 \to \mathrm{p}_2))$, donde hemos reemplazado A por $\mathrm{p}_1 \to \mathrm{p}_2$ y B por p_1.

Relación de consecuencia

Definición 1.4.6. Una *prueba* o *deducción* de B en **S** es una sucesión finita de fórmulas $\mathrm{A}_1, \ldots, \mathrm{A}_{n-1}$, $\mathrm{A}_n = \mathrm{B}$ tal que cada A_i es una instancia de un axioma o se deduce de las anteriores por las reglas de deducción.

Diremos que B es un *teorema* si existe una prueba de B. En tal caso escribiremos $\vdash_{\mathbf{S}} \mathrm{B}$ o simplemente $\vdash \mathrm{B}$, si no hay lugar a confusión.

En particular, toda instancia de un axioma es un teorema.

Más en general, una *deducción* de B en **S** a partir de un conjunto de fórmulas Γ (las "hipótesis") es una sucesión finita de fórmulas $A_1, \ldots, A_{n-1}$, $A_n = B$ tal que cada A_i es una instancia de un axioma o una fórmula de Γ o se deduce de las anteriores por las reglas. Diremos que B es una *consecuencia* de Γ si existe una deducción de B a partir de Γ. En tal caso escribiremos $\Gamma \vdash_{\mathbf{S}} B$.

Por ejemplo, en el Cálculo Proposicional Implicativo se puede deducir la fórmula $B \to C$ de las hipótesis A y $B \to (A \to C)$.

En efecto, (empezando "por el final") podríamos obtener por Modus Ponens $B \to C$ de $(B \to A) \to (B \to C)$ si tuviéramos $(B \to A)$. Pero ¡tenemos $(B \to A)$! porque tenemos la hipótesis A y el axioma (A1): $A \to (B \to A)$. Nos faltaría $(B \to A) \to (B \to C)$. Pero también lo tenemos, ya que puede deducirse por (MP) de la hipótesis $B \to (A \to C)$ y el axioma (A2): $(B \to (A \to C)) \to ((B \to A) \to (B \to C))$. Luego, la prueba buscada es la siguiente:

1. A (hipótesis),
2. $B \to (A \to C)$ (hipótesis),
3. $A \to (B \to A)$, por (A1),
4. $B \to A$, de 1. y 3. por (MP),
5. $(B \to (A \to C)) \to ((B \to A) \to (B \to C))$, por (A2),
6. $(B \to A) \to (B \to C)$, de 2. y 5. por (MP),
7. $B \to C$, de 4. y 6. por (MP).

Denotaremos

$$\Gamma^{\vdash} = \{B \in \mathcal{L} : \Gamma \vdash B\}$$

al conjunto de consecuencias de Γ.

En relación con el ejemplo de prueba que dimos, podemos decir que $B \to C \in \Gamma^{\vdash}$, siendo $\Gamma = \{A, B \to (A \to C)\}$.

Definición 1.4.7. Dados dos sistemas formales **S** y **S**$'$ se dice que **S**$'$ *extiende* o *es extensión* de **S** si todo teorema de **S** es teorema de **S**$'$.

Los sistemas **L** y $\mathbf{L}_4$ que veremos en el Capítulo 3 son extensiones del sistema que vimos para el Cálculo Proposicional Implicativo.

Definición 1.4.8. Una *teoría* de **S** es un conjunto de fórmulas Σ que cumple las siguientes condiciones:

1. Σ contiene todas las instancias de axiomas.

2. Σ es cerrado por las reglas de **S**. Es decir, si $\frac{\Gamma}{\mathrm{A}}$ es una regla y $\Gamma \subseteq \Sigma$ entonces A pertenece a Σ.

Veamos algunas propiedades de las teorías.

Lema 1.4.9. *Sea* **S** *un sistema deductivo y sea* $\Gamma \subseteq \mathcal{L}$.

(a) *El conjunto* Γ *es una teoría si y solo si existe un conjunto de fórmulas* Σ *tal que* $\Sigma^{\vdash} = \Gamma$.

(b) *El conjunto* $\mathcal{T}$ *de los teoremas es la menor teoría de* **S** *y* $\mathcal{T} = \emptyset^{\vdash}$.

Demostración.

(a) Sea Γ un conjunto de fórmulas, Σ tal que $\Sigma^{\vdash} = \Gamma$. Las instancias de axiomas son consecuencias del conjunto vacío de fórmulas (no se necesitan hipótesis), luego, también son consecuencia de Σ, por lo tanto están en Γ.

Veamos que Γ es cerrado por las reglas.

Sea $\frac{\Delta}{\mathrm{A}}$ una regla, $\Delta \subseteq \Gamma$. Se tiene entonces que para cada $\mathrm{C} \in \Delta$, $\Sigma \vdash \mathrm{C}$, o sea que hay una deducción de C a partir de Σ. Uniendo todas esas deducciones (que son finitas) y agregando como último paso la aplicación de la regla $\frac{\Delta}{\mathrm{A}}$, se obtiene una deducción de A a partir de Σ. O sea, $\Sigma \vdash \mathrm{A}$, con lo cual $\mathrm{A} \in \Gamma$.

Recíprocamente, sea Γ una teoría y veamos que $\Gamma^{\vdash} = \Gamma$. Una inclusión es obvia. Probemos $\Gamma^{\vdash} \subseteq \Gamma$. Sea A tal que $\Gamma \vdash \mathrm{A}$. Luego, A se obtiene a partir de fórmulas de Γ aplicando las reglas. Pero Γ es cerrado por las reglas, luego $\mathrm{A} \in \Gamma$.

(b) Se deja como ejercicio. □

La *relación de consecuencia* $\vdash$ tiene las siguientes propiedades.

Lema 1.4.10. *Sean* Δ *y* Γ *conjuntos de fórmulas,* A, B *fórmulas. Entonces:*

(1) *Para toda* $\mathrm{A} \in \Delta$, $\Delta \vdash \mathrm{A}$.

(2) *Si* $\Delta \vdash \mathrm{A}$ *y* $\Delta \subseteq \Gamma$, *entonces* $\Gamma \vdash \mathrm{A}$.

(3) *Si* $\Gamma \vdash \mathrm{A}$ *para toda* $\mathrm{A} \in \Delta$ *y* $\Delta \vdash \mathrm{B}$, *entonces* $\Gamma \vdash \mathrm{B}$.

(4) *Si* $\Delta \vdash \mathrm{A}$, *entonces existe* Γ *finito tal que* $\Gamma \subseteq \Delta$ *y* $\Gamma \vdash \mathrm{A}$. *Diremos que* **S** *es* finitario.

(5) *Si* $\Delta \vdash \mathrm{A}$*, entonces para toda sustitución* s*,* $s(\Delta) \vdash s(\mathrm{A})$*. Diremos que* **S** *es* estructural*.*

Demostración. Los ítems (1) y (2) salen aplicando la definición de deducción.

Probemos (3). Supongamos que $\mathrm{A}_1, \ldots, \mathrm{A}_r$ son fórmulas de Δ que se usan en la deducción de B. Entonces, habrá una deducción $\mathrm{B}_1^i, \ldots, \mathrm{B}_{n_i}^i$ de A_i a partir de Γ, para cada $i = 1, \ldots, r$. Por lo tanto, reuniendo estas r deducciones con la deducción de B a partir de Δ, obtenemos una deducción de B a partir de Γ.

El ítem (4) se prueba teniendo en cuenta que solo se usa un número finito de fórmulas en una deducción. El ítem (5) sale considerando que las sustituciones son instancias (de axiomas o de las hipótesis). □

Observación 1.4.11. Algunas de estas propiedades no se cumplen en las lógicas llamadas *subestructurales*, según veremos en el Capítulo 12, Sección 4.

Valuaciones

Hemos definido, si $\mathcal{L}$ es un lenguaje proposicional, la sintaxis de ese lenguaje. Para esto se especificaron formalmente las reglas de construcción de $\mathcal{L}$.

Pero interesa también analizar la *semántica*, es decir el significado de las fórmulas, que estará dado por su "valor de verdad".

Ya hemos observado que un lenguaje proposicional tiene cierto tipo, de la misma manera que las álgebras. Podemos "evaluar" las fórmulas de $\mathcal{L}$ en álgebras del mismo tipo por medio de funciones (*valuaciones*) de manera que cada conectivo n-ario se transforme en su correspondiente operación n-aria. En el cálculo proposicional clásico (que veremos con detalle en el Capítulo 3) esas funciones son las conocidas "tablas de verdad":

p	¬p
V	F
F	V

p	q	p ∧ q
V	V	V
V	F	F
F	V	F
F	F	F

p	q	p ∨ q
V	V	V
V	F	V
F	V	V
F	F	F

p	q	p → q
V	V	V
V	F	F
F	V	V
F	F	V

Las valuaciones asignan a cada fórmula un elemento de un álgebra, que podemos pensar como su valor de verdad. En el caso clásico, esa álgebra tendrá solo los elementos 0 y 1, identificando F con 0 y V con 1.

Definición 1.4.12. Sea un lenguaje proposicional $\mathcal{L}$ cuyo conjunto de conectivos es $(\mathrm{c}_i)_{i\in I}$ y sea $\langle A, G\rangle$ un álgebra donde $G = (g_i)_{i\in I}$. Una *valuación* es una función $v : \mathcal{L} \longrightarrow A$ tal que para cada conectivo n-ario c y fórmulas $\mathrm{B}_1, \ldots, \mathrm{B}_n$ verifica

$$v(\mathrm{c}(\mathrm{B}_1, \ldots, \mathrm{B}_n)) = g(v(\mathrm{B}_1), \ldots, v(\mathrm{B}_n)),$$

siendo g la operación n-aria en A correspondiente a c.

Podemos dar, por ejemplo, valuaciones del cálculo implicativo positivo en ciertas álgebras, que definiremos a continuación.

Sea $\mathbf{A} = \langle A, \rightarrow, 1\rangle$ un álgebra donde se verifican la siguientes condiciones:

(I) $x \rightarrow (y \rightarrow x) = 1$,

(II) $(x \rightarrow (y \rightarrow z)) \rightarrow ((x \rightarrow y) \rightarrow (x \rightarrow z)) = 1$,

(III) Si $x \rightarrow y = 1$, $y \rightarrow x = 1$ entonces $x = y$.

El álgebra $\mathbf{A}$ es conocida como *álgebra de Hilbert*.

Las valuaciones solo deben cumplir aquí la condición

$$v(\mathrm{A} \rightarrow \mathrm{B}) = v(\mathrm{A}) \rightarrow v(\mathrm{B}).$$

Observemos que el mismo símbolo $\rightarrow$ designa en el primer miembro un conectivo y en el segundo una operación.

Observemos también que las condiciones (I) y (II) tienen la misma forma que los axiomas del sistema axiomático. Eso no es casual; en efecto, las propiedades de una lógica se corresponden con las de las álgebras asociadas a ella de acuerdo a un cierto proceso de “algebrización” que veremos más adelante.

1.5. Ejercicios

Conjuntos ordenados

1. Sea R una relación reflexiva sobre un conjunto. Probar que R es una relación de equivalencia si y solo si $R \circ R = R$ y $R = R^o$, siendo $R^o = \{(x, y) : (y, x) \in R\}$.

2. Probar que el orden dual es un orden.

3. Probar que el orden producto es un orden.

4. Probar que el orden lexicográfico es un orden.

5. Sea R una relación en un conjunto P y sea $\Delta = \{(x, x) \in P \times P\}$ la *diagonal* de $P \times P$. Probar que R es de orden si y solo si $R \circ R = R$ y $R \cap R^o = \Delta$.

6. Sean $A = \{0, 1\}$, $B = \{3, 4, 5\}$. Hacer los diagramas de Hasse de A y B con el orden usual, $\mathcal{P}(B)$ con el orden inclusión, $A \times A$ con el orden producto y lexicográfico.

7. Sean $(P, \leq)$, $(Q, \preceq)$ conjuntos ordenados, $f : P \to Q$ una biyección que es un morfismo de orden (ver Definición 1.2.3).

   a) ¿Es f un isomorfismo de orden (ver Definición 1.2.4)?

   b) Si $(P, \leq)$ y $(Q, \preceq)$ son conjuntos totalmente ordenados. ¿Es f un isomorfismo de orden?

8. Sea $(P, \leq)$ un conjunto ordenado, $R \subseteq P$. Se dice que R es *decreciente* P si se cumple que $x \in R$ e $y \leq x$ implica $y \in R$.

   Sean $f : P \to Q$ función y $(Q, \leq)$ un conjunto ordenado. Probar que si f es un morfismo de orden entonces la imagen inversa de un conjunto decreciente de Q es un conjunto decreciente de P.

9. Sean X, Y conjuntos no vacíos. Sean $f : X \to Y$ una función y $f_1 : \mathcal{P}(X) \to \mathcal{P}(Y)$ la función que asocia a cada subconjunto de X su imagen por f. Probar que f_1 preserva el orden inclusión y que es un isomorfismo de orden si y solo si f es una biyección.

10. Sean R_1 y R_2 relaciones de orden en A_1 y en A_2 respectivamente.

    a) Probar que la relación $R_1 \times R_2$ es un orden en $A_1 \times A_2$.

    b) Sean R_1 y R_2 órdenes totales. ¿Es $R_1 \times R_2$ un orden total? ¿Es el orden lexicográfico un orden total?

11. Sean A un conjunto y $\mathcal{F} = \{f : A \to \{0,1\}\}$. Definimos en $\mathcal{F}$ la siguiente relación:

$$f \preceq g \text{ si y solo si } f^{-1}(\{1\}) \subseteq g^{-1}(\{1\}).$$

a) Probar que $\preceq$ es un orden en $\mathcal{F}$.

b) ¿Qué relación hay entre los conjuntos ordenados $(\mathcal{F}, \preceq)$ y $(\mathcal{P}(A), \subseteq)$?

12. Sea $\mathcal{W} = \{X : X \text{ subconjunto finito de } \mathbb{N}\}$. Indicaremos con $|X|$ al número de elementos de X. Sea $\propto$ la relación definida por: $X \propto Y$ si y solo si $|X| \leq |Y|$. Probar que $\propto$ es un preorden y que no es simétrica ni antisimétrica. ¿Qué propiedades tiene la relación R definida por $X\ R\ Y$ si $X \propto Y$ e $Y \propto X$?

13. Sea R_1 el orden usual en $\mathbb{R}$ y R_2 la relación "divide a" en $\mathbb{N}$. Sea $R_1 \times R_2$ el orden producto en $\mathbb{R} \times \mathbb{N}$, es decir,

$$(x,y)\, R_1 \times R_2\, (u,v) \quad \text{si } x \leq u \text{ en } \mathbb{R} \text{ e } y \text{ divide a } v \text{ en } \mathbb{N}.$$

Sea $R_1 \bigotimes R_2$ el orden lexicográfico en $\mathbb{R} \times \mathbb{N}$, es decir,

$$(x,y)\, R_1 \bigotimes R_2\, (u,v) \text{ si } x < u \text{ en } \mathbb{R}, \text{ o bien } x = u \text{ e } y \text{ divide a } v \text{ en } \mathbb{N}.$$

a) ¿Es $R_1 \times R_2$ un orden total?

b) ¿Es $R_1 \bigotimes R_2$ un orden total?

Álgebra Universal

1. Sean $\langle G, +, -, 0\rangle$ un grupo, H un subuniverso de G y R una congruencia en G. Definimos el conjunto $K = \{x \in G : x\, R\, y\ , y \in H\}$. Probar que K es un subuniverso de G.

2. Sea $\equiv_p$ la relación de congruencia módulo p definida en el grupo $\mathbb{Z}$ de los enteros. Probar que si p es múltiplo de q entonces la relación $\equiv_p$ es *más fina* que la relación $\equiv_q$, o sea, que para todo x, y, $x \equiv_p y$ implica $x \equiv_q y$. En ese caso escribiremos $\equiv_p \subseteq \equiv_q$.

3. Sean $\langle \mathbb{Z}, +, -, 0\rangle$ el grupo de los enteros, $\equiv_n$ la congruencia módulo n, H el subuniverso de los múltiplos de 6, $K = \{x \in \mathbb{Z},\ x \equiv_n y,\ y \in H\}$.

a) Probar que K es un subuniverso de $\mathbb{Z}$.

b) Calcular K para $n = 3$ y para $n = 12$. ¿Son subuniversos?

4. Sea $f : \mathbb{Z} \to \mathbb{Z}$ la función que a cada z asigna el resto de dividir z por 7. ¿Es cierto que $x \equiv_{21} y$ implica $f(x) = f(y)$? ¿Existe una función $g : \mathbb{Z}_{21} \to \mathbb{Z}$ tal que $g(|x|) = f(x)$? ¿Es verdad que $\equiv_{21} \subseteq \equiv_7$?

5. Sea S la siguiente relación de equivalencia definida en el conjunto $\mathbb{R}$ de los números reales: $x\,S\,y$ si y solo si $x - y \in \mathbb{Z}$. Analizar si S es una congruencia en los siguientes casos: a) en el grupo $\langle \mathbb{R}, +, -, 0\rangle$; b) en el anillo $\langle \mathbb{R}, +, ., -, 0\rangle$.

6. Sean A y B álgebras de una clase $\mathcal{K}$ libremente generadas en $\mathcal{K}$ por X e Y respectivamente. Probar que si existe una biyección $h : X \longrightarrow Y$ entonces A y B son isomorfas.

7. Sea W un conjunto, $\langle W^*, \star, e\rangle$ el monoide de las palabras sobre el vocabulario W (ver 1.4). Probar que dicho monoide es libremente generado por W en la clase de los monoides.

8. Sea $W = \{a\}$. Probar que los monoides W^* y $\langle \mathbb{N}, +, 0\rangle$ son isomorfos.

9. Sea W finito, $f : W \longrightarrow \mathbb{N}$ la función constante igual a 1. a) Definir la extensión $f' : W^* \longrightarrow \mathbb{N}$. b) Si es R la congruencia asociada a f', probar que W^*/R es isomorfo a $\mathbb{N}$. c) Si W tiene k elementos ¿cuántos elementos tiene la clase correspondiente al número 1? ¿cuántos la clase del número n?

10. Sean $\mathbf{A} = \langle A, F\rangle$ y $\mathbf{B} = \langle B, G\rangle$ álgebras del mismo tipo. Sean $p_1 : A \times B \longrightarrow A$ y $p_2 : A \times B \longrightarrow B$ la primera y segunda proyección respectivamente. Probar que ambas son homomorfismos.

Lógica

1. Consideremos el siguiente sistema formal (ver [61]).

   El lenguaje está constituido por las variables $x, y, \ldots$, las constantes (conectivos 0-arios) M, I, U y el único conectivo binario la concatenación (a la que no damos ningún símbolo). El único axioma es la cadena MI y las reglas son las siguientes:

   1) $\frac{xI}{xIU}$, 2) $\frac{Mx}{Mxx}$, 3) $\frac{xIIIy}{xUy}$, 4) $\frac{xUUy}{xy}$.

   Encontrar la derivación de los teoremas: MUI, MIU, $MUIUI$, $MUIU$, $MIUIU$, $MUIIU$. ¿Son $MIIIIII$, $MUIIIU$, $MUUIIII$ teoremas?

2. Sea el sistema formal que tiene MP como única regla y los siguientes esquemas de axiomas:

(A1) $\mathrm{A} \to (\mathrm{B} \to \mathrm{A})$,

(A2) $(\mathrm{A} \to \mathrm{B}) \to ((\mathrm{B} \to \mathrm{C}) \to (\mathrm{A} \to \mathrm{C}))$.

Probar que $(\mathrm{A} \to \mathrm{C}) \to (\mathrm{B} \to \mathrm{C})$ es consecuencia de A y que $\mathrm{A} \to \mathrm{C}$ es consecuencia de $\mathrm{A} \to \mathrm{B}$ y $\mathrm{B} \to \mathrm{C}$. Llamando $\mathrm{A} \vee \mathrm{B}$ a la fórmula $(\mathrm{A} \to \mathrm{B}) \to \mathrm{B}$, probar que $\mathrm{A} \vee \mathrm{B}$ es consecuencia de B.

3. Demostrar la parte (b) del Lema 1.4.9.

4. Sea un lenguaje proposicional $\mathcal{L}$ que tiene los conectivos $\neg, \vee, \wedge, \to$. Sea el álgebra $\langle \{0,1\}, \wr, \sqcup, \sqcap, \rightsquigarrow \rangle$ con las operaciones definidas por:

$$\begin{aligned} \wr x &= 1 - x, \\ x \sqcup y &= \text{máx}\{x, y\}, \\ x \sqcap y &= \text{mín}\{x, y\}, \\ x \rightsquigarrow y &= \text{máx}\{(1-x), y\}. \end{aligned}$$

Una valuación en $\{0,1\}$ es una función $v : \mathcal{L} \longrightarrow \{0,1\}$ tal que: $v(\neg\mathrm{A}) = \wr v(\mathrm{A})$, $v(\mathrm{A} \vee \mathrm{B}) = v(\mathrm{A}) \sqcup v(\mathrm{B})$, $v(\mathrm{A} \wedge \mathrm{B}) = v(\mathrm{A}) \sqcap v(\mathrm{B})$, $v(\mathrm{A} \to \mathrm{B}) = v(\mathrm{A}) \rightsquigarrow v(\mathrm{B})$.

(a) Construir las tablas de las operaciones $\wr, \sqcup, \sqcap, \rightsquigarrow$ ¿Qué relación tienen con las tablas de verdad?

(b) Dadas las fórmulas $\mathrm{A}, \mathrm{B}, \mathrm{C}$ de $\mathcal{L}$, calcular todos los valores posibles de $v((\neg\mathrm{A} \vee \mathrm{B}) \to \mathrm{C})$.

(c) Dadas las fórmulas $\mathrm{A}, \mathrm{B}, \mathrm{C}$ de $\mathcal{L}$ tales que $v(\mathrm{A} \to \mathrm{B}) = 1$, ¿Qué se puede decir del valor de v en las fórmulas $(\mathrm{A} \vee \mathrm{C}) \to (\mathrm{B} \vee \mathrm{C})$, $(\mathrm{A} \wedge \mathrm{C}) \to (\mathrm{B} \wedge \mathrm{C})$, $((\neg\mathrm{A} \wedge \mathrm{B}) \to (\mathrm{A} \vee \mathrm{B})) \wedge ((\mathrm{A} \vee \mathrm{B}) \to (\neg\mathrm{A} \wedge \mathrm{B}))$?

(d) Encontrar, si existe, una valuación v para las fórmulas $\mathrm{A}, \mathrm{B}, \mathrm{C}$ tal que $v(\mathrm{B} \to \neg\mathrm{C}) = v(\neg(\neg\mathrm{B} \vee \mathrm{A})) = v(\mathrm{A} \vee \neg\mathrm{C})$.

Bibliografía del Capítulo 1

- Balbes R. and Dwinger, P., *Distributive Lattices*. University of Missouri Press, 1974.
- Burris S. and Sankappanavar H.P., *A Course in Universal Algebra*. Springer-Verlag, 1980.
- Caicedo X., *Elementos de Lógica y Calculabilidad*. Una Empresa Docente, Bogotá, 1990.
- Davey B.A. and Priestley H.A., *Introduction to Lattices and Order*. Cambridge University Press, 1990.
- Gentile E.R., *Notas de Álgebra I*, Ediciones Previas, Eudeba, Buenos Aires, 1976. Versión digitalizada
- Hamilton A.G., *Logic for Mathematicians*. Cambridge University Press, 1978.
- Hofstadter D., *Gödel, Escher, Bach*, Tusquets, Barcelona, 1987.
- Kneale M. y Kneale W., *El Desarrollo de la Lógica*, Tecnos, Madrid, 1980.
- Miraglia F., *Cálculo Proposicional: uma Interação da Álgebra e a Lógica*. Universidade Estadual de Campinas, Centro de Lógica, Epistemologia e História de Ciência, Campinas, 1987.
- Oubiña L., *Estructuras Algebraicas*. Editorial Exacta, La Plata, 1994.
- Oubiña L., *Introducción a la Teoría de Conjuntos*. Eudeba, 1965.
- Rasiowa R. and Sikorski R., *The Mathematics of Metamathematics*. Polska Akademia Nauk, Warsawa, 1963.

Capítulo 2

Retículos y álgebras de Boole

El objetivo de este capítulo es estudiar las álgebras de Boole, que son, históricamente, el primer intento de tratar la lógica desde un punto de vista algebraico. Posteriormente se aplicaron esos resultados al diseño de circuitos electrónicos que son básicos para la informática.

Introduciremos previamente los retículos o reticulados y nos referiremos especialmente a los distributivos. La gran mayoría de las álgebras asociadas a la lógica tienen como reducto un retículo.

La estructura de álgebra de Boole está intrínsecamente ligada a aquellas álgebras cuyo universo es de la forma $\mathcal{P}(X)$, para cierto conjunto X. En efecto, probaremos que toda álgebra de Boole finita es isomorfa a una de esa forma y, en general, toda álgebra de Boole es isomorfa a una subálgebra de una de esa forma.

Asimismo, mostraremos que los anillos en los cuales vale la propiedad de *idempotencia* $x \cdot x = x$ pueden ser dotados de una estructura de álgebra de Boole y recíprocamente.

2.1. Retículos

En esta sección vamos a considerar una clase particular de conjuntos ordenados, los retículos, que pueden ser considerados también como álgebras. Los retículos aparecen como base de las estructuras algebraicas que estudiaremos y que son asociadas naturalmente a la lógica.

Definición 2.1.1. Un conjunto ordenado $(P, \leq)$ tal que para todo $x \in P$ e $y \in P$ existen $x \vee y$ y $x \wedge y$ se denomina *retículo* o *reticulado*.

Si $(P, \leq)$ es un retículo entonces $(P, \leq^o)$ es un retículo (siendo $\leq^o$ el orden dual de $\leq$, ver Capítulo 1, Definición 1.2.1). Si denotamos con $\vee^o$ y $\wedge^o$ a las operaciones en el dual entonces $x \vee^o y = x \wedge y$ y $x \wedge^o y = x \vee y$. Si $(P, \leq)$ tiene primer elemento 0 (respectivamente último elemento 1) entonces $(P, \leq^o)$ tiene último elemento 1 (respectivamente último elemento 0).

Observación 2.1.2. Sea $(P, \leq)$ un retículo y sean $x, y, z, w \in P$. Si $x \leq y$ y $z \leq w$ entonces $x \wedge z \leq y \wedge w$ y $x \vee z \leq y \vee w$ (la prueba se deja como ejercicio).

Un retículo puede ser definido alternativamente como un álgebra $\langle P, \vee, \wedge \rangle$ que verifica las siguientes condiciones para cada $x, y, z \in P$ (ver Capítulo 1, Sección 3):

R0 $x \vee x = x$, $x \wedge x = x$ (idempotencia),

R1 $x \vee y = y \vee x$, $x \wedge y = y \wedge x$ (conmutatividad),

R2 $x \vee (y \vee z) = (x \vee y) \vee z$, $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ (asociatividad),

R3 $(x \vee y) \wedge y = y$, $(x \wedge y) \vee y = y$ (absorción).

Cometeremos a menudo el abuso de notación de nombrar a un retículo dando solo su conjunto subyacente, como se anticipó en 1.3.3.

Demostraremos ahora que, efectivamente, son equivalentes las siguientes definiciones de retículo:

(1) Un retículo es un conjunto ordenado $(L, \leq)$ en el cual, para cada par de elementos $x, y \in L$ existen el supremo $\sup\{x, y\}$ y el ínfimo $\inf\{x, y\}$, denotados $\vee$ y $\wedge$ respectivamente.

(2) Un retículo es un álgebra $\langle L, \overline{\wedge}, \underline{\vee} \rangle$ de tipo $\langle 2, 2 \rangle$, donde $\overline{\wedge}$ y $\underline{\vee}$ son símbolos de operaciones binarias que verifican las condiciones **R0, R1, R2, R3**.

(1) $\Longrightarrow$ (2):

Sea $(L, \leq)$ un conjunto ordenado tal que para cada par de elementos $x, y \in L$ existen $\inf\{x, y\}$ y $\sup\{x, y\}$, denotados $\wedge$ y $\vee$ respectivamente. Veamos que $\wedge$ y $\vee$ cumplen las propiedades **R0, R1, R2, R3**.

En efecto, idempotencia y conmutatividad salen por propiedades de conjuntos: $\{x, x\} = \{x\}$, $\{x, y\} = \{y, x\}$.

Para demostrar absorción tengamos en cuenta que, si $u \leq v$ entonces $u \wedge v = u$, $u \vee v = v$. Luego, al ser $x \vee y \geq y$, se tiene que $(x \vee y) \wedge y = y$ y análogamente $(x \wedge y) \vee y = y$.

Demostremos la asociatividad, o sea, veamos que: $x \vee (y \vee z) = (x \vee y) \vee z$ (la propiedad dual se demuestra de manera análoga).

Mostremos que un elemento u es cota superior del conjunto $\{x, y \vee z\}$ si y solo si es cota superior del conjunto $\{x, y, z\}$. Se tiene que $y \vee z \leq u$ implica $y \leq u$, $z \leq u$ (por transitividad de $\leq$) y recíprocamente, $y \leq u$, $z \leq u$ implica que $y \vee z \leq u$, por ser el supremo la mínima cota superior. De la misma manera podemos probar que u es cota superior del conjunto $\{x \vee y, z\}$ si y solo si es cota superior del conjunto $\{x, y, z\}$. Entonces, es fácil ver que ambos miembros de la igualdad coinciden con $\sup\{x, y, z\}$.

(2) $\Longrightarrow$ (1):

Demostremos ahora que, recíprocamente, si se tiene un conjunto L munido de dos operaciones, digamos $\bar{\wedge}$, $\veebar$ que cumplen las condiciones de idempotencia, conmutatividad, asociatividad y absorción, entonces podemos definir en L un orden para el cual $x \wedge y = x \,\bar{\wedge}\, y$, $x \vee y = x \veebar y$.

Definimos la siguiente relación binaria: $x \preceq y$ si y solo si $x \,\bar{\wedge}\, y = x$. Demostremos algunas propiedades:

1. Por idempotencia resulta $\preceq$ reflexiva y por la conmutatividad, antisimétrica. Demostremos la transitividad.

   Sean $x \preceq y$, $y \preceq z$, o sea, $x \,\bar{\wedge}\, y = x$, $y \,\bar{\wedge}\, z = y$. Veamos que $x \,\bar{\wedge}\, z = x$:

   $$\begin{aligned} x \,\bar{\wedge}\, z &= (x \,\bar{\wedge}\, y) \,\bar{\wedge}\, z \\ &= x \,\bar{\wedge}\, (y \,\bar{\wedge}\, z) \\ &= x \,\bar{\wedge}\, y \\ &= x. \end{aligned}$$

   Por lo tanto, $\preceq$ es un orden.

2. Veamos que se cumple:

   $$x \,\bar{\wedge}\, y = x \qquad \text{si y solo si} \qquad x \veebar y = y.$$

   En efecto, si $x \,\bar{\wedge}\, y = x$ entonces $y \veebar (x \,\bar{\wedge}\, y) = y \veebar x$, pero, por absorción, $y \veebar (x \,\bar{\wedge}\, y) = y$, o sea que $y \veebar x = y$. La recíproca es similar.

   Luego, la relación binaria $\preceq'$ definida por $x \preceq' y$ si y solo si $x \veebar y = y$ es un orden.

3. Veamos que $\bar{\wedge}$ y $\veebar$ son, efectivamente, las operaciones supremo e ínfimo correspondientes al orden $\preceq$.

   Sean $x, y \in L$ y probemos que $x \,\bar{\wedge}\, y$ es cota inferior de $\{x, y\}$ y que es la máxima.

Se tiene que

$$\begin{aligned} x \barwedge (x \barwedge y) &= (x \barwedge x) \barwedge y, \\ &= x \barwedge y. \end{aligned}$$

de donde: $x \barwedge y \preceq x$ y análogamente $x \barwedge y \preceq y$. Luego, es cota inferior.

Supongamos que es s tal que $s \preceq x$ y $s \preceq y$ (cota inferior de $\{x, y\}$). Por definición, esto significa que: $s \barwedge x = s$, $s \barwedge y = s$. Luego:

$$\begin{aligned} s \barwedge (x \barwedge y) &= (s \barwedge x) \barwedge y, \\ &= s \barwedge y, \\ &= s. \end{aligned}$$

Luego, $s \preceq x \barwedge y$, de donde $x \barwedge y$ es el ínfimo de x e y, que denotamos $x \wedge y$.

4. Análogamente, usando la otra definición de la relación $\preceq$ podemos demostrar que $x \veebar y$ es el supremo de x e y, que denotamos $x \vee y$.

Se dice que un retículo $\langle P, \vee, \wedge \rangle$ es *distributivo* si se cumplen las siguientes condiciones para cada $x, y, z \in P$:

D1 $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$,

D2 $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

Observación 2.1.3. Se puede verificar que las condiciones **D1** y **D2** son equivalentes. Por lo tanto basta que se cumpla solo una de ellas, por ejemplo, **D1**, que en adelante llamaremos **D**.

Podemos observar además que una de las dos desigualdades en **D** siempre vale.

En todo retículo:

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

En efecto, $x \wedge y \leq x$, $x \wedge y \leq y \leq y \vee z$. Luego vale que $x \wedge y \leq x \wedge (y \vee z)$. Además se tiene que $x \wedge z \leq x$, $x \wedge z \leq z \leq y \vee z$. Por esta razón tenemos que $x \wedge z \leq x \wedge (y \vee z)$. Por lo tanto, $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$.

Una propiedad útil en retículos distributivos es la que daremos en el siguiente lema:

Lema 2.1.4. *Sean x e y elementos de un retículo distributivo dado L. Si existe z tal que*

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

entonces $x = y$.

Demostración. Usando las ecuaciones y las propiedades distributiva, conmutativa y de absorción obtenemos que

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

□

Si un retículo tiene primer y último elemento entonces el mismo se llama *acotado*. Indicaremos al primer elemento con 0 y al último elemento con 1.

Si un retículo es acotado, podemos agregar a las operaciones binarias $\vee$ y $\wedge$ las dos operaciones 0-arias $0, 1$, que verifican:

Ac $x \wedge 0 = 0$, $x \vee 1 = 1$.

Consideraremos entonces el álgebra $\langle P, \vee, \wedge, 0, 1\rangle$, que es de tipo $\langle 2, 2, 0, 0\rangle$.

Ejemplos 2.1.5.

1. Cualquier conjunto totalmente ordenado es un retículo. En efecto, sea $(P, \leq)$ un conjunto totalmente ordenado, y sean x e y elementos de P. Luego, $x \leq y$ o bien $y \leq x$. Por lo tanto, $x \vee y = y$ o bien $x \vee y = x$ (análogamente para el ínfimo). Luego, existen el supremo y el ínfimo del conjunto $\{x, y\}$. Es decir, $(P, \leq)$ es un retículo. En particular, $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$ y $(\mathbb{R}, \leq)$ (con el orden usual) son retículos.

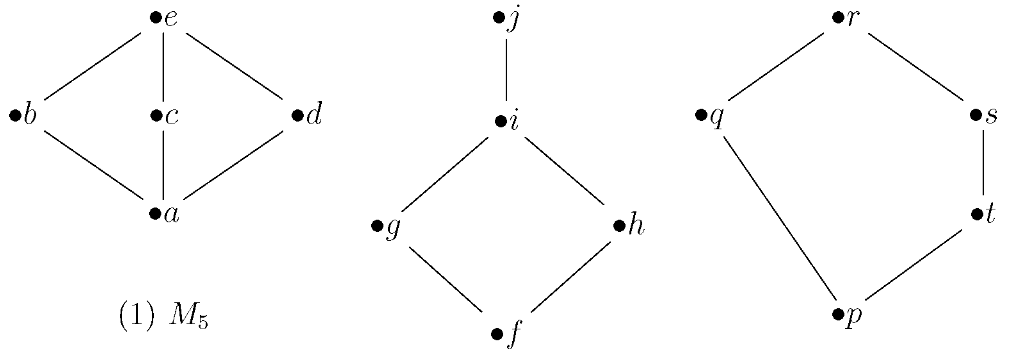
2. En la Figura 2.1 se dan algunos retículos finitos por sus diagramas de Hasse.

   Los retículos representados en (1) y (3) no son distributivos. En efecto,

   $$d \wedge (b \vee c) = d \neq a = (b \wedge d) \vee (d \wedge c).$$

   También

   $$s \wedge (q \vee t) = s \neq t = (s \wedge q) \vee (s \wedge t).$$



(1) M_5 (2) (3) L_5

Figura 2.1: Retículos

3. Sea $(\mathbb{N}, \preceq)$ el conjunto parcialmente ordenado cuyo orden $\preceq$ está dado por $x \preceq y$ si y solo si x divide a y. Dado un par de elementos x e y, el conjunto $\{x, y\}$ tiene como cotas superiores a todos los múltiplos comunes a x y a y. La menor cota superior (es decir, el supremo) es el mínimo común múltiplo (m.c.m.) de x e y. Luego $x \vee y =$ m.c.m. (x, y) y, análogamente, $x \wedge y =$ M.C.D. (x, y) (donde M.C.D. indica el máximo común divisor). Por lo tanto, $(\mathbb{N}, \preceq)$ es un retículo, cuyo diagrama se indica en la Figura 2.2. Su primer elemento es el 1 y, curiosamente, el último elemento es el 0, pues todo número natural es divisor de cero.

4. Un ejemplo de retículo finito es $(D_n, \preceq)$, siendo D_n el conjunto de los divisores de un número natural n y $\preceq$ el orden dado en el ejemplo anterior. En $(D_n, \preceq)$, 1 es el primer elemento y n el último. Podemos denotarlo también como $\langle D_n, m.c.m., M.C.D., 1, n\rangle$. En la Figura 2.3 se dan los diagramas de D_{12} y D_{30}.

5. En la Figura 2.4 se dan ejemplos de conjuntos ordenados donde para algunos pares de elementos no existen el supremo o el ínfimo. Por ejemplo, en (1), u y v no tienen cotas superiores comunes (v no tiene ninguna cota superior), luego no pueden tener supremo. En (2), el conjunto de cotas inferiores de a y b es $\{0, p, q\}$, que no tiene máximo.

6. Sea $(\mathcal{P}(X), \subseteq)$ el conjunto ordenado de las partes o subconjuntos de un conjunto X cuyo orden está dado por la inclusión. Tomemos $Z \subseteq X$ e $Y \subseteq X$. Tenemos que de todos los conjuntos contenidos simultáneamente en Z y en Y, la intersección es el mayor (el que contiene a todos).

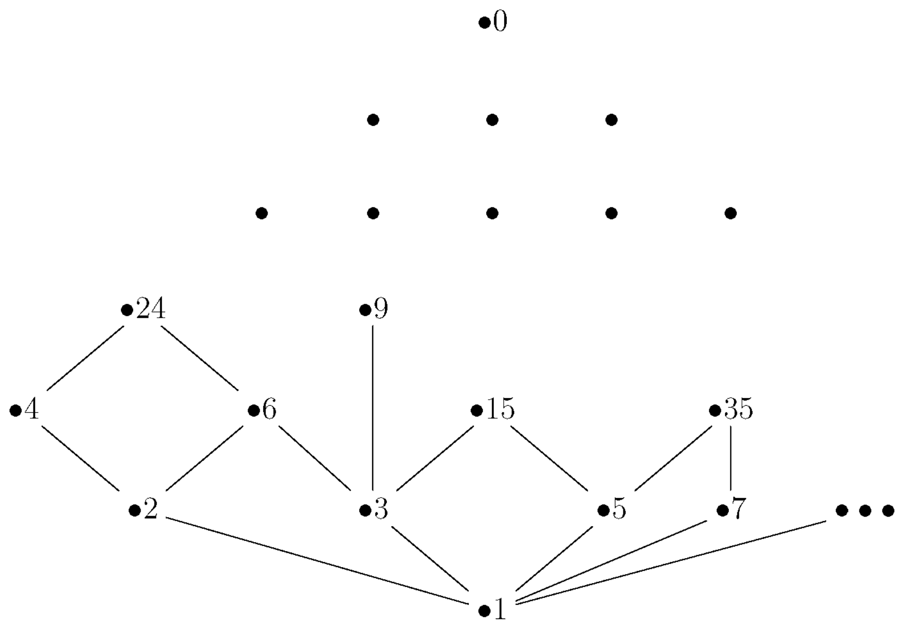
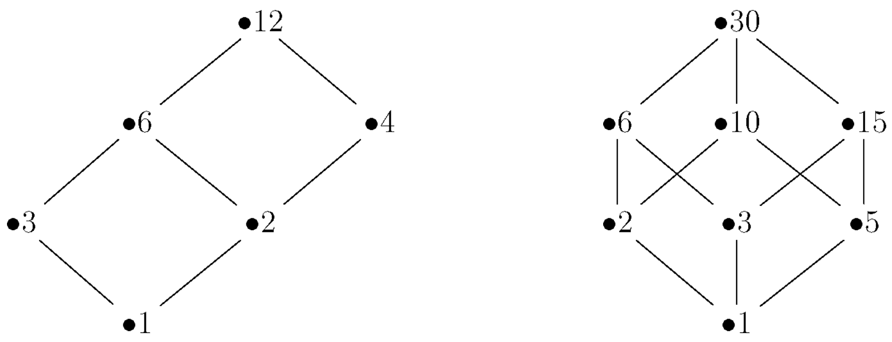
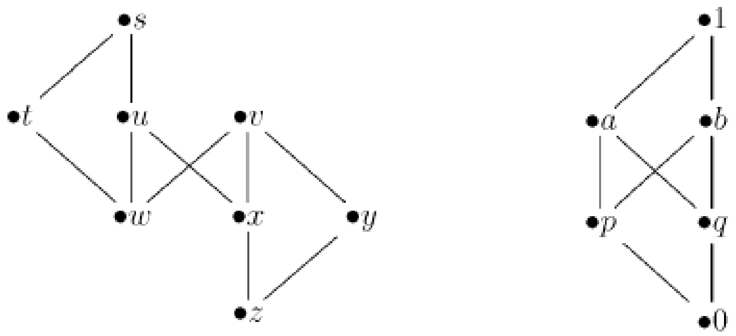


Figura 2.2: $(N, \preceq)$



(1) (2)

Figura 2.3: D_{12} y D_{30}



(1) (2)

Figura 2.4: No retículos

En efecto: en primer lugar notemos que $Z \cap Y \subseteq Z$ y que $Z \cap Y \subseteq Y$ (es decir, $Z \cap Y$ es cota inferior de $\{Z, Y\}$). Además, si U es un conjunto tal que $U \subseteq Z$ y $U \subseteq Y$ (es decir, U es cota inferior de $\{Z, Y\}$) entonces $U \subseteq Z \cap Y$. Luego $Z \cap Y$ es la mayor cota inferior, o sea el ínfimo. Por lo tanto $Z \wedge Y = Z \cap Y$, y análogamente, $Z \vee Y = Z \cup Y$. Además, $\emptyset$ es el mínimo subconjunto de X y X es el máximo subconjunto de X. Luego, $\langle \mathcal{P}(X), \cup, \cap, \emptyset, X \rangle$ es un retículo acotado. Además se puede probar que este retículo es distributivo.

7. Sea $(A, \leq)$ un conjunto ordenado. Llamaremos *conjunto creciente* (respectivamente *decreciente*) a un subconjunto X de A que cumple la siguiente condición: si $x \in X$, $y \in A$ e $y \geq x$ entonces $y \in X$ (respectivamente si $x \in X$, $y \in A$ e $y \leq x$ entonces $y \in X$).

   También podemos definir a los conjuntos crecientes y decrecientes de la siguiente manera. Sea $X \subseteq A$. Sean

$$(X] = \{a \in A : \ a \leq x \text{ para algún } x \in X\},$$
$$[X) = \{a \in A : \ a \geq x \text{ para algún } x \in X\}.$$

   Entonces diremos que X es creciente si $X = [X)$ y que es decreciente si $X = (X]$.

   La clase de los conjuntos crecientes (respectivamente decrecientes) de $(A, \leq)$ tiene estructura de retículo (con respecto a la inclusión). Sean

$$A^+ = \{X : X \subseteq A \text{ y } X \text{ creciente}\},$$
$$A^- = \{X : X \subseteq A \text{ y } X \text{ decreciente}\}.$$

Notemos que $A^+ \subseteq \mathcal{P}(A)$, $A^- \subseteq \mathcal{P}(A)$ y podemos considerar entonces en A^+ y A^- el orden dado por la inclusión entre subconjuntos de A. Puede probarse que la unión $X \cup Y$ de dos conjuntos crecientes (respectivamente decrecientes) X e Y es un conjunto creciente (respectivamente decreciente). Si consideramos en A^+ y A^- como relación de orden la de la inclusión de conjuntos, se tiene que $X \cup Y$ es el supremo de X e Y. En forma dual se prueba que la intersección de dos conjuntos crecientes (respectivamente decrecientes) es un conjunto creciente (respectivamente decreciente) y además es el ínfimo de ambos. Se tiene también que $\emptyset$ y A son respectivamente el mínimo y el máximo. Es decir, $\langle A^+, \cup, \cap, \emptyset, A\rangle$ y $\langle A^-, \cup, \cap, \emptyset, A\rangle$ son retículos acotados (más aún, son retículos distributivos).

8. Dado un conjunto X, una clase $\mathcal{T}$ de subconjuntos de X se llama una *topología* sobre X si $\emptyset$ y X pertenecen a $\mathcal{T}$, y si $\mathcal{T}$ es cerrado por intersecciones finitas y uniones (arbitrarias). Un *espacio topológico* $(X, \mathcal{T})$ es un par formado por un conjunto X y una topología $\mathcal{T}$ sobre X. Los elementos de $\mathcal{T}$ se llaman *abiertos* de la topología. Dado un espacio topológico, sus abiertos forman un retículo distributivo acotado $\langle \mathcal{T}, \cup, \cap, \emptyset, X\rangle$. El ejemplo anterior es un caso particular de este ejemplo, ya que, como veremos más adelante, A^+ (también A^-) es una topología sobre A.

Observación 2.1.6. Hemos visto en la Sección 1.3 del Capítulo 1 los conceptos de subálgebra, homomorfismo e isomorfismo.

De acuerdo a eso, diremos que $\langle M, \vee, \wedge\rangle$ es subretículo de $\langle L, \vee, \wedge\rangle$ si $M \subseteq L$, $M \not\subseteq \emptyset$ y M es cerrado con respecto a $\vee$ y $\wedge$.

Sean L y M retículos, $f : L \to M$ una función.

(a) f es un homomorfismo de retículos si $f(x \wedge y) = f(x) \wedge f(y)$ y $f(x \vee y) = f(x) \vee f(y)$. Si f es biyectiva, entonces f se denomina isomorfismo de retículos.

(b) Si L y M son retículos acotados y f es tal que $f(0) = 0$ y $f(1) = 1$, entonces f es un homomorfismo de retículos acotados, y se llamará isomorfismo si f es biyectiva.

Para una prueba del teorema siguiente puede consultarse la Sección 5 del Capítulo II de [2], o bien la Sección 3 del Capítulo 1 de [13].

Teorema 2.1.7. *Un retículo $\langle L, \vee, \wedge\rangle$ es distributivo si y solo si no existe subretículo $\langle L', \vee, \wedge\rangle$ de $\langle L, \vee, \wedge\rangle$ isomorfo a M_5 o a L_5.*

Como consecuencia de este teorema, podemos probar que vale el siguiente resultado.

Teorema 2.1.8. *Un retículo L es distributivo si y solo si para todo par de elementos x, y, si existe z tal que*

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

entonces $x = y$.

Demostración. Si L es distributivo, entonces vale la propiedad del enunciado (ver Lema 2.1.4).

Supongamos ahora que vale dicha propiedad. Veamos que L no puede contener un subretículo isomorfo a M_5 o a L_5. En efecto, en la Figura 2.1, para M_5 se tiene:

$$b \wedge d = c \wedge d, \quad b \vee d = c \vee d,$$

sin embargo,

$$b \neq c.$$

Para L_5,

$$q \wedge s = q \wedge t, \quad q \vee s = q \vee t,$$

sin embargo,

$$s \neq t.$$

Luego, L es distributivo. □

2.2. Complementos y pseudocomplementos

Entre los ejemplos de retículos, tenemos el de las partes de un conjunto X, $\langle \mathcal{P}(X), \cup, \cap, \emptyset, X \rangle$, que es distributivo y acotado. En esta álgebra podríamos agregar una operación más, que es el complemento de conjuntos. Obtendríamos entonces un álgebra de Boole.

En general, en un retículo, el complemento $\overline{x}$ de un elemento x se caracteriza por dos condiciones: el supremo de ambos es 1 y su ínfimo es 0. Si solo se cumple la segunda condición, entonces hablaremos de pseudocomplemento.

Definiremos en esta sección las álgebras de Boole y daremos algunos ejemplos.

Definición 2.2.1. Sea $\langle L, \vee, \wedge \rangle$ un retículo con 0, y sea $x \in L$. Se denomina *pseudocomplemento* de x, si existe, al máximo del conjunto

$$\{z \in L : x \wedge z = 0\}.$$

Se denomina *complemento* de x, si existe, a un elemento $u \in L$ tal que $x \vee u = 1$ y $x \wedge u = 0$.

Observación 2.2.2. Si $\langle L, \vee, \wedge \rangle$ es un retículo con 0 en donde existe el pseudocomplemento de 0, entonces L tiene necesariamente último elemento 1 porque $\text{máx}\{z \in L : 0 \wedge z = 0\} = \text{máx}\, L$.

En lo que sigue consideraremos algunos ejemplos y propiedades del complemento.

Ejemplos 2.2.3.

1. En el diagrama de D_{30} (ver (2) de Figura 2.3) se tiene que 2 es complemento de 15, 3 es complemento de 10 y 5 es complemento de 6.

2. En el diagrama del retículo M_5, hecho en (1) de la Figura 2.1, se tiene que b tiene como complemento a c y también a d.

3. En el retículo L_5 dado en (3) de la misma Figura 2.1 tenemos que q tiene tanto a s como a t de complemento.

Veremos que la situación anterior (que un elemento tenga más de un complemento) no puede darse en retículos distributivos, como se prueba en el siguiente lema.

Lema 2.2.4. *Sea $\langle L, \vee, \wedge, 0, 1 \rangle$ un retículo distributivo acotado. Si un elemento $x \in L$ tiene complemento, el mismo es único y es también el pseudocomplemento de x.*

Demostración. Sea $x \in L$, y sean u, u' complementos de x. Usando las propiedades del primer elemento 0, del último elemento 1 y la distributividad del retículo tenemos que

$$\begin{aligned} u &= u \wedge 1 \\ &= u \wedge (x \vee u') \\ &= (u \wedge x) \vee (u \wedge u') \\ &= 0 \vee (u \wedge u') \\ &= u \wedge u'. \end{aligned}$$

De este modo vemos que $u = u \wedge u'$. Es decir, $u \leq u'$. De manera similar se prueba que $u' \leq u$, con lo cual $u = u'$.

Llamemos $\overline{x}$ al complemento de x, y sea $X = \{z \in L : x \wedge z = 0\}$. Es inmediato que $\overline{x} \in X$. Veamos que $\overline{x}$ es mayor o igual que cualquier elemento de X. Si $z \in L$ es tal que $z \wedge x = 0$ entonces

$$\begin{aligned} \overline{x} &= \overline{x} \vee 0 = \overline{x} \vee (z \wedge x) \\ &= (\overline{x} \vee z) \wedge (\overline{x} \vee x) \\ &= (\overline{x} \vee z) \wedge 1 \\ &= \overline{x} \vee z. \end{aligned}$$

Luego, $\overline{x} = \overline{x} \vee z$, es decir, $\overline{x} \geq z$. □

Definición 2.2.5. Un *álgebra de Boole* es un retículo distributivo acotado en el cual todo elemento tiene complemento.

Podemos adoptar otra definición de álgebra de Boole.

Definición 2.2.6. Un álgebra de Boole es un álgebra $\langle B, \vee, \wedge, ^-, 0, 1\rangle$ de tipo $\langle 2, 2, 1, 0, 0\rangle$ tal que las operaciones $\vee$, $\wedge$, 0 y 1 satisfacen las condiciones **R1**, **R2**, **R3**, **D** y **Ac** dadas en la Sección 2.1 junto a la siguiente condición adicional para cada $x \in B$:

C $x \wedge \overline{x} = 0$ y $x \vee \overline{x} = 1$.

Dejamos como ejercicio demostrar la equivalencia de las dos definiciones.

Se puede probar que en toda álgebra de Boole se cumplen también las siguientes condiciones:

01 $\overline{1} = 0, \overline{0} = 1$,

DC $\overline{\overline{x}} = x$,

M1 $\overline{(x \vee y)} = \overline{x} \wedge \overline{y}$,

M2 $\overline{(x \wedge y)} = \overline{x} \vee \overline{y}$.

Observación 2.2.7. Las dos últimas condiciones de denominan *leyes de De Morgan*. Un retículo distributivo acotado con un operador que las verifica junto con la propiedad (DC) se llama *álgebra de De Morgan*.

Ejemplos 2.2.8.

1. Exceptuando el álgebra de Boole *trivial*, que es la que posee un único elemento, el álgebra de Boole mínima (con respecto a la inclusión) es la que solo tiene al 0 y al 1 como elementos, es decir, $\langle\{0, 1\}, \wedge, \vee, ^-, 0, 1\rangle$. Llamaremos **2** a esta álgebra de Boole.

   Veremos más adelante que **2** juega un rol fundamental en la clase de las álgebras de Boole.

   Sean p, q elementos de **2**. En las siguientes tablas mostramos las operaciones de complemento, ínfimo y supremo.

p	$\overline{\text{p}}$
1	0
0	1

p	q	p ∧ q
1	1	1
1	0	0
0	1	0
0	0	0

p	q	p ∨ q
1	1	1
1	0	1
0	1	1
0	0	0

2. Como dijimos al principio de esta sección, en el Ejemplo 6 de la Sección 2.1 probamos que si X es un conjunto entonces $\langle \mathcal{P}(X), \cup, \cap, \emptyset, X \rangle$ es un retículo distributivo acotado con las operaciones de unión, intersección y las constantes dadas por el conjunto vacío $\emptyset$ y el total X. Si agregamos la operación unaria ^{c_X} de tomar complemento con respecto a X, tenemos que $\langle \mathcal{P}(X), \cup, \cap, ^{c_X}, \emptyset, X \rangle$ es un álgebra de Boole. Más adelante veremos el teorema de Stone que prueba que cada álgebra de Boole finita es isomorfa a un álgebra de Boole de esta forma. Sin embargo, hay álgebras de Boole infinitas que no son isomorfas a un álgebra de Boole de esta forma, como prueba un ejemplo que trataremos a continuación.

   También veremos más adelante un teorema de representación de Stone que caracteriza a las álgebras de Boole como subálgebras de álgebras de partes.

   Sea X un conjunto *numerable*, es decir, tal que existe una biyección del conjunto $\mathbb{N}$ de los números naturales en X. Sean $F(X)$ y $C(X)$ (respectivamente los subconjuntos finitos y cofinitos de X) definidos como $F(X) = \{Y \subseteq X : Y \text{ es finito}\}$ y $C(X) = \{Y \subseteq X : X - Y \text{ es finito}\}$. Definimos $Z(X) = F(X) \cup C(X)$. Como $Z(X) \subseteq \mathcal{P}(X)$, para probar que $(Z(X), \subseteq)$ es un álgebra de Boole, basta ver que $Z(X)$ es cerrado con respecto de las operaciones $\cap, \cup$, complemento y que contiene al vacío y al total (que son respectivamente el 0 y el 1 del álgebra). Lo dejamos como ejercicio.

   Luego, asumimos que $(Z(X), \subseteq)$ es un álgebra de Boole.

   Por la Proposición A7 en el Apéndice de [57] se tiene que si A es un conjunto numerable, entonces $\mathcal{P}(A)$ es un conjunto no numerable. También es un resultado conocido (ver por ejemplo Proposición A10 del Apéndice de [57]) que los subconjuntos finitos de un conjunto numerable forman un conjunto numerable. Por esta razón $F(X)$ es numerable y $C(X)$ también, ya que existe una biyección entre $F(X)$ y $C(X)$ dada por el complemento. Luego, como consecuencia de la Proposición A5

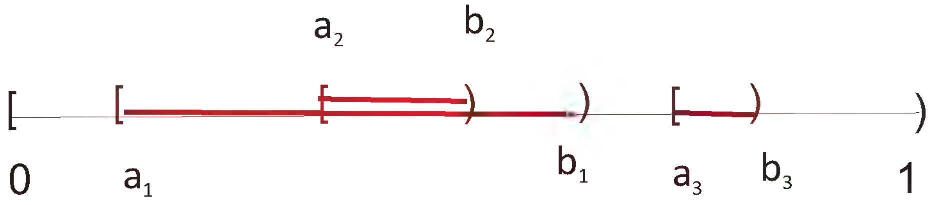


Figura 2.5: Intervalos semiabiertos

de [57] tenemos que $Z(X)$ es numerable, por tratarse de una unión disjunta de conjuntos numerables. Por lo tanto $Z(X) \neq \mathcal{P}(A)$, para cualquier A. En efecto, si A es finito entonces $\mathcal{P}(A)$ es finito; si A es numerable entonces $\mathcal{P}(A)$ es no numerable.

3. Consideremos los retículos D_n considerados en el Ejemplo 4 de la Sección 2.1. Se puede probar que si n es un producto de números primos distintos, entonces todo elemento p tiene un complemento, el cual está dado por $\overline{p} = n/p$. En la Figura 2.3 de la Sección 2.1, el retículo D_{30} es un álgebra de Boole.

4. Sabemos que los conjuntos abiertos de un espacio topológico forman un retículo distributivo acotado. Sin embargo, este retículo no es necesariamente un álgebra de Boole porque en general el complemento de un conjunto abierto no es un conjunto abierto. Si consideramos solo los conjuntos “clopen”, es decir los conjuntos abiertos cuyos complementos son conjuntos abiertos entonces el retículo sí resulta ser un álgebra de Boole, que se llama el *álgebra característica* del espacio topológico.

5. Consideremos el intervalo real semiabierto $[0, 1)$, es decir, el conjunto de los números reales x tales que $0 \leq x < 1$. Tomemos el conjunto B de todas las uniones finitas de intervalos semiabiertos contenidos en $[0, 1)$. Es decir, X es un elemento de B si $X = I_1 \cup I_2 \cup \cdots \cup I_n$, donde $I_1, I_2, \ldots, I_n$ son intervalos de la forma $[a, b)$ contenidos en $[0, 1)$. En la Figura 2.5 tenemos que $X = [a_1, b_1) \cup [a_2, b_2) \cup [a_3, b_3) = [a_1, b_1) \cup [a_3, b_3)$ es un elemento de B. Se tiene que uniones e intersecciones finitas de elementos de B están en B. El conjunto vacío es el primer elemento de B y $[0, 1)$ es el último elemento de B. Asimismo, si tomamos como complemento ^{c} la operación definida por $I^c = [0, 1) - I$, tenemos que B con dichas operaciones forma un álgebra de Boole.

6. Un anillo conmutativo con unidad $\langle A, +, \cdot, -, 0, 1\rangle$ tal que $x \cdot x = x$

para todo $x \in A$ se denomina *idempotente*. Por ejemplo, A puede ser $\{0,1\}$ con las operaciones $0+1=1+0=1$, $1+1=0+0=0$, $0\cdot 0=0\cdot 1=1\cdot 0=0$, $1\cdot 1=1$.

Definimos la siguiente relación de orden en un anillo conmutativo con unidad idempotente dado:

$$x \leq y \;\text{ si y solo si }\; x\cdot y = x.$$

En particular, $x\cdot y$ es cota inferior de x y de y. En lo que sigue probaremos que existe el ínfimo entre x e y, siendo $x\wedge y = x\cdot y$. Sea $z\leq x$ y $z\leq y$. Luego $z\cdot(x\cdot y)=(z\cdot x)\cdot y = z\cdot y = z$, es decir, $z\leq x\cdot y$. De este modo probamos que $x\wedge y = x\cdot y$.

Como el ínfimo es el producto, notemos que $x\wedge(1-x)=0$ (por distributividad del anillo y por ser $x\cdot x = x$). Por esta razón tenemos que $1-x$ es un “candidato” a ser el complemento de x. Veamos que la única cota superior común a x y a $1-x$ es 1. En efecto, sea $x\leq z$ y $1-x\leq z$. Luego $x\cdot z = x$ y $(1-x)\cdot z = 1-x$. Sumando miembro a miembro y sacando factor común z obtenemos que $(x+(1-x))\cdot z = x+(1-x)$, de donde resulta $z=1$.

Utilizando las leyes de De Morgan (ver 2.2.7), tenemos ahora un candidato a supremo:

$$\begin{aligned} x\vee y &= 1-((1-x)\wedge(1-y))\\ &= 1-((1-x)\cdot(1-y))\\ &= x+y-x\cdot y. \end{aligned}$$

La última igualdad se obtiene distribuyendo y efectuando las operaciones de suma y resta correspondientes.

Hasta aquí solo hemos conjeturado cuáles podrían ser las operaciones $\wedge$, $^-$ y $\vee$ a definirse sobre A para obtener un álgebra de Boole. Puede probarse que esta conjetura es correcta. Es decir, $\langle A,\wedge,\vee,^-,0,1\rangle$ resulta un álgebra de Boole definiendo $x\wedge y = x\cdot y$, $x\vee y = x+y-x\cdot y$ y $\overline{x} = 1-x$.

Lo interesante de este ejemplo es que *toda álgebra de Boole es de esta forma*. Es decir, que dada un álgebra de Boole B puede encontrarse un anillo idempotente asociado a B, definiendo $a+b=(a\wedge\overline{b})\vee(b\wedge\overline{a})$, ($a+b$ es la llamada “diferencia simétrica” de a y b) y $a\cdot b = a\wedge b$. La operación de opuesto es la identidad, es decir $-a=a$.

Como hemos dicho al principio de la sección, el pseudocomplemento de un elemento x, si existe, es el máximo de los z tales que $x \wedge z = 0$, lo que es equivalente a decir que $x \wedge z \leq 0$. La definición de pseudocomplemento puede generalizarse tomando un elemento arbitrario y en lugar de 0.

Definición 2.2.9. Sea L un retículo, y sean x, y elementos de L. Se llama *pseudocomplemento relativo de x con respecto a y* y se denota $x \to y$, si existe, al máximo del conjunto $\{z \in L : x \wedge z \leq y\}$. Vamos a denotar por $\to$ a la operación binaria definida como $x \to y = \text{máx}\{z \in L : x \wedge z \leq y\}$, a la cual llamaremos también *implicación*.

Lema 2.2.10. *Sea L un retículo y sean $x, y \in L$. Si existe $x \to y$ entonces para cada $z \in L$ vale que*

$$x \wedge z \leq y \quad \textit{si y solo si} \quad z \leq x \to y.$$

Recíprocamente, si existe una operación binaria $\to: L \times L \to L$ tal que para todo $z \in L$ vale que $x \wedge z \leq y$ si y solo si $z \leq x \to y$, entonces $x \to y = \text{máx}\{z \in L : x \wedge z \leq y\}$.

Definición 2.2.11. Un *álgebra de Heyting* L es un retículo que tiene primer elemento y tal que para cada par de elementos $x, y \in L$ existe la implicación $x \to y$.

Observación 2.2.12. En un álgebra de Boole siempre existe $x \to y$ para todo x, y, siendo $x \to y = \overline{x} \vee y$.

Consideremos el retículo L_5 de la Figura 2.1 de la Sección 2.1. Como $p = 0$ (primer elemento), tenemos que $q \to p = \overline{q} = \text{máx}\{p, t, s\} = s$. Otros casos: $q \to t = \text{máx}\{p, t, s\} = s$, $t \to q = \text{máx}\{p, q\} = q = t \to p$, $t \to s = \text{máx}\{p, q, t, s, r\} = r$. En cambio no existe $s \to t$, pues $\{z : z \wedge s \leq t\} = \{p, t, q\}$ no tiene máximo.

Dado que L_5 es uno de los dos retículos no distributivos "emblemáticos" (ver último teorema de la Sección 2.1), el ejemplo anterior nos lleva a preguntarnos si la existencia del pseudocomplemento relativo tiene algo que ver con la distributividad del retículo. Es interesante ver que, efectivamente, hay una relación.

Lema 2.2.13. *Si L es un retículo tal que para todo par de elementos x e y existe $x \to y$ entonces L es distributivo.*

Demostración. Sean $x, y, z \in L$. Por la Observación 2.1.3 basta probar la desigualdad $x \wedge (y \vee z) \leq (x \wedge y) \vee (x \wedge z)$. Por propiedades del supremo tenemos que $x \wedge y \leq (x \wedge y) \vee (x \wedge z)$, es decir,

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

Análogamente tenemos que

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

Por lo tanto se tiene que $y \vee z \leq x \to ((x \wedge y) \vee (x \wedge z))$, es decir,

$$x \wedge (y \vee z) \leq (x \wedge y) \vee (x \wedge z). \qquad \square$$

Observación 2.2.14. La existencia de la implicación en un retículo se vincula asimismo con el orden. En efecto, puede probarse que

$$x \leq y \text{ si solo si existe } x \to y = 1.$$

En particular, en un retículo con implicación tenemos que $x \leq y$ si y solo si $x \to y = 1$.

2.3. Congruencias en álgebras de Boole

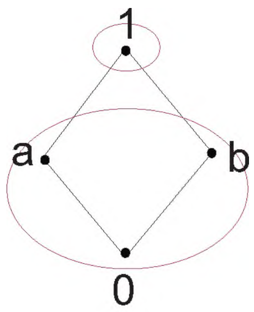
¿Cómo son las congruencias en las álgebras de Boole?

Hemos visto en el Capítulo 1, Sección 3, el ejemplo de la congruencia módulo p definida en el grupo $\langle \mathbb{Z}, +, -, 0\rangle$ y también en el anillo $\langle \mathbb{Z}, +, \cdot, -, 0\rangle$. El conjunto de los múltiplos de p es un ideal. Un *ideal en un anillo* A es un subconjunto I de A que cumple las siguientes condiciones: 1) $0 \in I$; 2) si $i, j \in I$ entonces $i - j \in I$; y 3) si $i \in I$ y $a \in A$ entonces $i \cdot a \in I$ y $a \cdot i \in I$. La relación $\equiv_p$ considera "iguales" (los identifica en el conjunto cociente) a dos elementos si su diferencia está en el ideal de los múltiplos de p, que es justamente la clase del 0.

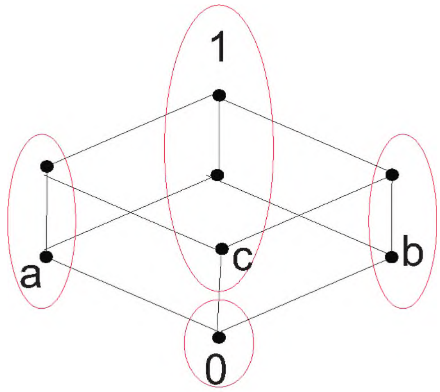
El hecho anterior es una propiedad general en anillos: toda congruencia es "dirigida" por un ideal, que es la clase del 0. Es decir, se tiene que dada una congruencia, su clase del 0 es un ideal y, recíprocamente, todo ideal define una congruencia a la manera de $\equiv_p$, es decir: x estará relacionado con y si su diferencia está en el ideal.

En el Ejemplo 6 de la Sección 2.2 vimos la propiedad de que a toda álgebra de Boole se le puede asociar un anillo idempotente y recíprocamente. Se verifica además que las congruencias de una estructura y de la otra son las mismas. En las álgebras de Boole se define también el concepto de ideal y su dual, el concepto de *filtro*. Los ideales de un álgebra de Boole resultan ser exactamente los de su anillo asociado.

En general, en álgebras de Boole se consideran los filtros más que los ideales al estudiar las congruencias.



(1)



(2)

Figura 2.6: Particiones malas

Probaremos que hay una biyección entre las congruencias en un álgebra de Boole y sus filtros.

De acuerdo a lo que hemos visto en el Capítulo 1, una congruencia en un retículo $\langle L, \vee, \wedge \rangle$ es una relación de equivalencia R tal que se cumplen las siguientes condiciones de *compatibilidad* con respecto al ínfimo y al supremo:

(Inf) Si xRy y uRv entonces $(x \wedge u)R(y \wedge v)$.

(Sup) Si xRy y uRv entonces $(x \vee u)R(y \vee v)$.

Análogamente, una congruencia en un álgebra de Boole $\langle B, \vee, \wedge, ^-, 0, 1 \rangle$ es una relación de equivalencia que cumple (**Inf**), (**Sup**) y la condición adicional (de compatibilidad respecto del complemento):

(Comp) Si xRy entonces $\overline{x}R\overline{y}$.

Observación 2.3.1. Más adelante probaremos que las relaciones de equivalencia sobre un álgebra Boole que son congruencias del reducto $\langle B, \vee, \wedge \rangle$ necesariamente satisfacen también (**Comp**), es decir, son congruencias de álgebra de Boole.

En la partición (1) de la Figura 2.6 tenemos dos clases de equivalencia en el conjunto cociente, pero el supremo no estará bien definido entre ellas. En efecto, $a \vee b = 1$ implicaría que $|a| \vee |b| = |1|$. Sin embargo, como $|a| = |b|$ tenemos que $|a| \vee |b| = |a| \neq |1|$. En (2) de la misma Figura tenemos la siguiente situación. Como c está en la clase de equivalencia de 1, la clase de equivalencia de $a \vee c$ debería ser la misma que la de $a \vee 1 = 1$, pero $a \vee c$

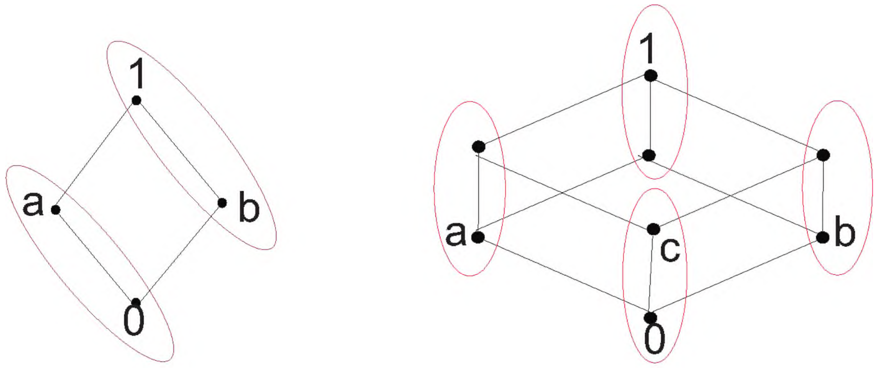


Figura 2.7: Particiones buenas

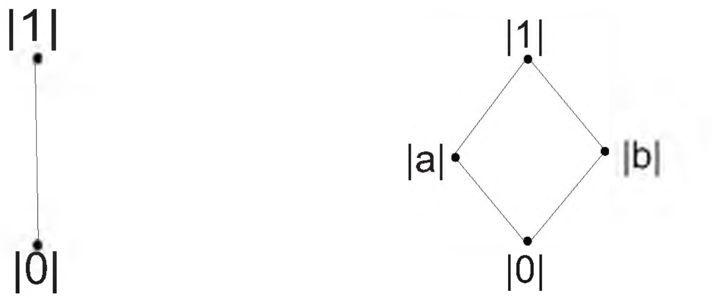


Figura 2.8: Cocientes

está en la clase de equivalencia de a y no en la clase de equivalencia del 1. En cambio, en la Figura 2.7 se muestran particiones "buenas", que permiten definir correctamente los respectivos cocientes de la Figura 2.8.

Vamos a definir la noción de filtro en retículos y veremos que a todo filtro F se le asocia una congruencia de manera que la clase del 1 es F. En álgebras de Boole, además, a cada congruencia R le corresponde un filtro (la clase del 1) de manera que su congruencia asociada es R. De esta manera veremos que existe una biyección entre los filtros y las congruencias de un álgebra de Boole dada, que no es sino la traducción de la biyección que existe entre los ideales y las congruencias en su correspondiente anillo idempotente.

Definición 2.3.2. Sea L un retículo, $F \subseteq L$ e $I \subseteq L$. Diremos que F es un *filtro* si se cumplen las siguientes condiciones:

(a) $F \neq \emptyset$.

(b) Si $x \in F$ e $y \geq x$ entonces $y \in F$.

(c) Si $x \in F$ e $y \in F$, entonces $x \wedge y \in F$.

Diremos que I es un *ideal* si se cumplen las siguientes condiciones:

(a) $I \neq \emptyset$.

(b) Si $x \in I, y \leq x$ entonces $y \in I$.

(c) Si $x \in F$ e $y \in F$ entonces $x \vee y \in I$.

Definición 2.3.3. Sea B un álgebra de Boole. Un subconjunto F de B es un *filtro implicativo* si se satisfacen las siguientes condiciones:

(a) $1 \in F$.

(b) Si $x \in F$ y además $x \to y \in F$ entonces $y \in F$.

Observación 2.3.4.

(a) Sea L un retículo. Si L tiene último elemento 1 entonces en la definición de filtro podemos cambiar la condición $F \neq \emptyset$ por la condición $1 \in F$. Si I es un ideal y $1 \in I$ entonces $I = L$. Análogamente, si L tiene primer elemento 0 entonces en la definición de ideal podemos cambiar la condición $I \neq \emptyset$ por la condición $0 \in I$. Si F es un filtro y $0 \in F$ entonces $F = L$.

(b) Sea F un filtro implicativo de un álgebra de Boole. Sean $x, y \in F$ tales que $x \in F$, $x \leq y$. Como $x \to y = 1 \in F$, tenemos que $y \in F$. Es decir, F es un conjunto creciente.

Lema 2.3.5. *Sea B un álgebra de Boole, y sea $F \subseteq B$. Entonces, F es un filtro implicativo si y solo si F es un filtro.*

Demostración. Sea F un filtro implicativo. Sean $x, y \in F$. De $x \wedge y \leq x \wedge y$ deducimos $x \leq y \to (x \wedge y)$, de donde $x \to (y \to (x \wedge y)) = 1$. Usando que $x \in F$ se tiene que $y \to (x \wedge y) \in F$. Ahora podemos usar que $y \in F$ para afirmar que $x \wedge y \in F$. De este modo queda probado que F es cerrado por ínfimos finitos. Por la Observación 2.3.4 tenemos que F es un filtro.

Recíprocamente, supongamos que F es un filtro. Sean $x, x \to y \in F$. En particular, tenemos que $x \wedge (x \to y) \in F$ y $x \wedge (x \to y) \leq y$, con lo cual llegamos a que $y \in F$. Por lo tanto considerando nuevamente la Observación 2.3.4 tenemos que F es un filtro implicativo. $\square$

Definición 2.3.6.

a) Sea L un retículo y sea X un subconjunto no vacío de L. Se puede probar que la intersección de filtros es un filtro. El menor filtro que contiene a X es la intersección de todos los filtros que contienen a X, lo llamaremos *filtro generado por* X y lo denotaremos $F(X)$. Análogamente, al menor ideal que contiene a X lo denominaremos *ideal generado por* X y lo notaremos como $I(X)$.

b) Si L es un retículo con 1 se puede probar que el menor filtro que contiene al conjunto vacío, denotado por $F(\emptyset)$, es $\{1\}$. Análogamente, si L es un retículo con 0 se puede probar que el menor ideal que contiene al conjunto vacío, denotado por $I(\emptyset)$, es $\{0\}$.

Observación 2.3.7. Si L es un retículo y $x \in L$ entonces

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

es el filtro generado por $\{x\}$. En general diremos que este es el *filtro principal* generado por x. Análogamente,

$$(x] = \{y \in L : y \leq x\}$$

es el ideal generado por $\{x\}$. En general diremos que este ideal es el *ideal principal* generado por x.

Ejemplos 2.3.8.

1. Sea L un retículo acotado. Entonces $\{1\}$ es el menor filtro de L y L es el mayor filtro de L. Análogamente, $\{0\}$ es el menor ideal de L y L es el mayor ideal de L.

2. Sea X un conjunto numerable. Consideremos el retículo $\langle Z(X), \cup, \cap\rangle$ (ver ejemplos de Sección 2.1). Se puede probar que $C(X)$ es un filtro, que no es principal. Además $F(X)$ es un ideal.

3. Consideremos el retículo $\langle \mathbb{R}, \vee, \wedge\rangle$. Sea $F = \{x \in \mathbb{R} : x > 0\}$. Tenemos que F es un filtro no principal.

4. Dado un filtro F en un álgebra de Boole, probaremos que el conjunto $\overline{F} = \{x : \; \overline{x} \in F\}$ es un ideal. Notemos que $0 \in \overline{F}$ (pues $1 \in F$). Si $x \in \overline{F}$ e $y \leq x$ entonces $y \wedge x = y$. Utilizando las leyes de De Morgan se puede probar que $\overline{y} \geq \overline{x}$. Esto implica que $\overline{y} \in F$, es decir, $y \in \overline{F}$. También por las leyes de De Morgan tenemos que $\overline{F}$ es cerrado por supremo.

En el siguiente teorema veremos la relación asociada a un filtro en un retículo.

Teorema 2.3.9. *Sea F un filtro en un retículo L. Sea $\equiv_F$ la siguiente relación binaria definida en L:*

$$x \equiv_F y \text{ si y solo si existe } f \in F \text{ tal que } x \wedge f = y \wedge f.$$

Entonces, $\equiv_F$ es una congruencia. Más aún, $F = |1|$.

Demostración. Dejamos como ejercicio al lector probar que $\equiv_F$ es una relación de equivalencia. Veamos que esta relación de equivalencia resulta ser una congruencia. Sea $x \equiv_F x'$ e $y \equiv_F y'$. Luego existen $f, f' \in F$ tales que $x \wedge f = x' \wedge f$ y $y \wedge f' = y' \wedge f'$, por lo cual se tiene que $x \wedge f \wedge y \wedge f' = x' \wedge f \wedge y' \wedge f'$. Como $f \wedge f' \in F$ se tiene que $x \wedge y \equiv_F x' \wedge y'$. De manera similar se puede probar que $x \vee y \equiv_F x' \vee y'$ si consideramos al elemento $f \wedge f'$.

A continuación probaremos que $F = |1|$. Sea $f \in F$. Como $f \wedge f = f \wedge 1$ tenemos que $f \equiv_F 1$, es decir, que $f \in |1|$. Recíprocamente, sea $f \equiv_F 1$. Luego existe $f' \in F$ tal que $f \wedge f' = 1 \wedge f' = f'$, con lo cual tenemos que $f' \leq f$. Como F es un filtro llegamos a que $f \in F$. Por lo tanto, $F = |1|$. □

Corolario 2.3.10. *Sea $a \in L$ y sea F el filtro principal generado por a. La relación $\equiv_F$ está dada por: $x \equiv_F y$ si y solo si $x \wedge a = y \wedge a$.*

Demostración. Se tiene que $F = [a)$. De este modo, $x \equiv_{[a)} y$ si y solo si existe $b \geq a$, $x \wedge b = y \wedge b$.

Veamos que basta tomar $b = a$. En efecto, si es $b \geq a$,

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

□

Surge naturalmente la siguiente pregunta: dado un retículo, ¿el conjunto de congruencias está en biyección con el conjunto de filtros? Veremos a través de un ejemplo que en general la respuesta es no.

Sea R la relación definida por la Figura 2.9. Tenemos que R es una congruencia y que $|1|$ es un filtro. Sin embargo, no "dirige" la congruencia. En efecto, aRe pero $a \wedge d = a \neq c = e \wedge d$ y $a \wedge 1 = a \neq e = e \wedge 1$. Es decir, no existe $f \in |1|$ tal que $a \wedge f = e \wedge f$. Pregunta (ejercicio): ¿cuál es la partición determinada por el filtro $|1| = \{d, 1\}$?

Veremos que en las álgebras de Boole la situación es diferente.

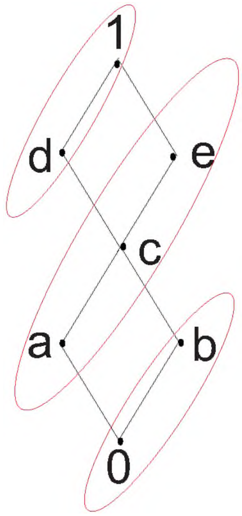


Figura 2.9: Congruencia de retículo

Lema 2.3.11. *Sea R una relación de equivalencia definida en un álgebra de Boole. Supongamos que R satisface las condiciones* (**Inf**) *y* (**Sup**)*. Luego xRy si y solo si $(x \to y)\, R\, 1$ y $(y \to x)\, R\, 1$ (ver 2.2.12).*

Demostración: Se deja al lector.

Corolario 2.3.12. *Sea R en las condiciones del Lema 2.3.11. Luego R satisface la condición* (**Comp**)*.*

Demostración. Sea xRy. Por el Lema 2.3.11 tenemos que $(\overline{x} \vee y)R1$ y $(\overline{y} \vee x)R1$, de donde, por la condición (**Inf**) tenemos que $(\overline{x} \vee y) \wedge (\overline{y} \vee x)R1$. Como vale que $\overline{x}R\overline{x}$, nuevamente aplicando la condición (**Inf**) se obtiene que

$$\overline{x}R(\overline{x} \wedge (\overline{x} \vee y) \wedge (\overline{y} \vee x)).$$

Como $\overline{x} \wedge (\overline{x} \vee y) \wedge (\overline{y} \vee x) = \overline{x} \wedge \overline{y}$ obtenemos que $\overline{x}R(\overline{x} \wedge \overline{y})$. Análogamente, tomando $\overline{y}R\overline{y}$ y operando obtenemos también que $\overline{y}R(\overline{x} \wedge \overline{y})$. Por lo tanto concluimos que $\overline{x}R\overline{y}$. □

Teorema 2.3.13. *Sea R una congruencia de un álgebra de Boole B. Luego $|1|$ es un filtro y R es la asociada a ese filtro. Es decir, xRy si y solo si existe $f \in |1|$ tal que $x \wedge f = y \wedge f$.*

Demostración. Notemos que $1 \in |1|$. Sea $x \in |1|$ e $y \geq x$. Luego $(x \wedge y)Ry$, dado que yRy. Como $x \wedge y = x$ tenemos que xRy, por lo cual $y \in |1|$. Sean ahora $x, y \in |1|$. Es inmediato que $x \wedge y \in |1|$. De este modo, $|1|$ es un filtro.

Sea xRy. Por el Lema 2.3.11 y por ser $|1|$ un filtro tenemos que $(x \to y) \wedge (y \to x) \in |1|$, es decir, $(x \to y) \wedge (y \to x)R1$. Además:

$$x \wedge (x \to y) \wedge (y \to x) = x \wedge y = y \wedge (x \to y) \wedge (y \to x).$$

Luego, tomando $f = (x \to y) \wedge (y \to x)$ tenemos que $x \wedge f = y \wedge f$. Recíprocamente, sea $f \in |1|$ tal que $x \wedge f = y \wedge f$. Como $fR1$ tenemos que $(x \wedge f)Rx$ (ya que xRx) y también tenemos que $(y \wedge f)Ry$. Por lo tanto, xRy. □

Sea B un álgebra de Boole. Sean Fil(B) el conjunto de los filtros de B y Con(B) el conjunto de las congruencias de B. El Teorema 2.3.9 establece un mecanismo que a cada filtro F le asigna la congruencia $\equiv_F$. Este mecanismo permite definir una función de Fil(B) en Con(B) dada por $F \mapsto \equiv_F$. Análogamente, el Teorema 2.3.13 permite definir otra función de Con(B) en Fil(B) dada por $R \mapsto |1|$. El corolario siguiente muestra que estas dos funciones son una inversa de la otra, estableciéndose entonces una biyección entre Fil(B) y Con(B).

Corolario 2.3.14. *Sea B un álgebra de Boole. Existe una biyección entre* Con(B) *y* Fil(B)*.*

Demostración. En el Teorema 2.3.9 se probó que, dado un filtro F, $\equiv_F$ es una congruencia. Además, si tomamos la clase del 1 por dicha congruencia, ella coincide con F. Recíprocamente, el Teorema 2.3.13 muestra que, dada una congruencia R, la clase del 1 por R, que llamamos $|1|$, es un filtro. También se prueba que la congruencia asociada a ese filtro es justamente R. □

Observación 2.3.15. Puede demostrarse (¡ejercicio!), en base a la demostración del Teorema 2.3.13 y al Lema 2.3.11, que dado un filtro F se verifica:

$$x \equiv_F y \text{ si y solo si } (\overline{x} \vee y) \wedge (\overline{y} \vee x) \in F.$$

Tomando el ideal $\overline{F}$, vemos que

$$(\overline{x} \vee y) \wedge (\overline{y} \vee x) \in F \text{ si y solo si } (x \wedge \overline{y}) \vee (y \wedge \overline{x}) \in \overline{F}.$$

De esta manera, vemos que da lo mismo tomar filtros o ideales para definir las congruencias. Es decir que hay una biyección entre los ideales y las congruencias de un álgebra de Boole, que podemos trasladar a una biyección entre los ideales y las congruencias del correspondiente anillo idempotente. Como dijimos para el caso de $\equiv_p$, las congruencias en un anillo son de la forma:

$$x \equiv_I y \text{ si y solo si } x - y \in I,$$

siendo I un ideal (la clase del 0). Pero por ser $x - y = x + y = (x \wedge \overline{y}) \vee (y \wedge \overline{x})$ esta última condición es equivalente a la anterior, tomando $I = \overline{F}$.

Podríamos preguntarnos si hay alguna manera de asociar filtros con congruencias en retículos de manera de establecer una biyección. El siguiente ejemplo prueba que no.

Sea L la cadena de tres elementos, digamos $\{0, a, 1\}$. Hay cinco particiones posibles de ese conjunto: $P_0 = \{\{0\}, \{a\}, \{1\}\}$, $P_1 = \{\{0\}, \{a, 1\}\}$, $P_2 = \{\{a\}, \{0, 1\}\}$, $P_3 = \{\{1\}, \{0, a\}\}$, $P_4 = \{\{0, a, 1\}\}$. De ellas, todas son congruencias menos P_2. Luego, tenemos cuatro congruencias. Sin embargo, hay solo tres filtros: $\{1\}$, $\{a, 1\}$, $\{0, a, 1\}$.

Para finalizar esta sección vamos a remarcar cuáles son los homomorfismos e isomorfismos de álgebras de Boole.

Sea $f : B \to B'$ una función, B y B' álgebras de Boole. Entonces f es un homomorfismo (respectivamente isomorfismo) de álgebras de Boole si f es un homomorfismo (respectivamente isomorfismo) de retículos acotados tal que preserva el complemento, i.e., tal que $f(\overline{x}) = \overline{f(x)}$.

Lema 2.3.16. *Sean B, B' álgebras de Boole y $f : B \to B'$ un homomorfismo de retículos acotados. Entonces, f es un homomorfismo de álgebras de Boole.*

Demostración. Para probar que $f(\overline{x})$ es el complemento de $f(x)$ debemos ver que $f(x) \wedge f(\overline{x}) = 1$ y que $f(x) \vee f(\overline{x}) = 0$, lo que se deduce porque f preserva $\wedge$, $\vee$, 0 y 1. $\square$

La congruencia R_f del lema que sigue fue definida en 1.1 de la Sección 1.

Lema 2.3.17. *Sea $f : B \to B'$ un homomorfismo de álgebras de Boole. El filtro asociado a la congruencia R_f es $f^{-1}(\{1\})$.*

Demostración. En primer lugar, probemos que $f^{-1}(\{1\})$ es un filtro.

Es obvio que $1 \in f^{-1}(\{1\})$. Si son $x, y \in B$ tales que $x \leq y$, $x \in f^{-1}(\{1\})$, se tiene que $f(x) = 1 = f(x \wedge y) = f(x) \wedge f(y) = 1 \wedge f(y) = f(y)$, o sea $y \in f^{-1}(\{1\})$. Además, si son $z, t \in f^{-1}(\{1\})$ entonces $f(z) \wedge f(t) = 1 = f(z \wedge t)$, por lo que $z \wedge t \in f^{-1}(\{1\})$.

El filtro asociado a R_f es la clase del 1, o sea que x está en el filtro si y solo si xR_f1 si y solo si $f(x) = f(1) = 1$ si y solo si $x \in f^{-1}(\{1\})$. $\square$

Corolario 2.3.18. *Si f es suryectivo, las álgebras de Boole $B/f^{-1}(\{1\})$ y B' son isomorfas.*

Demostración. Es consecuencia del Teorema 1.3.20 del Capítulo 1. $\square$

2.4. Teorema del filtro primo

Veremos aquí este teorema, que es de fundamental importancia dada por sus vinculaciones con otros teoremas y axiomas que están en los fundamentos de las teorías algebraicas que estamos considerando. Tal es el caso del axioma de elección o del Lema de Zorn (ver Sección 6 de este capítulo). Usaremos el Lema de Zorn para demostrar el teorema del filtro primo.

En adelante consideraremos solamente retículos distributivos.

Definición 2.4.1. Sea L un retículo.

1. Un elemento $p \in L$ se llama *primo* o $\vee$-*irreducible* si $p \neq 0$ (en caso de que L tenga primer elemento) y si $p = x \vee y$ implica que $p = x$ ó $p = y$.

2. Si L tiene mínimo 0, un elemento $a \neq 0$ es un *átomo* si $x \leq a$ implica que $x = 0$ ó $x = a$.

Observación 2.4.2. Pueden probarse como ejercicio las siguientes propiedades.

1. Sea L un retículo y $p \in L$. Luego p es primo si y solo si $p \leq x \vee y$ implica $p \leq x$ ó $p \leq y$.

2. Sea L un retículo con primer elemento, y sea $x \in L$. Si x es un átomo entonces x es primo.

Consideremos el retículo dado en Figura 2.2 de la Sección 2.1. En este caso los átomos son los números primos, y los únicos elementos que no son supremo de otros dos elementos son los números primos y sus potencias. Otros ejemplos de elementos primos en retículos están señalados en ls Figura 2.10.

Sea L un retículo. Un filtro P de L se denomina *propio* si $P \neq L$.

Definición 2.4.3. Sea L un retículo y P un filtro propio de L.

1. Diremos que P es un *filtro primo* si dado un par de elementos x e y de L tales que $x \vee y \in P$ se verifica que $x \in P$ ó $y \in P$.

2. Diremos que P es un *filtro maximal* o un *ultrafiltro* si los únicos filtros que lo contienen son P y L.

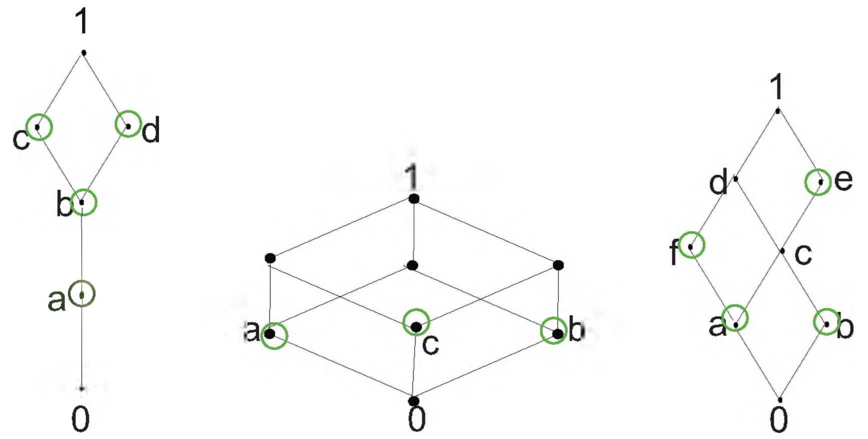


Figura 2.10: Átomos y elementos primos

Ejemplos 2.4.4.

1. Consideremos el álgebra de Boole $\mathcal{P}(\mathbb{N})$. Sea $\mathcal{C}(\mathbb{N})$ el filtro de los subconjuntos cofinitos de $\mathbb{N}$ (ver Sección 2.2). Este filtro no es primo. En efecto, sean A el conjunto de los números pares y B el conjunto de los números impares. Tenemos $A \cup B = \mathbb{N}$ (que es cofinito), y sin embargo ni A ni B son cofinitos. Obtendríamos el mismo resultado considerando un conjunto X cualquiera en lugar de $\mathbb{N}$.

2. Sea X un conjunto. Consideremos el álgebra de Boole $\langle Z(X), \cup, \cap, ^{cX}, \emptyset, X\rangle$ (ver Ejemplo 2 de la Sección 2.2), y el filtro $C(X)$. Este filtro es maximal. En efecto, supongamos que $U' \supset C(X)$, por lo cual U' debe contener algún conjunto finito Y. Pero $X - Y$ es un conjunto cofinito y pertenece a $C(X)$. Por esta razón $X - Y$ está en U'. Como en U' están Y y $X - Y$, entonces está su intersección, que es el conjunto el vacío. Por lo tanto $U' = Z(X)$. Observemos entonces que $C(X)$ es maximal en $Z(X)$ pero no en $\mathcal{P}(X)$, ya que en $\mathcal{P}(X)$ pueden existir conjuntos que no son finitos ni cofinitos.

3. En todo retículo finito los filtros primos son exactamente los filtros principales asociados a los elementos primos. Es decir, un filtro P es primo si y solo si existe un elemento primo p tal que $P = [p)$.

4. Sean X un conjunto y $x_0 \in X$. Consideremos el retículo distributivo acotado $\langle \mathcal{P}(X), \cup, \cap, \emptyset, X\rangle$, y definamos $U_0 = \{Y \subseteq X : x_0 \in Y\}$. Tenemos que U_0 es el filtro principal generado por $\{x_0\}$. Sea U un filtro tal que contiene estrictamente a U_0. Luego existe un $Y \subseteq X$, $Y \in U$

tal que $x_0 \notin Y$. Pero entonces $Y \subseteq \{x_0\}^c$, de donde $\{x_0\}^c \in U$, con lo cual $\emptyset \in U$. Es decir, $U = \mathcal{P}(X)$.

Este ejemplo es un caso particular de la siguiente propiedad: si a es un átomo de un álgebra de Boole, entonces $[a)$ es un ultrafiltro (probarlo como ejercicio).

Para demostrar el teorema del filtro primo necesitaremos algunos resultados que veremos a continuación.

Lema 2.4.5. *Sean L un retículo y X un subconjunto no vacío de L. Luego $F(X)$, el filtro generado por X (ver Definición 2.3.6) tiene la siguiente forma:*

$$F(X) = \{z \in L : z \geq x_1 \wedge x_2 \wedge \cdots \wedge x_n \text{ para ciertos } x_1, x_2, \ldots, x_n \in X\}.$$

Demostración. Sea

$$F_X = \{z \in L : z \geq x_1 \wedge x_2 \wedge \cdots \wedge x_n \text{ para ciertos } x_1, x_2, \ldots, x_n \in X\}.$$

Primero notemos que $X \subseteq F_X$ porque $x \geq x$ para todo $x \in X$.

A continuación veremos que F_X es un filtro. Como $X \subseteq F_X$ y $X \neq \emptyset$ tenemos que $F_X \neq \emptyset$. También tenemos que F_X es un conjunto creciente. Veamos que si $z, t \in F_X$ entonces $z \wedge t \in F_X$. Sean $z, t \in F_X$. Luego existen $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m, \in X$ tales que $z \geq x_1 \wedge x_2 \wedge \cdots \wedge x_n$ y $t \geq y_1 \wedge y_2 \wedge \cdots \wedge y_m$. En consecuencia tenemos que $z \wedge t \geq x_1 \wedge x_2 \wedge \cdots \wedge x_n \wedge y_1 \wedge y_2 \wedge \cdots \wedge y_m$, de donde se sigue que $z \wedge t \in F_X$.

Por último, probaremos que F_X es el menor filtro que contiene a X. Sea G un filtro que contiene a X. Sea $z \in F_X$, por lo cual existen $x_1, x_2, \ldots, x_n \in X$ tales que $z \geq x_1 \wedge x_2 \wedge \cdots \wedge x_n$. Como $X \subseteq G$ se tiene que $x_1 \wedge x_2 \wedge \cdots \wedge x_n \in G$. Teniendo ahora en cuenta que G es creciente se tiene que $z \in G$. Por esta razón tenemos que $F_X \subseteq G$. Por lo tanto hemos probado que $F_X = F(X)$. $\square$

Observación 2.4.6. Sean L un retículo y X un subconjunto no vacío de L. Luego $I(X)$, el ideal generado por X (ver Definición 2.3.6) tiene la siguiente forma:

$$I(X) = \{z \in L : z \leq x_1 \vee x_2 \vee \cdots \vee x_n \text{ para ciertos } x_1, x_2, \ldots, x_n \in X\}.$$

La prueba se deja como ejercicio.

El Lema 2.4.5 implica que si $X = \{x\}$ entonces $F(\{x\}) = [x)$ (el filtro principal generado por x), como se observó en 2.3.7 de la Sección 3.

Corolario 2.4.7. *Sea L un retículo, $x \in L$ y $X \subseteq L$. Si $X \neq \emptyset$ entonces*

$$F(X \cup \{x\}) = \{z \in L : z \geq x_1 \wedge x_2 \wedge \cdots \wedge x_n \wedge x \text{ para ciertos } x_1, x_2, \ldots, x_n \in X\}.$$

Si $X = \emptyset$ entonces $F(X \cup \{x\}) = [x)$.

Corolario 2.4.8 (Teorema algebraico de la deducción). *Sea L un álgebra de Boole. Sean $x, y \in L$ y $X \subseteq L$. Luego*

$$y \in F(X \cup \{x\}) \text{ si y solo si } x \to y \in F(X).$$

Corolario 2.4.9. *Sea L un retículo y G un filtro de L. Luego*

$$F(G \cup \{x\}) = \{z \in L : z \geq g \wedge x \text{ para cierto } g \in G\}.$$

Lema 2.4.10. *Sea L un retículo.*

(a) *Si P es un filtro maximal entonces P es un filtro primo.*

(b) *Sea L un álgebra de Boole. Si P un filtro primo entonces P es un filtro maximal.*

Demostración. (a) Sean $x, y \in L$ tales que $x \vee y \in M$. Supongamos que $x \notin M$, por lo cual el filtro generado por $M \cup \{x\}$ es L. Luego por el Corolario 2.4.9 tenemos que existe $m \in M$ tal que $0 = x \wedge m$. En consecuencia, $(x \vee y) \wedge m = (x \wedge m) \vee (y \wedge m) \in M$ porque $x \vee y \in M$ y $m \in M$. Como $(x \wedge m) = 0$ e $y \geq y \wedge m$ concluimos que $y \in M$.

(b) Sea P un filtro primo. Sea F un filtro tal que $P \subset F$, y sea $x \in F - P$. Como $1 \in P$ y $1 = x \vee \overline{x}$ tenemos que $\overline{x} \in P$. Luego $\overline{x} \in F$, de donde se sigue que $0 \in F$. Por lo tanto $F = L$. □

Corolario 2.4.11. *Sea L un álgebra de Boole, P un filtro de L, $p \in L$.*

(a) *P es un filtro primo si y solo si P es un filtro maximal.*

(b) *p es un elemento primo si y solo si p es un átomo.*

Demostración. La afirmación (a) es consecuencia del Lema 2.4.10.

Probemos la afirmación (b). Por la Observación 2.4.2 tenemos que todo átomo es un elemento primo. Recíprocamente, sea p un elemento primo y supongamos que $x \leq p$. Como $p = p \wedge (x \vee \overline{x})$ tenemos que $p = (p \wedge x) \vee (p \wedge \overline{x})$. Utilizando que p es primo tenemos que $p = p \wedge x$ o bien $p = p \wedge \overline{x}$. En el primer caso resulta $x \geq p$, de donde $x = p$. En el segundo resulta que $p \leq \overline{x}$, por lo cual tomando ínfimos con x obtenemos que $p \wedge x \leq \overline{x} \wedge x = 0$, de donde se deduce que $p \wedge x = 0$ (es decir, $x = 0$). Luego, p es un átomo. □

Ejemplo 2.4.12. En la Figura 2.11 se muestra un ejemplo de filtro primo que no es maximal en un retículo.

Teorema 2.4.13 (Teorema del filtro primo). *Sean L un retículo distributivo, F un filtro e I un ideal tales que $F \cap I = \emptyset$. Entonces existe un filtro primo P tal que $P \supseteq F$ y $P \cap I = \emptyset$.*

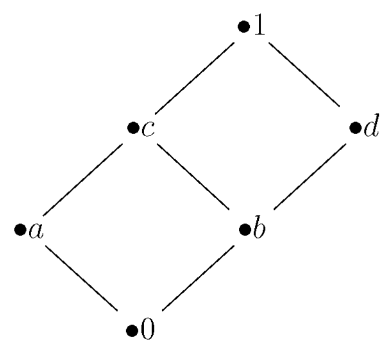


Figura 2.11: [d) primo no maximal

Demostración. Sea $\mathcal{T}$ la familia de filtros de L que contienen a F y que son disjuntos con I. Como $F \in \mathcal{T}$ tenemos que $\mathcal{T} \neq \emptyset$. Si $(F_k)_k$ es una cadena de filtros de $\mathcal{T}$ entonces se puede probar que $\bigcup F_k$ está en $\mathcal{T}$. Luego aplicando el Lema de Zorn tenemos que $\mathcal{T}$ tiene un elemento maximal P. En particular, $P \supseteq F$ y $P \cap I = \emptyset$. Por esta segunda condición P es un filtro propio. A continuación probaremos que P es primo.

Sean x, y tales que $x \vee y \in P$. Supongamos que $x \notin P$ y que $y \notin P$. Sea $V = F(P \cup \{x\})$. La maximalidad de P con respecto a $\mathcal{T}$ implica que V no puede estar en $\mathcal{T}$. Como $F \subseteq P \subset V$ tenemos que $V \cap I \neq \emptyset$. Luego existe $i \in I \cap V$, por lo cual $i \geq s \wedge x$, para algún $s \in P$. Análogamente, sea $W = F(P \cup \{y\})$ y sea $j \in I \cap W$. Tenemos que $j \geq t \wedge y$, para algún $t \in P$. Por esta razón obtenemos que $i \vee j \in I$ y además

$$i \vee j \geq (s \wedge x) \vee (t \wedge y) = (s \vee t) \wedge (x \vee t) \wedge (s \vee y) \wedge (x \vee y).$$

Como $(s \vee t)$, $(x \vee t)$, $(s \vee y)$, $(x \vee y)$ pertenecen a P, se tiene que $i \vee j \in P$. Por lo tanto $i \vee j \in I \cap P$, lo cual es un absurdo. □

Sean L un retículo e I un ideal propio de L (es decir, un ideal tal que $I \neq L$). Diremos que I es un *ideal primo* de L si para cada $x, y \in L$ se cumple que si $x \wedge y \in I$ entonces $x \in I$ o bien $y \in I$.

El Teorema del filtro primo (TFP) es equivalente al Teorema del ideal primo (TIP) (ver [2]), cuyo enunciado es el siguiente:

Teorema 2.4.14 (Teorema del ideal primo)**.** *Sean L un retículo distributivo, I un ideal y F un filtro tales que $F \cap I = \emptyset$. Entonces existe un ideal primo J tal que $J \supseteq I$ y $J \cap F = \emptyset$.*

Para demostrar (TIP) basta considerar (TFP) en el retículo dual del dado. Recíprocamente, se puede demostrar el (TFP) utilizando el (TIP).

Corolario 2.4.15. *Sean L un retículo distributivo, F un filtro y $x \notin F$. Entonces existe un filtro primo P tal que $F \subseteq P$ y $x \notin P$.*

Demostración. Es consecuencia del (TFP) tomando $I = (x]$. □

Teorema 2.4.16. *Sean L un álgebra de Boole y F un filtro propio. Entonces existe un ultrafiltro U tal que $F \subseteq U$.*

Demostración. Sabemos que $F \neq L$, con lo cual $0 \notin F$. De este modo podemos aplicar el Corolario 2.4.15. □

La prueba del siguiente corolario se deja como ejercicio.

Corolario 2.4.17. *Si L es un álgebra de Boole y x es un elemento no nulo de L, entonces existe un ultrafiltro U tal que $x \in U$.*

El Corolario 2.4.17 también vale en el contexto de retículos con primer elemento (ver, por ejemplo, [2, ch. III, 6, Th. 1]).

Corolario 2.4.18. *Sea L un retículo distributivo, $x, y \in A$, $x \nleq y$. Luego existe un filtro primo P tal que $x \in P$, $y \notin P$.*

Demostración. Considerar $I = (y]$ y $F = [x)$. Luego aplicar (TFP). □

Corolario 2.4.19. *Sea L un retículo distributivo finito, $x, y \in A$, $x \nleq y$. Existe un elemento primo p tal que $p \leq x$, $p \nleq y$.*

Demostración. En efecto, $P = [p)$ para algún elemento primo p. □

Teorema 2.4.20. *Sean L un álgebra de Boole y U un filtro de L. Entonces U es un ultrafiltro de L si y solo si $L/\equiv_U$ es isomorfo a $\mathbf{2}$.*

Demostración. Sea U ultrafiltro de L. Luego $U = |1|$ por la congruencia $\equiv_U$. Veremos que si $x \notin U$ entonces $x \in |0|$. Definimos

$$U' = F(U \cup \{x\}) = \{y \in A : y \geq x \wedge u \text{ para algún } u \in U\}.$$

Tenemos que U' es un filtro, que $x \in U'$ y que $U \subseteq U'$ (ya que para $u \in U$,$u \geq x \wedge u$ implica $u \in U'$). Además $U \neq U'$, pues $x \in U' - U$. Luego, por ser U maximal se concluye que $U' = A$. Luego, $0 \in U'$, es decir, existe $u \in U$ tal que $0 = x \wedge u = 0 \wedge u$. Por lo tanto, $x \equiv_U 0$.

Recíprocamente, supongamos que el cociente $L/\equiv_U$ es isomorfo al álgebra de Boole $\mathbf{2}$. Sea U' un filtro tal que $U' \supseteq U$. Sea $x \in U' - U$. Luego $x \equiv_U 0$, de donde resulta que $\overline{x} \equiv_U 1$. Es decir, $\overline{x} \in U$. Pero esto implica que $x, \overline{x} \in U'$, con lo cual $0 \in U'$. Por lo tanto $U' = L$. □

Corolario 2.4.21. *Si U es ultrafiltro, y si $x \notin U$, entonces $\overline{x} \in U$.*

Observación 2.4.22. Si L es un álgebra de Boole no trivial y U es un ultrafiltro de L (que sabemos que existe por el Corolario 2.4.17) entonces vamos a considerar la función $X_U : L \to \mathbf{2}$ dada por $X_U(x) = 1$ si $x \in U$ y $X_U(x) = 0$ si $x \notin U$ (X_U es la función característica de U).

En el siguiente diagrama llamamos f al isomorfismo dado por el Teorema 2.4.20 y p a la aplicación canónica al cociente. Resulta entonces que $X_U = f \circ p$ es un homomorfismo.

$$\begin{tikzcd}
L \arrow[r, "X_U"'] \arrow[d, "p"] & \mathbf{2} \\
L/\equiv_U \arrow[ur, "f"'] &
\end{tikzcd}$$

Corolario 2.4.23. *Sea L un álgebra de Boole no trivial. La función F definida por $F(U) = X_U$ es una biyección entre el conjunto de ultrafiltros de L y el conjunto de homomorfismos de L en $\mathbf{2}$.*

Demostración. La inyectividad de F es consecuencia directa de la definición.

Para probar que F es suryectiva, sea $h : L \to \mathbf{2}$ un homomorfismo. Hemos visto en el Lema 2.3.17 de la Sección 3 que $h^{-1}(\{1\})$ es un filtro de L. En lo que sigue escribiremos U en lugar de $h^{-1}(\{1\})$. Probaremos a continuación que U es un filtro primo. Sea $x \vee y \in U$, es decir, $h(x \vee y) = 1$. Como $h(x \vee y) = h(x) \vee h(y)$ debe valer que $h(x) = 1$ o $h(y) = 1$, con lo cual $x \in U$ o $y \in U$. Como en álgebras de Boole todo filtro primo es un ultrafiltro, tenemos que U es un ultrafiltro. De la definición de F se desprende que $F(U) = h$, lo cual prueba la suryectividad de F.

Por lo tanto, F es una función biyectiva. □

2.5. Teoremas de Birkhoff y Stone

El teorema de G. Birkhoff que vamos a mostrar establece una dualidad entre retículos distributivos finitos y conjuntos ordenados. La idea central es que “toda la información” del retículo está concentrada en el conjunto ordenado de sus elementos primos. Dado este conjunto, puede construirse el retículo y recíprocamente. Veremos más adelante que este resultado se generaliza, extendiéndose a una dualidad que vincula a un retículo distributivo acotado cualquiera con el conjunto ordenado de sus filtros primos munido de una cierta topología.

El teorema de Stone que caracteriza a las álgebras de Boole finitas como álgebras de partes de un conjunto resulta un corolario del teorema de

Birkhoff, dado que en las álgebras de Boole finitas los elementos primos son exactamente los átomos. El teorema de Stone para el caso general dice que toda álgebra de Boole es isomorfa a una subálgebra de un álgebra de partes.

Observación 2.5.1. Sea $\langle L, \vee, \wedge, 0, 1\rangle$ un retículo finito. Llamaremos L^{pr} al conjunto de sus elementos primos. ¿Qué estructura tiene L^{pr}? Sabemos que tiene un orden, el inducido por el $\leq$ de L. Pero también podemos dotar a L^{pr} del orden dual, con lo cual tendremos el conjunto ordenado $(L^{pr}, \leq^o)$. Éste es el que consideraremos en el siguiente teorema.

Teorema 2.5.2 (Birkhoff). *Sean $\langle L, \vee, \wedge, 0, 1\rangle$ un retículo distributivo finito y $(L^{pr}, \leq^o)$ el conjunto de sus elementos primos con el orden dual del inducido por el de L. Sea $(L^{pr})^+$ el conjunto de los conjuntos crecientes de $(L^{pr}, \leq^o)$. El retículo $\langle (L^{pr})^+, \cup, \cap, \emptyset, L^{pr}\rangle$ es isomorfo al retículo $\langle L, \vee, \wedge, 0, 1\rangle$.*

Demostración. Sea $\sigma : L \longrightarrow (L^{pr})^+$ la función definida como

$$\sigma(x) = \{p \in L^{pr} : p \leq x\}.$$

Si $q \geq^o p$ para $p \in \sigma(x)$, se tiene que $q \leq p$, de donde resulta $q \in \sigma(x)$. Luego, $\sigma(x)$ es creciente, o sea que σ está bien definida.

Veamos que $\sigma(x)$ es una biyección.

Para probar que σ es inyectiva, sean $x, y \in L$ tales que $\sigma(x) = \sigma(y)$. Por lo tanto no existe p tal que $p \leq x$, $p \not\leq y$. Luego, por el Corolario 2.4.19, $x \leq y$. Análogamente, $y \leq x$. Luego, $x = y$.

Probaremos ahora que σ es una función suryectiva. Sea $C \in (L^{pr})^+$. Siendo C finito, existen $p_1, \ldots, p_n \in L^{pr}$ tales que $C = \{p_1, p_2, \ldots, p_n\}$. Consideremos el elemento $u = p_1 \vee p_2 \vee \cdots p_n$. Vamos a mostrar que $\sigma(u) = C$, es decir, que $C = \{p \in L^{pr} : p \leq u\}$. La inclusión $C \subseteq \sigma(u)$ resulta inmediata. Recíprocamente, sea $q \leq u$. En particular, tenemos que

$$q \wedge u = q = q \wedge (p_1 \vee p_2 \vee \cdots \vee p_n) = (q \wedge p_1) \vee (q \wedge p_2) \vee \cdots \vee (q \wedge p_n).$$

Como $q \in L^{pr}$ entonces existe $i \in \{1, \ldots, n\}$ tal que $q = q \wedge p_i$. Es decir, $q \leq p_i$ (o sea, $q \geq^o p_i$ en L^{pr}) para algún $p_i \in C$. Como C es creciente obtenemos que $q \in C$.

Finalmente veremos que σ preserva las operaciones. Es inmediato que $\sigma(0) = \emptyset$ y que $\sigma(1) = L^{pr}$. La igualdad $\sigma(x \wedge y) = \sigma(x) \cap \sigma(y)$ es consecuencia directa de la definición de ínfimo. La igualdad $\sigma(x \vee y) = \sigma(x) \cup \sigma(y)$ es consecuencia directa del hecho de que los elementos de $\sigma(x \vee y)$ son primos. $\square$

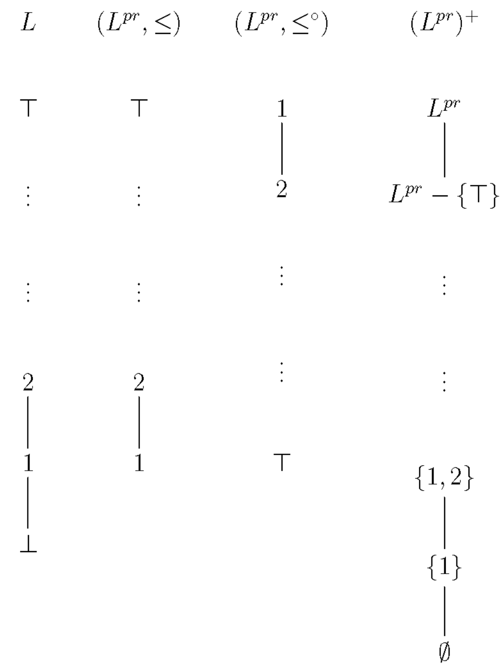


Figura 2.12: $\mathbb{N}$ con $\top$

Observación 2.5.3. Podríamos preguntarnos si para un retículo distributivo acotado cualquiera también vale este teorema. El ejemplo de la Figura 2.12 prueba que no es así. El retículo L considerado es el definido por el conjunto ordenado de los naturales (denotamos el mínimo con $\perp$) al cual agregamos un elemento máximo $\top$. Todos sus elementos distintos de $\perp$ son primos. Consideremos en L^{pr} el orden dual y calculemos los conjuntos crecientes. Ellos son $\emptyset$, $\{1\}$, $\{1,2\}$,..., $\{1,2,\ldots,n\}$,..., $L^{pr} - \{\top\}$, L^{pr}, como se ve en la figura. La función σ queda definida por: $\sigma(\perp) = \emptyset$, $\sigma(1) = \{1\}$, $\sigma(2) = \{1,2\}$,..., $\sigma(n) = \{1,2,\ldots,n\}$,..., $\sigma(\top) = L^{pr}$ (pues el último elemento debe ir al último elemento). Observamos que la función no es suryectiva, ya que $L^{pr} - \{\top\}$ no es imagen de ningún elemento.

Si en lugar de tomar el conjunto de elementos primos tomáramos el de los filtros primos la situación no cambiaría, ya que todos ellos son principales.

En el Teorema 2.5.2 mostramos que, si partimos de un retículo finito, en dos "pasos" podemos obtener un retículo isomorfo al dado. Los pasos son: (1°) construir el conjunto ordenado de sus elementos primos y (2°) construir el retículo de los conjuntos crecientes de este conjunto ordenado. A continuación veremos que si se tiene un conjunto ordenado finito, entonces haciendo las mismas construcciones (los mismos dos pasos) pero en orden inverso, obtenemos un conjunto ordenado isomorfo al dado (ver 1.2.4). Tenemos así una "dualidad" entre retículos distributivos finitos y conjuntos ordenados.

Pero primero debemos probar el siguiente lema.

Lema 2.5.4. *Sea $(P,\leq)$ un conjunto ordenado finito. Sea $\langle P^+,\cup,\cap,\emptyset,P\rangle$ el retículo acotado en el cual P^+ es el conjunto de los conjuntos crecientes de P. Sea $(P^+)^{pr}$ el conjunto de los elementos primos de P^+. Entonces tenemos que $C\in P^+$ si y solo si $C=\bigcup_{x\in C}[x)$. Además, $C\in(P^+)^{pr}$ si y solo si existe $x\in P$ tal que $C=[x)$.*

Demostración. En primer lugar, como para cada $x\in C$, $[x)\subseteq C$ (pues C es creciente), se tiene: $\bigcup_{x\in C}[x)\subseteq C$. Por otra parte, si $x\in C$, es $x\in[x)$ luego $x\in\bigcup_{x\in C}[x)$, de donde $C\subseteq\bigcup_{x\in C}[x)$.

Sea $C\in P^+$, C primo. Por lo anterior: $C=[x_1)\cup[x_2)\cup\cdots,[x_n)$, siendo $C=\{x_1,x_2,\ldots,x_n\}$. Pero si C es el supremo de los $[x_1),[x_2),\ldots,[x_n)$, por ser primo, debe ser igual a uno de ellos: existe i tal que $C=[x_i)$. Recíprocamente, sea $C=[x)$ y supongamos que existen C_1 y C_2 en P^+ tales que $C=C_1\cup C_2$. Pero $x\in C_1$ o $x\in C_2$. Luego, $[x)\subseteq C_1$ o $[x)\subseteq C_2$. Como (por ser unión de ambos) $C\supseteq C_1$ y $C\supseteq C_2$, se tiene que $C=C_1$ o $C=C_2$. Luego, C es primo. □

Teorema 2.5.5. *Sea $(P,\leq)$ un conjunto ordenado finito. Sean P^+ y $(P^+)^{pr}$ como en el lema anterior. El conjunto ordenado $((P^+)^{pr},\subseteq^o)$ es isomorfo a $(P,\leq)$.*

Demostración. Sea $\rho:P\longrightarrow(P^+)^{pr}$ definida por $\rho(x)=[x)$. Probaremos que es un isomorfismo de conjuntos ordenados.

Por el lema anterior vemos que ρ está bien definida.

Sea $\rho(x)=\rho(y)$, o sea $[x)=[y)$. Luego: $x\in[y)$, de donde $x\leq y$. Análogamente, $y\leq x$. Por lo tanto, ρ es inyectiva.

Sea $C\in(P^+)^{pr}$. Por el lema anterior, existe $x\in P$ tal que $C=[x)$; luego, ρ es suryectiva.

Además preserva el orden: se tiene $x\leq y$ si y solo si $[x)\supseteq[y)$ si y solo si $[x)\subseteq^o[y)$.

Por lo tanto ρ es un isomorfismo de orden. □

Ejemplo 2.5.6. En la Figura 2.13 se da un conjunto ordenado P y al lado el retículo P^+, en el que hemos indicado abreviadamente los conjuntos crecientes. Por ejemplo, al conjunto $\{r,s,t\}$ lo indicamos rst.

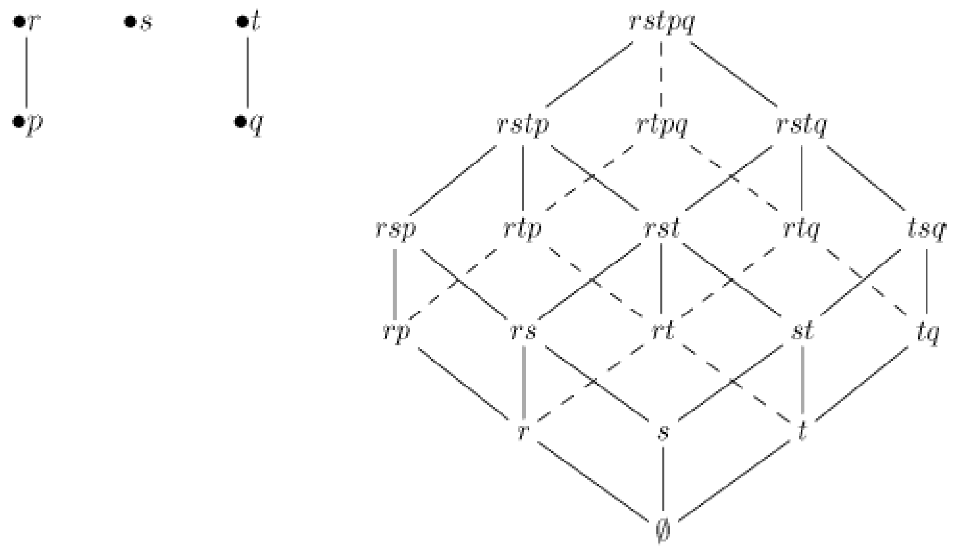


Figura 2.13: Construcción de Birkhoff

Álgebras de Boole

Aplicaremos primero el Teorema 2.5.2 para caracterizar a las álgebras de Boole finitas.

Observación 2.5.7. Por el Corolario 2.4.11 sabemos que todo elemento primo de un álgebra de Boole B es un átomo. Además, de la definición de átomo se deduce que si a y b son átomos, ellos no son comparables. Por lo tanto, si A es el conjunto de átomos de B, entonces $A = B^{pr}$ y $(B^{pr})^+ = \mathcal{P}(A)$.

Teorema 2.5.8 (Stone). *Si B es un álgebra de Boole finita, A el conjunto de sus átomos, entonces $\langle B, \vee, \wedge, ^-, 0, 1\rangle$ es isomorfa a $\langle \mathcal{P}(A), \cup, \cap, ^c, \emptyset, A\rangle$.*

Demostración. Es consecuencia del Teorema 2.5.2 y del Corolario 2.3.16. □

Observación 2.5.9. Para intuir cómo puede ser la generalización del teorema anterior al caso general, pensemos lo siguiente: en un retículo finito, todo filtro es principal y los filtros primos están en biyección con los elementos primos ¿Bastará entonces reemplazar en el teorema "elemento primo" o "átomo" por "filtro primo"? Los filtros principales generados por los átomos son ultrafiltros, es decir, primos. Observemos que el orden de los filtros principales es el dual del de los elementos. En efecto, $p \leq q$ si y solo si $[p) \supseteq [q)$. Además, si p es un elemento primo, $x \geq p$ si y solo si $x \in [p)$. Con estas ideas en mente, vayamos a la demostración del teorema de Stone. Dos capítulos más adelante lo demostraremos de otra manera: como corolario de un resultado para álgebras de Heyting.

Teorema 2.5.10 (Stone). *Toda álgebra de Boole B es isomorfa a una subálgebra del álgebra de Boole $\langle \mathcal{P}(B^\star), \cup, \cap, ^c, \emptyset, B^\star \rangle$, siendo $B^\star$ el conjunto de los ultrafiltros de B.*

Demostración. Sea $\sigma : B \longrightarrow \mathcal{P}(B^\star)$ la aplicación definida por:

$$\sigma(x) = \{U \in B^\star : x \in U\}.$$

Veamos que es un homomorfismo. Basta probar que σ preserva el ínfimo, el supremo, el 0 y el 1 (ver Lema 2.3.16 en Sección 4).

$$\begin{aligned} U \in \sigma(x \vee y) \text{ si y solo si } & x \vee y \in U \\ \text{si y solo si } & x \in U \ \text{ o } \ y \in U, \text{ pues } U \text{ es primo} \\ \text{si y solo si } & U \in \sigma(x) \ \text{ o } \ U \in \sigma(y) \\ \text{si y solo si } & U \in \sigma(x) \cup \sigma(y). \end{aligned}$$

Luego, $\sigma(x \vee y) = \sigma(x) \cup \sigma(y)$.

$$\begin{aligned} U \in \sigma(x \wedge y) \text{ si y solo si } & x \wedge y \in U \\ \text{si y solo si } & x \in U \ \text{ e } \ y \in U, \text{ por ser } U \text{ filtro} \\ \text{si y solo si } & U \in \sigma(x) \ \text{ y } \ U \in \sigma(y) \\ \text{si y solo si } & U \in \sigma(x) \cap \sigma(y). \end{aligned}$$

Luego, $\sigma(x \wedge y) = \sigma(x) \cap \sigma(y)$.

Como ningún ultrafiltro contiene al 0 y todos contienen al 1, $\sigma(0) = \emptyset$ y $\sigma(1) = B^\star$.

Probemos la inyectividad.

Sea $\sigma(x) = \sigma(y)$ y supongamos que es $x \neq y$, por ejemplo, $x \not\leq y$. Por el (TFP) existe un ultrafiltro U tal que $x \in U$, $y \notin U$. Pero entonces $U \in \sigma(x)$, $U \notin \sigma(y)$, que contradice lo supuesto.

Luego, B es isomorfa a $\sigma(B)$. □

Álgebras libres finitas

Aplicando estos resultados, daremos una descripción de las álgebras de Boole con un número finito de generadores libres. Probaremos en primer lugar que son finitas y veremos cuáles son sus átomos.

Dado un elemento x de un álgebra de Boole, denotaremos $x^0 = \overline{x}$ y $x^1 = x$. Con esta convención, llamaremos *conjunciones elementales* en el conjunto de variables $X = \{x_1, x_2, \ldots, x_n\}$ a las expresiones de la forma $x_1^{i_1} \wedge x_2^{i_2} \wedge \cdots \wedge x_n^{i_n}$, para $i_j = 0$ o $i_j = 1$, $j = 1, \ldots, n$.

Teorema 2.5.11. *El álgebra de Boole libre generada por un conjunto de n elementos tiene 2^{2^n} elementos. Sus átomos son las conjunciones elementales.*

Demostración. Sea $X = \{x_1, x_2, \ldots, x_n\}$ un conjunto, $f : X \longrightarrow \mathbf{2}$ una aplicación. Existe un homomorfismo $h : \mathbb{F}_n \longrightarrow \mathbf{2}$, siendo $\mathbb{F}_n$ el álgebra de Boole libre generada por X, tal que $h(x_i) = f(x_i)$ para $i = 1, 2, \ldots, n$. Por el Corolario 2.4.23 de la sección anterior, $h^{-1}(\{1\})$ es un ultrafiltro de $\mathbb{F}_n$. Entonces para cada $f : X \longrightarrow \mathbf{2}$ hay un ultrafiltro $\mathbb{F}_n$. Recíprocamente, dado un ultrafiltro U, podemos tomar la aplicación $f : X \longrightarrow \mathbb{F}_n/U$, donde f es la restricción a X de la aplicación al cociente, pues, por el Teorema 2.4.20 de la sección anterior, es $\mathbb{F}_n/U \cong \mathbf{2}$. Luego, hay una biyección entre ultrafiltros y aplicaciones.

¿Cuántas aplicaciones hay? Como X tiene n elementos y para cada uno hay dos posibilidades (asignarle 0 o 1) habrá 2^n aplicaciones. Por lo tanto, 2^n ultrafiltros en $\mathbb{F}_n$. El número 2^n es entonces el número de elementos del conjunto $\mathbb{F}_n^\star$, siendo entonces este un conjunto finito. También será finito entonces el conjunto $\mathcal{P}(\mathbb{F}_n^\star)$, que como es sabido (ver Capítulo 1, 1.1.1), tiene 2^{2^n} elementos. Por el teorema de Stone resulta entonces que $\mathbb{F}_n \cong \mathcal{P}(\mathbb{F}_n^\star)$ y, por lo tanto, $\mathbb{F}_n$ tiene también 2^{2^n} elementos.

Para cada aplicación f, sea $f(x_j) = i_j$, para $j = 1, \ldots, n$. Entonces: si $i_j = 0$ es $h(x_j) = f(x_j) = 0$ por lo que $h(\overline{x_j}) = 1$, o sea $\overline{x_j} \in h^{-1}\{1\}$. Si $i_j = 1$ es $h(x_j) = f(x_j) = 1$ por lo que $h(x_j) = 1$, o sea $x_j \in h^{-1}\{1\}$. Es decir que: $x_j^{i_j} \in h^{-1}\{1\}$, para $j = 1, \ldots, n$.

Sea la conjunción elemental $c_{i_1 \ldots i_n} = x_1^{i_1} \wedge x_2^{i_2} \wedge \cdots \wedge x_n^{i_n}$. Entonces, por ser $h^{-1}\{1\}$ filtro, $c_{i_1 \ldots i_n} \in h^{-1}\{1\}$. Es fácil ver que $h^{-1}\{1\} = [c_{i_1 \ldots i_n})$, o sea que, por ser $h^{-1}\{1\}$ ultrafiltro, $c_{i_1 \ldots i_n}$ es un átomo. □

Observación 2.5.12. Observemos que, por el teorema de Stone para el caso finito, todo elemento de $\mathbb{F}_n$ es supremo de conjunciones elementales. El diagrama de la Figura 2.14 muestra el álgebra de Boole libre con el conjunto de generadores $X = \{x, y\}$ de dos elementos.

Interpolación "algebraica"

Daremos aquí una versión algebraica del Lema de interpolación de Craig basada en propiedades de las álgebra de Boole libres finitas. Más adelante daremos también la formulación usual.

En primer lugar, observemos que si tenemos un conjunto X de n elementos incluido en otro de m elementos Y se verifica que $\mathbb{F}_n \subseteq \mathbb{F}_m$. En efecto, cada elemento de X está en $\mathbb{F}_m$, por lo tanto también están las conjunciones básicas que son los átomos de $\mathbb{F}_n$, por lo tanto cada elemento de $\mathbb{F}_n$, por ser supremo

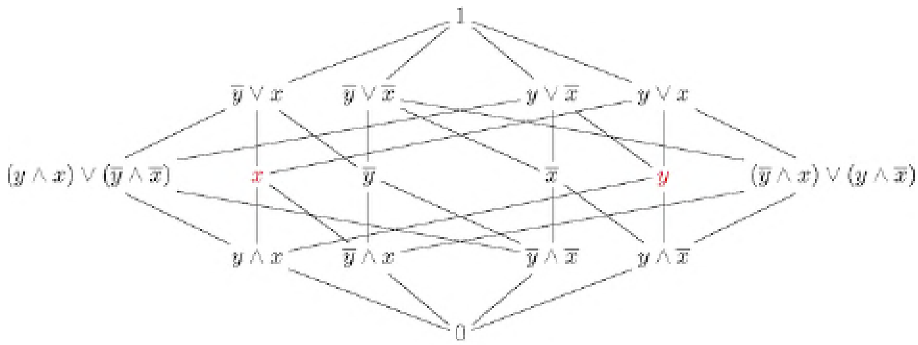


Figura 2.14: $\mathbb{F}_2$

de conjunciones básicas, también estará en $\mathbb{F}_m$. Llamaremos indistintamente, para un conjunto finito T de t elementos, $\mathbb{F}(T)$ o $\mathbb{F}_t$ al álgebra de Boole libre generada por T.

Teorema 2.5.13. *Sean X, Y conjuntos finitos con intersección no vacía. Sean $u \in \mathbb{F}(X)$, $v \in \mathbb{F}(Y)$ tales que, considerados como elementos de $\mathbb{F}(X \cup Y)$, verifican $u \leq v$. Existe $w \in \mathbb{F}(X \cap Y)$ tal que $u \leq w \leq v$.*

$$\begin{tikzcd}
\mathbb{F}(X \cap Y) \arrow[r, "inc"] \arrow[d, "inc"'] & \mathbb{F}(X) \arrow[d, "inc"] \\
\mathbb{F}(Y) \arrow[r, "inc"'] & \mathbb{F}(X \cup Y)
\end{tikzcd}$$

Demostración. Sea $X = \{x_1, x_2, \ldots, x_n\}$, sean u, v como en el enunciado. Demostraremos la existencia de w por inducción sobre el número n de elementos de X.

En primer lugar, lo demostraremos para el caso en que u sea un átomo, es decir, una de las conjunciones básicas.

Si $n = 1$, será $X = \{x\}$ y $\mathbb{F}(X) = \{0, x, \overline{x}, 1\}$. Luego u es x o $u = \overline{x}$ (los otros casos son triviales), o sea: $x \leq v$ o $\overline{x} \leq v$. Entonces, x debe ser una variable que figure en v, porque si fueran independientes no serían comparables. Por lo tanto, $x \in X \cap Y$ y tomando $w = u$ se tiene lo pedido.

Supongamos que la propiedad vale para todo conjunto X de $k-1$ elementos. Sea u con variables en un conjunto X de k elementos, $u = c_{i_1 \ldots i_k}$ átomo, $u \leq v$. Si todas las variables de u están en v, de nuevo resulta u mismo el w buscado. Si no, sea x_r una variable de u que no es variable de v.

Construimos u' a partir de u reemplazando x_r por 1 si $i_r = 1$ y por 0 si $i_r = 0$. Es decir, si $u = x_1^{i_1} \wedge \cdots \wedge x_r^{i_r} \wedge \cdots \wedge x_k^{i_k}$ entonces $u' = x_1^{i_1} \wedge \cdots \wedge 1 \wedge \cdots \wedge x_k^{i_k}$.

Luego, como $u = u' \wedge x_r$ o $u = u' \wedge \overline{x}_r$ resulta $u \leq u'$ y , como x_r no es variable de v, sigue siendo $u' \leq v$.

Como u' tiene variables en $X' = X - \{x_r\}$ que tiene $k-1$ elementos, podemos aplicar la hipótesis inductiva: existirá w con variables en $X' \cap Y$ tal que $u' \leq w \leq v$. Luego, como $X \subseteq X'$ tenemos que existe w con variables en $X \cap Y$ que verifica lo pedido.

Veamos ahora el caso general.

Sea $u \in \mathbb{F}(X)$. Luego, por ser $\mathbb{F}(X)$ finita, $u = \bigvee a_t$ es supremo finito de átomos. Si $u \leq v$, entonces para cada átomo a_t debe ser $a_t \leq v$. Luego, por la primera parte existe w_t tal que $a_t \leq w_t \leq v$. Pero entonces $w = \bigvee w_t$ cumple lo pedido. □

2.6. Sobre el axioma de elección

Expondremos brevemente aquí, a modo de apéndice, algunos resultados referentes al axioma de elección. Para profundizar el tema pueden consultarse los textos mencionados como referencia.

El *axioma de elección* fue enunciado por Zermelo en 1904 y dice lo siguiente:

AE Para todo conjunto no vacío de conjuntos $\mathcal{T}$ cuyos elementos son no vacíos existe un conjunto X que contiene un elemento y solo uno de cada conjunto de $\mathcal{T}$.

Fue probado que **AE** es equivalente a cada uno de los siguientes enunciados (ver [85], [93]).

LZ (Lema de Zorn) Dado un conjunto ordenado $(P, \leq)$, si todo subconjunto totalmente ordenado de P tiene una cota superior entonces P tiene un elemento maximal.

PBO (Postulado de buena ordenación) Existe un buen orden sobre todo conjunto (buen orden fue definido en 1.2.5).

Otro resultado importante es que **AE** implica el Teorema del filtro primo (TFP). Sin embargo, estos enunciados no resultan equivalentes ([55], [56]).

En la Sección 5 se vio que (TFP) es equivalente a (TIP). Los siguientes enunciados son también equivalentes al (TIP) (y también son equivalentes a los que usan filtros en lugar de ideales). La demostración de la equivalencia entre ellos puede consultarse en [2].

(1) Todo retículo distributivo $L \neq \{0\}$ contiene un ideal primo.

(2) Sea B un álgebra de Boole, I un ideal de B, F un filtro de B tales que $I \cap F = \emptyset$. Luego existe un ideal primo J tal que $J \supseteq I$, $J \cap F = \emptyset$.

(3) Toda álgebra de Boole $B \neq \{0\}$ contiene un ideal primo.

Un enunciado parecido al dado en (**1**) es el siguiente:

(1′) Todo retículo distributivo $L \neq \{0\}$ contiene un ideal maximal.

Sin embargo, el enunciado **(1′)** es más fuerte que el **(1)**. En efecto, es inmediato que el enunciado **(1′)** implica el enunciado **(1)**. Pero estos enunciados no resultan equivalentes porque Klimovsky probó que **(1′)** implica **AE** (ver [67]), con lo cual **(1′)** es equivalente a **AE**.

Hay otros teoremas de “mundos matemáticos” distintos, como en teoría de modelos o en topología, que resultan también equivalentes al (TFP). Por ejemplo, el teorema de Tychonoff (topología), el cual afirma que el producto de espacios topológicos compactos es compacto (ver [51]).

2.7. Ejercicios

Retículos

1. a) Construya los diagramas de Hasse de todos los conjuntos ordenados de tres elementos. ¿Cuáles son retículos?

   b) Construya los diagramas de Hasse de todos los retículos de cuatro elementos. ¿Son todos distributivos?

2. Sea L un retículo. Probar las siguientes propiedades:

   a) Si $x_i \leq y_i$ para $i = 1, \ldots, n$ entonces $\bigvee_{i=1}^{n} x_i \leq \bigvee_{i=1}^{n} y_i$ y $\bigwedge_{i=1}^{n} x_i \leq \bigwedge_{i=1}^{n} y_i$.

   b) Si $x_i \leq y_j$ para $i = 1, \ldots, n$ y $j = 1, \ldots, m$ entonces $\bigvee_{i=1}^{n} x_i \leq \bigwedge_{i=1}^{m} y_j$. Probar que también vale la recíproca.

3. Sean L un retículo y R una relación de equivalencia. Probar que R es congruencia si y solo si para todo $x, y, z \in L$, xRy implica $(x \vee z)R(y \vee z)$ y $(x \wedge z)R(y \wedge z)$.

4. Sea R una congruencia en un retículo L. Sean $x, y, z \in L$. Probar las siguientes afirmaciones:

   a) Cada clase de equivalencia es un subretículo de L.

   b) Cada clase de equivalencia es convexa. Es decir, si xRy y $x \leq z \leq y$ entonces xRz.

   c) xRy si y solo si $(x \vee y)R(x \wedge y)$.

5. Sean L un retículo distributivo, $a, b \in L$. Denotaremos como R_{ab} a la menor congruencia que contiene al par (a, b) (ver Capítulo 1, Ejemplos 1.3.17). Probar que $(x, y) \in R_{ab}$ si y solo si $x \wedge a \wedge b = y \wedge a \wedge b$, $x \vee a \vee b = y \vee a \vee b$.

6. Sea L un retículo distributivo. Sea $B(L) = \{x \in L : x \text{ es complementado}\}$. Probar que $B(L)$ es un subretículo de L.

7. Probar que si L y M son retículos, y $f : L \to M$ es inyectiva y conserva el orden, entonces $f(L)$ no es necesariamente un subretículo de M.

8. Sea L un retículo tal que existen ínfimo y supremo para todo subconjunto de L (esto significa que L es completo). Sea $f : L \to L$ una función que preserva el orden. Probar que existe un punto fijo, es decir, que existe $x \in L$ tal que $f(x) = x$.

   Sugerencia: considerar el conjunto $\{x \in L : x \leq f(x)\}$.

9. Sean X e Y conjuntos. Sean $f : X \to Y$ y $g : Y \to X$ funciones inyectivas. Probar que existe una biyección de X en Y.

   Sugerencia: definir $k : \mathcal{P}(X) \to \mathcal{P}(X)$ por $k(S) = X - g(Y - f(S))$ y aplicar el Ejercicio 8.

10. Sea L un retículo distributivo, $a \in L$ y $(a]$ el intervalo decreciente de a. Probar que $(a]$ es un subretículo de L y que la aplicación $f : L \to (a]$ dada por $f(x) = x \wedge a$ es un homomorfismo de retículos que resulta suryectivo.

11. Probar que si $f : L \to M$ es un homomorfismo de retículos entonces $f^{-1}(\{1\})$ es un filtro de L.

12. Sean L un retículo y $f : L \to \{0, 1\}$ una función. Probar las siguientes propiedades:

    a) f es un homomorfismo de retículos suryectivo si y solo si $f^{-1}(\{1\})$ es un filtro primo.

    b) L/R_f es isomorfo a $\{0, 1\}$, en donde recordemos que la relación de equivalencia R_f asociada a una función f está definida por $(x, y) \in R_f$ si y solo si $f(x) = f(y)$.

    c) Dado el filtro $F = f^{-1}(\{1\})$ y $\equiv_F$ (relación asociada al filtro F) ¿Qué relación hay entre R_f y R_F?

13. Probar que en una cadena todo elemento no nulo es primo.

Álgebras de Boole

1. Demostrar que en toda álgebra de Boole el supremo de las conjunciones elementales de n variables es igual a 1.
   a) Para $n = 2$: $(x \wedge y) \vee (x \wedge \overline{y}) \vee (\overline{x} \wedge y) \vee (\overline{x} \wedge \overline{y}) = 1$.
   b) En general: $\bigvee_{(k_1,\ldots,k_n)\in\{0,1\}^n} (x_1^{k_1} \wedge \cdots x_n^{k_n}) = 1$, donde $x_i^0 = \overline{x}_i$ y $x_i^1 = x_i$.

2. Sea F un filtro de un álgebra de Boole. a) Probar que $x\, R_F\, y$ si y solo si $x \to y \in F$ e $y \to x \in F$ (recordar: $x \to y = \overline{x} \vee y$). b) Probar que $x\, R_F\, y$ si y solo si $\overline{(x \Delta y)} \in F$, siendo $x \Delta y = (x \wedge \overline{y}) \vee (y \wedge \overline{x})$.

3. Sea $\overline{F}$ el ideal asociado a F (ver ejemplo 4 de 2.3.8). Sabemos que $\overline{F}$ es un ideal en el anillo asociado a B, cuya suma es la diferencia simétrica: $a + b = (a \wedge \overline{b}) \vee (b \wedge \overline{a})$ y tal que el opuesto de cada elemento es él mismo (ver ejemplo 6 de 2.2.8). Probar que $\equiv_F$ coincide con la relación

asociada al ideal $\overline{F}$ en el anillo: $x \equiv_F y$ sii $x - y \in \overline{F}$. Tener en cuenta que $x - y = x + y$.

4. Sea B un álgebra de Boole y a un átomo de B. Probar que el filtro $[a)$ es maximal.

5. Probar que una congruencia de retículos en un álgebra de Boole es congruencia de álgebras de Boole.

6. Sea B un álgebra de Boole. Probar que $x \wedge y \leq u \vee v$ si y solo si $x \wedge \overline{v} \leq \overline{y} \vee u$. Deducir de esto que $x \wedge y = 0$ si y solo si $x \leq \overline{y}$.

7. Sea la siguiente relación de equivalencia $\sim$ definida en el conjunto $\mathcal{P}(\mathbb{N})$ de las partes de los naturales por:

$$A \sim B \text{ si y solo si } (A - B) \cup (B - A) \text{ es finito.}$$

Sea $X = \mathcal{P}(\mathbb{N})/\sim$ y sea $\preceq$ la relación en X definida por:

$$|A| \preceq |B| \text{ si y solo si } (A - B) \text{ es finito.}$$

Probar que $\preceq$ está bien definida y que $\langle X, \preceq \rangle$ es un álgebra de Boole sin átomos.

8. Sean B un álgebra de Boole, $a \in B$ y $B_a = \{x \in B : 0 \leq x \leq a\}$.

a) Probar que B_a es un álgebra de Boole.

b) Probar que la función $f : B \to B_a$ definida por $f(x) = x \wedge a$ es un homomorfismo de álgebras de Boole.

9. a) Sean B un álgebra de Boole y X un subconjunto de B. Describir el subuniverso generado por X cuando X tiene un elemento y cuando X tiene dos elementos.

b) Mismo ejercicio que a) reemplazando B por un retículo acotado.

10. Sea X un conjunto infinito, $F(X) = \{Y \subseteq X : Y \text{ finito}\}$ y $C(X) = \{Y \subseteq X : Y^c \text{ es finito}\}$. Probar que $F(X) \cup C(X)$ es un subuniverso del álgebra de Boole $\langle \mathcal{P}(X), \cup, \cap, ^c, \emptyset, X \rangle$.

11. Probar que en toda álgebra de Boole finita vale lo siguiente:

a) Si $x \neq 0$ entonces existe un átomo a tal que $a \leq x$.

b) $x \leq y$ si y solo si $x \wedge \overline{y} = 0$.

12. Sea B un álgebra de Boole finita. Probar que todo elemento no nulo de B es el supremo de los átomos menores o iguales que él.

    Sugerencia: usar que $x \not\leq y$ si y solo si $x \wedge \overline{y} \neq 0$.

13. Sean $\mathbf{2}$ el álgebra de Boole $\{0,1\}$ y F_n el conjunto de todas las funciones de $\mathbf{2}^n$ en $\mathbf{2}$. Definimos el ínfimo, el supremo y el complemento en F_n como:

    $(\wedge)$ $(f \wedge g)(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \wedge g(x_1, \ldots, x_n)$,

    $(\vee)$ $(f \vee g)(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \vee g(x_1, \ldots, x_n)$,

    $(^-)$ $(\overline{f})(x_1, \ldots, x_n) = \overline{(f(x_1, \ldots, x_n))}$.

    a) Probar que F_n con las operaciones que acabamos de definir es un álgebra de Boole.

    b) Calcular los elementos de F_n para $n = 2$. ¿Cuáles son los átomos?

14. Sea X un conjunto. Sean $\mathbf{2}$ y $\mathbf{F_X}$ las álgebras de Boole $\langle\{0,1\}, \vee, \wedge, ^-, 0, 1\rangle$ y $\langle F_X, \vee, \wedge, ^-, \mathbf{0}, \mathbf{1}\rangle$, siendo F_X el conjunto de funciones de X en $\{0,1\}$, $\mathbf{0}$ la función que tiene ceros en todas las coordenadas y $\mathbf{1}$ la función que tiene 1 en todas las coordenadas.

    a) Probar que $\mathbf{F_X}$ es un álgebra de Boole.

    b) Sean $Y \subseteq X$ y χ_Y la función característica asociada a Y (ver Sección 1 del Capítulo 1). Es decir, χ_Y vale 1 en Y y 0 en $X - Y$. Probar que la función $C : \mathcal{P}(X) \to F_X$ definida por $C(Y) = \chi_Y$ es un isomorfismo de álgebras de Boole.

    c) Sean $\mathbf{2}^n$ el álgebra producto $\mathbf{2} \times \cdots \times \mathbf{2}$ (n veces) y $X = \{x_1, x_2, \ldots, x_n\}$. Probar que la función $I : F_X \to \mathbf{2}^n$ dada por $I(f) = (f(x_1), f(x_2), \ldots, f(x_n))$ es un isomorfismo de álgebras de Boole.

15. Sean L un retículo distributivo y $a \in L$ un elemento complementado. Probar que L es isomorfo a $(a] \times (\overline{a}]$.

    Sugerencia: definir $h(x) = (x \wedge a, x \wedge \overline{a})$.

16. Sea f homomorfismo de álgebras de Boole. Probar que f es inyectiva si y solo si $f^{-1}(\{0\}) = \{0\}$.

TFP

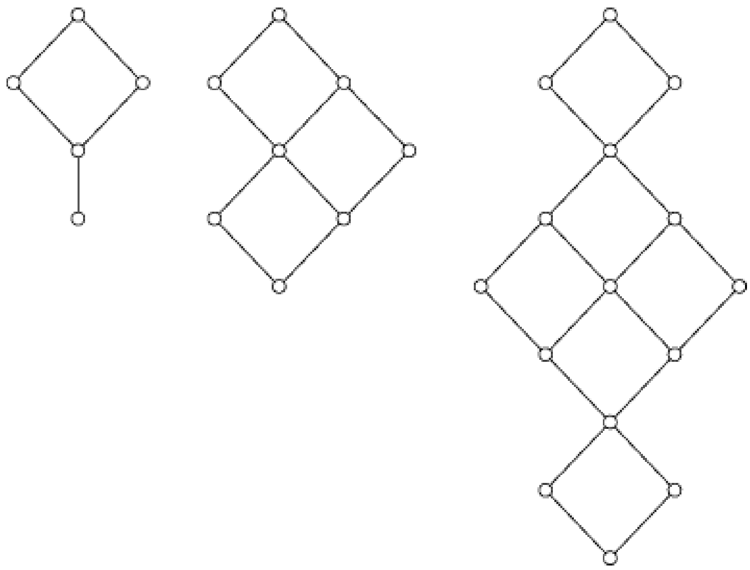
1. Demostrar el Teorema algebraico de la deducción (Corolario 2.4.8).

2. Sea B un álgebra de Boole y sea F un filtro de B, sea $I = \{\overline{x} : x \in F\}$. Probar que: a) I es un ideal, b) $B' = F \cup I$ es una subálgebra de B y c) F es un ultrafiltro de B'.

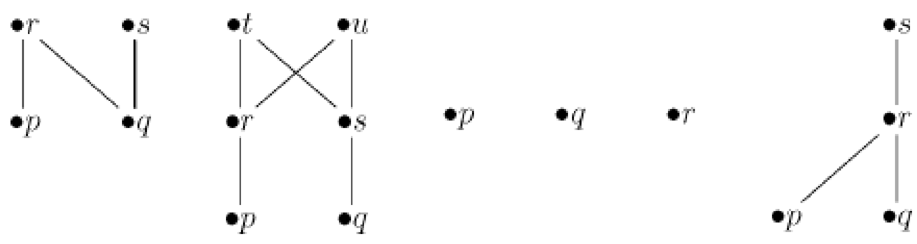
Teorema de Birkhoff

1. Construir el diagrama del conjunto $(L^{pr}, \leq^{o})$ para los siguientes retículos: $\mathbf{2}$, $\mathbf{2} \times \mathbf{2}$, $\mathbf{2} \times C_3$, $C_3 \times C_3$, $\mathbf{2} \times C_3 \times \mathbf{2}$, siendo C_3 la cadena de tres elementos. ¿Qué observa?

2. Mismo ejercicio para los retículos siguientes:



3. Dados los diagramas de los cuatro siguientes conjuntos ordenados construir los diagramas de los correspondientes retículos de conjuntos crecientes.



4. Sea L un retículo con 0, $S \subseteq L$, $S \neq \emptyset$. Probar que $F(S)$, el filtro generado por S, es propio si y solo si S tiene la siguiente propiedad (*propiedad de intersección finita* o *pif*): si $x_1, \ldots, x_n \in S$ entonces $x_1 \wedge \cdots \wedge x_n \neq 0$.

Bibliografía del Capítulo 2

- Balbes R. and Dwinger, P., *Distributive Lattices.* University of Missouri Press, 1974.

- Bell J.L. and Slomson A.B., *Models and Ultraproducts.* North-Holland, 1969.

- Burris S. and Sankappanavar H.P., *A Course in Universal Algebra.* Springer-Verlag, 1980.

- Cignoli R., D'Ottaviano I. and Mundici D., *Álgebras das Lógicas de Łukasiewicz.* Coleção CLE, vol. 12. Centro de Lógica, Epistemología e História da Ciencia, Universidade Estadual de Campinas, Campinas, San Pablo, 1994.

- Cignoli R., D'Ottaviano I. and Mundici D., *Algebraic Foundations of Many-Valued Reasoning.* Trends in Logic—Studia Logica Library, vol. 7, Kluwer Academic Publishers, 2000.

- Davey B.A. and Priestley H.A., *Introduction to Lattices and Order.* Cambridge University Press, 1990.

- Fitting M.C., *Intuitionistic Logic, Model Theory and Forcing.* North-Holland, 1969.

- González Asenjo F., *Introducción a la Teoría de Modelos.* Universidad de Zaragoza, Departamento de Álgebra y Fundamentos, 1978.

- Halpern J.D., *The independence of the axiom of choice from the Boolean prime ideal theorem.* Fund. Math., 55 (1964), 57–66.

- Halpern J.D. and Levy A., *The Boolean prime ideal theorem does not imply the axiom of choice.* In: Axiomatic Set Theory (Proc. Sympos. Pure Math., Vol. 18, Part I, Univ. California, Los Angeles, Calif., 1967) 83–134, Amer. Math. Soc., 1971.

- Hamilton A.G., *Logic for Mathematicians.* Cambridge University Press, 1978.

- Klimovsky G., *El teorema de Zorn y la existencia de filtros e ideales en los reticulados distributivos.* Revista de la UMA, 18 (1958), 160–164.

- Miraglia F., *Cálculo Proposicional: uma Interação da Álgebra e a Lógica*. Universidade Estadual de Campinas, Centro de Lógica, Epistemologia e História de Ciência, Campinas, 1987.

- Monteiro L., *Álgebras de Boole*. Informe Técnico Interno nº 66, Instituto de Matemática de Bahía Blanca, Universidad Nacional del Sur, 1998, revisado en 2000, 2001, 2002.

- Oubiña L., *Introducción a la Teoría de Conjuntos*. Eudeba, 1965.

- Rubin H. and Rubin J. *Equivalents of the Axiom of Choice*. Studies in Logic and the foundations of mathematics, North Holland, 1963.

Capítulo 3

Cálculo proposicional clásico

Hemos visto en el Capítulo 1 nociones lógicas generales como la de sistema formal, consecuencia sintáctica, etc. En este capítulo estudiaremos el caso particular del *Cálculo Proposicional Clásico*, abreviadamente, CPC. Definiremos un sistema formal precisando las fórmulas bien formadas, los axiomas o fórmulas que tomaremos como punto de partida y las reglas de deducción que nos permiten obtener consecuencias de los axiomas o bien de estos y de ciertas hipótesis adicionales. Podemos así trabajar con la forma de las proposiciones y determinar cuáles de ellas pueden derivarse del sistema *sintácticamente*. También abordaremos el aspecto *semántico*, es decir, el de las valuaciones y los valores de verdad.

Mostraremos que el sistema es *completo* en el sentido de que todo lo derivable del sistema es verdadero y todo lo verdadero puede derivarse del sistema. Más aún, mostraremos que la completud es *fuerte*, es decir que las nociones de consecuencia sintáctica y semántica de un conjunto de fórmulas cualquiera coinciden.

Con el propósito de mostrar una importante herramienta que establece un vínculo entre el álgebra y la lógica, introduciremos el método de Lindenbaum-Tarski que asocia a un sistema deductivo un álgebra. En el caso que nos ocupa, al CPC se le asocia un álgebra de Boole. Daremos posteriormente otros ejemplos de este método.

3.1. Sistema formal

En esta sección definiremos tres de los sistemas que pueden darse para el cálculo proposicional clásico, que llamaremos $\mathbf{L}$, $\mathbf{C}$ y $\mathbf{L}_4$ respectivamente. Como hemos dicho, un sistema formal es algo "confiable", en el sentido de que no dará lugar a paradojas y, en este caso, describirá formalmente las que entendemos clásicamente como “verdades lógicas”. Observemos que lo que se expresa en el sistema refleja el aspecto formal, sintáctico, donde no juega para nada la intuición. En cambio lo que se refiere a la verdad está relacionado con el constatar con la realidad, con asignar un significado o valor de verdad, es decir, con la parte semántica de la cuestión.

Denotaremos a las variables proposicionales con letras romanas minúsculas $\mathrm{p}_1,\ldots,\mathrm{p}_n,\ldots$ y a las fórmulas con letras romanas mayúsculas A, B,. . . .

Sistema L

Lenguaje

Está dado por las variables $\mathrm{p}_1,\ldots,\mathrm{p}_n,\ldots$ y los conectivos $\neg$, $\rightarrow$ sujetos a las reglas de construcción habituales.

Axiomas

(L1) $\mathrm{A} \rightarrow (\mathrm{B} \rightarrow \mathrm{A})$.

(L2) $(\mathrm{A} \rightarrow (\mathrm{B} \rightarrow \mathrm{C})) \rightarrow ((\mathrm{A} \rightarrow \mathrm{B}) \rightarrow (\mathrm{A} \rightarrow \mathrm{C}))$.

(L3) $(\neg\mathrm{A} \rightarrow \neg\mathrm{B}) \rightarrow (\mathrm{B} \rightarrow \mathrm{A})$.

Reglas

Modus Ponens:

$$(\mathrm{MP})\ \frac{\mathrm{A}\ ,\ \mathrm{A} \rightarrow \mathrm{B}}{\mathrm{B}}\,.$$

Sistema C

Lenguaje

Se agregan al lenguaje de **L** los conectivos $\vee$, $\wedge$ y las reglas de construcción de fórmulas correspondientes.

Axiomas

(I) $\mathrm{A} \rightarrow (\mathrm{A} \wedge \mathrm{A})$.

(II) $(\mathrm{A} \wedge \mathrm{B}) \rightarrow (\mathrm{B} \wedge \mathrm{A})$.

(III) $(\mathrm{A} \rightarrow \mathrm{B}) \rightarrow ((\mathrm{A} \wedge \mathrm{C}) \rightarrow (\mathrm{A} \wedge \mathrm{C}))$.

(IV) $((\mathrm{A} \rightarrow \mathrm{B}) \wedge (\mathrm{B} \rightarrow \mathrm{C})) \rightarrow (\mathrm{A} \rightarrow \mathrm{C})$.

(V) $B \rightarrow (A \rightarrow B)$.

(VI) $(A \wedge (A \rightarrow B)) \rightarrow B$.

(VII) $A \rightarrow (A \vee B)$.

(VIII) $(A \vee B) \rightarrow (B \vee A)$.

(IX) $((A \rightarrow C) \wedge (B \rightarrow C)) \rightarrow ((A \vee B) \rightarrow C)$.

(X) $\neg A \rightarrow (A \rightarrow B)$.

(XI) $((A \rightarrow B) \wedge (A \rightarrow \neg B)) \rightarrow \neg A$.

(XII) $A \vee \neg A$.

Reglas

Modus Ponens.

Sistema $\mathbf{L}_4$

Lenguaje y reglas

Son los mismos que los de **C**.

Axiomas

($\mathbf{L}_4$1) $A \rightarrow (B \rightarrow A)$.

($\mathbf{L}_4$2) $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$.

($\mathbf{L}_4$3) $(A \wedge B) \rightarrow A$.

($\mathbf{L}_4$4) $(A \wedge B) \rightarrow B$.

($\mathbf{L}_4$5) $A \rightarrow (B \rightarrow (A \wedge B))$.

($\mathbf{L}_4$6) $A \rightarrow (A \vee B)$.

($\mathbf{L}_4$7) $B \rightarrow (A \vee B)$.

($\mathbf{L}_4$8) $(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow ((A \vee B) \rightarrow C))$.

($\mathbf{L}_4$9) $(A \rightarrow B) \rightarrow ((A \rightarrow \neg B) \rightarrow \neg A)$.

($\mathbf{L}_4$10) $\neg\neg A \rightarrow A$.

En lo que sigue utilizaremos las definiciones de deducción, consecuencia, teoría, etc. dadas en el Capítulo 1, Sección 4.

Observación 3.1.1. Como dijimos en el Capítulo 1, 1.4.7 el sistema $\mathbf{L}_4$ es una extensión del sistema del Cálculo Proposicional Implicativo. En efecto, este tiene solo los dos primeros axiomas de $\mathbf{L}_4$; luego, todo teorema que se deduce a partir de esos dos axiomas es teorema en $\mathbf{L}_4$.

Los sistemas $\mathbf{L}$, $\mathbf{C}$ y $\mathbf{L}_4$ son equivalentes en el sentido de que tienen el mismo "poder deductivo". Más específicamente: ellos tienen los mismos teoremas, siempre que convengamos en traducir las fórmulas de los sistemas $\mathbf{C}$ y $\mathbf{L}_4$ considerando que $\mathrm{A} \vee \mathrm{B}$ es una abreviatura para la fórmula $\neg\mathrm{A} \to \mathrm{B}$ y que $\mathrm{A} \wedge \mathrm{B}$ es una abreviatura para la fórmula $\neg(\mathrm{A} \to \neg\mathrm{B})$. Dicho de otra manera, cada uno de ellos extiende a los otros y recíprocamente.

En adelante nos referiremos, sin mencionarlo cada vez, solo a fórmulas y propiedades del sistema $\mathbf{L}_4$.

Ejemplos 3.1.2.

1. Vamos a probar que, para cualquier par de fórmulas A y B,

$$(\mathrm{A} \to \mathrm{B}) \to (\mathrm{A} \to \mathrm{A})$$

   es un teorema. Numeraremos las sucesivas fórmulas de la deducción, que vamos obteniendo a partir de instancias de axiomas y aplicando MP. En adelante suprimiremos los paréntesis que no sean necesarios.

   (i) $\mathrm{A} \to (\mathrm{B} \to \mathrm{A})$, por axioma ($\mathrm{L}_4 1$).

   (ii) $(A \to (B \to A)) \to ((A \to B)) \to (A \to A))$, por axioma ($\mathrm{L}_4 2$).

   (iii) $(\mathrm{A} \to \mathrm{B}) \to (\mathrm{A} \to \mathrm{A})$, por (i), (ii) y (MP).

2. Probemos que para cualquier fórmula A tenemos que $\vdash (\mathrm{A} \to \mathrm{A})$.

   (i) $\mathrm{A} \to ((\mathrm{A} \to \mathrm{A}) \to \mathrm{A})$, por axioma ($\mathrm{L}_4 1$).

   (ii) $(\mathrm{A} \to ((\mathrm{A} \to \mathrm{A}) \to \mathrm{A})) \to ((\mathrm{A} \to (\mathrm{A} \to \mathrm{A})) \to (\mathrm{A} \to \mathrm{A}))$, por axioma ($\mathrm{L}_4 2$).

   (iii) $(\mathrm{A} \to (\mathrm{A} \to \mathrm{A})) \to (\mathrm{A} \to \mathrm{A})$, por (i), (ii) y (MP).

   (iv) $\mathrm{A} \to (\mathrm{A} \to \mathrm{A})$, por axioma ($\mathrm{L}_4 1$).

   (v) $\mathrm{A} \to \mathrm{A}$, por (iii), (iv) y (MP).

3. Sea $\Gamma = \{\mathrm{A} \to \mathrm{C}, \mathrm{B} \to \mathrm{C}\}$. Puede probarse, usando ($\mathrm{L}_4 8$), que $\Gamma \vdash (\mathrm{A} \vee \mathrm{B}) \to \mathrm{C}$. Hacerlo como ejercicio.

4. Probemos que la fórmula $\mathrm{A} \to \mathrm{C}$ es consecuencia de Γ, siendo $\Gamma = \{\mathrm{A} \to \mathrm{B}, \mathrm{B} \to \mathrm{C}\}$.

   (i) $\mathrm{A} \to \mathrm{B}$, por ser fórmula de Γ.

   (ii) $\mathrm{B} \to \mathrm{C}$, por ser fórmula de Γ.

   (iii) $(\mathrm{B} \to \mathrm{C}) \to (\mathrm{A} \to (\mathrm{B} \to \mathrm{C}))$, por ser instancia de axioma ($\mathrm{L}_4 1$).

   (iv) $\mathrm{A} \to (\mathrm{B} \to \mathrm{C})$, por (ii), (iii) y (MP).

   (v) $(\mathrm{A} \to (\mathrm{B} \to \mathrm{C})) \to ((\mathrm{A} \to \mathrm{B}) \to (\mathrm{A} \to \mathrm{C}))$, por ser instancia de axioma ($\mathrm{L}_4 2$).

   (vi) $(\mathrm{A} \to \mathrm{B}) \to (\mathrm{A} \to \mathrm{C})$, por (iv), (v) y (MP).

   (vii) $\mathrm{A} \to \mathrm{C}$, por (i), (vi) y (MP).

En lo que sigue estudiaremos algunas propiedades del sistema $\mathbf{L}_4$.

Teorema 3.1.3. *Sean* A *y* B *fórmulas cualesquiera y sea* Γ *un conjunto de fórmulas. Si* $\mathrm{A} \to \mathrm{B}$ *es consecuencia de* Γ*, entonces* B *es consecuencia del conjunto* $\Gamma \cup \{\mathrm{A}\}$*.*

Demostración. Existe una deducción de $\mathrm{A} \to \mathrm{B}$, digamos $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_\mathrm{k}$, donde $\mathrm{A}_\mathrm{k} = \mathrm{A} \to \mathrm{B}$. Si agregamos a A como paso número $k+1$, entonces por (MP) tenemos que en un paso $k+2$ obtenemos B. Es decir, obtuvimos una deducción de B a partir de $\Gamma \cup \{\mathrm{A}\}$. □

Podríamos preguntarnos si vale la recíproca del teorema anterior. Es decir, ¿es verdad que si $\Gamma \cup \{\mathrm{A}\} \vdash \mathrm{B}$ entonces $\Gamma \vdash \mathrm{A} \to \mathrm{B}$? La respuesta es positiva, como veremos a continuación.

Pero antes hagamos la siguiente observación.

Observación 3.1.4. El resultado anterior, así como otros que veremos, muestran propiedades del sistema $\mathbf{L}_4$. Debemos distinguir dos "niveles" de resultados: por una parte, hemos definido lo que es un teorema del sistema $\mathbf{L}_4$, podríamos llamar a los mismos "teoremas internos". Por otra parte, hay resultados acerca de las pruebas, de cómo obtener deducciones, de cómo se vinculan unas pruebas con otras, etc., en general, resultados que muestran propiedades del sistema. Estos resultados son los *metateoremas*, es decir, "teoremas externos", resultados que obtenemos mirando el sistema desde afuera.

El siguiente metateorema, llamado *Teorema de la deducción*, resulta una herramienta valiosa para simplificar las pruebas en $\mathbf{L}_4$. Es una propiedad que tienen todos los sistemas que contienen entre sus axiomas al ($\mathrm{L}_4 1$) y al ($\mathrm{L}_4 2$).

Teorema 3.1.5 (Teorema de la deducción). *Sean* A *y* B *fórmulas cualesquiera, y sea* Γ *un conjunto de fórmulas. Si* B *es consecuencia de* $\Gamma \cup \{\mathrm{A}\}$ *entonces* $\mathrm{A} \to \mathrm{B}$ *es consecuencia de* Γ.

Demostración. Supongamos que existe una deducción de B a partir de $\Gamma \cup \{\mathrm{A}\}$. Sean $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_\mathrm{n}$ los pasos de dicha deducción. Debemos demostrar que existe una prueba de $\mathrm{A} \to \mathrm{B}$ a partir de Γ. Para probar esto utilizaremos el principio de inducción sobre el número n de pasos de la prueba anteriormente mencionada.

Caso base: $n = 1$.

En este caso tenemos que $\mathrm{A}_1 = \mathrm{B}$. Se presentan tres posibilidades:

(a) B es una instancia de axioma. En este caso, tenemos la siguiente deducción de $\mathrm{A} \to \mathrm{B}$:

B, por ser una instancia de axioma.

$\mathrm{B} \to (\mathrm{A} \to \mathrm{B})$, por axioma ($\mathrm{L}_4 1$).

$\mathrm{A}_3 = \mathrm{A} \to \mathrm{B}$, por los dos ítems previos y (MP).

(b) B es una de las fórmulas de Γ. Se hace la misma deducción que en (a).

(c) $\mathrm{B} = \mathrm{A}$. En este caso debemos demostrar que $\mathrm{A} \to \mathrm{A}$. La deducción es la dada en el Ejemplo 2.

Supongamos que el teorema de la deducción vale cuando la deducción de una fórmula cualquiera a partir de $\Gamma \cup \{\mathrm{A}\}$ tiene un número de pasos menor o igual que $n-1$, y veamos que vale para la fórmula B que tiene una deducción de n pasos.

Tenemos cuatro casos posibles:

(a) B es una instancia de axioma, habiendo a lo sumo $n-1$ pasos anteriores. La deducción es como el primer caso del caso base.

(b) B es una de las fórmulas de Γ, habiendo a lo sumo $n-1$ pasos anteriores. La deducción es como el segundo caso del caso base.

(c) $\mathrm{B} = \mathrm{A}$, habiendo a lo sumo $n-1$ pasos anteriores. La deducción es como el tercer caso del caso base.

(d) B es se obtiene de dos pasos anteriores, digamos A_i y A_j por (MP), para ciertos $i, j < n$. Estas fórmulas tendrán la forma $\mathrm{A}_i = \mathrm{C}$ y $\mathrm{A}_j = \mathrm{C} \to \mathrm{B}$. Luego podemos afirmar que $\Gamma \cup \{\mathrm{A}\} \vdash \mathrm{C}$ y $\Gamma \cup \{\mathrm{A}\} \vdash \mathrm{C} \to \mathrm{B}$, y que en cada una de las dos deducciones se pueden emplear a lo sumo $n-1$

pasos. Luego por la hipótesis inductiva tenemos que $\Gamma \vdash A \to C$ y $\Gamma \vdash A \to (C \to B)$. La siguiente sucesión será entonces una deducción de $A \to B$ a partir de Γ:

.... (k) $A \to C, \ldots,$

(k+r) $A \to (C \to B)$,

(k+r+1) $(A \to (C \to B)) \to ((A \to C) \to (A \to B))$, por ser una instancia del axioma ($L_4 2$),

(k+r+2) $(A \to C) \to (A \to B)$, por (k+r), (k+r+1) y (MP),

(k+r+3) $A \to B$, por (k), (k+r+2) y (MP). $\square$

Veremos a continuación cómo se simplifican las deducciones usando el teorema de la deducción, que abreviaremos TD.

Ejemplos 3.1.6.

1. Vamos a probar lo mismo que en 4 de los Ejemplos 3.1.2 pero utilizando el TD. Es decir, veremos que $\Gamma \cup \{A\} \vdash C$, siendo $\Gamma = \{A \to B, B \to C\}$:

   (i) A (hipótesis adicional).

   (ii) $A \to B$ (hipótesis).

   (iii) B, por (i), (ii) y (MP).

   (iv) $B \to C$ (hipótesis).

   (v) C, por (iii), (iv) y (MP).

   El ejemplo previo es importante porque podemos usarlo como una regla de deducción, que se llama *silogismo hipotético* y que abreviaremos (SH). Es decir, tenemos la siguiente regla:

$$(\mathrm{SH})\ \frac{A \to B\ ,\ B \to C}{A \to C}.$$

2. Para probar que $\{C \to A, C \to B\} \vdash C \to (A \wedge B)$, por el TD basta probar que $\{C \to A, C \to B, C\} \vdash A \wedge B$. Hacerlo como ejercicio.

Para hacer más clara la forma de las deducciones vamos a considerar reglas, con lo que podremos simplificar el número de pasos de una deducción. Es decir que, si se prueba $\Gamma \vdash C$, podemos usar como regla:

$$\frac{\Gamma}{C}.$$

A continuación mencionaremos varias reglas. Las diez primeras reglas se derivan directamente de los axiomas, usando (MP).

Reglas derivadas de los axiomas

(R1) $\dfrac{\mathrm{A}}{\mathrm{B}\to\mathrm{A}}$,

(R2) $\dfrac{\mathrm{A}\to(\mathrm{B}\to\mathrm{C})\ ,\ \mathrm{A}\to\mathrm{B}}{\mathrm{A}\to\mathrm{C}}$,

(R3) $\dfrac{\mathrm{A}\wedge\mathrm{B}}{\mathrm{A}}$,

(R4) $\dfrac{\mathrm{A}\wedge\mathrm{B}}{\mathrm{B}}$,

(R5) $\dfrac{\mathrm{A}\ ,\ \mathrm{B}}{\mathrm{A}\wedge\mathrm{B}}$,

(R6) $\dfrac{\mathrm{A}}{\mathrm{A}\vee\mathrm{B}}$,

(R7) $\dfrac{\mathrm{B}}{\mathrm{A}\vee\mathrm{B}}$,

(R8) $\dfrac{\mathrm{A}\to\mathrm{C}\ ,\ \mathrm{B}\to\mathrm{C}}{(\mathrm{A}\vee\mathrm{B})\to\mathrm{C}}$,

(R9) $\dfrac{\mathrm{A}\to\mathrm{B}\ ,\ \mathrm{A}\to\neg\mathrm{B}}{\neg\mathrm{A}}$,

(R10) $\dfrac{\neg\neg\mathrm{A}}{\mathrm{A}}$.

Observemos que la regla (R8) ya había sido deducida en el Ejemplo 3.

Probaremos otras reglas, que se deducen de las ya enunciadas y de los axiomas. Las reglas que son sencillas de demostrar las dejaremos como ejercicios, sin hacer ningún comentario.

Otras Reglas

(R11) $\dfrac{\mathrm{C}\to\mathrm{A}\ ,\ \mathrm{C}\to\mathrm{B}}{\mathrm{C}\to(\mathrm{A}\wedge\mathrm{B})}$,

(R12) $\dfrac{\mathrm{A}\to\mathrm{B}}{(\mathrm{A}\wedge\mathrm{C})\to(\mathrm{B}\wedge\mathrm{C})}$,

(R12') $\dfrac{\mathrm{A}\to\mathrm{B}}{(\mathrm{C}\wedge\mathrm{A})\to(\mathrm{C}\wedge\mathrm{B})}$, (R13) $\dfrac{A \to (B \to C)}{(A \wedge B) \to C}$,

(R14) $\dfrac{A}{\neg\neg A}$.

A continuación haremos una deducción de la regla (R14):

(i) A (hipótesis).

(ii) $\neg A \to A$, por (i) y (R1).

(iii) $\neg A \to (A \to \neg A)$, por ser instancia de axioma ($L_4 1$).

(iv) $\neg A \to \neg A$, por (ii), (iii) y (R2).

(v) $\neg\neg A$, por (ii), (iv) y la regla (R9).

(R15) $\dfrac{A \to B}{\neg B \to \neg A}$.

(R16) $\dfrac{\neg A\ ,\ \neg B \to A}{B}$.

Para probar esta regla, haremos la siguiente deducción:

(i) $\neg A$ (hipótesis).

(ii) $\neg B \to A$, (hipótesis).

(iii) $\neg B \to \neg A$, por regla (R1) aplicada a (i).

(iv) $\neg\neg B$, de (ii), (iii) y (R9).

(v) B, por regla (R10).

(R17) $\dfrac{\neg B \to \neg A}{A \to B}$.

(R18) $\dfrac{\neg A}{A \to B}$.

Terminaremos esta sección haciendo una deducción de (R18) utilizando el TD:

(i) $\neg A$ (hipótesis).

(ii) A, (hipótesis).

(iii) $\neg B \to \neg A$, por la regla (R1) aplicada a (i).

(iv) $A \to B$, por regla (R17) aplicada a (iii).

(v) B, por (ii), (iv) y por la regla (MP).

3.2. Álgebra de Lindenbaum

En la sección anterior estudiamos propiedades lógicas del CPC expresado por el sistema $\mathbf{L}_4$. Vamos a mostrar ahora el aspecto algebraico del CPC. Por un pasaje al cociente del conjunto de fórmulas obtendremos un conjunto al cual se puede dotar de una estructura algebraica, de tal manera que los conectivos lógicos se transformen en operaciones de tal álgebra. Así se establece una relación lógica-álgebra que vincula propiedades, permitiendo pasar de uno a otro campo. Por ejemplo, según veremos después, el concepto de teoría en la lógica se corresponde con el de filtro en el álgebra.

Probaremos a continuación, en primer lugar, que la siguiente es una relación de equivalencia en el conjunto $\mathcal{L}_{CPC}$ de las fórmulas:

$$\mathrm{A} \equiv \mathrm{B} \text{ si y solo si } \vdash \mathrm{A} \to \mathrm{B} \text{ y } \vdash \mathrm{B} \to \mathrm{A}.$$

El conjunto cociente $\mathcal{L}_{CPC}/\equiv$ munido de las operaciones adecuadas es la llamada *álgebra de Lindenbaum* del Cálculo Proposicional Clásico. Probaremos que $\mathcal{L}_{CPC}/\equiv$ es un álgebra de Boole.

Veremos a continuación algunos resultados que facilitarán la demostración del resultado central de la sección.

Lema 3.2.1. *Si* A*,* B *y* C *son fórmulas de* $\mathcal{L}_{CPC}$ *entonces la siguiente fórmula es un teorema:*

$$((\mathrm{A} \vee \mathrm{B}) \wedge \mathrm{C}) \to ((\mathrm{A} \wedge \mathrm{C}) \vee (\mathrm{B} \wedge \mathrm{C})).$$

Demostración. Por la regla (R13), basta probar que

$$\vdash (\mathrm{A} \vee \mathrm{B}) \to (\mathrm{C} \to ((\mathrm{A} \wedge \mathrm{C}) \vee (\mathrm{B} \wedge \mathrm{C}))).$$

La afirmación anterior corresponde a la forma $\vdash (\mathrm{A} \vee \mathrm{B}) \to \mathrm{D}$, siendo $\mathrm{D} = \mathrm{C} \to ((\mathrm{A} \wedge \mathrm{C}) \vee (\mathrm{B} \wedge \mathrm{C}))$. De esta manera, en vista de la regla (R8), es suficiente probar $\vdash \mathrm{A} \to \mathrm{D}$ y $\vdash \mathrm{B} \to \mathrm{D}$.

Para probar que $\vdash \mathrm{A} \to (\mathrm{C} \to ((\mathrm{A} \wedge \mathrm{C}) \vee (\mathrm{B} \wedge \mathrm{C})))$, notemos que aplicando el TD dos veces obtenemos lo siguiente:

(i) A, hipótesis.

(ii) C, hipótesis.

(iii) $\mathrm{A} \wedge \mathrm{C}$, de (i) y (ii), por regla (R5).

(iv) $(\mathrm{A} \wedge \mathrm{C}) \vee (\mathrm{B} \wedge \mathrm{C})$, de (iii), por regla (R6).

Análogamente se prueba que $\vdash \mathrm{B} \to (\mathrm{C} \to ((\mathrm{A} \wedge \mathrm{C}) \vee (\mathrm{B} \wedge \mathrm{C})))$. □

Lema 3.2.2. *Sea* A *una fórmula de* $\mathcal{L}_{CPC}$. *Entonces,*

(a) $\vdash \neg(\mathrm{A} \wedge \neg\mathrm{A})$ *(principio de no contradicción).*

(b) $\vdash \mathrm{A} \vee \neg\mathrm{A}$ *(principio del tercero excluido).*

Demostración. En primer lugar, se tiene que, por ser instancia del axioma ($\mathrm{L}_4 3$), $\vdash (\mathrm{A} \wedge \neg\mathrm{A}) \to \mathrm{A}$. Análogamente $\vdash (\mathrm{A} \wedge \neg\mathrm{A}) \to \neg\mathrm{A}$, por ser instancia del axioma ($\mathrm{L}_4 4$). De estos dos teoremas podemos obtener, por aplicación de la regla (R9), que $\vdash \neg(\mathrm{A} \wedge \neg\mathrm{A})$.

En segundo lugar, hagamos la siguiente deducción de $\mathrm{A} \vee \neg\mathrm{A}$:

(i) $\mathrm{A} \to (\mathrm{A} \vee \neg\mathrm{A})$, instancia de axioma ($\mathrm{L}_4 6$).

(ii) $\neg\mathrm{A} \to (\mathrm{A} \vee \neg\mathrm{A})$, instancia de axioma ($\mathrm{L}_4 7$).

(iii) $\neg(\mathrm{A} \vee \neg\mathrm{A}) \to \neg\mathrm{A}$, de (i), por regla (R15).

(iv) $\neg(\mathrm{A} \vee \neg\mathrm{A}) \to \neg\neg\mathrm{A}$, de (ii), por regla (R15).

(v) $\neg\neg(\mathrm{A} \vee \neg\mathrm{A})$, por regla (R9) aplicada a (iii) y (iv).

(vi) $\mathrm{A} \vee \neg\mathrm{A}$, por regla (R10) aplicada a (v). □

Definición 3.2.3. Sea $\mathcal{L}_{CPC}$ el conjunto de fórmulas del CPC. Sea R la siguiente relación en $\mathcal{L}_{CPC}$:

$$\mathrm{A}\, R\, \mathrm{B} \text{ si y solo si } \vdash \mathrm{A} \to \mathrm{B}.$$

Lema 3.2.4. *La relación R es un preorden.*

Demostración. Es consecuencia de 2 y 4 de los Ejemplos 3.1.2. □

Lema 3.2.5. *La relación binaria $\equiv$ en $\mathcal{L}_{CPC}$ dada por*

$$\mathrm{A} \equiv \mathrm{B} \textit{ si y solo si } \mathrm{A}\, R\, \mathrm{B} \textit{ y } \mathrm{B}\, R\, \mathrm{A}$$

es una relación de equivalencia.

Sea $A_{CPC} = \mathcal{L}_{CPC}/\equiv$. Sean $X, Y \in A_{CPC}$ y sea $\preceq$ la siguiente relación en A_{CPC} : $X \preceq Y$ si y solo si $\mathrm{A}R\mathrm{B}$ para $\mathrm{A} \in X$ y $\mathrm{B} \in Y$. La relación $\preceq$ está bien definida y es un orden en A_{CPC}.

Demostración. Es consecuencia de la Observación 1.2.7 del Capítulo 1. □

Lema 3.2.6. (a) *Sea* $\mathrm{A} \in \mathcal{L}_{CPC}$. *Luego* $\vdash \mathrm{A}$ *si y solo si para toda clase* $|\mathrm{B}|$ *vale que* $|\mathrm{B}| \preceq |\mathrm{A}|$. *En particular, el conjunto de los teoremas forma una clase de equivalencia que resulta ser el último elemento de* A_{CPC}*, al cual llamaremos* $\mathbf{1}$.

(b) *Sea* $A \in \mathcal{L}_{CPC}$. *Luego* $\vdash \neg\mathrm{A}$ *si y solo si para toda clase* $|\mathrm{B}|$ *vale que* $|\mathrm{A}| \preceq |\mathrm{B}|$. *En particular, el conjunto de fórmulas cuya negación es un teorema forma una clase de equivalencia que resulta ser el primer elemento de* A_{CPC}*, al cual llamaremos* $\mathbf{0}$.

Demostración. Para probar el ítem (a), sea $\mathrm{A} \in \mathcal{L}_{CPC}$. Supongamos primero que $\vdash \mathrm{A}$. Por la regla (R1) vale que $\vdash \mathrm{B} \to \mathrm{A}$, para toda fórmula B, es decir, $|\mathrm{B}| \preceq |\mathrm{A}|$. Recíprocamente, sea $\vdash \mathrm{B} \to \mathrm{A}$ para toda fórmula B. Consideremos $\mathrm{B} = \mathrm{A} \to \mathrm{A}$. Utilizando la regla de (MP) obtenemos que $\vdash \mathrm{A}$.

Finalmente probemos el ítem (b). Sea $A \in \mathcal{L}_{CPC}$. Si $\vdash \neg\mathrm{A}$ entonces, por la regla (R18), se tiene $\vdash \mathrm{A} \to \mathrm{B}$. Es decir, $|\mathrm{A}| \preceq |\mathrm{B}|$. Recíprocamente, si $\vdash \mathrm{A} \to \mathrm{B}$ para toda fórmula B, tomemos $\mathrm{B} = \neg\mathrm{A}$. Luego se tiene que

$$\vdash \mathrm{A} \to \neg\mathrm{A}. \tag{3.1}$$

Además, por el Ejemplo 2 de la Sección 3.1 tenemos que

$$\vdash \mathrm{A} \to \mathrm{A}. \tag{3.2}$$

Utilizando la regla (R9) aplicada a (3.1) y a (3.2) obtenemos que $\vdash \neg\mathrm{A}$. □

Observación 3.2.7. En el siguiente teorema (y en lo que sigue) designaremos con el mismo símbolo al conectivo $\wedge$ (respectivamente $\vee$) de la lógica y a la operación de ínfimo (respectivamente de supremo) que definiremos en A_{CPC}.

Teorema 3.2.8. *El álgebra* $\mathbf{A}_{CPC} = \langle A_{CPC}, \wedge, \vee, ^-, \mathbf{0}, \mathbf{1} \rangle$ *es un álgebra de Boole, donde:*

$$\begin{aligned}
|\mathrm{A}| \wedge |\mathrm{B}| &:= |\mathrm{A} \wedge \mathrm{B}| \\
|\mathrm{A}| \vee |\mathrm{B}| &:= |\mathrm{A} \vee \mathrm{B}| \\
\overline{|\mathrm{A}|} &:= |\neg\mathrm{A}| \\
\mathbf{0} &:= \{\mathrm{A} : \vdash \neg\mathrm{A}\} \\
\mathbf{1} &:= \{\mathrm{A} : \vdash \mathrm{A}\}.
\end{aligned}$$

Demostración. Comenzaremos probando que $\langle A_{CPC}, \wedge, \vee\rangle$ es un retículo. Sean A y B en $\mathcal{L}_{CPC}$. Veremos que existe $|\mathrm{A}| \wedge |\mathrm{B}|$ y $|\mathrm{A}| \vee |\mathrm{B}|$, siendo $|\mathrm{A}| \wedge |\mathrm{B}| = |\mathrm{A} \wedge \mathrm{B}|$ y $|\mathrm{A}| \vee |\mathrm{B}| = |\mathrm{A} \vee \mathrm{B}|$.

En primer lugar, veamos que $|\mathrm{A}| \wedge |\mathrm{B}|$ es una operación bien definida. Sean $\mathrm{A}' \in |\mathrm{A}|$ y $\mathrm{B}' \in |\mathrm{B}|$. Se tiene que $\vdash \mathrm{B} \to \mathrm{B}'$ y $\vdash \mathrm{A} \to \mathrm{A}'$, de donde, por las reglas (R12) y (R12'), obtenemos que $\vdash (\mathrm{A} \wedge \mathrm{B}) \to (\mathrm{A} \wedge \mathrm{B}')$ y $\vdash (\mathrm{A} \wedge \mathrm{B}') \to (\mathrm{A}' \wedge \mathrm{B}')$. Utilizando luego (SH), inferimos que

$$\vdash (\mathrm{A} \wedge \mathrm{B}) \to (\mathrm{A}' \wedge \mathrm{B}'). \tag{3.3}$$

Análogamente podemos probar que

$$\vdash (\mathrm{A}' \wedge \mathrm{B}') \to (\mathrm{A} \wedge \mathrm{B}). \tag{3.4}$$

Utilizando (3.3) y (3.4) tenemos que $|\mathrm{A} \wedge \mathrm{B}| = |\mathrm{A}' \wedge \mathrm{B}'|$. De este modo hemos visto que la definición de la operación binaria $\wedge$ en A_{CPC} no depende de los representantes elegidos.

Ahora veremos que $|\mathrm{A} \wedge \mathrm{B}|$ es cota inferior común a $|\mathrm{A}|$ y a $|\mathrm{B}|$. Por las instancias de axiomas ($\mathrm{L}_4 3$) y ($\mathrm{L}_4 4$) tenemos que $\vdash (\mathrm{A} \wedge \mathrm{B}) \to \mathrm{A}$ y $\vdash (\mathrm{A} \wedge \mathrm{B}) \to \mathrm{B}$, es decir, $|\mathrm{A} \wedge \mathrm{B}| \preceq |\mathrm{A}|$ y $|\mathrm{A} \wedge \mathrm{B}| \preceq |\mathrm{B}|$. Sea $|\mathrm{C}|$ cota inferior común a $|\mathrm{A}|$ y a $|\mathrm{B}|$, es decir, $\vdash \mathrm{C} \to \mathrm{A}$ y $\vdash \mathrm{C} \to \mathrm{B}$. Por la regla (R11) se tiene que $\vdash \mathrm{C} \to (\mathrm{A} \wedge \mathrm{B})$, de donde resulta que $|\mathrm{C}| \preceq |\mathrm{A} \wedge \mathrm{B}|$. Luego, hemos demostrado que $|\mathrm{A} \wedge \mathrm{B}| = |\mathrm{A}| \wedge |\mathrm{B}|$.

Análogamente, usando los axiomas ($\mathrm{L}_4 6$), ($\mathrm{L}_4 7$) y la regla (R8), se obtiene que $|\mathrm{A} \vee \mathrm{B}| = |\mathrm{A}| \vee |\mathrm{B}|$.

Veamos que $\langle A_{CPC}, \wedge, \vee\rangle$ es un retículo distributivo, es decir, que $(|\mathrm{A}| \wedge |\mathrm{C}|) \vee (|\mathrm{B}| \wedge |\mathrm{C}|) = (|\mathrm{A}| \vee |\mathrm{B}|) \wedge |\mathrm{C}|$. La desigualdad $(|\mathrm{A}| \wedge |\mathrm{C}|) \vee (|\mathrm{B}| \wedge |\mathrm{C}|) \preceq (|\mathrm{A}| \vee |\mathrm{B}|) \wedge |\mathrm{C}|$ vale en todo retículo, por la Observación 2.1.3 del Capítulo 2. La otra desigualdad se sigue del Lema 3.2.1.

Luego, por el Lema 3.2.6 tenemos que $\langle A_{CPC}, \wedge, \vee, \mathbf{0}, \mathbf{1}\rangle$ es un retículo distributivo acotado.

Finalmente veremos que cada elemento $|\mathrm{A}|$ de A_{CPC} tiene complemento, y el mismo coincide con $|\neg \mathrm{A}|$. Por el Lema 3.2.2 tenemos que $\vdash \neg \mathrm{A} \vee \mathrm{A}$, de donde se sigue que $|\neg \mathrm{A} \vee \mathrm{A}| = \mathbf{1}$. Además se tiene que $\vdash \neg(\neg \mathrm{A} \wedge \mathrm{A})$, por lo cual $|\neg \mathrm{A} \wedge \mathrm{A}| = \mathbf{0}$. Por lo tanto, $\overline{|\mathrm{A}|} = |\neg \mathrm{A}|$. □

Definición 3.2.9. El álgebra de Boole $\langle A_{CPC}, \wedge, \vee, ^{-}, \mathbf{0}, \mathbf{1}\rangle$ es el *álgebra de Lindenbaum* del Cálculo Proposicional Clásico.

Observación 3.2.10. En la Observación 2.2.12 del Capítulo 2 vimos que para cada x e y existe $x \to y$, siendo $x \to y = \overline{x} \vee y$. Luego, si consideramos el álgebra de Boole A_{CPC}, entonces vale que $|\mathrm{A}| \to |\mathrm{B}| = |\neg \mathrm{A}| \vee |\mathrm{B}|$, para todo par de fórmulas A, B.

3.3. Filtros y teorías

En esta sección estudiaremos la relación entre las teorías del cálculo proposicional clásico y los filtros de la correspondiente álgebra de Lindenbaum.

Llamaremos $\mathcal{Z} = \emptyset^{\vdash}$ al conjunto de los teoremas.

Teorema 3.3.1. *Existe una biyección entre el conjunto de los filtros del álgebra de Lindenbaum A_{CPC} del* CPC *y el conjunto de las teorías del* CPC.

Demostración. Sea F un filtro de A_{CPC}. Definimos el siguiente conjunto:

$$\mathcal{T}_F = \{\mathrm{A} : |\mathrm{A}| \in F\},$$

que resulta ser la unión de las clases $|\mathrm{A}|$ de F.

Por otra parte, a una teoría $\mathcal{T}$ le asociamos el conjunto

$$|\mathcal{T}| = \{|\mathrm{C}| : \mathrm{C} \in \mathcal{T}\}.$$

Veremos que, en efecto, $\mathcal{T}_F$ es una teoría y que $|\mathcal{T}|$ es un filtro.

Por el Lema 2.3.5 del Capítulo 2, sabemos que la noción de filtro es equivalente a la de filtro implicativo en álgebras de Boole. La condición $\mathbf{1} \in F$ implica que $\mathcal{Z} \subseteq \mathcal{T}_F$, y el hecho de ser F cerrado por (MP) implica que $\mathcal{T}_F$ también lo es porque $|\mathrm{A} \to \mathrm{B}| = |\mathrm{A}| \to |\mathrm{B}|$, por la Observación 3.2.10. Luego $\mathcal{T}_F$ es una teoría. También se puede probar que $|\mathcal{T}|$ es un filtro.

Finalmente probaremos que las asignaciones $F \mapsto \mathcal{T}_F$ y $\mathcal{T} \mapsto |\mathcal{T}|$ son una inversa de la otra, es decir, determinan una biyección. En efecto, si F es un filtro entonces

$$|\mathcal{T}_F| = \{|\mathrm{C}| : \mathrm{C} \in \mathcal{T}_F\} = \{|\mathrm{C}| : |\mathrm{C}| \in F\} = F.$$

Análogamente, si $\mathcal{T}$ es una teoría entonces

$$\mathcal{T}_{|\mathcal{T}|} = \{\mathrm{A} : |\mathrm{A}| \in |\mathcal{T}|\} = \{\mathrm{A} : \mathrm{A} \in \mathcal{T}\} = \mathcal{T}.$$ □

Lema 3.3.2. *Sea Σ un conjunto de fórmulas de $\mathcal{L}_{CPC}$ y denotemos como $|\Sigma|$ al conjunto $\{|\mathrm{A}| : \mathrm{A} \in \Sigma\}$. Entonces el filtro generado por $|\Sigma|$ en A_{CPC}, $F(|\Sigma|)$, es igual al filtro asociado a la teoría $\Sigma^{\vdash}$. Es decir, $F(|\Sigma|) = |\Sigma^{\vdash}|$.*

Demostración. Observemos que $|\Sigma^{\vdash}|$ es un filtro y contiene a $|\Sigma|$. Por ser $F(|\Sigma|)$ el mínimo tenemos que $F(|\Sigma|) \subseteq |\Sigma^{\vdash}|$.

Recíprocamente, sea $|\mathrm{C}| \in |\Sigma^{\vdash}|$. Entonces $\Sigma \vdash \mathrm{C}$. Veamos, por inducción sobre el número de pasos de la prueba, que $|\mathrm{C}| \in F(|\Sigma|)$. Si la prueba tiene un paso, eso significa que $\mathrm{C} \in \Sigma$ o que C es instancia de axioma. Luego $|\mathrm{C}| \in |\Sigma| \subseteq F(|\Sigma|)$ o bien $|\mathrm{C}| = \mathbf{1} \in F(|\Sigma|)$.

Supongamos ahora que para pruebas de menos de n pasos de C a partir de Σ se tiene que $|\mathrm{C}| \in F(|\Sigma|)$, y sea $\mathrm{C}_1, \mathrm{C}_2, \ldots, \mathrm{C}_n = \mathrm{C}$ una prueba de C de n pasos. Entonces, existirán C_i, $\mathrm{C}_j = \mathrm{C}_i \to \mathrm{C}$ con i, j menores que n. Por la hipótesis inductiva, $|\mathrm{C}_i| \in F(|\Sigma|)$, $|\mathrm{C}_j| \in F(|\Sigma|)$. Por ser F cerrado por (MP) resulta $|\mathrm{C}| \in F(|\Sigma|)$. □

A continuación veremos una manera alternativa de demostrar el teorema de la deducción TD del CPC usando el que llamamos Teorema Algebraico de la Deducción (Corolario 2.4.8, Capítulo 2) y el Teorema 3.3.1.

Observación 3.3.3. A partir del comentario anterior surgen algunas preguntas: ¿En el Teorema 3.3.1 no se usa que el álgebra de Lindenbaum es un álgebra de Boole? Sí. Y para demostrar esto último ¿no se usó el TD? Sí. ¿Es correcto entonces lo que vamos a hacer? Sí. ¿Por qué?

Imaginemos haber demostrado que A_{CPC} es un álgebra de Boole **sin** usar el TD. ¿Es eso posible? Sí. Utilizamos siempre el TD como una herramienta, como un "atajo" para acortar las deducciones. Pero todas esas deducciones pudieron haber sido hechas sin usar el TD. Entonces, imaginemos que así fue y sigamos adelante confiadamente.

Teorema 3.3.4 (Teorema de la Deducción)**.** *Sea* Σ *un conjunto de fórmulas de* $\mathcal{L}_{CPC}$*, y sean* $\mathrm{A}, \mathrm{B} \in \mathcal{L}_{CPC}$*. Si* $\Sigma \cup \{\mathrm{A}\} \vdash \mathrm{B}$ *entonces* $\Sigma \vdash \mathrm{A} \to \mathrm{B}$*.*

Demostración. Sea $\Sigma \cup \{\mathrm{A}\} \vdash \mathrm{B}$. Luego, $\mathrm{B} \in (\Sigma \cup \{\mathrm{A}\})^{\vdash}$, de donde $|\mathrm{B}| \in |(\Sigma \cup \{\mathrm{A}\})^{\vdash})|$. Por el Lema 3.3.2, $|(\Sigma \cup \{\mathrm{A}\})^{\vdash})| = F(|\Sigma| \cup \{|\mathrm{A}|\})$. Luego, $|\mathrm{B}| \in F(|\Sigma| \cup \{|\mathrm{A}|\})$. Por el Teorema Algebraico de la Deducción (ver Capítulo 2, 2.4.8) esto último implica que $|\mathrm{A}| \to |\mathrm{B}| \in F(|\Sigma|)$. Nuevamente por el Lema 3.3.2 se tiene que $|\mathrm{A} \to \mathrm{B}| \in |\Sigma^{\vdash}|$. Luego, $\mathrm{A} \to \mathrm{B} \in \Sigma^{\vdash}$, es decir, $\Sigma \vdash \mathrm{A} \to \mathrm{B}$. □

3.4. Valuaciones

Para demostrar la completud del CPC empezaremos por definir para este cálculo proposicional el concepto semántico de valuación, concepto que se vio en general en el Capítulo 1, Sección 4.

Dar una valuación significa asignar a las variables proposicionales el valor 1 (verdadero) o 0 (falso) y extender luego esta asignación a todas las fórmulas de la manera especificada en la definición siguiente.

Una valuación es una función de las fórmulas en el álgebra de Boole **2** que respeta los conectivos. Más adelante veremos que este concepto de valuación puede extenderse considerando un álgebra de Boole cualquiera B en lugar de $\mathbf{2}$. Sin embargo, también veremos que ambos conceptos de valuación son equivalentes para demostrar completud.

Definición 3.4.1. Una *valuación* es una función $v : \mathcal{L}_{CPC} \to \{0, 1\}$ tal que:

(1) $v(\mathrm{A}) \neq v(\neg\mathrm{A})$.

(2) $v(\mathrm{A} \to \mathrm{B}) = 0$ si y solo si $v(\mathrm{A}) = 1$ y $v(\mathrm{B}) = 0$.

(3) $v(\mathrm{A} \wedge \mathrm{B}) = 1$ si y solo si $v(\mathrm{A}) = v(\mathrm{B}) = 1$.

(4) $v(\mathrm{A} \vee \mathrm{B}) = 0$ si y solo si $v(\mathrm{A}) = v(\mathrm{B}) = 0$.

Si A es tal que $v(\mathrm{A}) = 1$ para toda valuación v, entonces A se llama *tautología*.

Diremos que dos fórmulas A y B son *lógicamente equivalentes* si $\mathrm{A} \to \mathrm{B}$ y $\mathrm{B} \to \mathrm{A}$ son tautologías.

Observación 3.4.2. Una valuación quedará definida dando solo sus valores en las variables proposicionales. En efecto, puede probarse que con ese dato básico se puede evaluar inductivamente cualquier fórmula, basta respetar las reglas que acabamos de dar.

¿Qué tienen que ver las valuaciones con las tablas de verdad? Estas consideran solo finitas variables proposicionales; la tabla de verdad de una fórmula de n variables muestra todas las posibles valuaciones de esas n variables: cada fila representa una valuación, atribuyendo arbitrariamente cualquier valor 0 o 1 a las infinitas variables restantes.

La tabla de verdad de una tautología tiene como resultado 1 en todas las filas. Dos fórmulas lógicamente equivalentes tienen la misma tabla de verdad.

3.5. Completud

La propiedad de *corrección* (en inglés, “soundness”) de un sistema formal es la que asegura que cada teorema deducido de él es verdadero para toda valuación. La propiedad de *adecuación* (en inglés “adequacy”) nos dice que una fórmula que resulta verdadera para toda valuación puede ser deducida como teorema del sistema formal. Un sistema es *completo* (“complete”, en inglés) si es correcto y adecuado.

Es frecuente que se llame también *completo* a un sistema adecuado.

En esta sección estudiaremos teoremas de completud (corrección y adecuación) para el CPC. Ellos establecen una equivalencia entre el concepto sintáctico de *fórmula demostrable* con el concepto semántico de *fórmula válida* o *tautología*.

Filosóficamente, eso significa que el sistema que hemos elegido para el CPC es capaz de producir por procedimientos formales, sintácticos, todas aquellas proposiciones que percibimos como las verdades lógicas y solo ellas. Demostraremos que una fórmula es un teorema si y solo si es una tautología.

Teorema 3.5.1 (Corrección). *Sea* A *una fórmula de* $\mathcal{L}_{CPC}$. *Si* $\vdash$ A *entonces* A *es una tautología.*

Demostración. En primer lugar, si A es una instancia de axioma, puede probarse dando valores a las variables que A es una tautología.

Sea $\mathrm{A}_1, \ldots, \mathrm{A}_n = \mathrm{A}$ una deducción de A y supongamos que todo teorema con menos de n pasos de deducción es una tautología. Se tiene que A se obtiene por MP de dos fórmulas que tendrán la forma: B y B $\to$ A y que se han deducido antes, o sea con menos de n pasos. Por la hipótesis inductiva, B y B $\to$ A son tautologías. Además, si se tiene que B y B $\to$ A son tautologías, entonces es A una tautología. □

Lema 3.5.2. *Sea* v *una valuación. Si* A *y* B *son fórmulas tales que* $|\mathrm{A}| \preceq |\mathrm{B}|$ *entonces* $v(\mathrm{A}) \leq v(\mathrm{B})$.

Demostración. Se tiene $\vdash \mathrm{A} \to \mathrm{B}$ por definición de $\preceq$. Luego $v(\mathrm{A} \to \mathrm{B}) = 1$, por el Teorema 3.5.1. Si $v(\mathrm{A}) = 1$ y $v(\mathrm{B}) = 0$ entonces $v(\mathrm{A} \to \mathrm{B}) = 0$, lo cual es un absurdo. □

Corolario 3.5.3. *Si* $\mathrm{A} \equiv \mathrm{B}$ *entonces* $v(\mathrm{A}) = v(\mathrm{B})$ *para toda valuación* v.

Si v es una valuación entonces por el Corolario 3.5.3 la función $\hat{v} : A_{CPC} \to \mathbf{2}$ dada por $\hat{v}(|\mathrm{A}|) = v(\mathrm{A})$ es un homomorfismo de A_{CPC} en $\mathbf{2}$. A continuación probaremos el siguiente resultado.

Corolario 3.5.4. *La función* G *dada por* $G(v) = \hat{v}$ *es una biyección entre el conjunto de valuaciones y el conjunto de homomorfismos de* A_{CPC} *en* $\mathbf{2}$.

Demostración. La inyectividad de G es inmediata, por lo cual probaremos solo la suryectividad de la misma. Sea $h : A_{CPC} \to \mathbf{2}$ un homomorfismo. La función $v_h : \mathcal{L}_{CPC} \to \mathbf{2}$ definida por $v_h(\mathrm{A}) = h(|\mathrm{A}|)$ es una valuación (probarlo se deja como ejercicio al lector). Para cada $A \in \mathcal{L}_{CPC}$ tenemos que $\hat{v_h}(|\mathrm{A}|) = v_h(\mathrm{A}) = h(|A|)$, con lo cual $G(v_h) = \hat{v_h} = h$. Luego G es una función suryectiva. Por lo tanto tenemos que G es una biyección. □

Haciendo la composición de la función biyectiva F definida en el Corolario 2.4.23 del Capítulo 2 (considerando como álgebra de Boole A_{CPC}) con la inversa de la función biyectiva G definida en el Corolario 3.5.4 obtenemos el siguiente resultado.

Teorema 3.5.5. *La función $G^{-1} \circ F$ es una biyección entre el conjunto de ultrafiltros de A_{CPC} y el conjunto de valuaciones.*

Observación 3.5.6. Notemos, en particular, que si U es un ultrafiltro de A_{CPC} y llamamos v a la valuación $(G^{-1} \circ F)(U) : \mathcal{L}_{CPC} \to \mathbf{2}$ entonces v está definida como $v(\mathrm{A}) = 1$ si $|\mathrm{A}| \in U$ y $v(\mathrm{A}) = 0$ si $|\mathrm{A}| \notin U$.

Si consideramos que el isomorfismo $A_{CPC}/U \cong \mathbf{2}$ identifica las dos álgebras podemos pensar que la valuación v se obtiene componiendo las dos aplicaciones canónicas al cociente p y q, siendo $p : \mathcal{L}_{CPC} \longrightarrow A_{CPC}$ y $q : A_{CPC} \longrightarrow A_{CPC}/U$, según lo muestra el siguiente diagrama.

$$\begin{tikzcd}
\mathcal{L}_{CPC} \arrow[d, "p"'] \arrow[dr, "v"] & \\
A_{CPC} \arrow[r, "q"'] & A_{CPC}/U
\end{tikzcd}$$

Teorema 3.5.7 (Adecuación)**.** *Sea* A *una fórmula de* $\mathcal{L}_{CPC}$*. Si* A *es una tautología entonces* $\vdash \mathrm{A}$.

Demostración. Sea A una tautología, es decir, para toda v vale que $v(\mathrm{A}) = 1$. Supongamos que A no es un teorema. Luego $|\mathrm{A}| \neq 1$ en A_{CPC}. Pero entonces: $|\neg\mathrm{A}| \neq 0$ en A_{CPC}. Por el Corolario 2.4.17 del Capítulo 2 existe un ultrafiltro U de A_{CPC} tal que $|\neg\mathrm{A}| \in U$. Sea v la valuación asociada a este ultrafiltro dada en el Teorema 3.5.5. Entonces, $v(\neg\mathrm{A}) = 1$. Luego $v(\mathrm{A}) = 0$, lo cual contradice que A es una tautología. Luego, A es un teorema. □

Valuaciones en general

Consideraremos ahora valuaciones cuyos codominios pueden ser álgebras de Boole cualesquiera. Demostraremos también que, esencialmente, esto no extiende la noción de tautología y, en cambio, desdibuja su sentido. En efecto, las fórmulas evaluadas en **2** son verdaderas o falsas, mostrando el efecto del principio del tercero excluido. Las fórmulas **2**-válidas o tautologías son las "verdades lógicas evidentes", aquellas que son la base de cualquier razonamiento.

Para demostrar que validez y validez en **2** son equivalentes usamos el TFP. Más adelante analizaremos desde el punto de vista del Álgebra Universal este resultado. Intuitivamente, nos dice que en la clase de las álgebras de Boole, que es una variedad (ver Capítulo 1, 1.3.15), hay una sola álgebra (que es **2**) que funciona como "ladrillo", en base a la cual se construyen todas las otras álgebras de la clase.

De acuerdo a lo visto en el Capítulo 1, las valuaciones en general transforman conectivos en operaciones del álgebra.

Definición 3.5.8. Una *B-valuación* es una función $v : \mathcal{L}_{CPC} \to B$, donde B es un álgebra de Boole, tal que:

(1) $v(\mathrm{A} \wedge \mathrm{B}) = v(\mathrm{A}) \wedge v(\mathrm{B})$,

(2) $v(\mathrm{A} \vee \mathrm{B}) = v(\mathrm{A}) \vee v(\mathrm{B})$,

(3) $v(\mathrm{A} \to \mathrm{B}) = v(\mathrm{A}) \to v(\mathrm{B})$,

(4) $v(\neg\mathrm{A}) = \overline{(v(\mathrm{A}))}$.

Si A es tal que $v(\mathrm{A}) = 1$ para toda B-valuación v, entonces se dice que A es *B-válida* y se denota $\models_B$ A. Diremos que A es *válida* si es B-válida para toda álgebra de Boole B. Se denotará $\models$ A.

Lema 3.5.9. *Sea v una A-valuación, $h : A \longrightarrow B$ un homomorfismo. Entonces, $v' = h \circ v$ es una B-valuación.*

Demostración. Se deja como ejercicio. □

Teorema 3.5.10. *Una fórmula es válida si y solo si es una tautología.*

Demostración. Si A es válida, entonces es **2**-válida, o sea, es una tautología.

Recíprocamente, sea A una tautología y supongamos que existen un álgebra de Boole B y una B-valuación v tales que $v(\mathrm{A}) \neq 1$. Por el Corolario 2.4.17, por ser $v(\neg\mathrm{A}) \neq 0$, habrá un ultrafiltro U en B tal que $v(\neg\mathrm{A}) \in U$. Luego tenemos que $v(\mathrm{A}) \notin U$.

Sea $h : B \longrightarrow \mathbf{2}$ definida por: $h(x) = 1$ si $x \in U$, $h(x) = 0$ si $x \notin U$. Luego, $U = h^{-1}(\{1\})$. Por la Observación 2.4.22 del Capítulo 2 se tiene que $h = X_U$ es un homomorfismo. Luego, por el Lema 3.5.9, resulta que $v' = h \circ v$ es una valuación. Como $v(\mathrm{A}) \notin U$ tenemos que $h((v(\mathrm{A})) = 0$, es decir, $v'(\mathrm{A}) = 0$. Esto contradice el hecho de que A es una tautología. □

Observación 3.5.11. Podemos generalizar lo demostrado en el Lema 3.5.2 para valuaciones en general. Para ello supongamos que $|\mathrm{A}| \preceq |\mathrm{B}|$. Por definición de $\preceq$ se tiene que $\vdash \mathrm{A} \to \mathrm{B}$. Ahora consideremos un álgebra de Boole B y una B-valuación v. Por el Teorema 3.5.10 tenemos que $v(\mathrm{A} \to \mathrm{B}) = 1$, lo cual es equivalente a afirmar que $v(\mathrm{A}) \to v(\mathrm{B}) = 1$. Es decir, $v(\mathrm{A}) \leq v(\mathrm{B})$.

Teorema 3.5.12 (Completud)**.** *Para toda fórmula* A*:*

$$\vdash \mathrm{A} \ \ \textit{si y solo si} \ \ \models \mathrm{A}.$$

Demostración. Se sigue del Teorema 3.5.1 y del Teorema 3.5.10. □

El álgebra A_{CPC} es libre

Antes de cerrar esta sección veamos otra propiedad interesante del álgebra de Lindenbaum: tiene como conjunto de generadores libres al conjunto de las clases de las variables proposicionales, que son numerables.

Teorema 3.5.13. *Sea $\mathcal{V}$ el conjunto de las variables proposicionales y sea $|\mathcal{V}| = \{|p_i| : \ p_i \in \mathcal{V}\}$. El conjunto $|\mathcal{V}|$ genera libremente A_{CPC} en la clase de las álgebras de Boole.*

Demostración. En primer lugar, notemos que, si es $i \neq j$ entonces p_i no es equivalente a p_j, ya que $p_i \to p_j$ no es una tautología. Luego $|p_i| \neq |p_j|$, o sea que todas las clases son distintas.

Veamos que $|\mathcal{V}|$ genera A_{CPC}, es decir, que A_{CPC} mismo es la menor subálgebra de A_{CPC} que contiene a $|\mathcal{V}|$. En efecto, cualquier subálgebra que contenga a $|\mathcal{V}|$ debe contener también todas las combinaciones de elementos de $|\mathcal{V}|$ mediante las operaciones de A_{CPC}. Pero las combinaciones de elementos de $|\mathcal{V}|$ son exactamente los elementos de A_{CPC}.

Probemos ahora la propiedad universal de extensión de homomorfismos.

Sea $f : |\mathcal{V}| \longrightarrow B$, B un álgebra de Boole y veamos que f puede extenderse a un homomorfismo $g : A_{CPC} \longrightarrow B$.

La aplicación f induce $\widehat{f} : \mathcal{V} \longrightarrow B$, siendo $\widehat{f}$ definida por: $\widehat{f}(p_i) = f(|p_i|)$ para todo $i = 1, 2, \ldots$. A su vez, $\widehat{f}$ induce una valuación $v : \mathcal{L}_{CPC} \longrightarrow B$ de la manera usual, es decir, $v(p_i) = \widehat{f}(p_i)$ y se extendiende a las fórmulas inductivamente.

Por la Observación 3.5.11, v da lugar a una función $g : A_{CPC} \longrightarrow B$, ya que v es constante en cada clase de equivalencia. Es decir que g está definido por: $g(|\mathrm{A}|) = v(\mathrm{A})$. Pero por ser v valuación resulta ser g un homomorfismo y, además, vale que $g(|p_i|) = v(p_i) = \widehat{f}(p_i) = f(|p_i|)$. Es decir que g extiende a f, lo que se muestra en el siguiente diagrama conmutativo.

$$\begin{tikzcd}
|\mathcal{V}| \arrow[r, "f"'] \arrow[d, "inc"'] & B \\
A_{CPC} \arrow[ur, "g"'] &
\end{tikzcd}$$

□

Observación 3.5.14. Supongamos que queremos restringirnos a considerar un número finito de variables, digamos las n primeras $\{\mathrm{p}_1, \ldots, \mathrm{p}_n\}$. Construiríamos entonces un cálculo proposicional con n variables y tendríamos entonces la correspondiente álgebra de Lindenbaum, que podríamos llamar A_{CPCn}.

De la misma manera que hemos visto para A_{CPC}, podemos probar que A_{CPCn} es libremente generada por el conjunto de n elementos $\{|\mathrm{p}_1|, |\mathrm{p}_2|, \dots, |\mathrm{p}_n|\}$. El número de valuaciones sería también finito, porque para cada variable tenemos dos posibilidades, con lo que habría $2 \times 2 \times \cdots \times 2 = 2^n$ valuaciones. Por ejemplo, para dos variables tendríamos las siguientes, donde cada fila define una valuación y las A_i representan todas las fórmulas posibles no equivalentes entre sí:

p	q	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	A_{14}	A_{15}	A_{16}
1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
1	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
0	1	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

Por lo visto en el Capítulo 2, Teorema 2.5.11, el álgebra de Boole libre con n generadores tiene 2^n átomos, que corresponden a los ultrafiltros de A_{CPCn}, que a su vez corresponden a los homomorfismos de $A_{CPCn} \longrightarrow \mathbf{2}$, y estos a las valuaciones de las n variables proposicionales. También vimos que esos átomos son las conjunciones elementales

$$c_{i_1 \dots i_n} = |\mathrm{p}_1|^{i_1} \wedge \cdots \wedge |\mathrm{p}_n|^{i_n} = |(\mathrm{p}_1)^{i_1} \wedge \cdots \wedge (\mathrm{p}_n)^{i_n}|.$$

El álgebra A_{CPCn} tiene 2^{2^n} elementos, que son supremos de átomos.

En el caso de dos variables p_1 y p_2, que por simplicidad llamaremos x e y, las conjunciones elementales son $c_{11} = x \wedge y$, $c_{10} = x \wedge \overline{y}$, $c_{01} = \overline{x} \wedge y$ y $c_{00} = \overline{x} \wedge \overline{y}$. En la tabla anterior, ellas son equivalentes respectivamente a A_8, A_{12}, A_{14} y A_{15}. Las demás fórmulas A_i son supremos de algunas de estas cuatro. En la Figura 2.14 del Capítulo 2 se muestran las A_i.

3.6. Completud fuerte

En la sección anterior hemos probado la completud del CPC, es decir, que una fórmula A es una tautología si y solo si es un teorema. Podemos pensar que “ser tautología” es equivalente a “ser consecuencia semántica de la teoría $\emptyset$” así como también “ser teorema” es equivalente a “ser consecuencia sintáctica de $\emptyset$”.

Surge entonces la pregunta: ¿será verdad un resultado análogo para una teoría cualquiera? Tendríamos que definir primero qué significa ser consecuencia semántica de una teoría. Pero la respuesta es positiva, como demostraremos en lo que sigue.

Definición 3.6.1. Una valuación v es un *modelo* para un conjunto de fórmulas Γ si para toda $\mathrm{C} \in \Gamma$ vale que $v(\mathrm{C}) = 1$.

Una fórmula A es *consecuencia semántica* de un conjunto de fórmulas Γ si para todo modelo v de Γ se verifica $v(\mathrm{A}) = 1$. Se denota: $\Gamma \vDash \mathrm{A}$.

Teorema 3.6.2 (Completud fuerte del CPC)**.** *Sean* Γ *una teoría del CPC y* A *una fórmula. Luego* $\Gamma \vdash \mathrm{A}$ *si y solo si* $\Gamma \vDash \mathrm{A}$.

Demostración. Supongamos que $\Gamma \vdash \mathrm{A}$. Como Γ es una teoría entonces $A \in \Gamma$. Luego concluimos que $\Gamma \vDash \mathrm{A}$.

Recíprocamente, supongamos que $\Gamma \vDash \mathrm{A}$ y que no es verdad que $\Gamma \vdash \mathrm{A}$. Luego $\mathrm{A} \notin \Gamma^{\vdash} = \Gamma$, de donde $|\mathrm{A}| \notin |\Gamma|$. Por el TFP existe un ultrafiltro U en A_{CPC} tal que $|\mathrm{A}| \notin U$ y $|\Gamma| \subseteq U$. Tomemos v la valuación asociada a U, que es la dada por el diagrama

$$\begin{tikzcd} \mathcal{L}_{CPC} \arrow[d, "p"'] \arrow[dr, "v"] & \\ A_{CPC} \arrow[r, "q"'] & A_{CPC}/U \end{tikzcd}$$

De esta manera, si $\mathrm{C} \in \Gamma$ entonces $|\mathrm{C}| \in |\Gamma| \subseteq U$, por lo que $v(\mathrm{C}) = q(|\mathrm{C}|) = 1$. Luego, v es modelo de Γ y por lo tanto $v(\mathrm{A}) = q(|\mathrm{A}|) = 1$. Esto significa que $|\mathrm{A}| \in U$, lo cual resulta una contradicción. $\square$

El Teorema 3.6.2 vale también considerando conjuntos de fórmulas cualesquiera (no necesariamente teorías).

Corolario 3.6.3. *Sean* Γ *un conjunto de fórmulas del CPC y* A *una fórmula. Luego* $\Gamma \vdash \mathrm{A}$ *si y solo si* $\Gamma \vDash \mathrm{A}$.

Demostración. Sea A una fórmula tal que $\Gamma \vdash \mathrm{A}$. Luego por el Lema 1.4.10 del Capítulo 1 existen $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n \in \Gamma$ tales que

$$\{\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n\} \vdash \mathrm{A}.$$

Usando iteradamente el Teorema de la Deducción obtenemos que

$$\vdash (\mathrm{A}_1 \to (\mathrm{A}_2 \to (\ldots (\mathrm{A}_n \to \mathrm{A})))).$$

Utilizando el Teorema 3.5.1 inferimos que para toda valuación v vale que $v(\mathrm{A}_1 \to (\mathrm{A}_2 \to (\ldots (\mathrm{A}_n \to \mathrm{A})))) = 1$. Sea v un modelo de Γ. Luego $v(\mathrm{A}_1) = v(\mathrm{A}_2) = \ldots = v(\mathrm{A}_n) = 1$, de donde deducimos que $v(\mathrm{A}) = 1$. En consecuencia, $\Gamma \vDash \mathrm{A}$.

Recíprocamente, sea $\Gamma \vDash \mathrm{A}$. Luego, $\Gamma^{\vdash} \vDash \mathrm{A}$ pues $\Gamma \subseteq \Gamma^{\vdash}$. En virtud del Teorema 3.6.2 se tiene que $\Gamma^{\vdash} \vdash \mathrm{A}$, por lo que $\mathrm{A} \in (\Gamma^{\vdash})^{\vdash} = \Gamma^{\vdash}$, es decir, $\Gamma \vdash \mathrm{A}$. $\square$

3.7. Interpolación

Un resultado destacado que permite desdoblar deducciones en el CPC es el llamado Lema de Craig, que puede extenderse a otras lógicas. Ya hemos demostrado una versión algebraica de dicho lema en el Capítulo 2, Teorema 2.5.13, por lo que la demostración de la propiedad lógica que daremos aquí será entonces consecuencia de aquella.

Podemos considerar, por abuso de lenguaje, que

$$A_{CPC}(X \cap Y) \subseteq A_{CPC}(X) \subseteq A_{CPC}(X \cup Y),$$

$$A_{CPC}(X \cap Y) \subseteq A_{CPC}(Y) \subseteq A_{CPC}(X \cup Y),$$

por lo cual denotaremos $|\mathrm{A}|$ a una clase, sin especificar en cuál de los conjuntos $A_{CPC}(X)$, $A_{CPC}(Y)$, $A_{CPC}(X \cap Y)$ y $A_{CPC}(X \cup Y)$ está.

Teorema 3.7.1 (Lema de Craig)**.** *Si* A *y* B *son fórmulas del CPC que tienen variables proposicionales en común y tales que* $\vdash \mathrm{A} \to \mathrm{B}$ *entonces existe una fórmula* C *("interpolante"), cuyas variables son todas comunes a* A *y a* B*, tal que*

$$\vdash \mathrm{A} \to \mathrm{C} \quad y \quad \vdash \mathrm{C} \to \mathrm{B}.$$

Demostración. Sean X e Y los conjuntos de variables de A y B respectivamente, que por hipótesis tienen intersección no vacía. Sean $A_{CPC}(X)$, $A_{CPC}(Y)$, $A_{CPC}(X \cap Y)$ y $A_{CPC}(X \cup Y)$ las álgebras de Lindenbaum correspondientes a X, Y, $X \cap Y$, $X \cup Y$ respectivamente. Entonces tenemos que $|\mathrm{A}| \in A_{CPC}(X)$ y $|\mathrm{B}| \in A_{CPC}(Y)$, por lo cual $|\mathrm{A}|, |\mathrm{B}| \in A_{CPC}(X \cup Y)$. Como $\vdash \mathrm{A} \to \mathrm{B}$ obtenemos que $|\mathrm{A}| \leq |\mathrm{B}|$.

Por el Teorema 2.5.13 del Capítulo 2 se tiene que existe $|\mathrm{C}|$ tal que $|\mathrm{C}| \in A_{CPC}(X \cap Y)$ y $|\mathrm{A}| \leq |\mathrm{C}| \leq |\mathrm{B}|$.

Luego se tiene que $\vdash \mathrm{A} \to \mathrm{C}$ y $\vdash \mathrm{C} \to \mathrm{B}$, obteniendo así a C como interpolante. □

3.8. Lógica modal

Hemos visto algunas de las principales propiedades del sistema formal de la lógica proposicional clásica. Podríamos decir que esto es un primer paso hacia una fundamentación más correcta de los métodos de razonamiento, que son la base del conocimiento y del desarrollo de las ciencias, en especial de la matemática. Sin embargo, como hemos mencionado en el Capítulo 1 Sección 4, a principios del siglo XX surgen algunas cuestiones que inducen a pensar que la lógica clásica no basta para expresar algunas sutilezas del pensamiento. Se piensa entonces en “estirarla” mediante la introducción de conectivos adecuados (junto con sus correspondientes axiomas y reglas) o bien directamente “romper con el molde” de la lógica clásica negando alguno de sus principios básicos (ver [99]).

Las lógicas modales son ejemplos del primer método, mientras que la lógica intuicionista y las de Łukasiewicz, que trataremos más adelante, son ejemplos del segundo método.

¿Qué son las lógicas modales?

Esencialmente, se trata de sistemas formales en los cuales, además de los conectivos de la lógica clásica, hay otros que denotan modalidades. Los conectivos clásicos son “funcionales-de-verdad” en el sentido de que el valor de verdad de una fórmula compuesta es función solo de los valores de verdad de sus componentes. Consideremos, sin embargo, proposiciones como por ejemplo: *Necesariamente el ladrón es el vecino.* Vemos que su valor de verdad no depende solo de la verdad o falsedad de la proposición *el ladrón es el vecino* sino de otras circunstancias ambientales o temporales en que ella se expresa. Podemos considerar entonces que “necesariamente” es una modalidad que, sintácticamente, se traduce en un conectivo unario. Suele simbolizarse con $\Box$. Lo mismo ocurre con “posiblemente”, cuyo significado es “no es necesario que no” y se simboliza $\Diamond$. Podemos decir que una *modalidad* aplicada a una proposición expresa el modo en que ella es verdadera; por ejemplo, cuándo es verdadera (en qué tiempo) o dónde es verdadera (en qué lugar, en qué mundo).

Existen dos grandes líneas en Lógica Modal que se abrieron a principios del 1900: la Lógica Intensional que estudió Lewis a partir de 1912 y las Lógicas Polivalentes, cuyo estudio fue iniciado por I. Łukasiewicz en 1922 (ver [21] [23]). Estas dos corrientes de pensamiento tienen como motivación común el tratamiento semántico de operadores modales: se trata de cómo atribuir valores de verdad a sentencias con tales operadores.

La forma de Łukasiewicz de abordar el problema, según veremos en el Capítulo 9, es extender el conjunto de valores de verdad incluyendo uno más (el 1/2), con lo cual se obtiene una lógica trivalente. Lo que se extiende entonces es el *codominio* de las funciones de verdad. Luego se generaliza aquélla a la lógica n-valente, obtenida permitiendo un número natural n de valores de verdad: $0, 1/(n-1), \ldots, (n-2)/(n-1), 1$. Posteriormente se llega a admitir valores de verdad que sean números reales en el intervalo $[0, 1]$: es la lógica Ł infinitovalente de Łukasiewicz.

El tratamiento que adopta la Lógica Intensional, utilizada también por Montague (ver [95], [94], [105]) para su modelo de gramática, es el de extender el *dominio* de las funciones que atribuyen valores de verdad, haciendo que el valor de verdad de una proposición compuesta, además de depender del de sus componentes, dependa de otros parámetros o índices como tiempo, circunstancias, mundos posibles.

Como ejemplo, veamos esquemáticamente la definición del sistema K de Lógica Modal.

Los símbolos del lenguaje son: los conectivos $\neg$ (negación), $\vee$ (disyunción) y $\Box$ (operador necesidad), las variables proposicionales p_1, p_2,... y los símbolos auxiliares (,).

Las fórmulas se definen recursivamente como de costumbre (considerando $\Box$ como operador unario). Llamaremos $\mathcal{F}$ al conjunto de las fórmulas.

Se toman como axiomas:

1. Axiomas del sistema $\mathbf{L}_4$,
2. $\Box(\mathrm{A} \rightarrow \mathrm{B}) \rightarrow (\Box\mathrm{A} \rightarrow \Box\mathrm{B})$.

Se toman como reglas:

1. Modus Ponens,
2. A/ $\Box$A.

En cuanto a su semántica, para definirla se toman valuaciones que dependen no solo de las fórmulas sino de un conjunto M de "mundos posibles", que representa las circunstancias en las que la fórmula ocurre. El modelo incluye una relación R de "accesibilidad" entre los elementos de M. Esta puede ser, por ejemplo, una relación de orden que indique un orden temporal. Puede tomarse también como dato un elemento distinguido m_0 del conjunto M que sería el "mundo real".

Podemos definir un *modelo* para el sistema K como una cuaterna $\mathcal{M} = (M, m_0, R, V)$, donde: M es un conjunto no vacío, $m_0 \in M$, R es una relación binaria en M y V, la valuación, es una función $V : \mathcal{F} \times M \longrightarrow \{0, 1\}$ que cumple las siguientes condiciones:

- Si A es una variable, entonces $V(\mathrm{A}, m_0) = 0$ ó $V(\mathrm{A}, m_0) = 1$,
- Si A es $\neg$B, entonces $V(\mathrm{A}, m) = 1$ si y solo si $V(\mathrm{B}, m) = 0$,
- Si A es B$\vee$C, entonces $V(\mathrm{A}, m) = 1$ si y solo si $V(\mathrm{B}, m) = 1$ ó $V(\mathrm{C}, m) = 1$,
- Si A es $\Box$B, entonces $V(\mathrm{A}, m) = 1$ si y solo si para todo m' tal que mRm': $V(\mathrm{B}, m') = 1$.

- Si $V(\mathrm{A}, m) = 1$ y mRm', entonces $V(\mathrm{A}, m') = 1$.

Alternativamente, puede reemplazarse en el modelo la función V por una función $K : \mathcal{F} \longrightarrow \mathcal{P}(M)$ tal que $V(\mathrm{A}, m) = 1$ si y solo si $m \in K(\mathrm{A})$. Es decir,

$$K(\mathrm{A}) = \{m : V(\mathrm{A}, m) = 1\}.$$

Aquí, $K(\mathrm{A})$ es el "conjunto de verdad" de A.

Observemos que si A es $\neg\Box\neg$B ("es posible B") entonces $V(\mathrm{A}, m) = 1$ si y solo si existe m' tal que mRm': $V(\mathrm{B}, m') = 1$. Esto significa intuitivamente que "Necesariamente p" es verdadera si y solo si p es verdadera en todas las circunstancias en que pueda darse. Análogamente: "Posiblemente p" es verdadera si existe alguna circunstancia en la que p sea verdadera.

Esta noción de "mundos posibles" ya aparece por el 1500 en Luis de Molina, en el Siglo de Oro español, y es retomada posteriormente por Leibniz. En la segunda mitad del siglo XX trabajan sobre esas ideas Hintikka y Kripke. Este último interpreta la lógica modal dando la definición de modelo que vimos (particularmente en el caso en que R es una relación de orden) y la aplica después al cálculo intuicionista. Esto le permite obtener la completud de este con relación a los llamados posteriormente *modelos de Kripke*, según veremos en el Capítulo 5.

3.9. Ejercicios

1. Sea A una fórmula de $\mathbf{L}_4$ y sea $\mathbf{L_4}^+$ la extensión que tiene como axiomas los de $\mathbf{L}_4$ más el axioma A. Sean Υ y Υ^+ los conjuntos de teoremas de $\mathbf{L}_4$ y de $\mathbf{L_4}^+$ respectivamente. Probar que $\Upsilon = \Upsilon^+$ si y solo si A es un teorema de $\mathbf{L}_4$.

2. Sea C la fórmula $(\neg \mathrm{p} \to \mathrm{q}) \to (\mathrm{p} \to \neg \mathrm{q})$.

   a) Encontrar fórmulas A y B tales que $(\neg \mathrm{A} \to \mathrm{B}) \to (\mathrm{A} \to \neg \mathrm{B})$ sea una contradicción.

   b) Probar que $\mathbf{L_4}^+$ (la extensión de $\mathbf{L}_4$ que tiene como axiomas los de $\mathbf{L}_4$ más el axioma C) es tal que $\Upsilon \subsetneqq \Upsilon^+$. ¿Es $\mathbf{L_4}^+$ consistente?

3. Supongamos que $\mathbb{P}$ es un sistema formal en el que valen al menos los axiomas $(\mathrm{L_4}1)$,..., $(\mathrm{L_4}8)$. Sea $V_{\mathrm{A}} = \{\mathrm{B} \in \mathcal{L} : \ \vdash \mathrm{A} \to \mathrm{B}\}$.

   a) Probar que $V_{\mathrm{A}} = \mathrm{A}^{\vdash}$, donde, por abuso de notación, escribimos $\mathrm{A}^{\vdash}$ en lugar de $\{\mathrm{A}\}^{\vdash}$.

   b) Probar que $V_{\mathrm{A}\wedge\neg\mathrm{A}} = \mathcal{L}$.

4. En las mismas condiciones que en el ejercicio anterior:

   a) Probar que $\mathrm{A}^{\vdash} \cap \mathrm{B}^{\vdash} = (\mathrm{A} \vee \mathrm{B})^{\vdash}$.

   b) Deducir de esto que el conjunto $\Omega^- = \{\mathrm{A}^{\vdash} : \mathrm{A} \in \mathcal{L}\}$ es cerrado por intersecciones finitas, es decir que si se tiene que $\mathrm{A}_1^{\vdash}, \ldots, \mathrm{A}_n^{\vdash} \in \Omega^-$ entonces $\mathrm{A}_1^{\vdash} \cap \cdots \cap \mathrm{A}_n^{\vdash} \in \Omega^-$.

   c) Probar que el conjunto Ω de uniones de elementos de Ω^- más el vacío es una topología sobre $\mathcal{L}$.

5. En las mismas condiciones, sea $W_{\mathrm{A}} = \{\mathrm{B} \in \mathcal{L} : \ \vdash \mathrm{B} \to \mathrm{A}\}$.

   a) Probar que
   $$W_{\mathrm{A}} \cap W_{\mathrm{B}} = W_{\mathrm{A}\wedge\mathrm{B}}.$$

   b) Probar que $W_{\mathrm{A}\to\mathrm{A}} = \mathcal{L}$.

   c) Probar que $\Pi^- = \{W_{\mathrm{A}} : \mathrm{A} \in \mathcal{L}\}$ es cerrado por intersecciones finitas.

   d) Probar que el conjunto Π de uniones de elementos de Π^- más el vacío es una topología sobre $\mathcal{L}$.

   Nota: en los ejercicios que siguen el sistema formal de referencia será $\mathbf{L}_4$.

6. Sea $\Gamma = \{A_1, A_2, \ldots, A_n\}$ un conjunto finito de fórmulas, A y B fórmulas. Probar que si toda valuación que satisface $\Gamma \cup \{\mathrm{A}\}$ satisface también B entonces la siguiente fórmula es una tautología:

$$(\mathrm{A}_1 \wedge \cdots \wedge \mathrm{A}_\mathrm{n}) \to (\mathrm{A} \to \mathrm{B}).$$

7. Sea Γ un conjunto de fórmulas y A una fórmula tales que $\Gamma \vdash \mathrm{A}$. Probar que existe un subconjunto finito Γ_0 de Γ tal que $\Gamma_0 \vdash \mathrm{A}$.

8. (Teorema de la deducción) Sea Γ un conjunto de fórmulas, A, B fórmulas tales que $\Gamma \cup \{\mathrm{A}\} \vdash \mathrm{B}$. Probar usando los dos ejercicios precedentes y la completud que $\Gamma \vdash \mathrm{A} \to \mathrm{B}$.

9. Sea $\Gamma = \{\mathrm{A} \to \mathrm{C}, \mathrm{B} \to \mathrm{C}\}$. Probar, usando ($\mathrm{L}_4$8), que $\Gamma \vdash (\mathrm{A} \vee \mathrm{B}) \to \mathrm{C}$ (ver 3 en Ejemplo 3.1.2).

10. Probar que $\{\mathrm{C} \to \mathrm{A}, \mathrm{C} \to \mathrm{B}\} \vdash \mathrm{C} \to (\mathrm{A} \wedge \mathrm{B})$ usando el Teorema de la Deducción (el segundo de Ejemplos 3.1.6).

11. a) Deducir las reglas (R11), (R12) y (R13).

    b) Usando TD y las reglas (R1) y (R9) deducir (R15).

    c) Deducir (R17) aplicando TD y las reglas (R14) y (R16).

12. Sea Γ una teoría del CPC. Se dice que Γ es *completa* si para toda fórmula A de $\mathcal{L}$ se tiene que $\mathrm{A} \in \Gamma$ ó $\neg\mathrm{A} \in \Gamma$ y se dice que es *prima* si para todo par A, B de fórmulas de Γ tal que $\mathrm{A} \vee \mathrm{B} \in \Gamma$ se tiene que $\mathrm{A} \in \Gamma$ ó $\mathrm{B} \in \Gamma$. Probar que Γ es completa si y solo si es prima. (Ayuda: usar (R18), (R8) y el principio del tercero excluido).

13. Mostrar que la aplicación canónica $p : \mathcal{L} \longrightarrow A_{CPC}$ es una valuación.

14. Probar que si es v una A-valuación y $h : A \longrightarrow B$ un homomorfismo entonces, $v' = h \circ v$ es una B-valuación (Lema 3.5.9).

Bibliografía del Capítulo 3

- Bell J.L. and Slomson A.B., *Models and Ultraproducts.* North-Holland, 1969.
- Daigneault A., *Freedom in polyadic algebras and two theorems of Beth and Craig.* Michigan Math. J., 11 (1964), no. 2, 129–135.
- Hamilton A.G., *Logic for Mathematicians.* Cambridge University Press, 1978.
- Pitts A.M., *Amalgamation and interpolation in the category of Heyting algebras.* J. Pure Appl. Algebra, 29 (1983), 155–165.
- Sagastume de Gallego M. *Um exemplo de modelo intensional.* Cadernos de Estudos Linguísticos, 12 (1987), 25–41.
- Sagastume M., *Sobre la Gramática de Montague.* Manuscrito inédito.
- Sarrión Morillo E., Hernández Antón I., *Extensiones de la Lógica Clásica, Introducción a la Lógica Modal*, 2012.
- Shannon C., *A symbolic analysis of relay and switching circuits*, Trans. AIEE, 57 (1938), no. 12, 713–723.
- Thomason R., *Formal Philosophy: Selected Papers of R. Montague.* Editado por R. Thomason, New Haven and London, Yale University Press, 1974.

Capítulo 4

Álgebras de Heyting

Hemos visto en el Capítulo 2 que toda álgebra de Boole es isomorfa a una subálgebra de un álgebra de Boole cuyo universo es de la forma $\mathcal{P}(X)$ para cierto conjunto X. De manera que podemos siempre pensar a las álgebras de Boole como "dentro" de un álgebra de partes de un conjunto. En la clase de las álgebras de Heyting, aquellas cuyo universo es un conjunto de abiertos de un espacio topológico juegan un rol análogo a las álgebras de partes. Podemos pensar que un álgebra de Heyting siempre está "dentro" de un álgebra de abiertos de un espacio topológico. En particular, estos abiertos pueden ser los crecientes de cierto conjunto ordenado o los asociados a un álgebra de clausura, como veremos en los teoremas de representación.

Las álgebras de Heyting generalizan a las álgebras de Boole: toda álgebra de Boole puede ser dotada de una estructura de álgebra de Heyting.

Veremos en este capítulo las propiedades algebraicas básicas de las álgebras de Heyting, especialmente aquellas que pueden traducirse en propiedades lógicas; por ejemplo el teorema de la deducción o el de teorema de Glivenko.

Hemos visto que el Cálculo Proposicional Clásico (CPC) tiene como álgebra de Lindenbaum un álgebra de Boole. En el próximo capítulo trataremos el Cálculo Proposicional Intuicionista (CPI) y demostraremos que lo que llamaremos su álgebra de Lindenbaum es un álgebra de Heyting.

4.1. Ejemplos y propiedades

En el Capítulo 2 definimos las álgebras de Heyting como retículos con elemento mínimo 0 tales que para cada par de elementos x e y existe $x \to y$, siendo $x \to y$ el máximo de los elementos z tales que $x \wedge z \leq y$. Alternativamente, también vimos que las álgebras de Heyting pueden definirse como retículos con primer elemento en donde existe una operación binaria $\to$ que satisface para cada x, y, z la condición $x \wedge y \leq z$ si y solo si $y \leq x \to z$.

En lo que sigue vamos a definir a las álgebras de Heyting como álgebras, es decir, desde el punto de vista del Álgebra Universal. Posteriormente probaremos que esta definición es equivalente a la definición de álgebra de Heyting dada en 2.2.11 del Capítulo 2.

Definición 4.1.1. Un álgebra de Heyting es un álgebra $\langle H, \wedge, \vee, \to, 0, 1\rangle$ con tres operaciones binarias $\wedge, \vee, \to$ y dos ceroarias $0, 1$ tal que se verifican las condiciones:

H1 El reducto $\langle H, \wedge, \vee, 0, 1\rangle$ es un retículo distributivo acotado,

H2 $x \to x = 1$,

H3 $(x \to y) \wedge y = y, \quad (x \to y) \wedge x = x \wedge y$,

H4 $x \to (y \wedge z) = (x \to y) \wedge (x \to z), \quad (x \vee y) \to z = (x \to z) \wedge (y \to z)$.

Observación 4.1.2. Hay otras condiciones equivalentes a **(H1)**,...,**(H4)** que permiten definir la estructura de álgebra de Heyting. Por ejemplo, en [2], IX,4 se define como un álgebra $\langle H, \wedge, \vee, \to, 0\rangle$ tal que:

El reducto $\langle H, \wedge, \vee, 0\rangle$ es un retículo distributivo con 0,

$x \wedge (x \to y) = x \wedge y$,

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

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

Los dos lemas siguientes prueban que la definición de álgebra de Heyting como retículo con primer elemento en donde para cada x, y existe el máximo del conjunto de los z tales que $x \wedge z \leq y$ (ver Definición 2.2.11 dada en el Capítulo 2) es equivalente a la Definición 4.1.1.

Lema 4.1.3. *Sea $\langle H, \wedge, \vee, \to, 0, 1\rangle$ tal que el reducto $\langle H, \wedge, \vee, 0, 1\rangle$ es un retículo distributivo acotado en el que se verifican* **H2**, **H3**, **H4**. *Entonces la operación $\to$ satisface que $x \wedge y \leq z$ si y solo si $y \leq x \to z$.*

Demostración. Sea $x \wedge y \leq z$. Luego, $(x \wedge y) \wedge z = x \wedge y$. Por **H4** tenemos que

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

De allí obtenemos que $x \to (x \wedge y) \leq x \to z$.

Además, por **H2**, **H4** y por ser 1 el último elemento vale que $x \to (x \wedge y) = x \to y$. Por ende, $x \to y \leq x \to z$. En virtud de **H3** tenemos que $y \leq x \to y$, por lo cual $y \leq x \to z$.

Recíprocamente, sea $y \leq x \to z$. Luego $x \wedge y \leq x \wedge (x \to z)$ y por **H3**, $x \wedge (x \to z) = x \wedge z \leq z$. □

Lema 4.1.4. *En toda álgebra de Heyting valen las siguientes propiedades de monotonía:*

(M1) *si* $x \leq y$ *entonces* $z \to x \leq z \to y$*,*

(M2) *si* $x \leq y$ *entonces* $y \to z \leq x \to z$*.*

Demostración. Supongamos que $x \leq y$. Para probar (M1) basta ver que $z \wedge (z \to x) \leq y$. Pero esto es verdad, dado que por **H3** se tiene que $z \wedge (z \to x) = z \wedge x \leq x \leq y$. Análogamente se prueba (M2). □

Lema 4.1.5. *Sea* $\langle H, \wedge, \vee, 0 \rangle$ *un retículo en el cual existe la operación binaria* $\to$ *que verifica* $x \wedge y \leq z$ *si y solo si* $y \leq x \to z$*. Entonces,* $\langle H, \wedge, \vee, \to, 0, 1 \rangle$ *es un álgebra en la cual valen* **H2**, **H3**, **H4**.

Demostración. Primero recordemos que necesariamente existe último elemento 1, ya que por ejemplo $0 \to 0$ es el máximo elemento de H. También recordemos que $\langle H, \wedge, \vee, 0, 1 \rangle$ es un retículo distributivo acotado.

A continuación probaremos **H3** y **H4**, dejando **H2** como ejercicio.

Como $x \wedge y \leq y$, se tiene que $y \leq x \to y$. Luego, $x \wedge y \leq x \wedge (x \to y)$. Veamos la otra desigualdad. Como $x \to y \leq x \to y$, implica $x \wedge (x \to y) \leq y$. Además, $x \wedge (x \to y) \leq x$. De estas últimas desigualdades se deduce que $x \wedge (x \to y) \leq x \wedge y$. Por ende hemos probado **H3**.

A continuación probaremos **H4**. De $y \wedge z \leq y$ e $y \wedge z \leq z$ inferimos que $x \to (y \wedge z) \leq x \to y$ y $x \to (y \wedge z) \leq x \to z$. Tomando ínfimos en las desigualdades anteriores obtenemos que

$$x \to (y \wedge z) \leq (x \to y) \wedge (x \to z).$$

Para probar la otra desigualdad basta probar que

$$x \wedge ((x \to y) \wedge (x \to z) \leq (y \wedge z),$$

lo cual se deduce usando dos veces **H3**.

Para probar que

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

se usa (M2) de 4.1.4. □

Los lemas 4.1.3 y 4.1.5 justifican la Definición 4.1.1.

Frecuentemente nos referiremos a un álgebra de Heyting mencionando solo su conjunto subyacente (ver 1.3.3).

Ejemplos 4.1.6.

1. Todo retículo distributivo finito puede ser dotado de una estructura de álgebra de Heyting.

   En efecto, sea $\langle L, \vee, \wedge, 0, 1\rangle$ un retículo finito y sean $a, b \in L$. Consideremos el conjunto $I_{ab} = \{c \in L : \ a \wedge c \leq b\} = \{c_1, c_2, \ldots, c_n\}$. Este conjunto es no vacío porque contiene al 0. Definiendo $t = \bigvee I_{ab}$ se puede probar que $t = a \to b$. En efecto,

   $$\begin{aligned} a \wedge t &= a \wedge (c_1 \vee c_2 \vee \cdots \vee c_n) \\ &= (a \wedge c_1) \vee (a \wedge c_2) \vee \cdots \vee (a \wedge c_n) \\ &\leq b. \end{aligned}$$

   Sin embargo, existen retículos distributivos (infinitos) en los que no es posible definir la operación $\to$. En efecto, tomemos el retículo $(\mathbb{N}, \preceq)$ definido en 3. del Ejemplo 2.1.5 del Capítulo 2. Este retículo es distributivo y acotado. Para el elemento 2 y el 1 (1 es el mínimo del retículo) veamos que no existe $2 \to 1$. En efecto, se tiene que

   $$\begin{aligned} \{z : \ z \wedge 2 \preceq 1\} &= \{z : \ MCD(z, 2) = 1\} \\ &= \{z : \ z \text{ impar}\}. \end{aligned}$$

   Claramente este conjunto no tiene máximo.

2. Toda álgebra de Boole puede ser dotada de una estructura de álgebra de Heyting, siendo $x \to y = \overline{x} \vee y$.

3. Un conjunto totalmente ordenado puede ser dotado de una estructura de álgebra de Heyting.

   Sea $(P, \leq)$ un conjunto totalmente ordenado. En el Capítulo 2 vimos que existen supremo e ínfimo para cada par de elementos. Podemos además definir una implicación de la siguiente manera:

   $$p \to q = \begin{cases} 1 & \text{si } p \leq q \\ q & \text{si } q < p. \end{cases}$$

   Veamos que se cumple $r \wedge p \leq q$ si y solo si $r \leq p \to q$.

$\Longrightarrow$ Sea $r \wedge p \leq q$. Si $p \leq q$ entonces $r \leq 1 = p \to q$. Si $p > q$, entonces $r \wedge p = r \leq q$ (caso contrario sería $r \wedge p = p \leq q$, lo cual es un absurdo). Es decir, $r \leq p \to q$.

$\Longleftarrow$ Sea $r \leq p \to q$. Debemos probar que $r \wedge p \leq q$. Supongamos que $p \leq q$. Si $r \leq p$ entonces $r \leq p \leq q = p \to q$. Si $r > p$ entonces $q \geq p = r \wedge p$. Supongamos ahora que $p \geq q$. Como $r \leq p \to q < p$ tenemos que $r \leq p$. Por lo tanto, $p \wedge r = r \leq q$.

4. Ya hemos mencionado en el Capítulo 2 que los abiertos de un espacio topológico sobre un conjunto X, con las operaciones $\cup$, $\cap$ forman un retículo distributivo acotado, siendo $\emptyset$ el primer elemento y X el último. También observamos que no constituyen un álgebra de Boole, ya que el complemento de un abierto no tiene por qué ser abierto. Pero los abiertos de X sí forman un álgebra de Heyting. Nos falta definir la implicación.

   Sea $(X, \mathcal{T})$ un espacio topológico.[1] Dado un subconjunto Y de X, el *interior* de Y, denotado Y^o, es el mayor abierto contenido en Y. Se caracteriza por la siguiente condición:

   $$x \in Y^o \text{ si y solo si } Y \text{ contiene un abierto que contiene a } x.$$

   De esta caracterización surge que

   (1) $Y^o \subseteq Y$,

   (2) si un conjunto Y es abierto entonces $Y = Y^o$,

   (3) si $Y \subseteq Z$ entonces $Y^o \subseteq Z^o$.

   En forma dual, la *clausura* de un conjunto Y, denotada $\overline{Y}$, se define por:

   $$x \in \overline{Y} \text{ si y solo si para todo abierto } U \text{ que contiene a } x,\ U \cap Y \neq \emptyset.$$

   Se puede mostrar que

   (4) $\overline{Y^c} = (Y^o)^c$, siendo $A^c = X - A$ (el complemento de A en X).

   De esta manera, dados dos abiertos A y B de $\mathcal{T}$ definimos

   $$A \to B = (A^c \cup B)^o,$$

   Probaremos que para todo abierto D se cumple que

[1] Las nociones topológicas que usaremos pueden consultarse, por ejemplo, en [83].

$$D \cap A \subseteq B \quad \text{si y solo si} \quad D \subseteq A \to B$$

$\Longrightarrow$ Sea $D \cap A \subseteq B$. Entonces,
$A^c \cup (D \cap A) \subseteq A^c \cup B$, de donde
$A^c \cup D \subseteq A^c \cup B$.
Luego: $D \subseteq A^c \cup D \subseteq A^c \cup B$.
Por la propiedad (3) del interior: $D^o \subseteq (A^c \cup B)^o$.
Entonces, por (2): $D = D^o \subseteq (A^c \cup B)^o = A \to B$.

$\Longleftarrow$ Sea $D \subseteq A \to B$.
Luego, como $(A^c \cup B)^o \subseteq A^c \cup B$ (por la propiedad (1) del interior), se tiene que
$A \cap D \subseteq A \cap (A^c \cup B) = A \cap B \subseteq B$.

Hemos probado entonces que $\langle \mathcal{T}, \cup, \cap, \to, \emptyset, X \rangle$ es un álgebra de Heyting.

5. Sea $(P, \leq)$ un conjunto ordenado. Hemos visto en el Capítulo 2 que $\langle P^+, \cup, \cap, \emptyset, P \rangle$ es un retículo acotado, siendo

$$P^+ = \{Q : \; Q \subseteq P, \; Q \text{ creciente}\}.$$

Veamos que este es, en realidad, un caso particular del anterior (ver Ejemplos 2.1.5 del Capítulo 2). Podemos considerar a los conjuntos crecientes como los abiertos de una topología sobre P. Esto es correcto: $\emptyset$ y P son crecientes, intersección finita y unión cualquiera de crecientes es creciente.

Debemos calcular entonces $(R^c \cup S)^o$.

Para lograr este fin, calculemos primero la clausura de un conjunto cualquiera D. Queremos probar que $\overline{D} = (D]$, siendo $(D] = \{z : z \leq t$ para cierto $t \in D\}$ (ver 2.1.5, Ejemplo 7).

En efecto, $x \in \overline{D}$ si y solo si todo creciente U que contiene a x tiene intersección no vacía con D. Eso equivale a decir que $[x)$ tiene intersección no vacía con D. Esto significa que existirá un $y \geq x$ tal que $y \in D$, lo que es equivalente a decir que $x \in (D]$, como queríamos probar.

Usando esto y la propiedad (4) del interior tenemos que:

$$(R^c \cup S)^o = (\overline{(R^c \cup S)^c})^c = ((R^c \cup S)^c]^c = (R \cap S^c]^c.$$

Por lo tanto, hemos probado que $\langle P^+, \cup, \cap, \to, \emptyset, P \rangle$ es un álgebra de Heyting, siendo $R \to S = (R \cap S^c]^c$.

Propiedades

Veremos ahora algunas propiedades de las álgebras de Heyting que necesitaremos más adelante. Denotaremos como x^* al pseudocomplemento de x, que es $x \to 0$. Para las demostraciones usaremos indistintamente las definiciones equivalentes que hemos dado para las álgebras de Heyting. En particular, recordemos la siguiente propiedad del pseudocomplemento: $x \wedge y = 0$ si y solo si $x \leq y^*$.

Lema 4.1.7. *Sea $\langle H, \wedge, \vee, \to, 0, 1\rangle$ un álgebra de Heyting. Se verifican las siguientes propiedades para toda terna x, y, z de elementos de H:*

(a) $x \leq y$ *si y solo si* $x \to y = 1$,

(b) $x \to (y \to z) = (x \wedge y) \to z$,

(c) $(x \vee y)^* = x^* \wedge y^*$,

(d) $x \to y \leq y^* \to x^*$,

(e) $x \wedge (y \to z) = x \wedge ((x \wedge y) \to (x \wedge z))$.

Demostración.

(a) Si $x \leq y$ entonces: $x \wedge 1 = x \leq y$, luego 1 es el máximo de los z tales que $x \wedge z \leq y$, es decir, $x \to y = 1$. Recíprocamente, sea $x \to y = 1$. Como $1 \leq x \to y$ tenemos que $x \leq y$.

(b) La desigualdad $(x \wedge y) \to z \leq x \to (y \to z)$ equivale a probar que $(x \wedge y) \wedge ((x \wedge y) \to z) \leq z$, lo cual es verdadero. La recíproca se prueba similarmente.

(c) Es consecuencia de **H4**.

(d) Lo que se pide es equivalente a $y^* \wedge (x \to y) \leq x^*$, que a su vez es equivalente a $x \wedge (y^* \wedge (x \to y)) = 0$. Asociando y conmutando: $(x \wedge (x \to y)) \wedge y^* = (x \wedge y) \wedge y^* = x \wedge (y \wedge y^*) = x \wedge 0 = 0$.

(e) Probemos en primer lugar las siguientes desigualdades:

$$x \wedge (y \to z) \leq (x \wedge y) \to (x \wedge z) \tag{4.1}$$

$$x \wedge ((x \wedge y) \to (x \wedge z)) \leq y \to z. \tag{4.2}$$

Para probar (4.1) basta ver que $(x \wedge y) \wedge (x \wedge (y \to z)) \leq x \wedge z$. Esto se cumple porque el primer miembro es $x \wedge y \wedge z$. Análogamente, para probar (4.2) basta probar que $y \wedge (x \wedge ((x \wedge y) \to (x \wedge z))) \leq z$, lo cual también se cumple.

Tomando ínfimo con x en ambos miembros de (4.1) y (4.2) entonces obtenemos las dos desigualdades que prueban la igualdad buscada. □

Lema 4.1.8. *Sea $\langle H, \wedge, \vee, \to, 0, 1\rangle$ un álgebra de Heyting. Se verifican las siguientes propiedades para todo x e y de H:*

(a) $x \leq x^{**}$,

(b) $x^{***} = x^*$,

(c) $x \wedge y = 0$ *si y solo si* $x^{**} \wedge y = 0$,

(d) $(x \wedge y)^{**} = x^{**} \wedge y^{**}$,

(e) $(x \vee y)^{**} = (x^{**} \vee y^{**})^{**}$,

(f) $(x \to y)^* = x^{**} \wedge y^*$.

Demostración.

(a) Se deja como ejercicio.

(b) También se deja como ejercicio.

(c) Como $x \wedge y \leq x^{**} \wedge y$, $x^{**} \wedge y = 0$ implica $x \wedge y = 0$. Recíprocamente, sea $x \wedge y = 0$. Eso implica $y \leq x^* = x^{***}$, por (b). Luego, $x^{**} \wedge y = 0$.

(d) En primer lugar, por la propiedad de monotonía (M2), como $x \wedge y \leq x, y$ se tiene $x^*, y^* \leq (x \wedge y)^*$, de donde $(x \wedge y)^{**} \leq x^{**}, y^{**}$ y por lo tanto $(x \wedge y)^{**} \leq x^{**} \wedge y^{**}$.

A continuación probaremos la otra desigualdad, es decir, que $x^{**} \wedge y^{**} \leq (x \wedge y)^{**}$. Basta ver que $x^{**} \wedge y^{**} \wedge (x \wedge y)^* = 0$. Por (c), esto es equivalente a $x \wedge y^{**} \wedge (x \wedge y)^* = 0$, que a su vez es equivalente a $x \wedge y \wedge (x \wedge y)^* = 0$. Pero esto último es cierto.

(e) Por (c) del Lema 4.1.7, $(x \vee y)^{**} = (x^* \wedge y^*)^*$ y $(x^{**} \vee y^{**})^{**} = (x^{***} \wedge y^{***})^*$. Por (b) tenemos que $(x^{***} \wedge y^{***})^* = (x^* \wedge y^*)^*$. Luego, $(x \vee y)^{**} = (x^{**} \vee y^{**})^{**}$.

(f) En primer lugar, $y \leq x \to y$ implica que $(x \to y)^* \leq y^*$. Por (M1) del Lema 4.1.4 tenemos que $x^* = x \to 0 \leq x \to y$, lo que implica $(x \to y)^* \leq x^{**}$. Por ende, $(x \to y)^* \leq y^* \wedge x^{**}$.

Por otra parte, usando dos veces la propiedad (e) del Lema 4.1.7,

$$\begin{aligned}
x^{**} \wedge y^* \wedge (x \to y) &= x^{**} \wedge y^* \wedge ((x \wedge y^*) \to (y \wedge y^*)) \\
&= x^{**} \wedge y^* \wedge ((x \wedge y^*) \to 0) \\
&= x^{**} \wedge y^* \wedge ((x \wedge y^*) \to (0 \wedge y^*)) \\
&= x^{**} \wedge y^* \wedge (x \to 0) \\
&= x^{**} \wedge y^* \wedge x^* \\
&= 0.
\end{aligned}$$

Por lo tanto

$$y^* \wedge x^{**} \leq (x \to y)^*,$$

de donde $y^* \wedge x^{**} = (x \to y)^*$. □

Lema 4.1.9. *Sea* $\langle H, \wedge, \vee, \to, 0, 1\rangle$ *un álgebra de Heyting. Las siguientes aserciones son equivalentes:*

(a) $\langle H, \wedge, \vee, ^*, 0, 1\rangle$ *es un álgebra de Boole,*

(b) $x \vee x^* = 1$,

(c) $x^{**} = x$,

(d) $x \to y = y^* \to x^*$,

(e) $x \to y = x^* \vee y$.

Demostración.

(a)$\Longleftrightarrow$(b) Por ser * pseudocomplemento vale que $x \wedge x^* = 0$. La condición (b) asegura que * es complemento en H.

(b)$\Longrightarrow$(c) Por (a) del Lema 4.1.7, $x \leq x^{**}$. Luego obtenemos que

$$\begin{aligned}
x^{**} &= x^{**} \wedge 1 \\
&= x^{**} \wedge (x \vee x^*) \\
&= (x^{**} \wedge x) \vee (x^{**} \wedge x^*) \\
&= x \vee 0 \\
&= x.
\end{aligned}$$

(c)$\Longrightarrow$(d) Por (d) del Lema 4.1.8 tenemos que

$$y^* \to x^* \leq x^{**} \to y^{**}$$

y usando la hipótesis (c) tenemos que

$$y^* \to x^* \leq x \to y.$$

La otra desigualdad sale de (f) del Lema 4.1.8.

(d)$\Longrightarrow$(e) Probemos primero que (d) implica (b).

Sea $z \in H$. Veamos que $z \to (x^* \vee x) = 1$. Por (d) y por 4.1.7,(c):

$$\begin{aligned} z \to (x^* \vee x) &= (x^* \vee x)^* \to z^* \\ &= (x^{**} \wedge x^*) \to z^* \\ &= 0 \to z \\ &= 1. \end{aligned}$$

Luego $z \leq x^* \vee x$ para todo z. Tomando $z = 1$ obtenemos que $x^* \vee x = 1$.

Probemos ahora (e). Para esto debemos ver que $x^* \vee y$ es el máximo z tal que $z \wedge x \leq y$.

En primer lugar,

$$\begin{aligned} (x^* \vee y) \wedge x &= (x^* \wedge x) \vee (y \wedge x) \\ &= 0 \vee (y \wedge x) \\ &\leq y \end{aligned}$$

Veamos ahora que es máximo. Se tiene:

$$\begin{aligned} z \wedge x \leq y \quad &\text{si y solo si} \quad z \leq x \to y \\ &\text{si y solo si} \quad z \leq y^* \to x^* \\ &\text{si y solo si} \quad z \wedge y^* \leq x^*. \end{aligned}$$

Usando esa última desigualdad y el hecho de que $z \wedge y \leq y$ obtenemos tomando supremo en ambos miembros y distribuyendo:

$$z \wedge (y^* \vee y) \leq x^* \vee y,$$

y como $y^* \vee y = 1$, deducimos que

$$z \leq x^* \vee y,$$

como queríamos demostrar.

(e)$\Longrightarrow$(b) Es consecuencia de **H2**. $\square$

4.2. Congruencias y homomorfismos

En esta sección vamos a estudiar las congruencias en álgebras de Heyting, es decir, aquellas relaciones de equivalencia que permiten definir una estructura de álgebra de Heyting en el correspondiente cociente.

Algunas de las demostraciones que vimos en el Capítulo 2 para álgebras de Boole serán las mismas en este caso. En particular, probaremos que existe una biyección entre las congruencias y los filtros de un álgebra de Heyting dada.

Ya hemos definido filtro en un retículo y filtro implicativo en un álgebra de Boole, tomando como implicación: $x \to y = \overline{x} \vee y = x^* \vee y$.

Un *filtro implicativo* en un álgebra de Heyting se define como en el caso de las álgebras de Boole, solo que tomamos como implicación la regida por las condiciones **H1-H4**.

Lema 4.2.1. *Sean H un álgebra de Heyting y $F \subseteq H$. Entonces F es un filtro implicativo si y solo si F es un filtro.*

Demostración. La demostración es la misma que la hecha en el Lema 2.3.5, Capítulo 2, para álgebras de Boole. □

Analicemos ahora, dado un filtro, la condición que, según veremos, define una congruencia de álgebras de Heyting.

Lema 4.2.2. *Sea H un álgebra de Heyting, F un filtro de H. Las siguientes condiciones son equivalentes:*

(a) *Existe $f \in F$ tal que $x \wedge f = y \wedge f$,*

(b) $x \to y \in F$, $y \to x \in F$,

(c) $(x \to y) \wedge (y \to x) \in F$.

Demostración.

(a)$\Longrightarrow$(b) Supongamos que $x \wedge f = y \wedge f$. Luego, $x \wedge f \leq y$ y por ende $f \leq x \to y$, de donde se sigue que $x \to y \in F$. Análogamente, $y \to x \in F$.

(b)$\Longrightarrow$(c) Vale por ser F filtro.

(c)$\Longrightarrow$(a) Sea $f = (x \to y) \wedge (y \to x)$. Tenemos que

$$\begin{aligned} x \wedge ((x \to y) \wedge (y \to x)) &= x \wedge y \wedge (y \to x) \\ &= x \wedge y. \end{aligned}$$

Análogamente $y \wedge ((x \to y) \wedge (y \to x)) = x \wedge y$. Es decir, $x \wedge f = y \wedge f$. □

Observación 4.2.3. Según lo visto en las nociones de Álgebra Universal del Capítulo 1, una congruencia en un álgebra de Heyting es una relación de equivalencia R que verifica las siguientes condiciones:

(Inf) Si xRy y uRv entonces $(x \wedge u)R(y \wedge v)$,

(Sup) Si xRy y uRv entonces $(x \vee u)R(y \vee v)$,

(Imp) Si xRy y uRv entonces $(x \to u)R(y \to v)$.

A diferencia de lo que sucede con las álgebras de Boole, en un álgebra de Heyting sí puede haber congruencias de retículo que no sean de Heyting (que no cumplan **Imp**). El siguiente es un ejemplo sencillo de esa situación.

Sea $\langle K, \vee, \wedge, \to, 0, 1\rangle$ donde $K = \{0, a, 1\}$, la cadena de tres elementos con la implicación definida como en el tercero de los Ejemplos 4.1.6. Sea $P = \{\{0, a\}, \{1\}\}$ una partición, la cual determina una congruencia R de retículo. Sin embargo, no cumple **Imp**. En efecto, se tiene aRa y $0Ra$ pero $a \to 0 = 0$ no está relacionado con $a \to a = 1$.

Hemos visto en 2.3.9 del Capítulo 2 que la condición (a) del Lema 4.2.2 define una congruencia de retículos y que $F = |1|$. Veamos que dicha congruencia de retículos es también una congruencia de álgebras de Heyting.

Teorema 4.2.4. *Sea F un filtro en un álgebra de Heyting H. Sea $\equiv_F$ la siguiente relación binaria definida en H:*

$$x \equiv_F y \text{ si y solo si existe } f \in F \text{ tal que } x \wedge f = y \wedge f.$$

La relación $\equiv_F$ es una congruencia. Más aún, $F = |1|$.

Demostración. Solo debemos probar **Imp**. Para ello usaremos **H3** de la Definición 4.1.1. Sean $x, y, u, v \in H$ tales que xRy, uRv. Entonces, existen $f, f' \in F$ tales que $x \wedge f = y \wedge f$, $u \wedge f' = v \wedge f'$. Observemos que $f \wedge f' \in F$. Veamos que

$$(x \to u) \wedge (f \wedge f') = (y \to v) \wedge (f \wedge f').$$

Probar que $(x \to u) \wedge (f \wedge f') \leq y \to v$ equivale a ver que

$$(x \to u) \wedge y \wedge f \wedge f' \leq v.$$

Notemos que

$$\begin{aligned}(x \to u) \wedge y \wedge f \wedge f' &= (x \to u) \wedge x \wedge f \wedge f' \\ &\leq u \wedge f \wedge f' \\ &\leq v \wedge f \wedge f' \\ &\leq v.\end{aligned}$$

Por ende, $(x \to u) \wedge (f \wedge f') \leq y \to v$, por lo cual

$$(x \to u) \wedge (f \wedge f') \leq (y \to v) \wedge (f \wedge f').$$

La otra desigualdad sale automáticamente, por la simetría del razonamiento. □

Con esto hemos probado que a cada filtro le corresponde una congruencia con respecto a la cual ese filtro es justamente la clase del 1. Veamos, recíprocamente, que dada una congruencia, si tomamos la clase del 1 obtenemos un filtro y la congruencia es justamente la asociada a él.

Teorema 4.2.5. *Sea R una congruencia de un álgebra de Heyting H. Luego $|1|$ es un filtro y R es la relación asociada a ese filtro. Es decir, xRy si y solo si existe $f \in |1|$ tal que $x \wedge f = y \wedge f$, lo que equivale a afirmar que $R = \equiv_{|1|}$.*

Demostración. Para demostrar que $|1|$ es un filtro se procede como en el Teorema 2.3.13 para el caso de álgebras de Boole.

Supongamos ahora que xRy. Como yRy y R es congruencia de Heyting, $(x \to y)R(y \to y)$, o sea, $(x \to y)R1$. Análogamente $(y \to x)R1$, o sea que $x \to y \in |1|$, $y \to x \in |1|$. Por el Lema 4.2.2 se tiene que existe $f \in |1|$ tal que $x \wedge f = y \wedge f$, o sea, $x \equiv_{|1|} y$. Recíprocamente, si existe $f \in |1|$ tal que $x \wedge f = y \wedge f$, por ser $fR1$ y xRx tenemos que $(f \wedge x)R(1 \wedge x)$, de donde $(f \wedge y)Rx$. Análogamente podemos ver que $(f \wedge y)Ry$, por lo que xRy. Es decir, hemos probado que xRy si y solo si $x \equiv_{|1|} y$, es decir que $R = \equiv_{|1|}$. □

Basándonos en estos resultados, podemos generalizar lo demostrado para las álgebras de Boole en 2.3.14 del Capítulo 2: dada un álgebra de Heyting existe una biyección entre las congruencias y los filtros.

Corolario 4.2.6. *Sea H un álgebra de Heyting. Sean* Fil(H) *el conjunto de los filtros de H y* Con(H) *el conjunto de las congruencias de H. Existe una biyección entre* Con(H) *y* Fil(H).

Demostración. Se deja como ejercicio. □

Observación 4.2.7. El Corolario 2.3.10 del Capítulo 2, Sección 3, muestra que la congruencia de retículo $\equiv_{[a)}$ asociada a un filtro principal $[a)$ se define por: $x \equiv_{[a)} y$ si y solo si $x \wedge a = y \wedge a$. Con la misma demostración se prueba que la congruencia de álgebra de Heyting $\equiv_{[a)}$ es la asociada al filtro principal $[a)$. Abusaremos de notación y escribiremos $\equiv_a$ en lugar de $\equiv_{[a)}$.

La congruencia principal R_{ab} generada por un par de elementos (a, b) es la mínima congruencia R tal que aRb (ver Capítulo 1, Ejemplos 1.3.17).

Lema 4.2.8. *Sean $a, b \in H$, H álgebra de Heyting. La congruencia R_{ab} es la asociada al filtro principal generado por el elemento $(a \to b) \wedge (b \to a)$, que abreviaremos $a \leftrightarrow b$.*

Demostración. Por la observación 4.2.7, la congruencia $\equiv_{a\leftrightarrow b}$ se define por: $x \equiv_{a\leftrightarrow b} y$ si y solo si $x \wedge (a \leftrightarrow b) = y \wedge (a \leftrightarrow b)$. Veamos que ella coincide con R_{ab}, para lo cual debemos probar que $a \equiv_{a\leftrightarrow b} b$ y que es la mínima congruencia que contiene al par (a, b).

En primer lugar,

$$a \wedge (a \leftrightarrow b) = a \wedge b = b \wedge (a \leftrightarrow b).$$

Por lo tanto, $a \equiv_{a\leftrightarrow b} b$.

En segundo lugar, sea R una congruencia tal que aRb. Por lo tanto, se puede probar (ejercicio) que $1R(a \leftrightarrow b)$. Sean x, y tales que $x \equiv_{a\leftrightarrow b} y$, o sea, $x \wedge (a \leftrightarrow b) = y \wedge (a \leftrightarrow b)$. Como xRx y $1R(a \leftrightarrow b)$ entonces $xR(x \wedge (a \leftrightarrow b))$, de donde $xR(y \wedge (a \leftrightarrow b))$. Análogamente podemos obtener $yR(y \wedge (a \leftrightarrow b))$. Pero entonces, xRy. Luego, $\equiv_{a\leftrightarrow b}$ está contenida en R, con lo cual probamos que $\equiv_{a\leftrightarrow b}$ es la mínima congruencia que contiene al par (a, b). □

Veamos ahora que también hay correspondencia entre filtros y homomorfismos suryectivos. En efecto, a cada filtro le corresponde la aplicación canónica al cociente por ese filtro y a cada homomorfismo h le corresponde el filtro $h^{-1}(\{1\})$.

Observación 4.2.9. Sean H y K álgebras de Heyting, y $f : H \to K$ una función. Según lo visto en el Capítulo 1, diremos que f es un homomorfismo de álgebras de Heyting si se cumplen las siguientes condiciones para cada $x, y \in H$:

1. $f(x \wedge y) = f(x) \wedge f(y)$,
2. $f(x \vee y) = f(x) \vee f(y)$,
3. $f(0) = 0$, $f(1) = 1$,
4. $f(x \to y) = f(x) \to f(y)$.

Si f es biyectiva entonces f se llamará isomorfismo de álgebras de Heyting.

Teorema 4.2.10. *Sea H un álgebra de Heyting, F un filtro de H, sea H/F el conjunto de las clases de equivalencia determinadas por F. El álgebra $\langle H/F, \vee, \wedge, \to, |0|, |1|\rangle$ es un álgebra de Heyting, siendo las operaciones definidas por: $|x| \diamond |y| = |x \diamond y|$, donde $\diamond$ simboliza las operaciones $\vee, \wedge, \to$ respectivamente.*

La aplicación canónica al cociente $p_F : H \longrightarrow H/F$, definida por $p_F(x) = |x|$, es un homomorfismo suryectivo de álgebras de Heyting.

Demostración. Se desprende del resultado general 1.3.19 dado en el Capítulo 1. □

Si F es un filtro de un álgebra de Heyting H sabemos que $\equiv_F$ es su congruencia asociada. Muchas veces se escribe H/F en lugar del cociente de H por $\equiv_F$. La congruencia R_h del Lema que sigue fue mencionada en el Capítulo 1, 1.3.20.

Lema 4.2.11. *Si $h : H \longrightarrow K$ es un homomorfismo de álgebras de Heyting entonces el subconjunto $h^{-1}(\{1\})$ de H es un filtro, y su congruencia asociada es R_h.*

Demostración. Se demuestra de la misma manera que el Lema 2.3.17 del Capítulo 2. □

Teorema 4.2.12. *Sea $h : H \longrightarrow K$ un homomorfismo suryectivo de álgebras de Heyting. Entonces el cociente $H/h^{-1}(\{1\})$ es isomorfo a K.*

Demostración. Sale del Teorema 1.3.20 del Capítulo 1, teniendo en cuenta que la clase del 1 por la relación R_h es $h^{-1}(\{1\})$. □

Sea $p : H \longrightarrow H/h^{-1}(\{1\})$ la aplicación canónica al cociente. El isomorfismo $f : H/h^{-1}(\{1\}) \longrightarrow K$ del Teorema 4.2.12 está definido por $f(|x|) = h(x)$ y es el que hace conmutar el siguiente diagrama:

$$\begin{tikzcd} H \arrow[r, "h"] \arrow[d, "p"'] & K \\ H/h^{-1}(\{1\}) \arrow[ur, "f"'] & \end{tikzcd}$$

4.3. Teorema algebraico de la deducción

En el Capítulo 2 vimos el teorema algebraico de la deducción para álgebras de Boole, a partir de la expresión del filtro generado por un conjunto. Demostraremos ahora que vale de la misma manera para las álgebras de Heyting. Posteriormente aplicaremos este resultado para demostrar el teorema lógico de la deducción para el cálculo intuicionista.

Sea H un álgebra de Heyting. Hemos visto en el Lema 2.4.5 del Capítulo 2 la demostración de que el filtro generado por un conjunto $X \neq \emptyset$ tiene la forma

$$F(X) = \{z \in H : z \geq x_1 \wedge x_2 \wedge \cdots \wedge x_n \text{ para ciertos } x_1, x_2, \ldots x_n \in X\}.$$

Asimismo, para un elemento $x \in H$:

$F(X \cup \{x\}) = \{z \in H : z \geq x_1 \wedge x_2 \wedge \cdots \wedge x_n \wedge x$ para ciertos $x_1, x_2, \ldots, x_n \in X\}$.

Si $X = \emptyset$ tenemos que $F(\emptyset) = \{1\}$ y que $F(X \cup \{x\}) = [x)$.

Algunas demostraciones que hemos hecho valen también en el contexto de álgebras de Heyting dado que se usaron solo propiedades de retículos.

Teorema 4.3.1 (Teorema algebraico de la deducción)**.** *Sea H un álgebra de Heyting. Sean $x, y \in H$ y $X \subseteq H$. Luego*

$$y \in F(X \cup \{x\}) \text{ si y solo si } x \to y \in F(X).$$

Demostración. El caso $X = \emptyset$ es inmediato, por lo cual supondremos que $X \neq \emptyset$. Notemos que $y \in F(X \cup \{x\})$ si y solo si existen $x_1, x_2, \ldots, x_n \in X$ tales que $y \geq x_1 \wedge x_2 \wedge \cdots \wedge x_n \wedge x$. Esto último es equivalente a que $x \to y \geq x_1 \wedge x_2 \wedge \cdots \wedge x_n$, por la propiedad que caracteriza la implicación. Pero esto significa que $x \to y \in F(X)$. □

4.4. Teorema algebraico de Glivenko

En esta sección veremos un resultado que vincula las álgebras de Heyting con las de Boole y que tiene su correlato lógico. Veremos posteriormente, en efecto, que este teorema es como un "puente" que permite pasar de fórmulas del cálculo intuicionista a fórmulas del cálculo clásico. En primer lugar, necesitamos algunas definiciones, motivadas por el ejemplo del álgebra de Heyting de los abiertos de un espacio topológico.

Si $\langle X, \mathcal{T} \rangle$ es un espacio topológico, un subconjunto abierto Y de X se dice *denso* si $\overline{Y} = X$ y *regular* si $(\overline{Y})^o = Y$. Se tiene

$$Y^* = Y \to \emptyset = (Y^c \cup \emptyset)^o = (Y^c)^o = (\overline{Y})^c,$$

de donde

$$Y^{**} = (((\overline{Y})^c)^c)^o = (\overline{Y})^o.$$

Luego Y es denso si $Y^* = \emptyset$ e Y es regular si $Y^{**} = Y$.

Definición 4.4.1. Sea H un álgebra de Heyting, $x \in H$. Diremos que x es *denso* si $x^* = 0$ y *regular* si $x^{**} = x$. Denotaremos con $\mathcal{D}e(H)$ (respectivamente $\mathcal{R}eg(H)$) a los elementos densos (respectivamente regulares) de H. Observemos que 1 es denso, y que 0 y 1 son regulares.

Lema 4.4.2. *Sea H un álgebra de Heyting y $x \in H$.*

(a) *El elemento $x \vee x^*$ es denso,*

(b) *Un elemento x es regular si y solo si existe $y \in H$ tal que $x = y^*$.*

Demostración. Se deja como ejercicio. □

Lema 4.4.3. *El conjunto $\mathcal{D}e(H)$ es un filtro de H.*

Demostración. Para todo x vale que $1 \to x = x$, por lo cual $1^* = 0$. Es decir, $1 \in \mathcal{D}e(H)$.

Probaremos ahora que $\mathcal{D}e(H)$ es creciente. Sea $x \in \mathcal{D}e(H)$ tal que $y \geq x$, por lo cual $y^* \leq x^*$. Por ende, $y \in \mathcal{D}e(H)$.

Sean $x, y \in \mathcal{D}e(H)$ y veamos que $x \wedge y \in \mathcal{D}e(H)$. Se tiene:

$$(y \wedge x) \wedge (x \wedge y)^* = 0 = y \wedge (x \wedge (x \wedge y)^*),$$

de donde

$$x \wedge (x \wedge y)^* \leq y^* = 0.$$

Esto a su vez implica que

$$(x \wedge y)^* \leq x^* = 0.$$

Por lo tanto, $(x \wedge y)^* = 0$, es decir, $x \wedge y \in \mathcal{D}e(H)$. □

Teorema 4.4.4 (Teorema de Glivenko)**.** *Sean H un álgebra de Heyting y $r_H : H \longrightarrow \mathcal{R}eg(H)$ la aplicación definida por $r_H(x) = x^{**}$. Definimos en $\mathcal{R}eg(H)$ las siguientes operaciones:*

$$\begin{aligned} x \vee_r y &:= (x \vee y)^{**} \\ x \wedge_r y &:= x \wedge y \\ \overline{x} &:= x^*. \end{aligned}$$

Entonces, $\langle \mathcal{R}eg(H), \vee_r, \wedge_r, ^-, 0, 1 \rangle$ es un álgebra de Boole. Además, r_H es un homomorfismo suryectivo de álgebras de Heyting y se verifica que $H/\mathcal{D}e(H)$ es isomorfo a $\mathcal{R}eg(H)$.

Demostración. Por el Lema 4.4.2 tenemos que r_H está bien definida porque x^{**} es un elemento regular. Además r_H es suryectiva porque todo elemento regular es de la forma x^{**}.

Veremos a continuación que las operaciones definen una estructura de álgebra de Boole en $\mathcal{R}eg(H)$.

Tenemos que probar que $x \vee_r y$ es el mínimo regular mayor o igual que los elementos x e y. Por (a) del Lema 4.1.8 tenemos que

$$x, y \leq x \vee y \leq (x \vee y)^{**}.$$

Sea w tal que $w = w^{**}$ (es decir, regular) y es cota superior de x e y. Como $w \geq x \vee y$, se tiene que $w = w^{**} \geq (x \vee y)^{**}$. Luego, $x \vee_r y$ es la mínima cota superior.

El hecho de que el ínfimo de dos elementos regulares es un elemento regular es una consecuencia de (d) del Lema 4.1.8.

Como $0, 1$ son regulares, hemos probado que $\langle \mathcal{R}eg(H), \vee_r, \wedge_r, 0, 1\rangle$ es un retículo acotado. Veamos que r_H es homomorfismo con respecto a esa estructura.

En efecto, $r_H(0) = 0$, $r_H(1) = 1$. Además, por (e) del Lema 4.1.8:

$$\begin{aligned} r_H(x \vee y) &= (x \vee y)^{**} \\ &= (x^{**} \vee y^{**})^{**} \\ &= (r_H(x) \vee r_H(y))^{**} \\ &= r_H(x) \vee_r r_H(y). \end{aligned}$$

Con respecto al ínfimo, por la propiedad (d) del lema citado:

$$\begin{aligned} r_H(x \wedge y) &= (x \wedge y)^{**} \\ &= x^{**} \wedge y^{**} \\ &= r_H(x) \wedge_r r_H(y), \end{aligned}$$

probando entonces que r_H respeta las operaciones $\vee_r$, $\wedge_r$, 0 y 1.

Como r_H es suryectiva, por la distributividad de las operaciones en H se tiene que las operaciones en $\mathcal{R}eg(H)$ también distribuyen (probar como ejercicio).

Resta probar que el pseudocomplemento actúa como complemento sobre los regulares, para lo cual solo hay que ver que si x es un elemento regular entonces $x \vee_r x^* = 1$, es decir, $(x \vee x^*)^{**} = 1$. Esto se deduce de (a) del Lema 4.4.2.

Hasta aquí hemos probado que $\langle \mathcal{R}eg(H), \vee_r, \wedge_r, ^*, 0, 1\rangle$ es un álgebra de Boole. Luego, es un álgebra de Heyting con la implicación definida por

$$x \to_r y = x^* \vee_r y = (x^* \vee y)^{**}.$$

Probaremos ahora que r_H es homomorfismo de álgebras de Heyting, para lo cual solo falta ver que

$$r_H(x \to y) = r_H(x) \to_r r_H(y).$$

Primero notemos que por (f) del Lema 4.1.8 tenemos que

$$r_H(x \to y) = (x \to y)^{**} = (x^{**} \wedge y^*)^*. \tag{4.3}$$

Por otro lado, usando la definición de implicación en $\mathcal{R}eg(H)$ obtenemos que

$$\begin{aligned} r_H(x) \to_r r_H(y) &= x^{**} \to_r y^{**} \\ &= (x^{***} \vee y^{**})^{**}. \end{aligned}$$

Luego, por (b) del Lema 4.1.8 y por (c) del Lema 4.1.7, tenemos que

$$(x^{***} \vee y^{**})^{**} = (x^* \vee y^{**})^{**} = (x^{**} \wedge y^*)^*. \tag{4.4}$$

En virtud de (4.3) y (4.4) inferimos que

$$r_H(x \to y) = r_H(x) \to_r r_H(y).$$

Definimos el homomorfismo $f : H/\mathcal{D}e(H) \longrightarrow \mathcal{R}eg(H)$ como $f(|x|) = r_H(x)$. En otras palabras, el homomorfismo f hace conmutar el siguiente diagrama:

$$\begin{tikzcd} H \arrow[r, "r_H"] \arrow[d, "p"'] & \mathcal{R}eg(H) \\ H/\mathcal{D}e(H) \arrow[ur, "f"'] & \end{tikzcd}$$

Veremos finalmente que f es un isomorfismo. Por el Teorema 4.2.12 de la Sección 2 basta probar que $r_H^{-1}(\{1\}) = \mathcal{D}e(H)$. Esta igualdad es cierta ya que en efecto tenemos que

$$\begin{aligned} r_H(x) = 1 \quad &\text{si y solo si} \quad x^{**} = 1 \\ &\text{si y solo si} \quad x^* = 0 \\ &\text{si y solo si} \quad x \text{ es denso.} \end{aligned}$$

□

4.5. Teoremas de representación

¿Qué es un teorema de representación?

En este contexto, lo que resulta de un tal teorema es "representar" un álgebra de Heyting visualizándola a través de algún ejemplo conocido. Se trata de ver un álgebra de Heyting como algo un poco menos abstracto, en un marco más accesible.

Daremos dos teoremas de representación. Ambos muestran a un álgebra de Heyting como un álgebra de abiertos de cierto conjunto.

En el primer teorema, se la muestra como subálgebra de un álgebra de Heyting cuyos elementos son conjuntos crecientes de un conjunto ordenado (ver Ejemplos 4.1.6 al principio del capítulo). Dada un álgebra de Heyting H, el conjunto ordenado en cuestión será el de los filtros primos de H y el orden será el de la inclusión entre ellos.

En el segundo, el resultado de Mc Kinsey y Tarski dice que toda álgebra de Heyting puede verse como un álgebra de abiertos de un *álgebra de clausura*. Las álgebras de clausura aparecen como asociadas a la semántica de las *lógicas modales*, de las que hablamos en el Capítulo 3.

En el Capítulo 2 vimos, a partir del teorema de Birkhoff de representación de retículos distributivos finitos, que toda álgebra de Boole finita es isomorfa a una de la forma $\mathcal{P}(X)$, para cierto conjunto X. También probamos el teorema de Stone de representación de álgebras de Boole: toda álgebra de Boole es isomorfa a una subálgebra de una de esa forma. Este resultado también puede deducirse del primer teorema de representación de álgebras de Heyting que daremos a continuación.

Observación 4.5.1. Todo retículo distributivo finito admite una implicación de Heyting y por lo tanto, una estructura de álgebra de Heyting. Recíprocamente, toda álgebra de Heyting finita tiene un reducto que es un retículo distributivo finito. El teorema de Birkhoff de representación de retículos finitos que mencionamos recién también vale para álgebras de Heyting finitas, pues se prueba que la aplicación σ definida en el teorema de Birkhoff preserva $\to$.

El teorema de representación que veremos ahora puede considerarse una generalización de este. En efecto, un retículo distributivo finito es “generado por primos” en el sentido de que cada uno de sus elementos es supremo de elementos primos (los que son menores o iguales que él).

Definición 4.5.2. Un retículo L en el que existen $\bigwedge X$ y $\bigvee X$ para cualquier subconjunto X de L (finito o no) se llama *completo*.

Sea L un retículo completo. Un elemento $x \neq 0$ es *completamente primo* o *c-primo* si $\bigvee_{i \in I} x_i \geq x$ (I finito o infinito) implica que existe i tal que $x_i \geq x$.

Un retículo completo se llama *generado por primos* o abreviadamente *pg* si cada elemento es supremo de c-primos.

Puede probarse (ejercicio) que los elementos de la forma $[p) = \{q \in P : p \leq q\}$ son c-primos en todo retículo cuyo universo es de la forma P^+.

Luego P^+ es pg, ya que, si $U \in P^+$, $U = \bigcup_{p \in U} [p)$ (la igualdad se demuestra como en 2.5.4).

La recíproca también es cierta, es decir, si un retículo es pg entonces es isomorfo a uno de la forma P^+. En particular, el retículo tiene estructura de álgebra de Heyting.

Lo que vamos a demostrar es que toda álgebra de Heyting puede "mirarse" dentro de una cuyo retículo subyacente es pg.

Previamente se enuncia el siguiente lema, cuya demostración se propone como ejercicio.

Lema 4.5.3. *Un homomorfismo de álgebras de Heyting $f : H \longrightarrow K$ es inyectivo si y solo si $f^{-1}(\{1\}) = \{1\}$.*

Teorema 4.5.4. *Dada un álgebra de Heyting H, sea $(H^\star, \subseteq)$ el conjunto ordenado en donde H^* se define como el conjunto de filtros primos de H. Sea $(H^\star)^+ = \{C : C \subseteq H^\star,\ C \text{ creciente}\}$, y definimos la aplicación $e_H : H \longrightarrow (H^\star)^+$ como*

$$e_H(x) = \{F : F \in H^\star,\ x \in F\}.$$

Entonces, e_H es un homomorfismo inyectivo de álgebras de Heyting.

Demostración. En primer lugar, como $F \subseteq G$, $x \in F$ implica $x \in G$, se ve que $e_H(x)$ es efectivamente un conjunto creciente de filtros primos.

Veamos que e_H preserva las operaciones de álgebra de Heyting.

Por la condición de ser F filtro: $F \in e_H(x \wedge y)$ si y solo si $x \wedge y \in F$ sii $x \in F$, $y \in F$ si y solo si $F \in e_H(x)$, $F \in e_H(y)$. Luego, $e_H(x \wedge y) = e_H(x) \cap e_H(y)$.

Por ser F filtro primo: $F \in e_H(x \vee y)$ sii $x \vee y \in F$ sii $x \in F$ o $y \in F$ sii $F \in e_H(x)$ o $F \in e_H(y)$. Entonces: $e_H(x \vee y) = e_H(x) \cup e_H(y)$.

Veamos: $e_H(x \to y) = e_H(x) \Longrightarrow e_H(x)$.

Recordemos que la implicación en $(H^\star)^+$ es $X \Longrightarrow Y = (X \cap Y^c]^c$.

Sea $F \in e_H(x \to y)$, o sea, $x \to y \in F$.

Debemos ver que $F \in (e_H(x) \cap e_H(y)^c]^c$, es decir: $F \notin (e_H(x) \cap e_H(y)^c]$. Esto significa demostrar que no existe un filtro primo G tal que $F \subseteq G$ y $x \in G$, $y \notin G$. Supongamos que existe un filtro primo G tal que $F \subseteq G$ y $x \in G$. Como $x \to y \in F$, $G \supseteq F$, tendríamos $x \in G$, $x \to y \in G$ lo que implica $y \in G$, absurdo.

Recíprocamente, sea $F \in (e_H(x) \cap e_H(y)^c]^c$. Probemos, por la contrarecíproca, que $F \in e_H(x \to y)$, o sea, que $x \to y \in F$.

Supongamos que $x \to y \notin F$ y consideremos el filtro F' generado por $F \cup \{x\}$. Por el Corolario 2.4.9 del Capítulo 2,

$$F' = \{z : z \geq x \wedge f,\ f \in F\}.$$

Entonces, F' cumple las tres condiciones siguientes: $F' \supseteq F$, $x \in F'$, $y \notin F'$. En efecto, veamos esto último por el absurdo; si fuera $y \in F'$, entonces existiría $f \in F$ tal que $y \geq x \wedge f$. Luego, sería $f \leq x \to y$ y tendríamos $x \to y \in F$, contra lo supuesto.

El filtro F' no es necesariamente primo, pero por un corolario del TFP (teorema del filtro primo), como $y \notin F'$, existe un filtro primo G tal que $G \supseteq F'$ y $y \notin G$. Luego, $x \in G$ (pues $x \in F'$), $G \supseteq F$, $y \notin G$. Entonces, $F \notin (e_H(x) \cap e_H(y)^c]^c$. Hemos probado entonces que

$$(e_H(x) \cap e_H(y)^c]^c \subseteq e_H(x \to y).$$

Como todo filtro primo es propio, $0 \notin F$ para todo F primo. Es decir, $e_H(0) = \emptyset$. Además $1 \in F$ para todo F primo, luego $e_H(1) = H^\star$.

Para probar que e_H es un homomorfismo inyectivo basta probar, por el Lema 4.5.3, que $e_H^{-1}(\{H^\star\}) = \{1\}$.

Sea x tal que $e_H(x) = \{1\} = H^\star$, es decir, tal que $x \in F$ para todo filtro primo F. Si $x \not\geq 1$, entonces, por el teorema del filtro primo, existiría un filtro G tal que $x \notin G$, $1 \in G$, absurdo. □

Como dijimos, podemos deducir de este resultado el teorema de representación de las álgebras de Boole que vimos en el Capítulo 2:

Teorema 4.5.5 (Teorema de Stone)**.** *Sea B un álgebra de Boole. Existe un conjunto X tal que B es isomorfa a una subálgebra del álgebra de Boole $\mathcal{P}(X)$.*

Demostración. Sea X el conjunto $B^\star$ de todos los filtros primos de B. Como cada filtro primo F es maximal, $F \in B^\star$ es incomparable con todos los otros elementos de $B^\star$. Luego, los crecientes de $B^\star$ son todas las partes de $B^\star$, es decir, $(B^\star)^+ = \mathcal{P}(B^\star)$. Luego, B es isomorfa a una subálgebra de $\mathcal{P}(B^\star)$. El isomorfismo es e_B, considerado de B en la subálgebra $e_B(B)$ de $\mathcal{P}(B^\star)$. □

Veremos en seguida un corolario de este teorema, que es, en realidad, otra forma de presentar el teorema. Pero antes debemos probar el siguiente lema, que generaliza lo visto en el Ejercicio 14 del Capítulo 2.

Lema 4.5.6. *Dado un conjunto $S \neq \emptyset$, el álgebra de Boole cuyo universo es $\mathcal{P}(S)$, con las operaciones habituales, es isomorfa al álgebra de Boole producto $\mathbf{2}^S$.*

Demostración. Sean $h : \mathcal{P}(S) \longrightarrow \mathbf{2}^S$ y $k : \mathbf{2}^S \longrightarrow \mathcal{P}(S)$ definidas, para $T \subseteq S$, $u \in S$, por: $h(T) = (h(T)_u)_{u \in S}$, siendo

$$h(T)_u = \begin{cases} 1 & \text{si } u \in T \\ 0 & \text{si } u \notin T \end{cases}$$

$$k((a_s)_{s\in S}) = \{s \in S : a_s = 1\}.$$

Veamos que k es la inversa de h.

Se tiene

$$\begin{aligned} k(h(T)) &= \{s \in S : h(T)_s = 1\} \\ &= \{s \in S : s \in T\} = T. \end{aligned}$$

Por otra parte, $h(k((a_s)_{s\in S})) = h(\{s \in S : a_s = 1\})$, por lo que

$$h(k((a_s)_{s\in S}))_u = \begin{cases} 1 & \text{si } u \in \{s \in S : a_s = 1\} \\ 0 & \text{si } u \notin \{s \in S : a_s = 1\}, \end{cases}$$

lo que significa que

$$h(k((a_s)_{s\in S}))_u = \begin{cases} 1 & \text{si } a_u = 1 \\ 0 & \text{si } a_u = 0. \end{cases}$$

Luego,

$$h(k((a_s)_{s\in S}))_u = (a_s)_{s\in S}.$$

Probaremos ahora que h es un homomorfismo.

Es sencillo ver que para todo u $h(\emptyset)_u = 0$ y que $h(S)_u = 1$ para todo u. Veamos, componente a componente, que $h(T \cup U) = h(T) \vee h(U)$. En efecto,

$$\begin{aligned} h(T\cup U)_u = 1 \quad &\text{si y solo si} \quad u \in T \cup U \\ &\text{si y solo si} \quad u \in T \quad \text{o} \quad u \in U \\ &\text{si y solo si} \quad h(T)_u = 1 \quad \text{o} \quad h(U)_u = 1 \\ &\text{si y solo si} \quad h(T)_u \vee h(U)_u = (h(T) \vee h(U))_u = 1. \end{aligned}$$

Análogamente $h(T\cap U) = h(T)\cap h(U)$. Por último, veamos que $h(T^c) = \overline{h(T)}$.

$$\begin{aligned} h(T^c)_u = 1 \quad &\text{si y solo si} \quad u \in T^c \\ &\text{si y solo si} \quad u \notin T. \end{aligned}$$

Por otra parte:

$$\begin{aligned} \overline{h(T)}_u = 1 \quad &\text{si y solo si} \quad h(T)_u = 0 \\ &\text{si y solo si} \quad u \notin T. \end{aligned}$$

□

Observación 4.5.7. La función h del Lema 4.5.6 es la que lleva un subconjunto T en la función característica de T, generalmente denotada χ_T (ver la Sección 1 del Capítulo 1).

Si $S = \emptyset$, $\mathcal{P}(S)$ es un conjunto unitario que podemos pensar isomorfo al álgebra de Boole trivial.

Corolario 4.5.8. *Toda álgebra de Boole B es isomorfa a una subálgebra del producto A^I, donde $A = \mathbf{2}$, $I = B^\star$.*

Demostración. El isomorfismo f se obtiene componiendo e_B con h, como muestra el diagrama.

$$\begin{tikzcd} B \arrow[d, "e_B"'] \arrow[dr, "f"] & \\ \mathcal{P}(B^\star) \arrow[r, "h"] & \mathbf{2}^{B^\star} \end{tikzcd}$$

Es decir que $f : B \longrightarrow f(B) \subseteq \mathbf{2}^{B^\star}$ está dada por la asignación $f(x) = (a_P)_{P \in B^\star}$, siendo $a_P = 1$ si y solo si $x \in P$. $\square$

Hemos visto que los abiertos de un espacio topológico $\langle X, \mathcal{T} \rangle$ forman, con operaciones adecuadas, un álgebra de Heyting (ver Ejemplos 4.1.6 de la Sección 2). Los abiertos son partes del conjunto X. Las partes de un conjunto forman un álgebra de Boole a la cual le podemos agregar un operador de *clausura*, del cual ya vimos allí algunas propiedades.

Veremos ahora un segundo teorema de representación que muestra que toda álgebra de Heyting es isomorfa al álgebra de abiertos de un álgebra de clausura.

Definición 4.5.9. Un *álgebra de clausura* $\langle \mathbb{B}, cl \rangle$ es un álgebra de Boole $\mathbb{B} = \langle B, \vee, \wedge, ^-, 0, 1 \rangle$ munida de un operador $cl : B \longrightarrow B$ que cumple las siguientes condiciones:

1) $x \leq cl(x)$.

2) $x \leq y$ implica $cl(x) \leq cl(y)$.

3) $cl(cl(x)) = cl(x)$.

4) $cl(x \vee y) = cl(x) \vee cl(y)$.

5) $cl(0) = 0$.

Un elemento $x \in B$ es *cerrado* si $cl(x) = x$ y *abierto* si su complemento es cerrado: $cl(\overline{x}) = \overline{x}$. El *interior* x^o de un elemento x se define como $x^o = \overline{(cl(\overline{x}))}$. Luego, un elemento es abierto si coincide con su interior.

Como dijimos, el ejemplo motivador de un álgebra de clausura está dado a partir de un espacio topológico $(X, \mathcal{T})$, donde el álgebra de Boole es $\mathcal{P}(X)$ y la clausura es la dada por la topología. Es decir, si $Y \subseteq X$ entonces

$t \in cl(Y)$ si y solo si para todo abierto U tal que $t \in U$ vale que $U \cap Y \neq \emptyset$.

Ejercicio: probar que cl verifica las condiciones **1)**, ..., **5)**.

Teorema 4.5.10. *Sea* $\langle \mathbb{B}, cl\rangle$ *un álgebra de clausura,* B^o *el conjunto de los elementos abiertos de* B*. Entonces,* $\langle B^o, \vee, \wedge, \to, 0, 1\rangle$ *es un álgebra de Heyting, donde* $\to$ *se define por* $x \to y = \overline{(cl(x \wedge \overline{y}))} = (\overline{x} \vee y)^o$.[2]

Demostración. En esta demostración nos referiremos a las condiciones **1),...,5)** de la clausura.

Veamos en primer lugar que las operaciones $\vee$ y $\wedge$ están bien definidas en B^o.

Sean x, y elementos de B^o, es decir, abiertos. Luego, $\overline{x} = cl(\overline{x})$, $\overline{y} = cl(\overline{y})$. Probaremos que

$$\overline{x} \wedge \overline{y} = cl(\overline{x} \wedge \overline{y}).$$

Por la condición **2)** tenemos que $cl(\overline{x} \wedge \overline{y}) \leq cl(\overline{x})$ y $cl(\overline{x} \wedge \overline{y}) \leq cl(\overline{y})$. Por ende,

$$cl(\overline{x} \wedge \overline{y}) \leq cl(\overline{x}) \wedge cl(\overline{y}).$$

Por otro lado, por la propiedad **1)** tenemos que

$$\begin{aligned} \overline{x} \wedge \overline{y} &\leq cl(\overline{x} \wedge \overline{y}) \\ &\leq cl(\overline{x}) \wedge cl(\overline{x}) \\ &= \overline{x} \wedge \overline{y}. \end{aligned}$$

Por esta razón hemos probado que

$$\overline{x} \wedge \overline{y} = cl(\overline{x} \wedge \overline{y}).$$

Como $\overline{x} \wedge \overline{y}$ es cerrado, resulta su complemento $x \vee y$ abierto.

Por otra parte, usando la condición **4)** tenemos que

$$\begin{aligned} \overline{x} \vee \overline{y} &= cl(\overline{x}) \vee cl(\overline{y}) \\ &= cl(\overline{x} \vee \overline{y}). \end{aligned}$$

Luego, $\overline{(\overline{x} \vee \overline{y})} = x \wedge y$ es abierto.

Como $cl(1) \geq 1$ tenemos que $cl(1) = 1$. Por **5)** tenemos que $cl(0) = 0$. Por esto 0 y 1 son abiertos (y cerrados).

Finalmente veremos que la implicación $x \to y$ cumple la condición de ser el máximo elemento z tal que $x \wedge z \leq y$.

Debemos probar que $x \wedge (x \to y) = x \wedge \overline{(cl(x \wedge \overline{y}))} \leq y$, lo que es equivalente a $\overline{x} \vee cl(x \wedge \overline{y}) \geq \overline{y}$.

[2] No confundir: $\overline{x}$ (complemento de x) con $cl(x)$ (clausura de x).

Por la condición **1)** tenemos que

$$\begin{aligned}
\overline{x} \vee cl(x \wedge \overline{y}) &\geq \overline{x} \vee (x \wedge \overline{y}) \\
&= (\overline{x} \vee x) \wedge (\overline{x} \vee \overline{y}) \\
&= 1 \wedge (\overline{x} \vee \overline{y}) \\
&= \overline{x} \vee \overline{y} \\
&\geq \overline{y}.
\end{aligned}$$

Ahora probaremos que si es z abierto tal que $x \wedge z \leq y$, entonces $z \leq \overline{(cl(x \wedge \overline{y}))}$ o, lo que es equivalente,

$$\overline{z} \geq cl(x \wedge \overline{y}).$$

Notemos que $x \wedge z \leq y$ implica $\overline{x} \vee (x \wedge z) \leq \overline{x} \vee y$. Operando con el primer miembro y teniendo en cuenta que $z \leq \overline{x} \vee z$, tenemos que $z \leq \overline{x} \vee y$. Por esto, $\overline{z} \geq \overline{(\overline{x} \vee y)} = x \wedge \overline{y}$, de donde se deduce que $cl(\overline{z}) = \overline{z} \geq cl(x \wedge \overline{y})$, como queríamos demostrar. □

Teorema 4.5.11 (Mc Kinsey–Tarski)**.** *Toda álgebra de Heyting es isomorfa al álgebra de abiertos de un álgebra de clausura.*

La demostración de este teorema puede encontrarse, por ejemplo, en [2, IX, 9].

4.6. Ejercicios

1. Sea H un álgebra de Heyting. Probar que H es un álgebra de Boole si y solo si $\{x \in H : x^* = 0\} = \{1\}$.

2. Sean H un álgebra de Heyting y $f : H \to \{0,1\}$ una función. Probar que $f^{-1}(\{1\})$ es un filtro maximal si y solo si f es un homomorfismo de álgebras de Heyting.

3. Sea L un retículo distributivo acotado. Supongamos que para cada $x \in L$ existe $x^* = \text{máx}\{y \in L : x \wedge y = 0\}$. Probar las siguientes afirmaciones:

   a) $0^* = 1$, $1^* = 0$,

   b) $x \leq x^{**}$ y dar un ejemplo en donde $x \not\geq x^{**}$,

   c) $x \leq y$ implica $y^* \leq x^*$,

   d) $(x \vee y)^* = x^* \wedge y^*$,

   e)$x^* \vee y^* \leq (x \wedge y)^*$ y dar un ejemplo en donde $x^* \vee y^* \not\geq (x \wedge y)^*$,

   f) $x^{***} = x^*$,

   g) $x^* = 0 = y^*$ implica $(x \wedge y)^* = 0$,

   h) $(x \wedge y)^{**} = x^{**} \wedge y^{**}$,

   i) $(x \wedge y)^* = (x^* \vee y^*)^{**}$,

   j) $(x \vee y)^{**} = (x^{**} \vee y^{**})^{**}$.

4. Bajo las mismas hipótesis que el Ejercicio 3, probar que las siguientes condiciones son equivalentes:

   a) H es un álgebra de Boole.

   b) $x \leq y$ si y solo si $y^* \leq x^*$.

   c) $x^{**} = 1$ si y solo si $x = 1$.

   d) $x \wedge y = (x^* \vee y^*)^* = x^{**} \wedge y^{**}$.

5. Sean H un álgebra de Heyting, $\mathbf{3} = \{0,1,2\}$ y $f : H \longrightarrow \mathbf{3}$ una función. Definimos $F_1 = \{x \in H : f(x) \geq 1\}$ y $F_2 = \{x \in H : f(x) = 2\}$. Probar que f es un homomorfismo de álgebras de Heyting si y solo si valen las siguientes condiciones:

   a) $F_2 \subseteq F_1$.

   b) F_1 es un filtro maximal.

c) F_2 es un filtro primo.

d) Si $x \notin F_1$ entonces $x^* \in F_2$.

e) Si $x, y \in F_1 - F_2$ entonces $x \to y \in F_2$.

6. Sea L un retículo en el que para todo $x \in L$ existe el pseudocomplemento x^*. Sea F un filtro de L. Probar que, para $x, y \in L$, si $x \equiv_F y$ entonces $((x \wedge y^*) \vee (y \wedge x^*))^* \in F$. Mostrar un contraejemplo de que la recíproca no es cierta.

7. Sea H un álgebra de Heyting, R una congruencia de H. Probar que $x \, R \, y$ si y solo si $(x \leftrightarrow y) \, R \, 1$, donde $x \leftrightarrow y = (x \to y) \wedge (y \to x)$.

8. (Lema 4.4.2) Sea H un álgebra de Heyting, $x \in H$. Probar las siguientes afirmaciones:

   a) El elemento $x \vee x^*$ es denso.

   b) Un elemento x es regular si y solo si existe $y \in H$ tal que $x = y^*$.

9. (Lema 4.5.3) Probar que un homomorfismo de álgebras de Heyting $f : H \longrightarrow K$ es inyectivo si y solo si $f^{-1}(\{1\}) = \{1\}$.

10. Probar que en toda álgebra de Heyting H valen las siguientes afirmaciones:

    a) $x \wedge z = y \wedge z$ si y solo si $z \leq x \leftrightarrow y$.

    b) $x \wedge (x \leftrightarrow y) = y \wedge (x \leftrightarrow y)$.

    c) Dada una función $f : H^2 \longrightarrow H$, si $f(x, y) \wedge a = f(x \wedge a, y \wedge a) \wedge a$ para cada $x, y, a, b \in H$ entonces $f(x, y) \wedge a \wedge b = f(x \wedge a, y \wedge b) \wedge a \wedge b$ para cada $a, b, x, y \in H$. ¿Vale esta propiedad en un retículo?

    d) Sea $f : H^2 \longrightarrow H$ una función tal que $f(x, y) \wedge a = f(x \wedge a, y \wedge a) \wedge a$ para cada $x, y, a, b \in H$. Probar que

    $$f(a, b) \wedge (x \leftrightarrow a) \wedge (y \leftrightarrow b) = f(x, y) \wedge (x \leftrightarrow a) \wedge (y \leftrightarrow b).$$

    Sugerencia: usar (b) y (c).

11. Sea ρ_z una relación definida en el álgebra de Heyting H por

    $$x \, \rho_z \, y \ \text{ si y solo si } \ z \leq x \leftrightarrow y.$$

    Probar que ρ_z es una congruencia y determinar el filtro asociado a la misma.

    Sugerencia: usar el ejercicio anterior.

12. Si consideramos "conjunción elemental" de n variables a una expresión de la forma $x_1^{k_1} \wedge \cdots \wedge x_n^{k_n}$, donde $x_i^0 = (x_i)^*$ y $x_i^1 = x_i$, probar que en toda álgebra de Heyting vale que

$$(\bigvee_{(k_1,\ldots,k_n)\in\{0,1\}^n}(x_1^{k_1} \wedge \cdots \wedge x_n^{k_n}))^{**} = 1.$$

Sugerencia: usar el Ejercicio 1 del Capítulo 2 y el Teorema de Glivenko.

Bibliografía del Capítulo 4

- Balbes R. and Dwinger, P., *Distributive Lattices*. University of Missouri Press, 1974.

- Blok W.J. and Pigozzi D., *Abstract algebraic logic and the deduction theorem*, preprint, 2001. `http://orion.math.iastate.edu/dpigozzi`

- Caicedo X., *Investigaciones acerca de los conectivos intuicionistas*. Rev. Acad. Colombiana Ciencias Exactas Físicas Naturales, 19 (1995), no. 75, 705–716.

- Fitting M.C., *Intuitionistic Logic, Model Theory and Forcing*. North-Holland, 1969.

- Munkres J.R., *Topología*, segunda edición. Prentice Hall, 2002.

Capítulo 5

Cálculo proposicional intuicionista

Alrededor del año 1900, Hilbert pretendía fundamentar la matemática en un enorme sistema axiomático de manera que cualquier "verdad matemática" pudiera demostrarse mecánicamente aplicando reglas a partir de sus axiomas. Sin embargo, como hemos mencionado en el Capítulo 1, ya Lovachevsky en 1826 había logrado construir una teoría geométrica consistente (sin contradicciones) y "no euclidiana". Si algo que se creía básico e inamovible como la geometría de Euclides no tenía fundamento sólido, ¿sería posible fundamentar toda la matemática? Fue el inicio de una crisis, a la que contribuyó más tarde la para entonces sorprendente teoría de conjuntos de Cantor con su tratamiento novedoso del concepto de infinito y las paradojas, especialmente la de Russell. La lógica clásica empezaba a tambalear.

Hilbert proponía varias condiciones para su sistema axiomático: entre otras, que fuera **consistente** y **completo** desde el punto de vista sintáctico. La consistencia de un sistema axiomático significa que el mismo esté libre de contradicciones, es decir, para toda proposición p no puede ocurrir que p y $\neg p$ resulte un teorema. Que un sistema axiomático resulte sintácticamente completo significa que para cada proposición p existe una demostración de p o de $\neg p$. También resulta importante la cuestión de la **decidibilidad**: un sistema axiomático es decidible si para cada proposición puede encontrarse mecánicamente en un número finito de pasos la respuesta a la pregunta sobre si existe o no una demostración para ella. Esto puede hacerse en el cálculo proposicional clásico, que hemos visto, mediante las tablas de verdad, ya que toda tautología es un teorema. Aparecieron, sin embargo, problemas dentro de la matemática que no son decidibles de esa manera: el llamado décimo problema de Hilbert, por ejemplo (ver [57, 7.1]).

Posteriormente, en base a resultados que fueron apareciendo, quedó probado que las condiciones propuestas por Hilbert eran inalcanzables. El teorema de Gödel, en ese sentido, fue uno de los que tuvieron mayor repercusión. Afirma que cualquier sistema axiomático que formalice de manera adecuada la aritmética es incompleto: existe una proposición tal que ni ella ni su negación son demostrables. Surgieron también algunos sistemas lógicos, como el de Łukasiewicz que veremos más adelante, donde falta la consistencia. Pero, de todos modos, Hilbert y otros contemporáneos hicieron un aporte importante: estudiaron sistemáticamente los fundamentos de la matemática e iniciaron el estudio de lo que después se llamó *Lógica matemática.*

En realidad, Hilbert se refería a sistemas que axiomatizan fórmulas "de primer orden", más complejas que las tratadas en este libro, donde solo hablamos de proposiciones simples ligadas por conectivos (cálculo proposicional). Pero nos hemos extendido en este tema porque interesaba describir el contexto donde se desarrollaron las ideas de la *lógica intuicionista*, objetivo de este capítulo.

Uno de los axiomas básicos de la lógica clásica es el *principio del tercero excluido*: para toda proposición p, vale p $\vee \neg$p. La lógica intuicionista se caracteriza por no aceptar el *principio del tercero excluido* y estar ligada al *constructivismo.* Dentro de la matemática, esto se manifiesta como la corriente que solo acepta demostraciones de existencia constructivas. Para los que siguen esta corriente, demostrar que algo existe significa mostrarlo, exhibirlo, construirlo. ¿En qué influye en esto el tercero excluido? Daremos brevemente una explicación.

Supongamos que queremos demostrar que existe un cierto x que cumple una propiedad $\mathcal{P}$. Un matemático podría suponer que tal x no existe (para lo cual estaría asumiendo que *existe o no existe*) y llegar a un absurdo, con lo cual consideraría demostrada la existencia de x que verifica $\mathcal{P}$. Pero esto no conformaría a un constructivista. Como en la demostración se usa esencialmente el principio del tercero excluido $p \vee \neg p$, debe rechazar entonces este razonamiento.

Veamos un ejemplo simple de prueba de existencia donde la prueba no construye el objeto que existe (prueba no constructiva).

Consideremos la siguiente afirmación:

Existen a, b irracionales tales que a^b es racional.

Primera prueba (no constructiva):[1]

Consideremos $a = b = \sqrt{2}$. Si $\sqrt{2}^{\sqrt{2}}$ es racional, el problema está resuelto. Caso contrario vamos a considerar $a' = \sqrt{2}^{\sqrt{2}}$ y $b' = \sqrt{2}$. Entonces tenemos que

$$\begin{aligned}(a')^{b'} &= (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}\\ &= (\sqrt{2})^2\\ &= 2.\end{aligned}$$

Segunda prueba (constructiva):

Tomemos $a = \sqrt{2}$ y $b = \log_2 9$. Ambos números son irracionales. En efecto, se conoce el hecho de que $\sqrt{2}$ es irracional. Veamos que $\log_2 9$ también lo es. Supongamos que b es de la forma m/n con m y n números enteros. De esto se deduce que $2^m = 9^n$, esto implica que el primer miembro es par y el segundo miembro es impar, lo cual es un absurdo. Es inmediato ver que $a^b = 3$, que es un número racional.

Son muy comunes las demostraciones matemáticas en las que se prueba que si cierto ente no existiera entonces se llegaría a un absurdo. Muchos matemáticos cuestionaron este tipo de demostraciones: Kronecker, Poincaré, Borel, Lebesgue y especialmente Brouwer, que crea la corriente filosófica llamada *intuicionismo*. En 1930, Heyting estudia la teoría de Brouwer desde el punto de vista lógico-matemático y da un sistema axiomático para dicha lógica. En este capítulo estudiaremos al Cálculo Proposicional Intuicionista, abreviadamente, CPI.

5.1. Sistema formal

En el Capítulo 3 hemos mencionado tres sistemas formales para el CPC. Vamos a mencionar ahora dos para el CPI, que se obtienen respectivamente a partir de **C** y de $\mathbf{L}_4$.

En el sistema **C**, el principio del tercero excluido figura como axioma **(XII)**. Suprimiendo ese axioma y manteniendo el lenguaje, los demás axiomas y la regla (MP) obtenemos un sistema formal para el CPI.

Utilizaremos en este capítulo el sistema, debido al propio Heyting, que llamaremos **LI**. La única diferencia de este sistema con el $\mathbf{L}_4$ es el último axioma: $\neg A \to (A \to B)$, que sustituye al $\neg\neg A \to A$ del sistema $\mathbf{L}_4$.

[1] Dov Jarden, "A simple proof that a power of an irrational number to an irrational exponent may be rational", Curiosa No. 339 in Scripta Mathematica 19:229 (1953).

Sistema LI

Lenguaje y reglas

Son los mismos que los del sistema $\mathbf{L}_4$.

Axiomas

(LI1) $\mathrm{A} \to (\mathrm{B} \to \mathrm{A})$.

(LI2) $(\mathrm{A} \to (\mathrm{B} \to \mathrm{C})) \to ((\mathrm{A} \to \mathrm{B}) \to (\mathrm{A} \to \mathrm{C}))$.

(LI3) $(\mathrm{A} \wedge \mathrm{B}) \to \mathrm{A}$.

(LI4) $(\mathrm{A} \wedge \mathrm{B}) \to \mathrm{B}$.

(LI5) $\mathrm{A} \to (\mathrm{B} \to (\mathrm{A} \wedge \mathrm{B}))$.

(LI6) $\mathrm{A} \to (\mathrm{A} \vee \mathrm{B})$.

(LI7) $\mathrm{B} \to (\mathrm{A} \vee \mathrm{B})$.

(LI8) $(\mathrm{A} \to \mathrm{C}) \to ((\mathrm{B} \to \mathrm{C}) \to ((\mathrm{A} \vee \mathrm{B}) \to \mathrm{C}))$.

(LI9) $(\mathrm{A} \to \mathrm{B}) \to ((\mathrm{A} \to \neg\mathrm{B}) \to \neg\mathrm{A})$.

(LI10) $\neg\mathrm{A} \to (\mathrm{A} \to \mathrm{B})$.

Como dijimos, el axioma $\neg\neg\mathrm{A} \to \mathrm{A}$ de $\mathbf{L}_4$ ha sido sustituido por el axioma $\neg\mathrm{A} \to (\mathrm{A} \to \mathrm{B})$.

De $\neg\neg\mathrm{A} \to \mathrm{A}$ puede deducirse $\neg\mathrm{A} \to (\mathrm{A} \to \mathrm{B})$. En efecto, fue probado que en el cálculo proposicional clásico vale la regla

$$(R18) \quad \frac{\neg\mathrm{A}}{\mathrm{A} \to \mathrm{B}}.$$

Luego, por el Teorema de la deducción,

$$\vdash \neg\mathrm{A} \to (\mathrm{A} \to \mathrm{B}).$$

Sin embargo, de $\neg\mathrm{A} \to (\mathrm{A} \to \mathrm{B})$ no puede deducirse $\neg\neg\mathrm{A} \to \mathrm{A}$ en el CPI. Veremos esto semánticamente en la Sección 4, Observación 5.4.6.

Observación 5.1.1. En relación con lo que acabamos de señalar, podemos ver que el CPC es una extensión del CPI (ver 1.4.7). En efecto, basta agregar el axioma $\neg\neg\mathrm{A} \to \mathrm{A}$ (o bien el principio del tercero excluido $\neg\mathrm{A} \vee \mathrm{A}$) al CPI para obtener el CPC. Además es una extensión *propia*, porque hay teoremas del CPC (como $\neg\neg\mathrm{A} \to \mathrm{A}$) que no son teoremas del CPI.

En adelante nos referiremos, sin mencionarlo cada vez, solo a fórmulas y propiedades del sistema **LI**.

En lo que sigue utilizaremos las definiciones de deducción, teorema, consecuencia, teoría, etc. dadas en el Capítulo 1.

Observación 5.1.2. Las demostraciones del Capítulo 3 que no dependen del último axioma valen en este caso. Ya tenemos mucho "trabajo hecho". Por ejemplo, vale el teorema de la deducción, que es tan útil, puesto que depende solo de los dos primeros axiomas del sistema formal.

Haremos ahora una lista de algunos resultados demostrados para el CPC que siguen valiendo para el CPI.

Teorema 5.1.3. *Sean* A *y* B *fórmulas cualesquiera, y sea* Γ *un conjunto de fórmulas. Si* $A \to B$ *es consecuencia de* Γ*, entonces* B *es consecuencia del conjunto* $\Gamma \cup \{A\}$.

Teorema 5.1.4 (Teorema de la deducción). *Sean* A *y* B *fórmulas cualesquiera, y sea* Γ *un conjunto de fórmulas. Si* B *es consecuencia de* $\Gamma \cup \{A\}$ *entonces* $A \to B$ *es consecuencia de* Γ.

Las demostraciones de estos dos metateoremas son las mismas que las del Capítulo 3.

Valen para el CPI las siguientes reglas:

(R1) $\dfrac{A}{B \to A}$,

(R2) $\dfrac{A \to (B \to C)\ ,\ A \to B}{A \to C}$,

(R3) $\dfrac{A \wedge B}{A}$,

(R4) $\dfrac{A \wedge B}{B}$,

(R5) $\dfrac{A\ ,\ B}{A \wedge B}$,

(R6) $\dfrac{A}{A \vee B}$,

(R7) $\dfrac{B}{A \vee B}$,

(R8) $\dfrac{A \to C\ ,\ B \to C}{(A \vee B) \to C}$, (R9) $\dfrac{A\to B\ ,\ A\to\neg B}{\neg A}$,

(R11) $\dfrac{C\to A\ ,\ C\to B}{C\to(A\wedge B)}$,

(R12) $\dfrac{A\to B}{(A\wedge C)\to(B\wedge C)}$,

(R12') $\dfrac{A\to B}{(C\wedge A)\to(C\wedge B)}$,

(R13) $\dfrac{A\to(B\to C)}{(A\wedge B)\to C}$,

(R14) $\dfrac{A}{\neg\neg A}$,

(R15) $\dfrac{A\to B}{\neg B\to\neg A}$,

(R18) $\dfrac{\neg A}{A\to B}$.

Excepto la regla (R18), las reglas listadas aquí se demuestran de la misma manera que para el CPC. La regla (R18) se deduce del axioma (LI10).

5.2. Álgebra de Lindenbaum

Como hemos mencionado anteriormente, si construimos a partir de las fórmulas del CPI el cociente por la misma relación de equivalencia que para el CPC obtendremos en este caso un álgebra de Heyting, que será llamada el *álgebra de Lindenbaum del CPI.* El cambio del último axioma, que implica la falta del principio del tercero excluido, hace la diferencia. En efecto, al pasar al cociente obtendremos una operación $()^*$ (pseudocomplemento) que cumple la condición de "complemento" con respecto al ínfimo pero no al supremo.

Sea $\mathcal{L}_{CPI}$ el conjunto de fórmulas del cálculo proposicional intuicionista axiomatizado según el sistema **LI**. Los dos lemas siguientes se demuestran de la misma manera que los análogos Lema 3.2.1 y Lema 3.2.2, parte (a) del Capítulo 3.

Lema 5.2.1. *Si* A, B *y* C *son fórmulas de* $\mathcal{L}_{CPI}$ *entonces la siguiente fórmula es un teorema:*

$$((A\vee B)\wedge C)\to((A\wedge C)\vee(B\wedge C)).$$

Lema 5.2.2. *Sea* A *una fórmula de* $\mathcal{L}_{CPI}$. *Entonces tenemos que*

$$\vdash \neg(\mathrm{A} \wedge \neg \mathrm{A}) \qquad \textit{(principio de no contradicción).}$$

Lema 5.2.3. *Sea* P *la siguiente relación en* $\mathcal{L}_{CPI}$:

$$\mathrm{A}\, P\, \mathrm{B} \;\; \textit{si y solo si} \; \vdash \mathrm{A} \to \mathrm{B}\,.$$

La relación P *es un preorden.*

Demostración. En el Ejemplo 2 del Capítulo 3 se probó que $\vdash \mathrm{A} \to \mathrm{A}$ usando solo los dos primeros axiomas. Luego, también deducimos $\mathrm{A} \to \mathrm{A}$ en el CPI.

Análogamente, en el Ejemplo 4 del Capítulo 3 probamos que la fórmula $\mathrm{A} \to \mathrm{C}$ es consecuencia de Γ, siendo $\Gamma = \{\mathrm{A} \to \mathrm{B}, \mathrm{B} \to \mathrm{C}\}$. De nuevo, la prueba solo depende de los dos primeros axiomas, por lo que vale en el CPI.

Luego, P es preorden en $\mathcal{L}_{CPI}$. □

Lema 5.2.4. *La relación binaria* $\equiv$ *en* $\mathcal{L}_{CPI}$ *dada por*

$$\mathrm{A} \equiv \mathrm{B} \;\; \textit{si y solo si}\; \mathrm{A}\, P\, \mathrm{B} \;\; \textit{y}\; \mathrm{B}\, P\, \mathrm{A}$$

es una relación de equivalencia.

Lema 5.2.5. *Sea* $A_{CPI} = \mathcal{L}_{CPI}/\equiv$. *Sean* $X, Y \in A_{CPI}$ *y sea* $\preceq$ *la siguiente relación en* A_{CPI}: $X \preceq Y$ *si y solo si* $\mathrm{A} \preceq \mathrm{B}$ *para* $\mathrm{A} \in X$ *y* $\mathrm{B} \in Y$. *Entonces,* $\preceq$ *está bien definida y es un orden en* A_{CPI}.

Demostración. Es consecuencia de la Observación 1.2.7 dada en el Capítulo 1. □

Lema 5.2.6.

(a) *Sea* $\mathrm{A} \in \mathcal{L}_{CPI}$. *Entonces,* $\vdash \mathrm{A}$ *si y solo si para toda clase* $|\mathrm{B}|$ *vale que* $|\mathrm{B}| \preceq |\mathrm{A}|$. *En particular, el conjunto de los teoremas forma una clase de equivalencia que resulta ser el último elemento de* A_{CPI}, *al cual llamaremos* $\mathbf{1}$.

(b) *Sea* $\mathrm{A} \in \mathcal{L}_{CPI}$. *Entonces,* $\vdash \neg\mathrm{A}$ *si y solo si para toda clase* $|\mathrm{B}|$ *vale que* $|\mathrm{A}| \preceq |\mathrm{B}|$. *En particular, el conjunto de fórmulas cuya negación es un teorema forma una clase de equivalencia que resulta ser el primer elemento de* A_{CPI}, *al cual llamaremos* $\mathbf{0}$.

Demostración. La demostración es la misma que la del Lema 3.2.6 del Capítulo 3. □

Con todos estos resultados, estamos en condiciones de demostrar el siguiente teorema.

Teorema 5.2.7. *El conjunto ordenado* $(A_{CPI}, \preceq)$ *es un retículo acotado.*

Demostración. Se demuestra de la misma manera que se hace en el Teorema 3.2.8 del Capítulo 3 para el conjunto ordenado $(A_{CPC}, \preceq)$. □

Vamos a denotar con el mismo símbolo a las operaciones respectivamente de ínfimo, supremo e implicación definidos en A_{CPI} que a los conectivos $\wedge$, $\vee$ y $\rightarrow$, símbolos del lenguaje del sistema **LI**.

Teorema 5.2.8. *Sea* $\mathbf{A}_{CPI} = \langle A_{CPI}, \wedge, \vee, \rightarrow, \mathbf{1}, \mathbf{0}\rangle$ *el álgebra cuyas operaciones están definidas por:*

$$\begin{aligned} |\mathrm{A}| \wedge |\mathrm{B}| &= |\mathrm{A} \wedge \mathrm{B}|, \\ |\mathrm{A}| \vee |\mathrm{B}| &= |\mathrm{A} \vee \mathrm{B}|, \\ |\mathrm{A}| \rightarrow |\mathrm{B}| &= |\mathrm{A} \rightarrow \mathrm{B}|, \\ \mathbf{1} &= |\mathrm{A} \rightarrow \mathrm{A}|, \\ \mathbf{0} &= |\mathrm{A} \wedge \neg\mathrm{A}|. \end{aligned}$$

Entonces, $\mathbf{A}_{CPI}$ *es un álgebra de Heyting.*

Demostración. En primer lugar, probemos que $\rightarrow$ está bien definida en A_{CPI}. Sean A' y B' tales que $|\mathrm{A}| = |\mathrm{A}'|$ y $|\mathrm{B}| = |\mathrm{B}'|$ o sea: $\vdash \mathrm{A} \rightarrow \mathrm{A}'$, $\vdash \mathrm{A}' \rightarrow \mathrm{A}$, $\vdash \mathrm{B} \rightarrow \mathrm{B}'$, $\vdash \mathrm{B}' \rightarrow \mathrm{B}$. Veamos, usando el Teorema de la deducción, que $\vdash (\mathrm{A} \rightarrow \mathrm{B}) \rightarrow (\mathrm{A}' \rightarrow \mathrm{B}')$. Para eso basta probar que $(\mathrm{A} \rightarrow \mathrm{B}), \mathrm{A}' \vdash \mathrm{B}'$.

(i) $\mathrm{A}' \rightarrow \mathrm{A}$.

(ii) $\mathrm{B} \rightarrow \mathrm{B}'$.

(iii) $\mathrm{A} \rightarrow \mathrm{B}$ (hipótesis adicional).

(iv) A' (hipótesis adicional).

(v) A, de (i), (iv) y MP.

(vi) B, de (iii), (v) y MP.

(vii) B', de (ii), (vi) y MP.

Hemos probado entonces $\vdash (\mathrm{A} \rightarrow \mathrm{B}) \rightarrow (\mathrm{A}' \rightarrow \mathrm{B}')$. Análogamente, se prueba $\vdash (\mathrm{A}' \rightarrow \mathrm{B}') \rightarrow (\mathrm{A} \rightarrow \mathrm{B})$, y por lo tanto: $|\mathrm{A} \rightarrow \mathrm{B}| = |\mathrm{A}' \rightarrow \mathrm{B}'|$, con lo que $\rightarrow$ está bien definida.

Ahora veamos que la implicación definida es la correcta. Tenemos que probar que $|\mathrm{A} \rightarrow \mathrm{B}|$ cumple las siguientes dos condiciones:

(1) $|\mathrm{A} \to \mathrm{B}| \wedge |\mathrm{A}| \preceq |\mathrm{B}|$,

(2) Si $|\mathrm{C}|$ es tal que $|\mathrm{C}| \wedge |\mathrm{A}| \preceq |\mathrm{B}|$ entonces $|\mathrm{C}| \preceq |\mathrm{A} \to \mathrm{B}|$.

La condición (1) se cumple por (MP). Para probar (2) supongamos que $|\mathrm{C}| \wedge |\mathrm{A}| \preceq |\mathrm{B}|$, es decir, $\vdash (\mathrm{C} \wedge \mathrm{A}) \to \mathrm{B}$. De allí podemos deducir que $\mathrm{A}, \mathrm{C} \vdash \mathrm{B}$. Utilizando luego el Teorema de la deducción inferimos que $\vdash \mathrm{C} \to (\mathrm{A} \to \mathrm{B})$, es decir, $|\mathrm{C}| \preceq |\mathrm{A} \to \mathrm{B}|$.

Hemos completado entonces la prueba de que $\mathbf{A}_{CPI}$ es un álgebra de Heyting. □

El álgebra $\mathbf{A}_{CPI}$ es el *álgebra de Lindenbaum del CPI*.

5.3. Valuaciones

Daremos ahora la siguiente definición, de acuerdo con la Definición 1.4.12 del Capítulo 1.

Definición 5.3.1. Dada un álgebra de Heyting H, una *H-valuación* v es una aplicación $v : \mathcal{L}_{CPI} \longrightarrow H$, que verifica las siguientes condiciones:

(V1) $v(\mathrm{A} \wedge \mathrm{B}) = v(\mathrm{A}) \wedge v(\mathrm{B})$,

(V2) $v(\mathrm{A} \vee \mathrm{B}) = v(\mathrm{A}) \vee v(\mathrm{B})$,

(V3) $v(\mathrm{A} \to \mathrm{B}) = v(\mathrm{A}) \to v(\mathrm{B})$,

(V4) $v(\neg \mathrm{A}) = (v(\mathrm{A}))^*$.

En particular, la aplicación canónica $p : \mathcal{L}_{CPI} \longrightarrow A_{CPI}$ es una A_{CPI}-valuación (se deja como ejercicio).

Definición 5.3.2. Sean $\mathrm{A} \in \mathcal{L}_{CPI}$ y H un álgebra de Heyting. Diremos que A es válida en H (o *H-válida*) si para toda H-valuación v vale que $v(A) = 1$. Diremos que A es *válida* si es H-válida para toda álgebra de Heyting H, lo cual se denotará como $\models \mathrm{A}$.

Ejemplo 5.3.3. Daremos un ejemplo sencillo de una valuación a valores en el álgebra de Heyting de universo $\{0, a, 1\}$ (conjunto ordenado de tres elementos con $0 < a < 1$). Notar que la implicación está dada por

$\rightarrow$	0	a	1
0	1	1	1
a	0	1	1
1	0	a	1

Sea $v : \mathcal{L}_{CPI} \longrightarrow \{0, a, 1\}$ definida por $v(\mathrm{p}_1) = 1$, $v(\mathrm{p}_2) = a$ y $v(\mathrm{p}_4) = a$. Suponemos definido el valor de v en las demás variables, pero no nos interesa para evaluar fórmulas que solo contengan p_1, p_2 y p_4.

Sea A la fórmula $\neg(\mathrm{p}_1 \rightarrow \mathrm{p}_4) \vee \mathrm{p}_2$, entonces

$$\begin{aligned} v(\mathrm{A}) &= (v(\mathrm{p}_1 \rightarrow \mathrm{p}_4))^* \vee v(\mathrm{p}_2) \\ &= (v(\mathrm{p}_1) \rightarrow v(\mathrm{p}_4))^* \vee v(\mathrm{p}_2) \\ &= (1 \rightarrow a)^* \vee a \\ &= a. \end{aligned}$$

Asimismo, verifiquemos que ni $\mathrm{A} \vee \neg\mathrm{A}$ ni la fórmula $\neg\neg\mathrm{A} \rightarrow \mathrm{A}$ son válidas en esta álgebra. Sea B la fórmula $\mathrm{p}_2 \vee \neg\mathrm{p}_2$. Entonces

$$\begin{aligned} v(\mathrm{B}) &= v(\mathrm{p}_2) \vee (v(\mathrm{p}_2))^* \\ &= a \vee 0 \\ &= a \\ &\neq 1. \end{aligned}$$

Análogamente, sea C la fórmula $\neg\neg\mathrm{p}_2 \rightarrow \mathrm{p}_2$. Entonces,

$$\begin{aligned} v(\mathrm{C}) &= v(\mathrm{p}_2)^{**} \rightarrow v(\mathrm{p}_2) \\ &= a^{**} \rightarrow a \\ &= 1 \rightarrow a \\ &= a \\ &\neq 1. \end{aligned}$$

Por lo tanto, ni $\mathrm{A} \vee \neg\mathrm{A}$ ni la fórmula $\neg\neg\mathrm{A} \rightarrow \mathrm{A}$ son válidas.

Observación 5.3.4. Observemos que, como ya se vio en 1.4.12 del Capítulo 1, una valuación queda definida por sus valores en las variables proposicionales. En efecto, si una fórmula A se obtiene aplicando ciertos conectivos sucesivamente a sus variables $\mathrm{p}_1, \ldots, \mathrm{p}_n$, el valor de $v(\mathrm{A})$ por una valuación v se obtiene aplicando a los valores $v(\mathrm{p}_1), \ldots, v(\mathrm{p}_k)$ las operaciones en el álgebra correspondiente respectivamente a esos conectivos.

A continuación daremos algunos resultados análogos a los dados en el Capítulo 3.

Teorema 5.3.5 (Teorema de corrección). *Si* $\vdash \mathrm{A}$ *entonces* $\vDash \mathrm{A}$.

Demostración. Es la misma prueba hecha en el Teorema 3.5.1 del Capítulo 3, cambiando “tautología” por “fórmula válida”. $\square$

Lema 5.3.6. *Sea v una A-valuación y $h : A \longrightarrow B$ un homomorfismo. Luego $v' = h \circ v$ es una B-valuación.*

Lema 5.3.7. *Sean v una H-valuación y A, B fórmulas. Si $|\mathrm{A}| \preceq |\mathrm{B}|$ entonces $v(\mathrm{A}) \leq v(\mathrm{B})$. Si $\hat{v} : A_{CPI} \to H$ es la aplicación $\hat{v}(|\mathrm{A}|) = v(\mathrm{A})$ entonces $\hat{v}$ es un homomorfismo.*

Demostración. La primera afirmación se prueba como en la Observación 3.5.11 (utilizando el Teorema 5.3.5). Luego, $|\mathrm{A}| = |\mathrm{B}|$ si y solo si $v(\mathrm{A}) = v(\mathrm{B})$, lo que prueba que $\hat{v}$ está bien definida. Se deja como ejercicio ver que $\hat{v}$ es un homomorfismo. $\square$

Lema 5.3.8. *Sea $h : A_{CPI} \longrightarrow H$ un homomorfismo y sea $v_h = h \circ p$, siendo $p : \mathcal{L}_{CPI} \longrightarrow A_{CPI}$ la aplicación canónica. Entonces v_h es una valuación. La aplicación $v \mapsto \hat{v}$ es una biyección entre el conjunto de H-valuaciones y el conjunto de homomorfismos de A_{CPI} en H cuya inversa es $h \mapsto v_h$.*

Demostración. El hecho de que v_h es una valuación sale del Lema 5.3.6, por ser p A_{CPI}-valuación. Para probar que $v \mapsto \hat{v}$ es una biyección usamos la misma demostración que en el Corolario 3.5.4 reemplazando **2** por H. $\square$

5.4. Completud fuerte

La completud de un sistema formal puede pensarse como la “fidelidad” del sistema axiomático para contener como proposiciones demostrables las proposiciones válidas y solo ellas.

La completud fuerte significa que, para un conjunto de fórmulas Γ dado, las nociones de consecuencia sintáctica y consecuencia semántica de Γ coinciden. En particular, podemos deducir de la completud fuerte la completud, tomando como Γ el conjunto vacío.

Ya hemos demostrado ambas propiedades para el CPC, vamos a generalizarlas ahora para el CPI.

También demostraremos que el álgebra de Lindenbaum del CPI es libre con un número numerable de generadores, que son las clases de las variables proposicionales.

En lo que sigue utilizaremos las definiciones de deducción, consecuencia, teoría, etc. dadas en el Capítulo 1, Sección 4. La noción de teoría del CPI es análoga a la del CPC: una teoría del CPI es un conjunto de fórmulas que contiene todas las instancias de axiomas y es cerrado por la regla (MP).

Observación 5.4.1. Sea Γ un conjunto de fórmulas del CPI. Luego valen las siguientes condiciones:

(a) Si $\Gamma = \mathcal{Z}_{CPI}$ es el conjunto de los teoremas del CPI entonces, $\mathcal{Z}_{CPI} = \emptyset^{\vdash}$.

(b) $\Gamma \subseteq \Gamma^{\vdash}$ y $\Gamma^{\vdash}$ es una teoría.

(c) Si Υ es una teoría entonces $\Upsilon^{\vdash} = \Upsilon$. En particular, $(\Gamma^{\vdash})^{\vdash} = \Gamma^{\vdash}$ (con lo cual $\Gamma \vdash \mathrm{A}$ si y solo si $\Gamma^{\vdash} \vdash \mathrm{A}$).

Puede demostrarse el siguiente resultado, definiendo de la misma manera que en el CPC la asignación entre filtros y teorías.

Teorema 5.4.2. *Existe una biyección entre la clase de los filtros del álgebra de Lindenbaum A_{CPI} del CPI y la clase de las teorías del CPI.*

La siguiente definición y el siguiente lema nos serán útiles para probar la completud fuerte del CPI.

Definición 5.4.3. Sean $\Gamma \subseteq \mathcal{L}_{CPI}$ y $\mathrm{A} \in \mathcal{L}_{CPI}$.

a) Sea H un álgebra de Heyting. Una H-valuación v es un *modelo* para Γ si para toda $\mathrm{C} \in \Gamma$ vale que $v(\mathrm{C}) = 1$.

b) Diremos que A es *consecuencia semántica* de Γ si para toda álgebra de Heyting H y para toda H-valuación v vale que si v es un modelo de Γ entonces $v(\mathrm{A}) = 1$. Notación: $\Gamma \vDash \mathrm{A}$.

Lema 5.4.4. *Si H es un álgebra de Heyting y v es una H-valuación entonces v es un modelo para Γ si y solo si v es un modelo para $\Gamma^{\vdash}$. En particular, $\Gamma \vDash \mathrm{A}$ si y solo si $\Gamma^{\vdash} \vDash \mathrm{A}$.*

Demostración. Sea H un álgebra de Heyting y v una H-valuación. Primero supongamos que v es un modelo de Γ y probemos que v es un modelo de $\Gamma^{\vdash}$. Debemos mostrar que $v(C) = 1$ para todo $C \in \Gamma^{\vdash}$. Sea C una fórmula cuya deducción a partir de Γ tiene una única fórmula. Luego C es un axioma o bien $C \in \Gamma$. Si C es un axioma entonces $v(C) = 1$, por el Teorema 5.3.5. Si $C \in \Gamma$ entonces sabemos que $v(C) = 1$. Supongamos que para toda deducción C de Γ de menos que n pasos vale que $v(C) = 1$. Sea C una deducción a partir de Γ de n pasos, con lo cual existe una sucesión $C_1, \ldots, C_n = C$ tal que para cada i vale que C_i es axioma, $C_i \in \Gamma$ o C_i se deduce de dos miembros anteriores de la sucesión por (MP). Si C es un axioma o $C \in \Gamma$ entonces $v(C) = 1$. Supongamos que C se deduce de dos miembros anteriores de la sucesión, C_i y $C_j = C_i \to C$ por (MP). Por hipótesis inductiva vale que $v(C_i) = 1$ y $v(C_i) \to v(C) = 1$, por lo cual $v(C_i) \leq v(C)$. Pero $v(C_i) = 1$. Por ende, $v(C) = 1$. De este modo hemos probado que v es un modelo de $\Gamma^{\vdash}$. Recíprocamente, supongamos que v es un modelo de $\Gamma^{\vdash}$. Como $\Gamma \subseteq \Gamma^{\vdash}$ tenemos que v es un modelo de Γ. De esta propiedad se deduce de manera inmediata que $\Gamma \vDash \mathrm{A}$ si y solo si $\Gamma^{\vdash} \vDash \mathrm{A}$. $\square$

El siguiente resultado se denomina Teorema de Completud fuerte del CPI.

Teorema 5.4.5. *Sean* $\Gamma \subseteq \mathcal{L}_{CPI}$ *y* $\mathrm{A} \in \mathcal{L}_{CPI}$. *Luego* $\Gamma \vdash \mathrm{A}$ *si y solo si* $\Gamma \vDash \mathrm{A}$.

Demostración. En virtud de la Observación 5.4.1 (c) y del Lema 5.4.4 podemos asumir que Γ es una teoría.

En primer lugar, supongamos que $\Gamma \vdash \mathrm{A}$. Sea H un álgebra de Heyting y v una H-valuación tal que es un modelo de Γ. Es decir, $v(\mathrm{C}) = 1$ para toda $\mathrm{C} \in \Gamma$. Debemos probar que $v(\mathrm{A}) = 1$. Decir que $\Gamma \vdash \mathrm{A}$ es equivalente a decir que $\mathrm{A} \in \Gamma^{\vdash} = \Gamma$ (ya que Γ es una teoría). Luego $v(\mathrm{A}) = 1$. Por esta razón, $\Gamma \vDash \mathrm{A}$.

Sea ahora $\Gamma \vDash \mathrm{A}$ y supongamos que no es verdad que $\Gamma \vdash \mathrm{A}$, es decir que $\mathrm{A} \notin \Gamma^{\vdash} = \Gamma$. Luego, $|\mathrm{A}|$ no pertenece al filtro $|\Gamma|$ de A_{CPI}. Sea $v = q \circ p$ como lo muestra el diagrama, siendo p y q las respectivas aplicaciones canónicas al cociente.

$$\begin{tikzcd}
\mathcal{L}_{CPI} \arrow[d, "p"'] \arrow[dr, "v"] & \\
A_{CPI} \arrow[r, "q"'] & A_{CPI}/|\Gamma|
\end{tikzcd}$$

Como p es una valuación y q es un homomorfismo, resulta que v es una valuación. Sea $\mathrm{C} \in \Gamma$. Luego $|\mathrm{C}| \in |\Gamma|$, de donde $v(\mathrm{C}) = q(|\mathrm{C}|) = 1$. Entonces, v es un modelo de Γ. Por lo tanto, debe ser $v(\mathrm{A}) = 1$, o sea, $q(|\mathrm{A}|) = 1$. Pero esto último significa que $|\mathrm{A}| \in |\Gamma|$, contra lo supuesto.

Por lo tanto concluimos que $\Gamma \vdash \mathrm{A}$. $\square$

Observación 5.4.6. Como vimos en 5.3.3, existe una valuación a valores en el álgebra de Heyting de universo $\{0, a, 1\}$ que no satisface la fórmula $\neg\neg\mathrm{A} \to \mathrm{A}$. Como $\neg\mathrm{A} \to (\mathrm{A} \to \mathrm{B})$ es válida (por ser axioma) se tiene que $\neg\mathrm{A} \to (\mathrm{A} \to \mathrm{B}) \nvDash \neg\neg\mathrm{A} \to \mathrm{A}$. Luego, por el Teorema 5.4.5, $\neg\mathrm{A} \to (\mathrm{A} \to \mathrm{B}) \nvdash \neg\neg\mathrm{A} \to \mathrm{A}$ en el CPI.

Ahora estamos en condiciones de enunciar el siguiente resultado, conocido como Teorema de completud del CPI.

Corolario 5.4.7. *Si* $\mathrm{A} \in \mathcal{L}_{CPI}$ *entonces* $\vdash \mathrm{A}$ *si y solo si* $\models \mathrm{A}$.

Demostración. Se deduce del Teorema 5.4.5 tomando $\Gamma = \emptyset$. □

El álgebra A_{CPI} es libre

La demostración del Teorema 3.5.13 del Capítulo 3 se basa en que, en primer lugar, una valuación es constante en cada clase de equivalencia y además, cada valuación a valores en cierta álgebra de la clase permite definir un homomorfismo del álgebra de Lindenbaum en dicha álgebra. Estas propiedades también valen para el CPI, como podemos ver en el Lema 5.3.7.

Teorema 5.4.8. *Sea* $\mathcal{V}$ *el conjunto de las variables proposicionales del CPI y sea* $|\mathcal{V}| = \{|p_i| : \; p_i \in \mathcal{V}\}$. *El conjunto* $|\mathcal{V}|$ *genera libremente* A_{CPI} *en la clase de las álgebras de Heyting.*

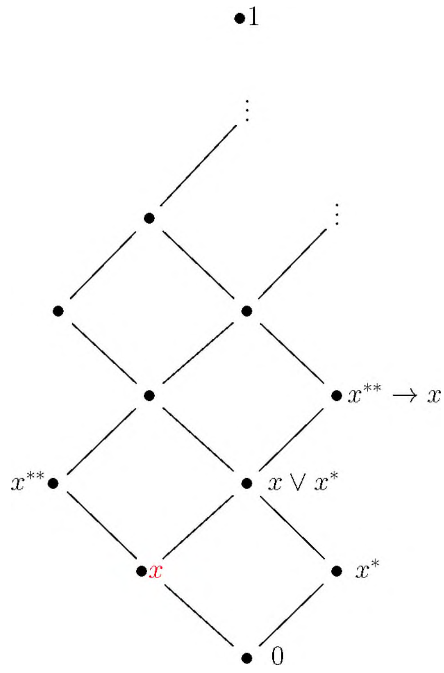
Demostración. El diagrama en este caso es el siguiente:

$$\begin{tikzcd} |\mathcal{V}| \arrow[r, "f"] \arrow[d, "inc"'] & H \\ A_{CPI} \arrow[ur, "g"'] & \end{tikzcd}$$

□

Observación 5.4.9. Las álgebras de Heyting libres con finitos generadores, que corresponden como antes al álgebras de Lindenbaum del CPI con un número finito de variables, **no son finitas**. Esto muestra una importante diferencia entre el CPC y el CPI: cada fórmula del CPC es equivalente a una que es disyunción de conjunciones básicas, propiedad que no se verifica en el CPI. Esto lleva a considerar la diferencia entre "conectivos booleanos" (que pueden reducirse por equivalencia a los conectivos básicos del CPC) y "conectivos intuicionistas". Trataremos a estos conectivos más adelante.

Como ejemplo podemos ver cuál es el álgebra de Heyting libre con un generador x, cuyo diagrama es el siguiente [2]:



Propiedad de modelos finitos

Vimos que en el CPC para demostrar completud basta con tomar un único modelo finito: **2**. Veremos que en el CPI debemos tomar todos los modelos finitos (es decir, todas las álgebras de Heyting finitas).

Nuestro siguiente objetivo es probar lo que se conoce con el nombre de *Propiedad de modelos finitos del CPI*:

$\vdash$ A si y solo si para toda álgebra de Heyting finita H y para toda H-valuación v vale que $v(\mathrm{A}) = 1$.

Antes de probar la propiedad de modelos finitos del CPI vamos a dar algunas definiciones y propiedades técnicas necesarias para la demostración.

Si L es un retículo distributivo acotado y $X \subseteq L$ entonces existe el menor subretículo acotado de L que contiene a X (es decir, el menor subretículo de L que contiene a X, 0 y 1). Denotaremos como $\langle X \rangle$ a este retículo distributivo acotado. Notar que $\langle X \rangle = \bigcap\{M : M \text{ subretículo acotado de } L, X \subseteq M\}$.

Lema 5.4.10. *Si L un retículo distributivo acotado y X es un subconjunto finito de L entonces $\langle X \rangle$ es finito.*

Demostración. La prueba se puede hacer por inducción sobre la cantidad de elementos de X. Si $X = \{x\}$ entonces es inmediato que $\langle X \rangle = \{0, x, 1\}$, con lo cual $\langle X \rangle$ es finito. Supongamos que: si X es un conjunto con n elementos entonces $\langle X \rangle$ es finito. Sea Y un subconjunto de L con $n + 1$ elementos. Entonces existen $X, x \in L$ tales que $Y = X \cup \{x\}$, donde X tiene n elementos. Se deja como ejercicio probar que

$$\langle Y \rangle = \langle X \rangle \cup T,$$

siendo $T = \{y \vee (z \wedge x) : y, z \in \langle X \rangle\}$. Por hipótesis inductiva resulta que $\langle X \rangle$ es finito. Además, es inmediato que T es finito. Luego $\langle Y \rangle$ es finito, como deseábamos probar. $\square$

Lema 5.4.11. *Sean H y G álgebras de Heyting, siendo G un subretículo acotado de H. Escribiremos $\rightarrow_H$ para la implicación en H y $\rightarrow_G$ para la implicación en G. Si $x, y, x \rightarrow_H y \in G$ entonces $x \rightarrow_H y = x \rightarrow_G y$.*

Demostración. Sean $x, y, x \rightarrow_H y \in G$. Sabemos que $x \wedge (x \rightarrow_H y) \leq y$. Siendo $x \rightarrow_H y = z$ un elemento de G que cumple $x \wedge z \leq y$, se tiene que $z = x \rightarrow_H y \leq x \rightarrow_G y$. Por otro lado, de la desigualdad $x \wedge (x \rightarrow_G y) \leq y$ en H se obtiene $x \rightarrow_G y \leq x \rightarrow_H y$. Por lo tanto, $x \rightarrow_H y = x \rightarrow_G y$. $\square$

Dada una fórmula A del CPI definimos el conjunto de subfórmulas de A como el menor conjunto de fórmulas $Sub(\mathrm{A})$ que satisface las siguientes condiciones:

1. $\mathrm{A} \in Sub(\mathrm{A})$.
2. Si $\neg\mathrm{B} \in Sub(\mathrm{A})$ entonces $\mathrm{B} \in Sub(\mathrm{A})$.
3. Si $\mathrm{B} \circ \mathrm{C} \in Sub(\mathrm{A})$ entonces $\mathrm{B}, \mathrm{C} \in Sub(\mathrm{A})$, siendo $\circ \in \{\wedge, \vee, \rightarrow\}$.

Por ejemplo, si $\mathrm{A} = (p_1 \rightarrow p_2) \vee \neg p_3$ entonces

$$Sub(\mathrm{A}) = \{\mathrm{A}, p_1 \rightarrow p_2, \neg p_3, p_3, p_1, p_2\}.$$

Teorema 5.4.12. *Sea A una fórmula del CPI. Luego $\vdash \mathrm{A}$ si y solo si para toda álgebra de Heyting finita H y para toda H-valuación v vale que $v(\mathrm{A}) = 1$.*

Demostración. Por el Corolario 5.4.7 basta probar que si H es un álgebra de Heyting y v es una H-valuación tal que $v(\mathrm{A}) \neq 1$ entonces existe un álgebra de Heyting finita G y una G-valuación w tal que $w(\mathrm{A}) \neq 1$.

Sean H un álgebra de Heyting y v una H-valuación tal que $v(\mathrm{A}) \neq 1$. Llamaremos $Sub(\mathrm{A})$ al conjunto de subfórmulas de A. Como $Sub(\mathrm{A})$ es finito, existen fórmulas $\mathrm{A_i}$ para $i = 1, \ldots, n$ tales que $Sub(\mathrm{A}) = \{\mathrm{A_1}, \ldots, \mathrm{A_n})\}$. Definamos el conjunto $X = \{v(\mathrm{A_1}), \ldots, v(\mathrm{A_n})\}$. Por el Lema 5.4.10 el retículo distributivo $G = \langle X \rangle$ es finito. En particular, G es un álgebra de Heyting. Nuestra meta es definir una G-valuación w tal que $w(\mathrm{A}) \neq 1$.

Sea Π el conjunto de variables proposicionales del CPI. Definimos una función $w : \Pi \to G$ como $w(p) = v(p)$ si $p \in \Pi \cap Sub(\mathrm{A})$ y $w(p) = 0$ en caso contrario. Esta función puede ser extendida de manera única a una G-valuación a la que también llamaremos w.

Queremos probar que para cada $i = 1, \ldots, n$ vale que $w(\mathrm{A_i}) = v(\mathrm{A_i})$. La prueba la haremos haciendo un razonamiento inductivo. Sea $\mathrm{A_i}$ una subfórmula de A en donde no aparecen conectivos. Luego $\mathrm{A_i} = p \in \Pi \cap Sub(\mathrm{A})$, con lo cual $w(\mathrm{A_i}) = v(\mathrm{A_i})$. Supongamos que $\mathrm{A_i} = \mathrm{A_j} \wedge \mathrm{A_k}$ ó $\mathrm{A_i} = \mathrm{A_j} \vee \mathrm{A_k}$; entonces es inmediato a partir de nuestra suposición que $w(\mathrm{A_i}) = v(\mathrm{A_i})$. Si $\mathrm{A_i} = \mathrm{A_j} \to \mathrm{A_k}$ entonces se deduce de nuestra suposición y del Lema 5.4.11 que $w(\mathrm{A_i}) = v(\mathrm{A_i})$. Finalmente sea $\mathrm{A_i} = \neg \mathrm{A_j}$. Como $v(\mathrm{A_i}) \in G$ y $v(\mathrm{A_j}) = w(\mathrm{A_i})$ entonces por el Lema 5.4.11 se tiene que $w(\mathrm{A_i}) = v(\mathrm{A_i})$. Luego para cada $i = 1, \ldots, n$ vale que $w(\mathrm{A_i}) = v(\mathrm{A_i})$. En particular tenemos que $w(\mathrm{A}) = v(\mathrm{A}) \neq 1$, es decir, $w(\mathrm{A}) \neq 1$. □

5.5. Teorema lógico de Glivenko

En esta sección aplicaremos el teorema algebraico de Glivenko visto en el capítulo anterior para demostrar el correspondiente metateorema lógico, que establece una vinculación entre el CPC y el CPI: cada teorema del CPC tiene su "traducción", la que resulta un teorema en el CPI.

Teorema 5.5.1. *Si* A *es un teorema del CPC entonces* $\neg\neg\mathrm{A}$ *es un teorema del CPI y recíprocamente.*

Demostración. Sea $\vdash_{CPC} \mathrm{A}$. Sea $h : \mathcal{L}_{CPI} \longrightarrow A_{CPI}$ la aplicación canónica y $r : A_{CPI} \longrightarrow \mathcal{R}eg(A_{CPI})$ la aplicación definida por $r(|A|) = |A^{**}|$. Definimos $v = r \circ h$ como lo muestra el siguiente diagrama:

$$\begin{tikzcd}
\mathcal{L}_{CPI} \arrow[d, "h"'] \arrow[dr, "v"] & \\
A_{CPI} \arrow[r, "r"'] & \mathcal{R}eg(A_{CPI})
\end{tikzcd}$$

Como h es una valuación y r es un homomorfismo resulta que v es una valuación (ver Lema 5.3.6) a valores en un álgebra de Boole. Luego, debe ser $v(\mathrm{A}) = (r \circ h)(\mathrm{A}) = 1$, es decir, $(|\mathrm{A}|)^{**} = 1$, que es lo mismo que: $|\neg\neg\mathrm{A}| = 1$. Pero esto último significa que $\vdash_{CPI} \neg\neg\mathrm{A}$.

Recíprocamente, supongamos que $\vdash_{CPI} \neg\neg$A. Como todos los axiomas del CPI son teoremas del CPC tenemos que existe una deducción de $\neg\neg$A en el CPC, y, por el axioma ($L_4$10), también una deducción de A. Es decir, $\vdash_{CPC}$ A. □

5.6. Modelos de Kripke

En el cálculo intuicionista no hay un álgebra "de valores de verdad" como el álgebra de Boole **2** del cálculo proposicional clásico. Sin embargo, existen ciertas álgebras de Heyting particulares, aquellas de la forma P^+, tales que para probar la validez de una fórmula basta verificar la validez en ellas. Este hecho es una consecuencia del Teorema 4.5.4 (de representación) visto en el Capítulo 4.

Veremos aquí ese nuevo concepto de validez que se da en los modelos de Kripke. Veremos que los dos conceptos de validez coinciden. En efecto, se prueba en el teorema de completud que una fórmula es válida en todo modelo de Kripke si y solo si es un teorema del cálculo intuicionista si y solo si es válida.

A través de los modelos de Kripke podemos probar resultados del CPI. Por ejemplo, una propiedad importante del CPI que es la *propiedad de la disyunción*: si una fórmula de la forma A $\vee$ B es un teorema, entonces A es un teorema o bien B es un teorema. Esta propiedad no vale en el cálculo clásico, pues basta tomar como A una variable p y considerar la disyunción p $\vee \neg$p, que es un teorema, sin serlo ni p ni $\neg$p.

Definición 5.6.1. Sea $(P, \leq)$ un conjunto ordenado y consideremos una *función de valuación* $K : \mathcal{L}_{CPI} \longrightarrow P^+$. Luego, para cada fórmula A, $K(\mathrm{A})$ es un subconjunto creciente de P, llamado el *conjunto de verdad* de A.

Sea $\mathcal{M} = ((P, \leq), K)$ un conjunto ordenado munido de una función de valuación. Diremos que $\mathcal{M}$ *fuerza* A en p y lo denotamos: $\mathcal{M} \Vdash_p$ A si $p \in K(\mathrm{A})$.

Llamaremos a $\mathcal{M} = ((P, \leq), K)$ *modelo de Kripke* si se cumplen las siguientes condiciones:

(1)	$\mathcal{M} \Vdash_p \neg\mathrm{A}$	si y solo si	$q \geq p$ implica $\mathcal{M} \nVdash_q$ A.
(2)	$\mathcal{M} \Vdash_p \mathrm{A} \vee \mathrm{B}$	si y solo si	$\mathcal{M} \Vdash_p$ A o $\mathcal{M} \Vdash_p$ B.
(3)	$\mathcal{M} \Vdash_p \mathrm{A} \wedge \mathrm{B}$	si y solo si	$\mathcal{M} \Vdash_p$ A y $\mathcal{M} \Vdash_p$ B.
(4)	$\mathcal{M} \Vdash_p \mathrm{A} \rightarrow \mathrm{B}$	si y solo si	$q \geq p$ implica:
			si $\mathcal{M} \Vdash_q$ A entonces $\mathcal{M} \Vdash_q$ B.

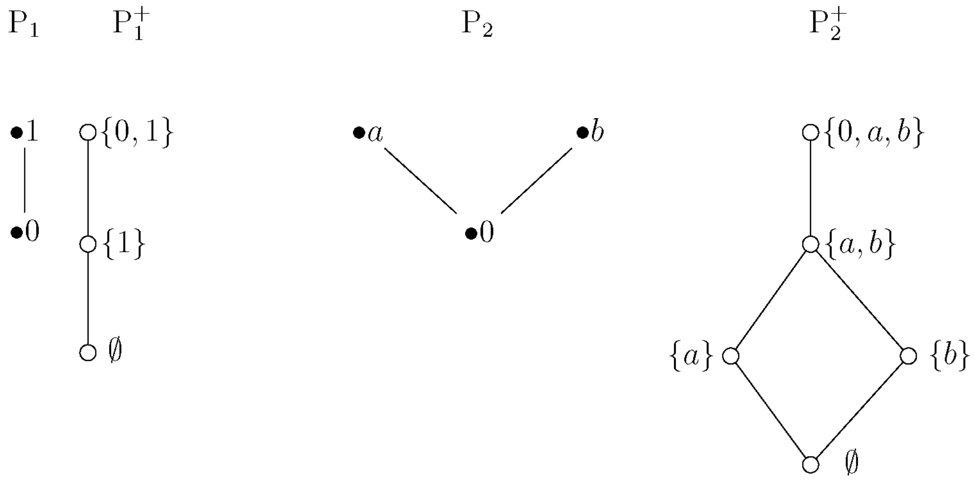


Figura 5.1: P_1 y P_2

Diremos que A es *válida en* $\mathcal{M}$, lo cual se denotará como $\mathcal{M} \Vdash$ A, si $\mathcal{M}$ fuerza A en p, para todo p, es decir, si $K(\text{A}) = P$.

Diremos que A es *válida por modelos de Kripke* o *válida* si para todo modelo $\mathcal{M}$ es $\mathcal{M} \Vdash$ A.

Es útil encontrar un *contramodelo* para una fórmula C, es decir, un modelo donde C no es válida. Con esto y usando el teorema de completud, podemos asegurar que C no es un teorema.

Observación 5.6.2. No debe confundirse el índice p usado para designar elementos del conjunto ordenado $(P, \leq)$ con el p usado para las variables proposicionales.

Ejemplo 5.6.3. Podemos presentar una **2**-valuación booleana v como un modelo de Kripke particular $\mathcal{M} = ((P, \leq), K)$, siendo P un conjunto unitario $P = \{x\}$. De esa manera, P^+ tendrá dos elementos ($\emptyset$ y $\{x\}$), por lo que resulta isomorfo a **2**. Tomamos $K = v$, con las debidas identificaciones.

Ejemplo 5.6.4. Sea $\mathcal{M}_1 = ((P_1, \leq), K_1)$, siendo P_1 el conjunto ordenado dado en la Figura 5.1, cuyos conjuntos crecientes están dados por P_1^+.[2] Definimos K_1 por $K_1(\text{p}) = \{1\}$, es decir:

$$\mathcal{M}_1 \Vdash_1 \text{p} \quad \text{y} \quad \mathcal{M}_1 \nVdash_0 \text{p}.$$

[2] Observemos que P_1^+ es isomorfo a la cadena de tres elementos, donde ya probamos, en 5.3.3, que A $\vee \neg$A no es válida.

Basta definir K_1 en una variable, ya que las dos fórmulas que estudiaremos solo tienen una variable.

Mostraremos que $\mathcal{M}_1$ es un contramodelo para la fórmula $\mathrm{C} = \mathrm{A} \vee \neg\mathrm{A}$. Basta ver que $\mathrm{p} \vee \neg\mathrm{p}$ no es válida, siendo p una variable proposicional.

Veamos que $\mathcal{M}_1 \nVdash_0 \mathrm{p} \vee \neg\mathrm{p}$.

En efecto, si fuera $\mathcal{M}_1 \Vdash_0 \mathrm{p} \vee \neg\mathrm{p}$ debería ser (por la condición (2)) $\mathcal{M}_1 \Vdash_0 \mathrm{p}$ o $\mathcal{M}_1 \Vdash_0 \neg\mathrm{p}$. Lo primero no se cumple por la definición de K_1. Para que valiera lo segundo, no debería haber ningún $q \geq 0$ donde valga $\mathcal{M}_1 \Vdash_q \mathrm{p}$, pero esto no se cumple tampoco, pues el único nodo $q > 0$ en P es $q = 1$, y $\mathcal{M}_1 \Vdash_1 \mathrm{p}$. Luego, $\mathcal{M}_1 \nVdash_0 \neg\mathrm{p}$, de donde $\mathcal{M}_1 \nVdash_0 \mathrm{p} \vee \neg\mathrm{p}$ y por lo tanto $\mathcal{M}_1 \nVdash \mathrm{p} \vee \neg\mathrm{p}$.

El modelo $\mathcal{M}_2 = ((P_2, \leq), K_2)$ será definido después de las siguientes observaciones.

Veamos que las condiciones (1), ..., (4) que definen un modelo de Kripke equivalen a que K sea una P^+-valuación.

(1) $p \in K(\neg\mathrm{A})$ si y solo si $q \geq p$ implica $q \notin K(\mathrm{A})$, o bien:

(1') $p \in K(\neg\mathrm{A})$ si y solo si $[p) \cap K(\mathrm{A}) = \emptyset$.

Las siguientes condiciones son equivalentes:

$[p) \cap K(\mathrm{A}) = \emptyset$.
$[p) \cap (K(\mathrm{A})] = \emptyset$.
$[p) \subseteq (K(\mathrm{A})]^c$.
$p \in (K(\mathrm{A})]^c$.

Es decir, tenemos que:

$p \in K(\neg\mathrm{A})$ si y solo si $p \in (K(\mathrm{A})]^c$, o sea:

$(\neg)$ $K(\neg\mathrm{A}) = (K(\mathrm{A})]^c$.

(2) $p \in K(\mathrm{A} \vee \mathrm{B})$ equivalente a $p \in K(\mathrm{A})$ o $p \in K(\mathrm{B})$, o bien:

$(\vee)$ $K(\mathrm{A} \vee \mathrm{B}) = K(\mathrm{A}) \cup K(\mathrm{B})$.

(3) $p \in K(\mathrm{A} \wedge \mathrm{B})$ equivalente a $p \in K(\mathrm{A})$ y $p \in K(\mathrm{B})$, o bien:

$(\wedge)$ $K(\mathrm{A} \wedge \mathrm{B}) = K(\mathrm{A}) \cap K(\mathrm{B})$.

(4) $p \in K(\mathrm{A} \to \mathrm{B})$ si y solo si para todo $q \geq p$ se tiene que $q \in K(\mathrm{A})$ implica $q \in K(\mathrm{B})$.

Las siguientes condiciones son equivalentes:

$[p) \cap K(\mathrm{A}) \subseteq K(\mathrm{B})$.

$([p) \cap K(\mathrm{A})) \cap (K(\mathrm{B}))^c = [p) \cap (K(\mathrm{A}) \cap (K(\mathrm{B}))^c) = \emptyset.$
$[p) \cap (K(\mathrm{A}) \cap (K(\mathrm{B}))^c] = \emptyset$ (pues $[p)$ creciente).
$[p) \subseteq (K(\mathrm{A}) \cap (K(\mathrm{B}))^c]^c.$
$p \in (K(\mathrm{A}) \cap (K(\mathrm{B}))^c]^c.$

Entonces, se tiene que
$p \in K(\mathrm{A} \to \mathrm{B})$ si y solo si $p \in (K(\mathrm{A}) \cap (K(\mathrm{B}))^c]^c$, es decir:

$(\to)$ $K(\mathrm{A} \to \mathrm{B}) = (K(\mathrm{A}) \cap (K(\mathrm{B}))^c]^c$.

Observación 5.6.5. Observemos que, para elementos X, Y del álgebra de Heyting P^+,

$$\begin{aligned} X^* &= (X]^c, \\ X \to Y &= (X \cap (Y)^c]^c, \\ X \wedge Y &= X \cap Y, \\ X \vee Y &= X \cup Y. \end{aligned}$$

Luego,

$(\neg)$ $K(\neg\mathrm{A}) = K(\mathrm{A})^*$,
$(\vee)$ $K(\mathrm{A} \vee \mathrm{B}) = K(\mathrm{A}) \vee K(\mathrm{B})$,
$(\wedge)$ $K(\mathrm{A} \wedge \mathrm{B}) = K(\mathrm{A}) \wedge K(\mathrm{B})$,
$(\to)$ $K(\mathrm{A} \to \mathrm{B}) = K(\mathrm{A}) \to K(\mathrm{B})$.

Estas igualdades, que hemos demostrado que son equivalentes a las condiciones (1), ..., (4), expresan que K es una P^+-valuación. Como consecuencia, teniendo en cuenta el Corolario 5.4.7, tenemos el siguiente resultado.

Corolario 5.6.6. *Sea $\mathcal{M} = ((P, \leq), K)$ un modelo de Kripke. Si $\vdash \mathrm{A}$ entonces $K(\mathrm{A}) = P$.*

Ejemplo 5.6.7. Sea $\mathcal{M}_2 = ((P_2, \leq), K_2)$, donde P_2 y P_2^+ son definidos como en la Figura 5.1 y $K_2(\mathrm{p}) = \{a\}$, $K_2(\mathrm{q}) = \{b\}$, para las variables proposicionales p y q. Se tiene entonces que $(K_2(\mathrm{p}))^* = \{b\}$, $(K_2(\mathrm{p}))^{**} = \{a\}$ y análogamente $(K_2(\mathrm{q}))^* = \{a\}$, $(K_2(\mathrm{q}))^{**} = \{b\}$.

Mostremos ahora que $\mathcal{M}_2$ es un contramodelo para la fórmula

$$\neg\neg(\mathrm{A} \vee \mathrm{B}) \to (\neg\neg\mathrm{A} \vee \neg\neg\mathrm{B}).$$

Según las observaciones anteriores y usando la ecuación $(x \vee y)^* = x^* \wedge y^*$ (ver Lema 4.1.7, Capítulo 4),

$$\begin{aligned} K(\neg\neg(\mathrm{p} \vee \mathrm{q})) &= (K(\mathrm{p} \vee \mathrm{q}))^{**} \\ &= (K(\mathrm{p}) \cup K(\mathrm{q}))^{**} \\ &= (K(\mathrm{p})^* \cap K(\mathrm{q})^*)^* \\ &= (\{b\} \cap \{a\})^* \\ &= (\emptyset)^* \\ &= \{0, a, b\}. \end{aligned}$$

Por otra parte:

$$\begin{aligned} K(\neg\neg\mathrm{p} \vee \neg\neg\mathrm{q}) &= K(\neg\neg\mathrm{p}) \cup K(\neg\neg\mathrm{q}) \\ &= K(\mathrm{p})^{**} \cup K(\mathrm{q})^{**} \\ &= \{a\} \cup \{b\} \\ &\neq \{0, a, b\}. \end{aligned}$$

Conectivos intuicionistas

Hemos establecido las igualdades:

($\neg$) $K(\neg\mathrm{A}) = (K(\mathrm{A})]^c$.

($\vee$) $K(\mathrm{A} \vee \mathrm{B}) = K(\mathrm{A}) \cup K(\mathrm{B})$.

($\wedge$) $K(\mathrm{A} \wedge \mathrm{B}) = K(\mathrm{A}) \cap K(\mathrm{B})$.

($\to$) $K(\mathrm{A} \to \mathrm{B}) = (K(\mathrm{A}) \cap (K(\mathrm{B}))^c]^c$.

Mirando el segundo miembro de las igualdades precedentes, vemos que definir la relación de forzamiento equivale a dar funciones "semánticas" Φ_{C}, para C cada uno de los conectivos: $\neg, \vee, \wedge, \to$. La función Φ_{C} opera sobre los conjuntos de verdad $K(\mathrm{A})$, $K(\mathrm{B})$ de manera que el conjunto $K(\mathrm{CA})$ *se define* como $\Phi_{\mathrm{C}}(K(\mathrm{A}))$ ó, si el conectivo es binario, $K(\mathrm{A}\ \mathrm{C}\ \mathrm{B}))$ se define: $\Phi_{\mathrm{C}}(K(\mathrm{A}), K(\mathrm{B}))$. Esto nos dice que estamos definiendo *semánticamente* el conectivo C, siendo C uno de los conectivos básicos. Parece entonces natural concebir a un *conectivo intuicionista* C semánticamente, definiéndolo en cada modelo $\mathcal{M} = ((P, \leq), K)$,por una función $\Phi_{\mathrm{C}} : P^+ \longrightarrow P^+$ (ver [15]).

Las funciones para los conectivos básicos son, respectivamente:

$\Phi_\neg(U) = (U]^c$,
$\Phi_\vee(U, V) = U \cup V$,
$\Phi_\wedge(U, V) = U \cap V$,

$\Phi_{\to}(U, V) = (U^c \cap V]^c$.

Si consideramos los conectivos básicos $\neg, \vee, \wedge, \to$ como conectivos del CPC, estos quedan determinados semánticamente por las condiciones que deben cumplir las valuaciones en $\mathbf{2} = \{0, 1\}$, es decir, por las tablas de verdad. Puede probarse en el caso del cálculo clásico que los conectivos básicos (bastaría, en realidad, tomar solo dos: $\neg$ y uno de los otros) forman un sistema *funcionalmente completo*. Esto significa que cualquier conectivo que podamos definir por medio de una función de $\mathbf{2}^n \longrightarrow \mathbf{2}$ resulta combinación de un número finito de aplicaciones de los conectivos básicos.

Esta propiedad no vale en el caso intuicionista. Existen conectivos que no son función de los básicos. ¿Qué significa entonces ser un *conectivo intuicionista*? ¿Cuál sería una definición apropiada? En 1997, X. Caicedo [16] dio una definición semántica de conectivo intuicionista basada en nociones categoriales. Asimismo, en [45], 1999, se muestra una definición equivalente. En seguida veremos estas dos definiciones.

Puede probarse que las funciones Φ_{C} asociadas a los conectivos básicos (considerados ahora en el cálculo intuicionista) verifican una condición "local" (supongamos por ahora que Φ_{C} unaria). Para $p \in P$, $T \in P^+$:

$$(C) \;\; p \in \Phi_{\text{C}}(T) \;\text{ si y solo si }\; p \in \Phi_{\text{C}}(T \cap [p)).$$

La condición (C) es equivalente a la siguiente:

Para $T, U \in P^+$:

$$(\circ) \;\; \Phi_{\text{C}}(T) \cap U = \Phi_{\text{C}}(T \cap U) \cap U.$$

Con esta motivación, para definir nuevos conectivos (intuicionistas) pediremos entonces a las funciones Φ_{C} que cumplan la condición (C) (o su equivalente, la condición ($\circ$)).

Definición 5.6.8. Un *conectivo intuicionista unario* C está dado en cada modelo de Kripke por una función $\Phi_{\text{C}} : P^+ \longrightarrow P^+$ que cumple (C).

La definición semántica del conectivo C estará dada estableciendo en cada modelo la siguiente igualdad:

$$K(\text{C}\,\text{A}) = \Phi_{\text{C}}(K(\text{A})),$$

o dicho de otra manera:

$$\Vdash_p \text{C}\,\text{A} \;\text{ si y solo si }\; p \in \Phi_{\text{C}}(K(\text{A})).$$

En general, si C fuera n-ario, la función cumpliría la condición

$$(\circ) \;\; \Phi_{\text{C}}(T_1, T_2, \ldots, T_n) \cap U = \Phi_{\text{C}}(T_1 \cap U, T_2 \cap U, \cdots, T_n \cap U) \cap U.$$

Aunque lo que diremos vale para conectivos n-arios, nos referiremos en lo que sigue solo a conectivos unarios por simplicidad de la exposición.

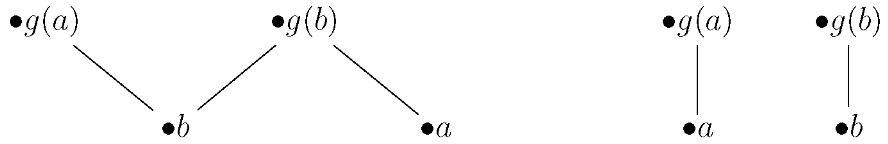


Figura 5.2: P_1 y P_2

Podemos pensar en esta definición semántica de conectivo en el CPI como algo análogo a la definición de un conectivo en el CPC mediante su tabla de verdad. La diferencia está en que en el CPI puede haber conectivos *nuevos*, cosa que no sucede en el CPC, ya que todos son combinaciones de los básicos.

Una vez demostrado que un conectivo es intuicionista, surge una difícil cuestión: obtener axiomas que caractericen dicho conectivo. No hay método general para esto. En [17] se dan, por ejemplo, axiomas para la función γ que se define en los modelos como veremos en seguida.

Ejemplos de conectivos que cumplen (C)

Sea $(P, \leq)$ un conjunto ordenado cualquiera. Para $X \subseteq P$ definimos X_M como el conjunto de elementos maximales de X.

Definimos las funciones $S : P^+ \to P^+$, $\gamma : P^+ \to P^+$ y $G : P^+ \to P^+$ como:

$$S(U) = U \cup (U^c)_M, \quad \gamma(U) = U \cup P_M, \quad G(U) = (U \cup (U^c)_M) \cap (([U]^c]^c.$$

Luego, para $\mathrm{R} = S$, γ, G tenemos que

1) $\mathrm{R}(U) \in P^+$,

2) $\mathrm{R}(U \cap V) \cap V = \mathrm{R}(U) \cap V$.

Ejemplos de conectivos que no cumplen (C)

Sea $(P_1, \leq)$ el conjunto ordenado dado por el diagrama izquierdo de la Figura 5.2, con g una involución allí indicada. Definimos N en P_1^+ por $N(T) = g(T^c)$.

La función N no satisface la condición (C).

Tomemos $T = \{g(a), g(b), b\}$. Entonces, $N(T) = \{g(a)\}$. Sea $S = \{g(b)\}$. Luego: $S \cap N(T) = \emptyset$. Por otra parte, $N(T \cap S) = N(S) = \{g(a), g(b), a\}$ y $S \cap N(T \cap S) = \{g(b)\} \neq \emptyset$.

Consideremos ahora $(P_2, \leq)$ dado por el diagrama de la derecha de la Figura 5.2.

La función Δ definida en P_2^+ por: $\Delta(X) = X \cap g(X)$ no cumple (C).

Sean $X = \{g(a), g(b), a\}$, $Y = \{g(a), g(b), b\}$. Entonces $\Delta(X) = \{g(a), a\}$, $\Delta(X) \cap Y = \{g(a)\}$. Por otra parte, $X \cap Y = \{g(a), g(b)\}$, $\Delta(X \cap Y) = \emptyset$ y por lo tanto, $\Delta(X \cap Y) \cap Y = \emptyset \neq \{g(a)\}$.

Propiedad semántica de la disyunción

Probaremos aquí la propiedad de la disyunción desde el punto de vista de los modelos de Kripke. Posteriormente la veremos desde el punto de vista sintáctico.

Pero antes necesitamos algunas definiciones.

Definición 5.6.9. Dado un modelo de Kripke $\mathcal{M} = ((P, \leq), K)$ y un elemento $p \in P$, llamaremos *modelo localizado en* p a $\mathcal{M}_p = (([p), \leq), K_p)$, donde K_p se define para una fórmula A por: $K_p(\mathrm{A}) = K(\mathrm{A}) \cap [p)$.

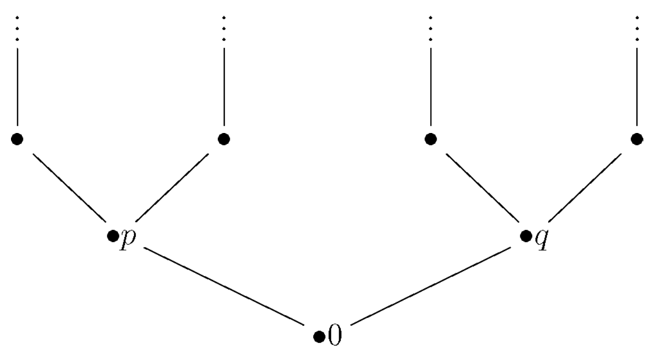
Diremos que dos modelos $\mathcal{M} = ((P, \leq), K)$ y $\mathcal{M}' = ((P', \leq), K')$ son *isomorfos* si existe un isomorfismo de orden $f : P \longrightarrow P'$ tal que, dada una fórmula A, se cumple que $p \in K(\mathrm{A})$ si y solo si $f(p) \in K'(\mathrm{A})$.

Teorema 5.6.10. *Sean* A *y* B *dos fórmulas tales que* $\Vdash \mathrm{A} \vee \mathrm{B}$. *Entonces* $\Vdash \mathrm{A}$ *o* $\Vdash \mathrm{B}$.

Demostración. Supongamos que ni A ni B son válidas. Luego, existirán dos modelos $\mathcal{M} = ((P, \leq), K)$ y $\mathcal{N} = ((Q, \leq), L)$ tales que $\mathcal{M} \nVdash \mathrm{A}$ y $\mathcal{N} \nVdash \mathrm{B}$ y por lo tanto existirán $p \in P$, $q \in Q$ tales que $\mathcal{M} \nvDash_p \mathrm{A}$ y $\mathcal{N} \nvDash_q \mathrm{B}$. Tomamos los modelos localizados $\mathcal{M}_p$ y $\mathcal{N}_q$. Podemos suponer que $[p) \cap [q) = \emptyset$. En efecto, si no fuera así, podemos tomar modelos isomorfos a $\mathcal{M}_p$ y a $\mathcal{N}_q$ que cumplan esa condición; por ejemplo, tomando $S_p = \{(0, u) : u \in [p)\}$ en lugar de $[p)$ y $S_q = \{(1, v) : v \in [q)\}$ en lugar de $[q)$ y definiendo adecuadamente las valuaciones respectivas.

Tenemos entonces que $\mathcal{M}_p \nvDash \mathrm{A}$ y $\mathcal{N}_q \nvDash \mathrm{B}$.

Definimos un nuevo modelo $\mathcal{O} = ((\{0\} \cup [p) \cup [q), \leq), V)$ cuyo conjunto ordenado es tal como se ve en el diagrama siguiente:



y cuya función V se define en cada fórmula C por:

$$V(\mathrm{C}) = K_p(\mathrm{C}) \cup L_q(\mathrm{C}).$$

Esto significa que $\mathcal{O} \Vdash_t$ C si y solo si $\mathcal{M}_p \Vdash_t$ C o $\mathcal{N}_p \Vdash_t$ C. Luego:

$\mathcal{O} \nVdash_p$ A y $\mathcal{O} \nVdash_q$ B.

Además,

$\mathcal{O} \nVdash_0$ A y $\mathcal{O} \nVdash_0$ B, pues el forzamiento en 0 implicaría el forzamiento en p y en q respectivamente.

Pero entonces

$\mathcal{O} \nVdash_0$ A $\vee$ B, por lo que $\mathcal{O} \nVdash$ A $\vee$ B. □

Completud por modelos de Kripke

Veamos que una fórmula es un teorema del CPI si y solo si es válida en todo modelo de Kripke.

Lema 5.6.11. *Si $\mathcal{M} = ((P, \leq), K)$ es un modelo de Kripke definimos $\hat{K} : A_{CPI} \to P^+$ por $\hat{K}(|A|) = K(A)$. La función $\hat{K}$ está bien definida y es un homomorfismo.*

Demostración. Se aplica el Lema 5.3.7. □

Corolario 5.6.12. *Sean $h : \mathcal{L}_{CPI} \longrightarrow A_{CPI}$ la aplicación canónica y $e = e_{A_{CPI}} : A_{CPI} \longrightarrow (A^\star_{CPI})^+$ el homomorfismo inyectivo dado en el Teorema 4.5.4 del Capítulo 4. Sea v la composición, como muestra el siguiente diagrama:*

$$\begin{tikzcd}
\mathcal{L}_{CPI} \arrow[d, "h"'] \arrow[dr, "v"] & \\
A_{CPI} \arrow[r, "e"'] & (A^\star_{CPI})^+
\end{tikzcd}$$

Luego v es una valuación y $\mathcal{M}_c = ((A^\star_{CPI}, \subseteq), v)$ es un modelo de Kripke, llamado modelo canónico.

Demostración. Como mencionamos luego de la Definición 5.3.1, la aplicación canónica h es una A_{CPI}-valuación. Como e es un homomorfismo entonces, por 5.3.6, $v = e \circ h$ es una $(A^\star_{CPI})^+$-valuación, de donde $\mathcal{M}_c$ es un modelo de Kripke. □

Observación 5.6.13. Por abuso de lenguaje suele considerarse también que $\mathcal{M}_c = ((A^\star_{CPI}, \subseteq), e)$ es un modelo de Kripke. Notemos que $e = \hat{v}$.

Teorema 5.6.14 (Teorema de completud). *Dada una fórmula* A,

$$\vdash \mathrm{A} \textit{ si y solo si } \mathcal{M} \Vdash \mathrm{A} \textit{ para todo modelo de Kripke } \mathcal{M}.$$

Demostración. La corrección fue probada en el Corolario 5.6.6.

Veamos que si A es válida en todo modelo de Kripke entonces A es un teorema. Sea A válida en todo modelo de Kripke y consideremos el modelo de Kripke $\mathcal{M}_c$. Luego $v(\mathrm{A}) = e(|\mathrm{A}|) = 1$. Como e es inyectiva concluimos que $|\mathrm{A}| = 1$. Por lo tanto, A es un teorema. □

En el siguiente corolario se muestra que la validez y la validez por modelos de Kripke coinciden.

Corolario 5.6.15. *Dada una fórmula* A*,*

$$\vDash \mathrm{A} \textit{ si y solo si } \mathcal{M} \Vdash \mathrm{A} \textit{ para todo modelo de Kripke } \mathcal{M}.$$

Demostración. Es consecuencia del Teorema 5.6.14 y del Corolario 5.4.7. □

Propiedad sintáctica de la disyunción

Una vez demostradas la propiedad semántica de la disyunción y la completud por modelos de Kripke, la propiedad sintáctica de la disyunción sale como corolario, según veremos en seguida.

Teorema 5.6.16. *Sean* A *y* B *dos fórmulas tales que* $\vdash \mathrm{A} \vee \mathrm{B}$*. Entonces* $\vdash \mathrm{A}$ *o* $\vdash \mathrm{B}$.

Demostración. Es consecuencia del Teorema 5.6.10 y del Teorema 5.6.14. □

Modelos de Kripke "enriquecidos"

Daremos ahora algunos ejemplos de modelos de Kripke a los que se agregan algunas funciones que no cumplen la condición (C), o sea, que no definen conectivos intuicionistas.

La necesidad de definir estos modelos provino de la creación de ciertos cálculos proposicionales que extienden el CPI con conectivos y sus correspondientes axiomas y reglas.

g-modelos

El Cálculo Proposicional Modal Simétrico definido por G. Moisil, brevemente CPMS, (ver [79, Ch. II, 2]) puede describirse abreviadamente por:

Lenguaje

Está dado por las variables $\mathrm{p}_1, \ldots, \mathrm{p}_n, \ldots$ y los conectivos $\neg$, $\rightarrow$, $\vee$, $\wedge$ del CPI más un conectivo $(\ )'$, sujetos a las reglas de construcción habituales.

Axiomas
Los del CPI más los dos siguientes:

$$(\mathrm{DM})\ \mathrm{A} \to \mathrm{A}'', \quad \mathrm{A}'' \to \mathrm{A}.$$

Reglas
Regla Modus Ponens más la de contraposición (CR):

$$(\mathrm{CR})\ \frac{\mathrm{A} \to \mathrm{B}}{\mathrm{B}' \to \mathrm{A}'}.$$

El álgebra de Lindenbaum de este cálculo es un *álgebra de Heyting simétrica* (ver [79]) también llamada *álgebra de De Morgan–Heyting*, esto es, un álgebra $\langle \mathbb{A}, \vee, \wedge, \to, (\ )', 0, 1\rangle$ donde $\langle \mathbb{A}, \vee, \wedge, \to, 0, 1\rangle$ es un álgebra de Heyting y $\langle \mathbb{A}, \vee, \wedge, (\ )', 0, 1\rangle$ es un álgebra de De Morgan (ver Capítulo 2, 2.2.7).

Se definen valuaciones del CPMS en álgebras de Heyting simétricas y se prueba el siguiente teorema de completud:

Teorema 5.6.17. *Una fórmula es un teorema en el CPMS si y solo si es válida en toda álgebra de Heyting simétrica.*

Definición 5.6.18. Un *g-modelo* es un par $(\mathcal{M}, g)$ donde $\mathcal{M} = ((P, \leq), K)$ es un modelo de Kripke y $g : P \longrightarrow P$ es un isomorfismo de orden de $(P, \leq)$ sobre $(P, \leq^o)$.

Para el nuevo conectivo, se define:

$$(\mathcal{M}, g) \Vdash_p \mathrm{A}' \text{ si y solo si } (\mathcal{M}, g) \nVdash_{g(p)} \mathrm{A}.$$

En un g-modelo, se prueba (ver [45]) que P^+ puede ser dotado de una estructura de álgebra de De Morgan, definiendo la negación N de la siguiente manera $N(X) = g(X^c)$, para $X \in P^+$. Luego, P^+ puede ser dotado de una estructura de álgebra de Heyting simétrica.

La validez con respecto a un g-modelo se define de manera análoga a la validez en modelos de Kripke.

Observemos que el operador N es el que consideramos en 5.6.

Puede demostrarse entonces la completud del CPMS con respecto a los g-modelos.

Teorema 5.6.19 ([45])**.** *Una fórmula del CPMS es válida en g-modelos si y solo si es válida en toda álgebra de Heyting simétrica.*

Como corolario de 5.6.17 y 5.6.19 se obtiene:

Teorema 5.6.20. *Una fórmula del CPMS es un teorema si y solo si es válida en g-modelos.*

3Ł-modelos

Las álgebras de Łukasiewicz trivalentes son, como se suele decir, la "contraparte algebraica" del Cálculo Proposicional trivalente de Łukasiewicz, abreviadamente CP3Ł, en el sentido de que dichas álgebras proveen la semántica con respecto a la cual este cálculo es completo. Trataremos brevemente CP3Ł en el Capítulo 9.

Definición 5.6.21 ([78]). Un *álgebra de Łukasiewicz trivalente* o 3Ł-álgebra es un sistema $\langle A, \vee, \wedge, (\,)', \nabla, 1\rangle$ tal que:

- $\langle A, \vee, \wedge, (\,)', 1, 1'\rangle$ es un álgebra de De Morgan,
- $x' \vee \nabla x = 1$,
- $x \wedge x' = x' \wedge \nabla x$,
- $\nabla(x \wedge y) = \nabla x \wedge \nabla y$.

Las álgebras de Łukasiewicz n-valentes (ver [12]), para n un número natural $n \geq 2$, fueron llamadas posteriormente *álgebras de Łukasiewicz–Moisil*, porque fue G. Moisil quien las definió, en 1940.

Sigamos analizando el caso $n = 3$. En estas álgebras, el operador ∇ y su dual, el operador Δ dado por $\Delta x = (\nabla x')'$ tienen las propiedades de un operador posibilidad y necesidad respectivamente, en el sentido que vimos en la última sección del Capítulo 3.

Se prueba el siguiente teorema de completud:

Teorema 5.6.22. *Una fórmula es un teorema en el CP3Ł si y solo si es válida en toda 3Ł-álgebra.*

Un álgebra de Łukasiewicz trivalente puede ser caracterizada como un sistema $\langle A, \vee, \wedge, \rightarrow, (\,)', \Delta, \nabla, 0, 1\rangle$ tal que

- $\langle A, \vee, \wedge, \rightarrow, (\,)', 0, 1\rangle$ es un álgebra de Heyting simétrica,
- $\Delta(x \vee y) = \Delta x \vee \Delta y$, $\nabla(x \vee y) = \nabla x \vee \nabla y$,
- $\Delta(\nabla x) = \nabla(\nabla x) = \nabla x$, $\nabla(\Delta x) = \Delta(\Delta x) = \Delta x$,
- $\Delta x' = (\nabla x)'$,
- $\Delta x \vee (\Delta x)' = 1$,
- $\Delta x \vee x = x$,
- $\Delta(x \rightarrow y) = (\Delta x \rightarrow \Delta y) \wedge (\nabla x \rightarrow \nabla y)$.

Esta caracterización (que se generaliza a las álgebras de Łukasiewicz n-valentes, ver [64]) nos permite definir el Cálculo Proposicional trivalente de Łukasiewicz extendiendo el CPI de modo análogo al que usamos para extender el CPMS: se agregan los conectivos $(\ )'$, Δ y ∇, los axiomas correspondientes y la regla de deducción llamada "de Gödel":

$$(\mathrm{G})\ \frac{\mathrm{A}}{\Delta\mathrm{A}}.$$

Definición 5.6.23. Un *3Ł-modelo* es un g-modelo $(\mathcal{M}, g)$ con $\mathcal{M} = (P, \leq)$ que cumple la siguiente propiedad:

- Para todo $p \in P$, $q \leq p$ o $q \geq p$ (q comparable con p) implica $q = p$ o $q = g(p)$.

Para los nuevos conectivos Δ y ∇ se define:

$$\begin{aligned}(\mathcal{M}, g) \Vdash_p \Delta\mathrm{A} \quad &\text{si y solo si} \quad (\mathcal{M}, g) \Vdash_p \mathrm{A} y (\mathcal{M}, g) \Vdash_{g(p)} \mathrm{A},\\ (\mathcal{M}, g) \Vdash_p \nabla\mathrm{A} \quad &\text{si y solo si} \quad (\mathcal{M}, g) \Vdash_p \mathrm{A} o (\mathcal{M}, g) \Vdash_{g(p)} \mathrm{A}.\end{aligned}$$

En un 3Ł-modelo se prueba que P^+ puede ser dotado de una estructura de 3Ł-álgebra, definiendo:

$$\begin{aligned}\Delta(X) &= X \cap g(X), \text{ como en 5.6}\\ \nabla(X) &= X \cup g(X).\end{aligned}$$

Se define validez en 3Ł-modelos de la manera usual.

Puede demostrarse entonces la completud del CP3Ł con respecto a los 3Ł-modelos:

Teorema 5.6.24 ([44])**.** *Una fórmula del CP3Ł es válida en 3Ł-modelos si y solo si es válida en toda 3Ł-álgebra.*

De donde, en base al teorema de completud del CP3Ł que veremos más adelante, se deduce el siguiente resultado.

Teorema 5.6.25. *Una fórmula del CP3Ł es un teorema si y solo si es válida en 3Ł-modelos.*

Una generalización de este resultado para $n = 4, 5$ puede verse en [46] y para un n cualquiera en [39].

5.7. Ejercicios

1. Probar que todo teorema de **LI** es teorema de $\mathbf{L}_4$. Encontrar contraejemplo de la recíproca.

2. ¿Cuáles de los ejercicios 6, 7, ..., 13 del Capítulo 3 pueden probarse para **LI**?

   En los siguientes ejercicios nos referiremos al sistema formal **LI**.

3. Sea Γ un conjunto de fórmulas de $\mathcal{L}$. Se dice que Γ es *inconsistente* si existe una fórmula A tal que $\mathrm{A} \in \Gamma^{\vdash}$ y también $\neg\mathrm{A} \in \Gamma^{\vdash}$ y se dice que es *trivial* o que *trivializa el sistema* si $\Gamma^{\vdash} = \mathcal{L}$. Probar que Γ es inconsistente si y solo si es trivial. ¿Vale lo mismo en $\mathbf{L}_4$?

4. Sea Γ un conjunto de fórmulas de $\mathcal{L}$. Probar que Γ es inconsistente si y solo si $|\Gamma|$, el conjunto de clases de equivalencia de las fórmulas de Γ, no tiene la pif (ver Ejercicio 4 del Capítulo 4).

5. ¿Es válido el análogo del Lema 3.3.2 del Capítulo 3 para el CPI? ¿Puede demostrarse de la misma manera que allí el TD?

6. Con referencia a las definiciones dadas en el Ejercicio 12 del Capítulo 3, demostrar que si una teoría Σ del CPI es completa, entonces es prima.

7. Probar que la aplicación canónica $\mathcal{L}_{CPI} \longrightarrow A_{CPI} = \mathcal{L}_{CPI}/\equiv$ es una A_{CPI}-valuación.

8. Probar que: si son v una A-valuación, $h : A \longrightarrow B$ un homomorfismo, entonces, $v' = h \circ v$ es una B-valuación (ver Ejercicio 14 del Capítulo 3).

9. Sea Γ un conjunto de fórmulas del CPI. Probar que existen modelos de Γ si y solo si existen modelos de Γ a valores en **2** (ver Sección 3 de este capítulo y Definición 3.6.1 en el Capítulo 3).

10. Con referencia al modelo $\mathcal{M}_1$ dado en la Sección 6, Ejemplo 5.6.4, probar que también es contramodelo de la fórmula $\mathrm{C} = \neg\neg\mathrm{A} \rightarrow \mathrm{A}$.

11. Probar el Teorema 5.6.11 y el Corolario 5.6.12.

Bibliografía del Capítulo 5

- Caicedo X., *Investigaciones acerca de los conectivos intuicionistas.* Rev. Acad. Colombiana Ciencias Exactas Físicas Naturales, 19 (1995), no. 75, 705–716.

- Caicedo X., *Conectivos intuicionistas sobre espacios topológicos.* Rev. Acad. Colombiana Ciencias Exactas Físicas Naturales, 21 (1997), no. 81, 521–534.

- Caicedo X. and Cignoli R., *An algebraic approach to intuitionistic connectives.* J. Symbolic Logic, 66 (2001), no. 4, 1620–1636.

- Fidel M., *Un cálculo modal correspondiente a las álgebras de Moisil de orden n.* Manuscrito inédito.

- Fitting M.C., *Intuitionistic Logic, Model Theory and Forcing.* North-Holland, 1969.

- Galli A. and Sagastume M., *Symmetric-intuitionistic connectives.* In: Models, Algebras and Proofs (Bogotá, 1995), 267–277, Lecture Notes in Pure and Appl. Math., 203, Dekker, New York, 1999.

- Galli A. and Sagastume M., *Kripke models for 3-valued Lukasiewicz algebras.* Notas de la Sociedad de Matemática de Chile, XV (1996), no. 1, 135–140.

- Galli A. and Sagastume M., *Some operators in Kripke models with an involution.* J. Applied Non-Classical Logics, 8 (1999), no. 1-2, 107–121.

- Iturrioz L., *Łukasiewicz and symmetrical Heyting algebras.* Z. Math. Logik Grundlagen Math., 23 (1977), 131–136.

- Monteiro A., *Sur les algébres de Heyting symétriques.* Port. Math., 39 (1980), 1–237.

- Monteiro A., *Álgebras de Łukasiewicz trivalentes.* Notas de Lógica Matemática, no. 21, 1–20, Universidad Nacional del Sur, 1964.

- Sagastume M., *Conectivos intuicionistas.* Rev. Educación Matemática (UMA), 24 (2009), no. 3, 3–21.

- Van Dalen D., *Intuitionistic Logic.* In: Handbook of Philosophical Logic, Synthese Library, vol. 166, 225–339, D. Reidel, 1986.

Capítulo 6

Dualidades en la teoría de retículos

Vamos a introducir algunas nociones básicas de teoría de categorías y de topología con el objeto de hacer autocontenido a este capítulo. Nuestra meta principal consiste en establecer, entre otras propiedades, una conexión entre los retículos distributivos acotados y ciertos espacios topológicos ordenados. Estudiaremos además los casos particulares de álgebras de Heyting y de álgebras de Boole.

6.1. Categorías

Los conceptos de categorías que utilizamos en este capítulo se reducen básicamente a las definiciones clásicas para definir el concepto de *categorías equivalentes* ([73]).

Una *categoría* $\mathcal{C}$ consiste de los siguientes datos:

1. Una colección de *objetos*.

2. Una colección de *morfismos*.

3. Para cada morfismo f, un objeto *dominio* de f y un objeto *codominio* de f. Usaremos la notación $f : A \to B$ para abreviar la información: f es un morfismo que tiene dominio A y codominio B.

4. Para cada objeto A un morfismo distinguido $id_A : A \to A$, al cual llamaremos la *identidad* (de A).

5. Para cualquier par de morfismos $f : A \to B$ y $g : B \to C$ un morfismo $g \circ f : A \to C$ que llamaremos la composición de g con f, sujeta a las siguientes restricciones:

a) si $f : A \to B$ entonces $id_B \circ f = f = f \circ id_A$,

b) si $f : A \to B$, $g : B \to C$ y $h : C \to D$ entonces $(h \circ g) \circ f = h \circ (g \circ f)$.

En una categoría $\mathcal{C}$, diremos que un morfismo $h : B \to C$ es un *monomorfismo* si para todo par $f, g : A \to B$, $h \circ f = h \circ g$ implica $f = g$. Diremos que h es un *epimorfismo* si para todo par $f, g : B \to C$, $f \circ h = g \circ h$ implica que $f = g$. Diremos que h es un *isomorfismo* si existe un morfismo $j : B \to A$ tal que $j \circ h = id_A$ y $h \circ j = id_B$.

Ejemplo 6.1.1. Si V es una clase de álgebras entonces definimos la categoría $\mathcal{C}_V$, en donde los objetos son las álgebras de V y los morfismos son homomorfismos entre álgebras de V. La noción de isomorfismo en $\mathcal{C}_V$ es equivalente a la definición de isomorfismo en V. Sea f un morfismo en $\mathcal{C}_V$: si f es una función inyectiva entonces f es un monomorfismo en $\mathcal{C}_V$ (la recíproca vale si V es una variedad). Si f es una función suryectiva entonces f es un epimorfismo en $\mathcal{C}_V$, aunque la recíproca podría no valer. Por ejemplo consideremos la categoría de anillos. Tenemos que la función $i : \mathbb{Z} \to \mathbb{Q}$ dada por $i(z) = z$ es un epimorfismo. Sin embargo i no es una función suryectiva.

Para más detalles ver la sección de Categorías en [2].

Para cualquier categoría $\mathcal{C}$, definimos $\mathcal{C}^{op}$ como la categoría cuyos objetos son los mismos de $\mathcal{C}$ pero invierte los morfismos de $\mathcal{C}$, es decir que, si es $f : A \to B$ en $\mathcal{C}$, entonces $f : B \to A$ en $\mathcal{C}^{op}$.

Dadas dos categorías $\mathcal{C}$ y $\mathcal{D}$, un *funtor* F de $\mathcal{C}$ en $\mathcal{D}$ (notación: $F : \mathcal{C} \to \mathcal{D}$) es una asignación que envía objetos de $\mathcal{C}$ en objetos de $\mathcal{D}$ y morfismos de $\mathcal{C}$ en morfismos de $\mathcal{D}$, y que satisface las siguientes condiciones:

1. Si $f : A \to B$ es un morfismo de $\mathcal{C}$ entonces $F(f) : F(A) \to F(B)$ es un morfismo de $\mathcal{D}$.

2. $F(id_A) = id_{F(A)}$, para cada objeto A de $\mathcal{C}$.

3. $F(f \circ g) = F(f) \circ F(g)$ para todo para par de morfismos en $\mathcal{C}$ tal que el dominio de f coincide con el codominio de g.

Los funtores suelen llamarse *funtores covariantes*. A un funtor $F : \mathcal{C}^{op} \to \mathcal{D}$ se lo llama *contravariante* de $\mathcal{C}$ en $\mathcal{D}$.

Dada una categoría $\mathcal{C}$ notaremos con $\mathbf{1}_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$ al funtor identidad, es decir al funtor tal que $\mathbf{1}_{\mathcal{C}}(A) = A$ para cada A objeto de $\mathcal{C}$ y $\mathbf{1}_{\mathcal{C}}(f) = f$ para cada morfismo f de $\mathcal{C}$.

Dados dos funtores $F, G : \mathcal{C} \to \mathcal{D}$, una *transformación natural* ξ de F en G (notación $\xi : F \to G$) es una asignación que a cada objeto A de $\mathcal{C}$ le asigna un morfismo $\xi_A : F(A) \to G(A)$ en $\mathcal{D}$, cumpliendo que, para cada morfismo

$f : A \to B$ en $\mathcal{C}$, $\xi_B \circ F(f) = G(f) \circ \xi_A$. Es decir que el siguiente diagrama conmuta:

$$\begin{tikzcd} F(A) \arrow[r, "\xi_A"] \arrow[d, "F(f)"'] & G(A) \arrow[d, "G(f)"] \\ F(B) \arrow[r, "\xi_B"'] & G(B) \end{tikzcd}$$

Si cada morfismo $\xi_A : F(A) \to G(A)$ es un isomorfismo entonces diremos que ξ es un *isomorfismo natural* entre F y G.

Dos categorías $\mathcal{C}$ y $\mathcal{D}$ son *equivalentes* si existen funtores $F : \mathcal{C} \to \mathcal{D}$, $G : \mathcal{D} \to \mathcal{C}$ y dos isomorfismos naturales $\xi : \mathbf{1}_{\mathcal{D}} \to F \circ G$ y $\sigma : \mathbf{1}_{\mathcal{C}} \to G \circ F$. Dos categorías $\mathcal{C}$ y $\mathcal{D}$ son *dualmente equivalentes* si y solo si $\mathcal{C}$ y $\mathcal{D}^{op}$ son equivalentes.

6.2. Dualidad de Birkhoff

En esta sección probaremos que la categoría de retículos distributivos finitos y la categoría de conjuntos ordenados finitos son dualmente equivalentes. En adelante, nos referiremos frecuentemente a los conjuntos ordenados (finitos o no) como *posets*.[1]

Sea FBDL la categoría que tiene como objetos retículos distributivos finitos y como morfismos los homomorfismos de retículos acotados. Llamaremos FPos a la categoría que tiene como objetos posets finitos y como morfismos funciones entre posets finitos tales que preservan el orden.

Sean L un retículo distributivo acotado y $\mathrm{X}(L)$ el conjunto de sus filtros primos. La prueba del siguiente lema se deja como ejercicio.

Lema 6.2.1. *Si $f : L \to M$ es un homomorfismo de retículos acotados y $P \in \mathrm{X}(M)$ entonces $f^{-1}(P) \in \mathrm{X}(L)$.*

Sean L un retículo distributivo finito y $\leq$ el orden subyacente a dicho retículo. Escribiremos $(L^{pr}, \leq^o)$ para indicar el poset en donde L^{pr} es el conjunto de elementos primos de L y $\leq^o$ es el orden dual de $\leq$ (ver notación usada en el Teorema 2.5.2 del Capítulo 2). Notemos que $(L^{pr}, \leq^o)$ es un poset finito.

Observación 6.2.2. Sea L un retículo distributivo finito y P un filtro de L. Recordemos que P es un filtro primo si y solo si $P = [p)$ para cierto $p \in L^{pr}$. En particular, la función $\alpha : L^{pr} \to X(L)$ dada por $\alpha(p) = [p)$ es una biyección.

[1]La palabra 'poset' viene del inglés *partially ordered set*.

Si L es un retículo distributivo finito definimos $F(L) = (L^{pr}, \leq^o)$.

En el siguiente lema utilizaremos la Observación 6.2.2.

Lema 6.2.3. *Sea $f : L \to M$ un morfismo en* FBDL. *Luego la función $F(f) : F(M) \to F(L)$ dada por $F(f)(q) = \bigwedge f^{-1}([q))$ es un morfismo en* FPos.

Demostración. Probaremos solo la buena definición de $F(f)$. Sea $q \in M^{pr}$. Como $[q) \in \mathrm{X}(M)$, por el Lema 6.2.1 tenemos que $f^{-1}([q)) \in \mathrm{X}(L)$. Luego existe $p \in L^{pr}$ tal que $[p) = f^{-1}([q))$. Por ende, $p = \bigwedge [p) = \bigwedge f^{-1}([q))$, con lo cual $\bigwedge f^{-1}([q)) \in L^{pr}$. El hecho de que $F(f)$ preserva el orden es consecuencia directa de la definición de $F(f)$. □

Tenemos que existe un funtor contravariente $F : \mathrm{FBDL} \to \mathrm{FPos}$.

Si $(X, \leq)$ es un poset finito entonces $G(X, \leq) = X^+$ es un retículo distributivo finito. Además, es sencillo probar que si $g : (X, \leq) \to (Y, \leq)$ es un morfismo en FPos entonces la función $G(g) : G(Y, \leq) \to G(X, \leq)$ dada por $G(g)(U) = g^{-1}(U)$ es un morfismo en FBDL. Luego tenemos un funtor contravariante $G : \mathrm{FPos} \to \mathrm{FBDL}$.

Por el Teorema 2.5.2 tenemos que si $L \in \mathrm{FBDL}$ entonces la función $\sigma_L : L \to G(F(L))$ dada por $\sigma_L(a) = \{p \in L^{pr} : p \leq a\}$ es un isomorfismo en FBDL. Por otro lado, en virtud del Teorema 2.5.5 tenemos que si $(X, \leq) \in \mathrm{FPos}$ entonces la función $\rho_X : (X, \leq) \to F(G(X, \leq))$ dada por $\rho_X(x) = [x)$ es un isomorfismo en FPos.

Sean $f : L \to M$ un morfismo en FBDL y $g : (X, \leq) \to (Y, \leq)$ un morfismo en FPos. Probaremos que los siguientes diagramas conmutan:

$$\begin{tikzcd} L \arrow[r, "\sigma_L"] \arrow[d, "f"'] & G(F(L)) \arrow[d, "G(F(f))"] \\ M \arrow[r, "\sigma_M"'] & G(F(M)) \end{tikzcd} \qquad \begin{tikzcd} (X, \leq) \arrow[r, "\rho_X"] \arrow[d, "g"'] & F(G(X, \leq)) \arrow[d, "F(G(g))"] \\ (Y, \leq) \arrow[r, "\rho_Y"'] & F(G(Y, \leq)) \end{tikzcd}$$

Primero veamos que para cada $a \in L$ vale la igualdad

$$(\sigma_M \circ f)(a) = (G(F(f)) \circ \sigma_L)(a).$$

En efecto, $p \in (\sigma_M \circ f)(a)$ si y solo si $p \leq f(a)$ si y solo si $f(a) \in [p)$ si y solo si $a \in f^{-1}([p))$. Pero la afirmación $a \in f^{-1}([p))$ es equivalente a que $\bigwedge f^{-1}([p)) \leq a$. Por otro lado, $p \in ((G \circ F)(f) \circ \sigma_L)(a)$ si y solo si $p \in F(f)^{-1}(\sigma_L(a))$, es decir, $F(f)(p) \in \sigma_L(a)$, lo cual es equivalente a que $\bigwedge f^{-1}([p)) \leq a$. Por lo tanto, $(\sigma_M \circ f)(a) = (G(F(f)) \circ \sigma_L)(a)$.

Finalmente veremos que $(\rho_Y \circ g)(x) = (F(G(g)) \circ \rho_X)(x)$. En efecto,

$$\begin{aligned}
(F(G(g)) \circ \rho_X)(x) &= \bigcap G(g)^{-1}([\rho_X(x)) \\
&= \bigcap \{V \in Y^+ : G(g)(V) \in [\rho_X(x))\} \\
&= \bigcap \{V \in Y^+ : [x) \subseteq f^{-1}(V)\} \\
&= \bigcap \{V \in Y^+ : f(x) \in V\} \\
&= [f(x)) \\
&= (\rho_Y \circ f)(x).
\end{aligned}$$

Los resultados anteriores nos permiten enunciar el siguiente teorema.

Teorema 6.2.4. *Los funtores F y G establecen una equivalencia dual entre las categorías* FBDL *y* FPos*.*

Este teorema es conocido con el nombre de *dualidad de Birkhoff.*

6.3. Topología

Las nociones de topología general que usaremos se restringen a las definiciones básicas, ver por ejemplo [83]. Más precisamente, las definiciones y propiedades utilizadas en este capítulo sobre espacios topológicos son las que necesitamos para estudiar la categoría de espacios de Priestley, que será introducida más adelante.

Recordemos primero algunas definiciones y propiedades que mencionamos en capítulos anteriores (ver 2.1.5, 2.5, 3.9, 4.1 y 4.5.9) ya que las mismas serán de fundamental importancia para este capítulo. Una *topología* sobre un conjunto X es una familia σ de subconjuntos de X cerrada bajo intersecciones finitas, uniones arbitrarias y tal que $\emptyset, X \in \sigma$. Un *espacio topológico* es un par (X, σ), donde X es un conjunto y σ una topología sobre X. A menudo omitiremos hacer mención específica de σ si no existe confusión. Los elementos $U \in \sigma$ son llamados *abiertos* del espacio topológico (X, σ). Un conjunto F se dirá *cerrado* si su complemento F^c es abierto. Un conjunto abierto y cerrado se llamará *clopen*. Si $x \in X$, diremos que U_x es un *entorno* de x si es un conjunto abierto que contiene al elemento x.

Si X es un conjunto, una *base* para una topología sobre X es una colección B de subconjuntos de X (llamados *elementos básicos*) tales que:

1. Para cada $x \in X$, hay al menos un elemento básico B que contiene a x.

2. Si x pertenece a la intersección de dos elementos básicos B_1 y B_2, entonces existe un elemento básico B_3 que contiene a x y tal que $B_3 \subseteq B_1 \cap B_2$.

Si B satisface estas dos condiciones, se define la topología σ generada por B como sigue: un subconjunto U de X se dice abierto en X, si para cada $x \in U$ existe un elemento básico B de B tal que $x \in B$ y $B \subseteq U$. Se puede probar que σ es igual a la colección de todas las uniones de elementos de B (Lema 13.1 de [83]).

Una *subbase* S para una topología sobre X es una colección de subconjuntos de X cuya unión es X. La *topología generada por la subbase* S se define como la colección σ de todas las uniones de intersecciones finitas de elementos de S (para probar que σ es una topología ver pág. 93 de [83]).

Dados dos espacios topológicos (X, σ) y (Y, υ), una función $f : X \to Y$ se dirá *continua* si $f^{-1}(U) \in \sigma$ para cada $U \in \upsilon$. Si f es una función biyectiva, continua y su función inversa también es continua, entonces diremos que f es un *homeomorfismo*.

Un espacio topológico X se dice *compacto* si para cada familia A de abiertos tal que $\bigcup_{U \in A} U = X$, existe una subfamilia finita $B \subseteq A$ tal que $\bigcup_{U \in B} U = X$. Un espacio topológico X es *Hausdorff* si para x, $y \in X$ distintos existen abiertos disjuntos U y V tales que $x \in U$ e $y \in V$.

Sea X un espacio topológico con topología σ. Si Y es un subconjunto de X, la colección $\sigma_Y = \{Y \cap U : U \in \sigma\}$ es una topología sobre Y, denominada *topología de subespacio*. En ese caso, (Y, σ_Y) se dice un *subespacio* de (X, σ). Si Y es un subespacio de X, una colección A se dice que cubre Y (o que es un cubrimiento de Y) si la unión de sus elementos contiene a Y.

Para una demostración del siguiente lema consultar el Capítulo 3 de [83]

Lema 6.3.1. *1. Sea Y un subespacio de un espacio topológico X. Entonces Y es compacto si y solo si cada cubrimiento de Y por abiertos de X contiene una subcolección finita que cubre Y.*

2. Cada subespacio cerrado de un espacio compacto es compacto.

3. Cada subespacio compacto de un espacio de Hausdorff es cerrado.

4. La imagen de un espacio compacto bajo una aplicación continua es un espacio compacto.

5. X es compacto si y solo si para cada colección C de conjuntos cerrados en X con la propiedad de intersección finita *(es decir, tal que cualquier intersección finita de conjuntos de C es no vacía), la intersección de todos los elementos de la colección de C es no vacía.*

6. *Sea $f : X \to Y$ una función continua y biyectiva. Si X es compacto e Y Hausdorff, entonces f es un homeomorfismo.*

6.4. Algunas consideraciones generales

En la década del '30, M. H. Stone demostró que existe una equivalencia entre la categoría de álgebras de Boole y una categoría de espacios topológicos cuyos objetos se denominan *espacios de Stone* [102]. Tiempo después, a comienzos de la década del '70, H. A. Priestley estableció una equivalencia entre la categoría de retículos distributivos acotados y cierta categoría de espacios topológicos ordenados, los cuales se denominan *espacios de Priestley* [88, 89]. Los objetos de esta categoría son espacios de Stone junto con un orden parcial que satisface una propiedad adicional. Algunos años después L. Esakia, basándose en la equivalencia categorial desarrollada por H. A. Priestley, estableció una equivalencia entre la categoría de álgebras de Heyting y una categoría de espacios topológicos ordenados, cuyos objetos son ciertos espacios de Priestley [38].

En lo que sigue de este capítulo vamos a probar las tres equivalencias categoriales antes mencionadas pero siguiendo un camino diferente al que históricamente fue utilizado para desarrollar las mismas. Vamos a comenzar estableciendo la equivalencia para la categoría de retículos distributivos acotados. Recordemos que toda álgebra de Heyting puede pensarse como un retículo distributivo acotado junto con una operación binaria adicional $\to$ que satisface la propiedad $a \wedge b \leq c$ si y solo si $a \leq b \to c$ para todo a, b, c. Por este motivo nuestro siguiente paso será estudiar la equivalencia para la categoría de álgebras de Heyting. Asimismo, toda álgebra de Boole puede pensarse como un caso particular de álgebra de Heyting. Esto nos va a llevar naturalmente a determinar la equivalencia para la categoría de álgebras de Boole. En este caso, en los espacios topológicos ordenados (asociados a las álgebras de Boole) el orden parcial $\leq$ es el orden dado por la igualdad, es decir, para cada x, y se tiene que $x \leq y$ si y solo si $x = y$.

6.5. Dualidad de Priestley

Un *espacio topológico totalmente disconexo en el orden* es una terna $(X, \leq, \sigma)$ tal que $(X, \leq)$ es un conjunto ordenado o poset, y dados $x, y \in X$ tal que $x \not\leq y$ existe un clopen creciente U tal que $x \in U$ e $y \notin U$. En tal caso diremos que $(X, \leq, \sigma)$ satisface el *axioma de separación de Priestley*. Un *espacio de Priestley* es un espacio topológico compacto que satisface el axioma de separación de Priestley. En lo que sigue escribiremos $(X, \leq)$ en lugar de $(X, \leq, \sigma)$. Sean $(X, \leq)$ e $(Y, \leq)$ posets y $f : (X, \leq) \to (Y, \leq)$ una función. Recordemos que f se llama *monótona* si para cada $x, y \in X$ tales que $x \leq y$ se tiene que $f(x) \leq f(y)$. Denotaremos como PS a la categoría que tiene como objetos espacios de Priestley y como morfismos funciones monótonas y continuas entre espacios de Priestley.

Es frecuente encontrar en la literatura que para la definición de espacio de Priesley se pide además que el espacio considerado sea Hausdorff y cero-dimensional (es decir, si $x \in X$ y U es un abierto tal que $x \in U$ entonces existe un conjunto clopen C tal que $x \in C \subseteq U$). Sin embargo estas condiciones no son necesarias pedirlas ya que se satisfacen en todo espacio de Priestley, como muestran los siguientes dos lemas.

Lema 6.5.1. *Todo espacio de Priestley es un espacio Hausdorff. Más aún, si $x, y \in X$ son tales que $x \neq y$ entonces existe un clopen U tal que $x \in U$ e $y \notin U$.*

Demostración. Sean x e y elementos distintos de un espacio de Priestley dado. Sin pérdida de generalidad, podemos asumir que $x \not\leq y$. Luego, por el axioma de separación de Priestley existe un clopen creciente U tal que $x \in U$ e $y \notin U$. □

Lema 6.5.2. *Todo espacio de Priestley $(X, \leq)$ es cero-dimensional.*

Demostración. Sean U un conjunto abierto y $x \in U$. Para cada $y \in U^c$ tenemos que $x \not\leq y$ ó $y \not\leq x$. Por el lema anterior existe un clopen creciente o decreciente V_y tal que $x \in V_y$ e $y \notin V_y$. Sea $V = \bigcap_{y \in U^c} V_y$. Veamos que $V \cap U^c = \emptyset$, o lo que es lo mismo, que $U^c \subseteq V^c$. Sea $z \in U^c$, con lo cual $z \notin V_z$, es decir, $z \in V^c$. De esta manera queda probado que $V \cap U^c = \emptyset$, es decir, $\bigcap_{y \in U^c}(U^c \cap V_y) = \emptyset$. Como X es un espacio compacto, utilizando la propiedad de intersección finita tenemos que existen $y_1, \ldots, y_n \in U^c$ tales que $U^c \cap V_{y_1} \cap \cdots \cap V_{y_n} = \emptyset$. Definiendo $C = V_{y_1} \cap \cdots \cap V_{y_n}$, tenemos que C es un clopen tal que $x \in C \subseteq U$. □

Denotamos como BDL a la categoría que tiene como objetos retículos distributivos acotados y como morfismos los homomorfismos de retículos acotados.

Sea L un retículo distributivo acotado. Para cada $a \in L$ definimos

$$\varphi(a) = \{P \in \mathrm{X}(L) : a \in P\}.$$

Es sencillo probar que para cada $a, b \in L$ tenemos que $\varphi(a \vee b) = \varphi(a) \cup \varphi(b)$, $\varphi(a \wedge b) = \varphi(a) \cap \varphi(b)$, $\varphi(0) = \emptyset$ y $\varphi(1) = \mathrm{X}$ (ver demostración del

Teorema 2.5.10 del Capítulo 2). Consideremos ahora

$$S = \{\varphi(a) : a \in L\} \cup \{\varphi(a)^c : a \in L\}.$$

Llamaremos σ a la topología sobre $\mathrm{X}(L)$ generada por la subbase S. De esta manera hemos construido un espacio topológico $(\mathrm{X}(L), \sigma)$.

Consideremos ahora la siguiente colección de elementos:

$$B = \{\varphi(a) \cap \varphi(b)^c : a, b \in L\}.$$

Notemos que B es una base (de conjuntos clopens) sobre el conjunto $\mathrm{X}(L)$. Para probarlo, sea $P \in \mathrm{X}(L)$. Como $1 \in P$ y $\varphi(1) = \varphi(1) \cap \varphi(0)^c$, tenemos que $P \in \varphi(1) \cap \varphi(0)^c$. Sean $P \in \mathrm{X}(L)$ y $a, b, c, d \in L$ tales que $P \in \varphi(a) \cap \varphi(b)^c$ y $P \in \varphi(c) \cap \varphi(d)^c$. Como $\varphi(a) \cap \varphi(c) \cap \varphi(b)^c \cap \varphi(d)^c = \varphi(a \wedge b) \cap \varphi(b \vee d)^c$ y $P \in \mathrm{X}(L)$, tenemos que $P \in \varphi(a \wedge b) \cap \varphi(b \vee d)^c$. De esta manera tenemos que B es una base sobre el conjunto $\mathrm{X}(L)$. Llamaremos τ a la topología sobre $\mathrm{X}(L)$ generada por la base B. Luego hemos construido un espacio topológico $(\mathrm{X}(L), \tau)$. Más aún, tenemos que $\sigma = \tau$. En lo que sigue, siempre que hablemos del espacio topológico $(\mathrm{X}(L), \sigma)$, vamos a escribir directamente $\mathrm{X}(L)$.

Observemos que $S \subseteq B$, pues para todo $a \in L$, $\varphi(a) = \varphi(a) \cap \varphi(0)^c$ y $\varphi(a)^c = \varphi(a)^c \cap \varphi(1)$. En particular, cada $\varphi(a)$ es clopen.

Lema 6.5.3. $\mathrm{X}(L)$ *es un espacio compacto.*

Demostración. Basta probar que si $\mathrm{X}(L) = \bigcup_{i \in I} \varphi(a_i) \cup \bigcup_{j \in J} \varphi(b_j)^c$ entonces existen números naturales n y m tales que $\mathrm{X}(L) = \bigcup_{i=1}^{n} \varphi(a_i) \cup \bigcup_{j=1}^{m} \varphi(b_j)^c$. Por esta razón, supongamos que $\mathrm{X}(L) = \bigcup_{i \in I} \varphi(a_i) \cup \bigcup_{j \in J} \varphi(b_j)^c$, es decir, $\bigcap_{j \in J} \varphi(b_j) \subseteq \bigcup_{i \in I} \varphi(a_i)$. Sea K el ideal generado por $\{a_i : i \in I\}$ y F el filtro generado por $\{b_j : j \in J\}$. Supongamos que $F \cap K = \emptyset$. Luego, por el teorema del filtro primo existe $P \in \mathrm{X}(L)$ tal que $F \subseteq P$ y $P \cap K = \emptyset$. En particular, $P \in \bigcap_{j \in J} \varphi(b_j) \subseteq \bigcup_{i \in I} \varphi(a_i)$, por lo cual existe $i \in I$ tal que $P \in \varphi(a_i)$. Pero entonces tenemos que $P \cap K \neq \emptyset$, lo cual es una contradicción. De esta manera queda probado que $F \cap K \neq \emptyset$. Luego, existe $x \in F \cap K$. Por ende (ver Lema 2.4.5 y Observación 2.4.6 del Capítulo 2) existen $a_1, \ldots, a_n, b_1, \ldots, b_m$ tales que $b_1 \wedge \cdots \wedge b_m \leq x \leq a_1 \vee \cdots \vee a_n$. Por esta razón, $\bigcap_{j=1}^{m} \varphi(b_j) \subseteq \bigcup_{i=1}^{n} \varphi(a_i)$. Por lo tanto, de esto se deduce que $\mathrm{X}(L) = \bigcup_{i=1}^{n} \varphi(a_i) \cup \bigcup_{j=1}^{m} \varphi(b_j)^c$. $\square$

En $\mathrm{X}(L)$ podemos definir la relación de orden dada por la inclusión, es decir, P es menor o igual que Q si y solo si $P \subseteq Q$. Es sencillo mostrar que $(\mathrm{X}(L), \subseteq)$ satisface el axioma de separación de Priestley. En efecto, sean $P, Q \in \mathrm{X}(L)$ tales que $P \subsetneq Q$. Luego, existe $a \in L$ tal que $a \in P$, $a \notin Q$. Luego: $P \in \varphi(a)$, $Q \notin \varphi(a)$. Por esta razón tenemos el siguiente resultado:

Teorema 6.5.4. $(\mathrm{X}(L), \subseteq)$ *es un espacio de Priestley.*

Sea $f : L \to M$ un morfismo en BDL. Vamos a definir la función $\mathrm{X}(f) : (\mathrm{X}(M), \subseteq) \to (\mathrm{X}(L), \subseteq)$ como $\mathrm{X}(f)(P) = f^{-1}(P)$. Por el Lema 6.2.1 tenemos que $\mathrm{X}(f)(P)$ está en $\mathrm{X}(L)$ y que $\mathrm{X}(f)$ es una función monótona. Además, para cada $a \in L$ tenemos que $\mathrm{X}(f)^{-1}(\varphi(a)) = \varphi(f(a))$. En efecto,

$$\begin{aligned} Q \in \mathrm{X}(f)^{-1}(\varphi(a)) &\text{ si y solo si } \mathrm{X}(f)(Q) \in \varphi(a) \\ &\text{ si y solo si } a \in \mathrm{X}(f)(Q) \\ &\text{ si y solo si } a \in f^{-1}(Q) \\ &\text{ si y solo si } f(a) \in Q \\ &\text{ si y solo si } Q \in \varphi(f(a)). \end{aligned}$$

La igualdad $\mathrm{X}(f)^{-1}(\varphi(a)) = \varphi(f(a))$ para cada $a \in L$ prueba la continuidad de $\mathrm{X}(f)$.

De esta manera obtenemos el siguiente resultado.

Teorema 6.5.5. *Si f es un morfismo en* BDL *entonces* $\mathrm{X}(f)$ *es un morfismo en* PS*.*

Por lo tanto podemos definir un funtor, al cual llamaremos X, que va de la categoría BDL hacia la categoría PS: si L es un objeto de BDL entonces $(\mathrm{X}(L), \subseteq)$ es un objeto de PS, y si f es un morfismo en BDL entonces $\mathrm{X}(f)$ es un morfismo en PS.

Teorema 6.5.6. *Existe un funtor contravariante* $\mathrm{X} : \mathrm{BDL} \to \mathrm{PS}$*.*

Sea $(X, \leq)$ un espacio de Priestley. Llamaremos $\mathrm{D}(X)$ al conjunto de clopens crecientes de X. Es inmediato que $\mathrm{D}(X)$ forma un retículo distributivo acotado si consideramos a la intersección como el ínfimo, a la unión como el supremo, a $\emptyset$ como primer elemento y a X como último elemento. Además, si $f : (X, \leq) \to (Y, \leq)$ es un morfismo en PS, la aplicación $\mathrm{D}(f) : \mathrm{D}(Y) \to \mathrm{D}(X)$ dada por $\mathrm{D}(f)(U) = f^{-1}(U)$ es un morfismo en BDL. Luego obtenemos el siguiente

Teorema 6.5.7. *Existe un funtor contravariante* $\mathrm{D} : \mathrm{PS} \to \mathrm{BDL}$*.*

En lo que sigue abusaremos de notación, y para cada $L \in \mathrm{BDL}$ llamaremos φ_L (o directamente φ, si no hay ambigüedad) a la función que va de L a $\mathrm{D}(\mathrm{X}(L))$ dada por $\varphi(a) = \{P \in \mathrm{X}(L) : a \in P\}$. Nuestro siguiente objetivo es ver que esta función es un isomorfismo en BDL. Para ello comenzaremos dando algunos resultados previos.

Lema 6.5.8. *Sean $a, b \in L$. Luego $a = b$ si y solo si $\varphi(a) = \varphi(b)$.*

Demostración. Sean $a, b \in L$ tales que $\varphi(a) = \varphi(b)$. Supongamos que $a \neq b$. Sin pérdida de generalidad podemos suponer que $a \nleq b$. Una de las consecuencias del Teorema del filtro primo nos asegura que existe $P \in \mathrm{X}(L)$ tal que $a \in P$ y $b \notin P$. Luego $\varphi(a) \neq \varphi(b)$, lo cual es una contradicción. En consecuencia, concluimos que $a = b$. □

Sabemos que para cada $a \in L$, $\varphi(a)$ es un clopen en $\mathrm{X}(L)$. Es fácil ver que también es creciente. El siguiente resultado nos muestra que todo clopen creciente de $\mathrm{X}(L)$ es de esta forma:

Lema 6.5.9. *Si U es un clopen creciente en $\mathrm{X}(L)$ entonces existe $a \in L$ tal que $U = \varphi(a)$.*

Demostración. Sea U un clopen creciente en $\mathrm{X}(L)$. Como U y U^c son conjuntos cerrados en un conjunto compacto, tenemos que U y U^c son compactos.

Para cada $P \in U$ y para cada $Q \in U^c$ tenemos que $P \nsubseteq Q$ porque U es un conjunto creciente. De esta manera tenemos que existe $a_{PQ} \in L$ tal que $a_{PQ} \in P$ y $a_{PQ} \notin Q$, es decir, $P \in \varphi(a_{PQ})$ y $Q \notin \varphi(a_{PQ})$. Fijemos $P \in U$, con lo cual $U^c \subseteq \bigcup_{Q_i \in U^c} \varphi(a_{PQ_i})^c$. Como U^c es compacto tenemos que existe un número natural n tal que $U^c \subseteq \bigcup_{i=1}^n \varphi(a_{PQ_i})^c$, es decir, $U^c \subseteq \varphi(a_{PQ_1} \wedge \cdots \wedge a_{PQ_n})^c$. Sea $a_P = a_{PQ_1} \wedge \cdots \wedge a_{PQ_n}$. Tenemos que $P \in \varphi(a_P) \subseteq U$. Luego $U = \bigcup_{P \in U} \varphi(a_P)$. La compacidad de U implica que existe un número natural m tal que $U = \varphi(a_{P_1}) \cup \cdots \cup \varphi(a_{P_m})$. Por lo tanto, si $a = a_{P_1} \vee \cdots \vee a_{P_m}$ entonces $U = \varphi(a)$. □

Teorema 6.5.10. *La función $\varphi : L \to \mathrm{D}(\mathrm{X}(L))$ es un isomorfismo en* BDL.

Demostración. Sabemos que φ es un morfismo en BDL. Por el Lema 6.5.8 tenemos que φ es una función inyectiva, y por el Lema 6.5.9 resulta que φ es una función suryectiva. Por lo tanto φ es un isomorfismo en BDL. □

Consideremos ahora un espacio de Priestley $(X, \leq)$. Definamos la función $\varepsilon_X : (X, \leq) \to (\mathrm{X}(\mathrm{D}(X)), \subseteq)$ como $\varepsilon_X(x) = \{U \in \mathrm{D}(X) : x \in U\}$. Si no hay ambigüedad, escribiremos ε en lugar de ε_X. Es sencillo mostrar que esta función está bien definida, es decir que $\varepsilon_X(x)$ es un filtro primo de $\mathrm{D}(X)$.

Lema 6.5.11. *Sea $(X, \leq)$ un espacio de Priestley. Si $x, y \in X$ entonces $x \leq y$ si y solo si $\varepsilon(x) \subseteq \varepsilon(y)$. Más aún, ε es un morfismo en* PS.

Demostración. Sean $x, y \in X$ tales que $x \leq y$. Sea $U \in \varepsilon(x)$, con lo cual $x \in U$. Como U es un conjunto creciente tenemos que $y \in U$, es decir, $U \in \varepsilon(y)$. Por esta razón $\varepsilon(x) \subseteq \varepsilon(y)$. Recíprocamente, supongamos que $\varepsilon(x) \subseteq \varepsilon(y)$ y que $x \nleq y$. Por esto existe $U \in \mathrm{D}(X)$ tal que $x \in U$ e $y \notin U$, con lo cual $U \in \varepsilon(x)$ y $U \notin \varepsilon(y)$ (una contradicción). Luego $x \leq y$.

Para ver que ε es una función continua, sea $U \in \mathrm{D}(X)$. Como $\varphi(U) = \{P \in \mathrm{X}(\mathrm{D}(X)) : U \in P\}$ y $\varphi(U)^c$ son elementos subbásicos de $\mathrm{X}(\mathrm{D}(X))$, para probar que ε es continua basta probar que $\varepsilon^{-1}(\varphi(U))$ es un clopen en X. Veamos que $\varepsilon^{-1}(\varphi(U)) = U$. En efecto:

$$\begin{aligned} \varepsilon^{-1}(\varphi(U)) &= \{x \in X : \ \varepsilon(x) \in \varphi(U)\} \\ &= \{x \in X : \ U \in \varepsilon(x)\} \\ &= \{x \in X : \ x \in U\} \\ &= U. \end{aligned}$$

Luego, $\varepsilon^{-1}(\varphi(U))$ es un clopen creciente en X. $\square$

Nuestro próximo objetivo es probar que ε es un isomorfismo en PS. Comenzaremos, como usualmente hacemos, con algunos resultados previos que nos conducirán a concretar nuestra meta.

Lema 6.5.12. *Sea $f : (X, \leq) \to (Y, \leq)$ un morfismo biyectivo de* PS*. Sea g la función inversa de f. Luego g es una función continua.*

Demostración. La prueba es consecuencia del último ítem del Lema 6.3.1. $\square$

Ahora estamos en condiciones de enunciar el siguiente

Teorema 6.5.13. *Sea $(X, \leq)$ un espacio de Priestley. Entonces, ε es un isomorfismo en* PS*.*

Demostración. Vamos a comenzar mostrando que ε es una función inyectiva. Sean $x, y \in X$ tales que $\varepsilon(x) = \varepsilon(y)$. Supongamos que $x \neq y$. Sin pérdida de generalidad podemos suponer que $x \not\leq y$. Luego, por el axioma de separación de Priestley tenemos que existe $U \in \mathrm{D}(X)$ tal que $x \in U$ e $y \notin U$. Pero este hecho implica que $\varepsilon(x) \neq \varepsilon(y)$, lo cual es una contradicción. Luego $x = y$ y así resulta que ε es una función inyectiva.

En lo que sigue probaremos que ε es una función suryectiva. Primero notemos que por el Lema 6.5.11 tenemos que ε es una función continua. Como X es un conjunto compacto se tiene que $\varepsilon(X)$ es un conjunto compacto, y por ende también es un conjunto cerrado. Ahora supongamos, para ver que ε es una función suryectiva, que $\varepsilon(X) \neq \mathrm{X}(\mathrm{D}(X))$. Luego existe $P \in \mathrm{X}(\mathrm{D}(X))$ tal que $P \notin \varepsilon(X)$. Como $\varepsilon(X)^c$ es abierto y $P \in \varepsilon(X)^c$ tenemos por el Lema 6.5.2 que existe un clopen V de $\mathrm{X}(\mathrm{D}(X))$ tal que $P \in V$ y $V \subseteq \varepsilon(X)^c$, con lo cual en particular tenemos que $V \cap \varepsilon(X) = \emptyset$, de donde $\varepsilon^{-1}(V) = \emptyset$. En particular, podemos suponer sin pérdida de generalidad que V es un elemento básico. Luego, existen $U, W \in \mathrm{D}(X)$ tales que $V = \varphi(U) \cap \varphi(W)^c$. Por esta razón llegamos a que $\emptyset = \varepsilon^{-1}(V) = \varepsilon^{-1}(\varphi(U)) \cap \varepsilon^{-1}(\varphi(W)^c) = U \cap W^c$. Esto a su vez implica que $U \subseteq W$, con lo cual $\varphi(U) \subseteq \varphi(W)$. Como $P \in \varphi(U)$ tenemos que $P \in \varphi(W)$, pero $P \in V$ y por esto $P \notin \varphi(W)$. Esto es una contradicción, con lo cual ε es una función suryectiva.

Teniendo en cuenta el Lema 6.5.11 y el Lema 6.5.12 concluimos que ε es un isomorfismo en PS. $\square$

Sean $f : L \to M$ un morfismo en BDL y $g : (X, \leq) \to (Y, \leq)$ un morfismo en PS. Es sencillo probar que los siguientes diagramas conmutan:

$$\begin{tikzcd} L \arrow[r, "\varphi_L"] \arrow[d, "f"'] & \mathrm{D}(\mathrm{X}(L)) \arrow[d, "\mathrm{D}(\mathrm{X}(f))"] \\ M \arrow[r, "\varphi_M"'] & \mathrm{D}(\mathrm{X}(M)) \end{tikzcd} \qquad \begin{tikzcd} X \arrow[r, "\varepsilon_X"] \arrow[d, "g"'] & \mathrm{X}(\mathrm{D}(X)) \arrow[d, "\mathrm{X}(\mathrm{D}(g))"] \\ Y \arrow[r, "\varepsilon_Y"'] & \mathrm{X}(\mathrm{D}(Y)) \end{tikzcd}$$

es decir, que para cada $a \in L$ y para cada $x \in X$ tenemos que $(\varphi_M \circ f)(a) = (\mathrm{D}(\mathrm{X}(f)) \circ \varphi_L)(a)$ y $(\varepsilon_Y \circ g)(x) = (\mathrm{X}(\mathrm{D}(g)) \circ \varepsilon_X)(x)$. Por lo tanto, teniendo en cuenta los resultados de esta sección tenemos el siguiente

Teorema 6.5.14. *Los funtores* X *y* D *establecen una equivalencia dual entre las categorías* BDL *y* PS*.*

Este teorema es conocido como *dualidad de Priestley.*

6.6. Dualidad de Esakia o de Heyting

Denotaremos como HA a la categoría cuyos objetos son álgebras de Heyting y cuyos morfismos son homomorfismos de álgebras de Heyting. Diremos que $(X, \leq)$ es un *espacio de Esakia* (o de Heyting) si es un espacio de Priestley tal que para cada $U \in \mathrm{D}(X)$, $(U]$ es clopen. Sea $f : (X, \leq) \to (Y, \leq)$ una función monótona. Esta función se dirá que es un *p-morfismo* si para cada para $x \in X$ y $z \in Y$ tales que $f(x) \leq z$, existe $y \in X$ tal que $x \leq y$ y $f(y) = z$. Denotaremos como HS la categoría que tiene como objetos espacios de Esakia y como morfismos funciones entre espacios de Esakia tales que son monótonas, continuas y p-morfismos.

Veremos que restringiendo la dualidad de Priestley se obtiene que los funtores X y D establecen una equivalencia dual entre las categorías HA y HS. El resultado previo es conocido con el nombre de *dualidad de Esakia* (o *dualidad de Heyting*). Comenzaremos con el siguiente

Lema 6.6.1. *Sean* $H \in \mathrm{HA}$ *y* $a, b \in H$*. Entonces,* $(\varphi(a) \cap \varphi(b)^c] = \varphi(a \to b)^c$*.*

Demostración. Sean $a, b \in H$. Como $a \wedge (a \to b) \leq b$ tenemos que $\varphi(a) \cap \varphi(a \to b) \subseteq \varphi(b)$, por lo cual $\varphi(a) \cap \varphi(b)^c \subseteq \varphi(a \to b)^c$. Usando que $\varphi(a \to b)^c$ es un conjunto decreciente llegamos a que $(\varphi(a) \cap \varphi(b)^c] \subseteq \varphi(a \to b)^c$. Para probar la otra inclusión consideremos $P \in \varphi(a \to b)^c$, con lo cual $a \to b \notin P$. Sea F el filtro generado por $P \cup \{a\}$. Supongamos que $a \to b \in F$, con lo cual existe $x \in P$ tal que $a \wedge x \leq a \to b$ y de este modo $a \wedge x \leq b$. Luego se tiene que $x \leq a \to b$, lo cual es una contradicción porque $x \in P$ y $a \to b \notin P$. Luego $a \to b \notin F$, con lo cual en virtud del Teorema del filtro primo tenemos que existe un filtro primo Q tal que $F \subseteq Q$ y $a \to b \notin Q$. En particular tenemos que $P \subseteq Q$, $a \in Q$ y $b \notin Q$ (si b estuviera en Q, como $b \leq a \to b$ tendríamos que $a \to b$ estaría en Q, lo cual es una contradicción). Luego $P \in (\varphi(a) \cap \varphi(b)^c]$. Por lo tanto $(\varphi(a) \cap \varphi(b)^c] = \varphi(a \to b)^c$. □

Lema 6.6.2. *Si* $H \in \mathrm{HA}$ *entonces* $(\mathrm{X}(H), \subseteq) \in \mathrm{HS}$.

Demostración. Sea U un clopen en $\mathrm{X}(H)$. Como $\mathrm{X}(H)$ es un conjunto compacto existen $a_1, b_1, \ldots, a_n, b_n \in H$ tales que $U = \bigcup_{i=1}^n \varphi(a_i) \cap \varphi(b_i)^c$. Por el Lema 6.6.1 tenemos que $(U] = \bigcup_{i=1}^n (\varphi(a_i) \cap \varphi(b_i)^c] = \bigcup_{i=1}^n \varphi(a_i \to b_i)^c$. Como la unión finita de conjuntos clopens es clopen, tenemos que $(U]$ es clopen. □

El siguiente resultado será de utilidad para el próximo lema.

Lema 6.6.3. *Dado un espacio de Priestley* $(X, \leq)$, *si* $x \in X$ *entonces la intersección de todos los clopens* U *que contienen a* x *es el conjunto unitario* $\{x\}$.

Demostración. Sea y un elemento que pertenece a todo clopen U que contiene a x. Queremos ver que $y = x$. Para ello supongamos que $y \neq x$. Usando que el espacio es Hausdorff (ver Lema 6.5.1) tenemos que existe $U \in \mathrm{D}(X)$ tal que $x \in U$ e $y \notin U$. Pero como $x \in U$, por hipótesis resulta que $y \in U$, lo cual es una contradicción. □

Lema 6.6.4. *Sea* $f : H \to G$ *un morfismo en* HA; *entonces* $\mathrm{X}(f)$ *es un morfismo en* HS.

Demostración. Escribiremos g para referirnos a $\mathrm{X}(f)$. Sean $P \in \mathrm{X}(H)$ y $Q \in \mathrm{X}(G)$ tales que $g(Q) \subseteq P$.

Sea C un conjunto clopen en $\mathrm{X}(H)$ tal que $P \in C$. Luego C es una unión finita de conjuntos de la forma $\varphi(a) \cap \varphi(b)^c$. Tenemos que

$$\begin{aligned} g^{-1}(((\varphi(a) \cap \varphi(b)^c)]) &= g^{-1}(\varphi(a \to b)^c) \\ &= (g^{-1}(\varphi(a \to b)))^c \\ &= (\varphi(f(a \to b)))^c \\ &= \varphi(f(a) \to f(b))^c \\ &= (\varphi(f(a)) \cap \varphi(f(b))^c] \\ &= (g^{-1}(\varphi(a)) \cap (g^{-1}(\varphi(b)))^c] \\ &= (g^{-1}(\varphi(a) \cap \varphi(b)^c)]. \end{aligned}$$

Luego $g^{-1}((C]) = (g^{-1}(C)]$. Como $g(Q) \subseteq P$, tenemos que $Q \in g^{-1}((C]) = (g^{-1}(C)]$. De este modo existe $Z \in \mathrm{X}(G)$ tal que $Z \in g^{-1}(C)$ y $Q \subseteq Z$. Luego $Z \in [Q) \cap g^{-1}(C)$. De este modo obtenemos que $[Q) \cap g^{-1}(C) \neq \emptyset$. Es decir:

$$\text{Si } C \text{ un conjunto clopen en } \mathrm{X}(H) \text{ tal que } P \in C \text{ entonces } [Q) \cap g^{-1}(C) \neq \emptyset. \tag{6.1}$$

Consideremos la siguiente familia de subconjuntos de $\mathrm{X}(G)$:

$$\Sigma = \{[Q) \cap g^{-1}(C) : C \text{ es clopen en } \mathrm{X}(H) \text{ y } P \in C\}.$$

Los elementos de Σ son conjuntos cerrados en $\mathrm{X}(G)$. En efecto, en todo espacio de Priestley $(X, \leq)$ se tiene que $[x)$ es un conjunto cerrado (ver los ejercicios al final de este capítulo). Luego los elementos de Σ resultan cerrados. Notemos además que toda intersección finita de elementos de Σ pertenece a Σ porque intersección finita de clopens es clopen. De este modo, por (6.1) toda intersección finita de elementos de Σ es no vacía. Luego la compacidad de $\mathrm{X}(G)$ implica que $\bigcap([Q) \cap g^{-1}(C)) \neq \emptyset$, donde la intersección es sobre todos los clopens C que contienen a P. Luego $[Q) \cap (\bigcap g^{-1}(C)) \neq \emptyset$. Pero por el Lema 6.6.3 tenemos que la intersección de todos los conjuntos $g^{-1}(C)$ para C clopen que contiene a P es igual a $g^{-1}(\{P\})$. Por ende, $[Q) \cap g^{-1}(\{P\}) \neq \emptyset$. Por lo tanto existe $W \in \mathrm{X}(G)$ tal que $Q \subseteq W$ y $g(W) = P$. Es decir, g es un p-morfismo. □

Los lemas previos prueban que existe un funtor contravariante $\mathrm{X} : \mathrm{HA} \to \mathrm{HS}$. En lo que sigue veremos que también podemos definir un funtor $\mathrm{D} : \mathrm{HS} \to \mathrm{HA}$.

Recordemos que si $(X, \leq)$ es un poset entonces X^+ es un álgebra de Heyting, en donde la implicación está dada por $U \Rightarrow V = (U \cap V^c]^c$.

Lema 6.6.5. *Si* $(X, \leq) \in \mathrm{HS}$ *entonces* $\mathrm{D}(X)$ *es un álgebra de Heyting.*

Demostración. Sean $U, V \in \mathrm{D}(X)$. Como estamos en un espacio de Esakia, tenemos que $(U \cap V^c]$ es un clopen decreciente, por lo cual $U \Rightarrow V \in \mathrm{D}(X)$. Es decir, $\mathrm{D}(X)$ es cerrado por la operación $\Rightarrow$. □

Lema 6.6.6. *Sea* $g : (X, \leq) \to (Y, \leq)$ *un morfismo en* HS. *Entonces* D(g) *es un morfismo en* HA.

Demostración. Solo necesitamos probar que D(g) preserva la implicación. Sean $U, V \in \mathrm{D}(Y)$. Como $U \cap (U \Rightarrow V) \subseteq V$ tenemos que $g^{-1}(U) \cap g^{-1}(U \Rightarrow V) \subseteq g^{-1}(V)$, es decir, $g^{-1}(U \Rightarrow V) \subseteq g^{-1}(U) \Rightarrow g^{-1}(V)$. Para probar la otra inclusión, sea $x \notin g^{-1}(U \Rightarrow V)$, con lo cual $g(x) \in (U \cap V^c]$. Luego existe $y \in U \cap V^c$ tal que $g(x) \leq y$. Como g es un p-morfismo existe z tal que $x \leq z$ y $g(z) = y$. Luego $z \in g^{-1}(U \cap V^c) = g^{-1}(U) \cap g^{-1}(V^c)$. Por esta razón $x \in (g^{-1}(U) \cap g^{-1}(V^c)]$. Es decir, $x \notin g^{-1}(U) \Rightarrow g^{-1}(V)$. □

Los dos lemas previos nos aseguran que existe un funtor contravariante D : HS → HA.

El Lema 6.6.1 nos dice que si $H \in$ HA entonces para cada $a, b \in H$ vale que $\varphi(a \to b) = \varphi(a) \Rightarrow \varphi(b)$. Luego, si $H \in$ HA entonces $\varphi : H \to \mathrm{D}(\mathrm{X}(H))$ es un isomorfismo en HA. Si $(X, \leq) \in$ HS, sabemos que ε es un isomorfismo en la categoría de espacios de Priestley. En particular, ε es una función biyectiva que preserva el orden y tal que su función inversa también preserva el orden: esto implica que ε y ε^{-1} son p-morfismos. Luego, si $(X, \leq) \in$ HS entonces $\varepsilon : X \to \mathrm{X}(\mathrm{D}(X))$ es un isomorfismo en HS.

Teniendo en cuenta los resultados de esta sección y la dualidad de Priestley, estamos en condiciones de enunciar el siguiente

Teorema 6.6.7. *Los funtores* X *y* D *establecen una equivalencia dual entre las categorías* HA *y* HS.

Este teorema es conocido como *dualidad de Esakia* o *dualidad de Heyting*.

6.7. Dualidad de Stone

En esta sección vamos a presentar una equivalencia categorial dual entre la categoría de álgebras de Boole, a la que denotaremos como $\mathbb{A}$, y cierta categoría de espacios topológicos. Sabemos que en todo retículo distributivo acotado los filtros maximales son primos, pero que en general la recíproca de esta propiedad no es cierta. Sin embargo, si un retículo distributivo acotado es un álgebra de Boole, entonces tenemos que un filtro es primo si y solo si es maximal.

Lema 6.7.1. *Sean* $B \in \mathbb{A}$. *En el espacio de Esakia* $(\mathrm{X}(B), \subseteq)$ *vale que si* $P, Q \in \mathrm{X}(B)$ *entonces* $P \subseteq Q$ *si y solo si* $P = Q$.

Consideremos ahora un espacio de Esakia $(X, \leq)$, en donde la relación de orden $\leq$ coincide con la relación de igualdad, es decir, $x \leq y$ si y solo si $x = y$. Sea $U \in \mathrm{D}(X)$, que en nuestro caso es equivalente a decir que U es sencillamente un conjunto clopen. Sabemos que $\mathrm{D}(X)$ es un álgebra de Heyting. Más aún, es inmediato probar que $U \Rightarrow \emptyset = U^c$, por lo cual $U \cup (U \Rightarrow \emptyset) = X$. De este modo $\mathrm{D}(X)$ es más que un algebra de Heyting: $\mathrm{D}(X)$ es un álgebra de Boole.

Lema 6.7.2. *Sea $(X, \leq)$ un espacio de Esakia que satisface la propiedad $x \leq y$ si y solo si $x = y$. Entonces $\mathrm{D}(X)$ es un álgebra de Boole.*

Si $(X, \leq)$ e $(Y, \leq)$ espacios de Esakia que satisfacen la hipótesis del Lema 6.7.2 y $g : (X, \leq) \to (Y, \leq)$ es una función, entonces g es un morfismo en HS si y solo si g es continua. Utilizando el Teorema 6.6.7 concluimos que existe una equivalencia categorial dual entre la categoría de álgebras de Boole y la categoría cuyos objetos son espacios de Esakia $(X, \leq)$ que satisfacen la condición $x \leq y$ si y solo si $x = y$, y cuyos morfismos son funciones continuas.

Un *espacio de Stone* es un espacio topológico compacto, Hausdorff y cero-dimensional. Esta definición está íntimamente ligada con las ideas que venimos presentando, ya que todo espacio de Priestley $(X, \leq)$ satisface que X es un espacio de Stone como consecuencia del Lema 6.5.1 y del Lema 6.5.2. Más aún, tenemos el siguiente resultado.

Teorema 6.7.3. *X es un espacio de Stone si y solo si $(X, =)$ es un espacio de Esakia (siendo $=$ la relación de igualdad).*

Demostración. Supongamos que X es un espacio de Stone. Para probar que $(X, =)$ es un espacio de Esakia basta probar que satisface el axioma de separación de Priestley. Sean $x, y \in X$ tales que $x \neq y$. Como X es un espacio Hausdorff existen conjuntos abiertos disjuntos U y V tales que $x \in U$ e $y \in V$. Como X es además un espacio cero-dimensional, tenemos que existe un clopen C tal que $x \in C \subseteq U$. En particular, $y \notin C$. Luego $(X, =)$ satisface el axioma de separación de Priestley. Por lo tanto $(X, =)$ es un espacio de Esakia.

La prueba de la recíproca es inmediata. □

Sea St la categoría cuyos objetos son espacios de Stone y cuyos morfismos son funciones continuas. Si B es un álgebra de Boole entonces $\mathrm{X}(B)$ es un espacio de Stone, y si f es un morfismo de álgebras de Boole entonces $\mathrm{X}(f)$ es una función continua. Recíprocamente, si X es un espacio de Stone entonces $\mathrm{D}(X)$ es un álgebra de Boole, y si g es una función continua entre espacios de Stone entonces $\mathrm{D}(g)$ es un morfismo de álgebras de Boole. Ahora podemos enunciar un resultado conocido en la literatura como *dualidad de Stone*:

Teorema 6.7.4. *Existe una equivalencia categorial dual entre* $\mathbb{A}$ *y* St.

6.8. Algunas conexiones entre las categorías

En esta última parte del capítulo nos basaremos principalmente en [2, 35]. Consideremos un retículo distributivo acotado L (o un morfismo f en BDL). A veces es posible encontrar una relación entre cierta información que nos proporciona L (o el morfismo f) con respecto a cierta información que nos proporciona el espacio topológico $\mathrm{X}(L)$ (o el morfismo $\mathrm{X}(f)$). La misma situación puede ser planteada para el caso de las categorías HS y St. Por ejemplo, existe una biyección entre las congruencias de L y los subconjuntos cerrados de $\mathrm{X}(L)$. También muchas propiedades de L pueden ser traducidas en propiedades de $\mathrm{X}(L)$. Es decir, frecuentemente es posible probar que una cierta propiedad P vale en L si y solo si otra cierta propiedad $\hat{P}$ vale en $\mathrm{X}(L)$. Supongamos que no sabemos si la propiedad P es cierta porque no logramos encontrar una demostración o una refutación de la misma. Sin embargo puede suceder que resulte posible demostrar la propiedad $\hat{P}$ o hallar una refutación de la misma en PS, con lo cual estaríamos resolviendo nuestro problema original.

En resumen: a veces es más sencillo trabajar con espacios de Priestley que con retículos distributivos acotados. Más aún, si estamos considerando la categoría de retículos distributivos finitos entonces los mismos se corresponden con la categoría de posets finitos y funciones monótonas entre posets finitos (en el caso finito los espacios de Priestley poseen la topología discreta, esto requiere una prueba que se deja como ejercicio para el lector). En este caso particular ni siquiera debemos preocuparnos por la topología, solo nos interesan propiedades de los posets finitos. Estas ideas pueden ser extrapoladas para cualesquiera dos categorías que sean equivalentes.

En lo que sigue listaremos con un poco más de detalle algunos ejemplos para ilustrar los fenómenos antes expuestos.

1. Sea L un retículo distributivo acotado. Existe un isomorfismo de retículos entre las congruencias de L y los subconjuntos cerrados de $\mathrm{X}(L)$. Si Y es un conjunto cerrado de $\mathrm{X}(L)$ entonces definimos

$$\Theta(Y) := \{(a,b) \in L \times L : \varphi(a) \cap Y = \varphi(b) \cap Y\}.$$

La aplicación Θ es un isomorfismo de retículos entre el retículo de cerrados de $\mathrm{X}(L)$ y el retículo de congruencias de L.

2. Sea $f : L \to M$ un morfismo en BDL. Entonces f es inyectiva si y solo si f es un monomorfismo si y solo si $\mathrm{X}(f)$ es un epimorfismo si y solo si $\mathrm{X}(f)$ es suryectiva. Además f es un epimorfismo si y solo si $\mathrm{X}(f)$ es inyectiva si y solo si $\mathrm{X}(f)$ es un monomorfismo. Finalmente f es suryectiva si y solo si $\mathrm{X}(f)$ (con el codominio restringido a $\mathrm{X}(L)$) es un homeomorfismo.

3. Un espacio topológico X es *extremadamente disconexo* si y solo si la clausura de todo conjunto abierto es abierto. Un álgebra de Boole B es completa si y solo si el espacio de Stone $\mathrm{X}(B)$ es extremadamente disconexo.

4. Sea K una clase de álgebras del mismo tipo. Se define $V(K)$ como la menor variedad que contiene a K. Las *álgebras de Heyting prelineales* fueron consideradas por Horn en [62] como un paso intermedio entre la lógica clásica y la intuicionista, y fueron estudiadas también por Monteiro [79], G. Martínez [74] y otros. Esta es la subvariedad de álgebras de Heyting generada por la clase de todas las cadenas, y puede ser axiomatizada con un conjunto de ecuaciones que caractericen a las álgebras de Heyting más la ecuación de prelinealidad $(x \to y) \vee (y \to x) = 1$. En [2, Ch. IX] y en [79] se dan caracterizaciones para las álgebras de Heyting prelineales. Un poset $(X, \leq)$ se llama *root system* si para cada $x \in X$ el conjunto $[x)$ forma una cadena. Tenemos la siguiente propiedad para un álgebra de Heyting H, cuya demostración detallaremos a continuación:

$$H \text{ es prelineal si y solo si } (\mathrm{X}(H), \subseteq) \text{ es un root system.}$$

Para probar esta propiedad, supongamos primero que H es prelineal. Sean $P, Q, Z \in \mathrm{X}(H)$ tales que $P \subseteq Q$ y $P \subseteq Z$. Debemos probar que $Q \subseteq Z$ o bien que $Z \subseteq Q$. Supongamos que esto no ocurre, con lo cual existen $x, y \in H$ tales que $x \in Q, y \in Z$, $y \notin Q$ y $x \notin Z$. Como $(x \to y) \vee (y \to x) = 1$ y $1 \in P$, sin pérdida de generalidad podemos suponer que $x \to y \in P$. En particular $x \to y \in Q$. Pero $x \in Q$ y $x \wedge (x \to y) \leq y$, con lo cual $y \in Q$. Esto resulta una contradicción. Luego $(\mathrm{X}(H), \subseteq)$ es un root system. Recíprocamente, supongamos que $(\mathrm{X}(H), \subseteq)$ es un root system y supongamos que existen $x, y \in H$ tales que $(x \to y) \vee (y \to x) \neq 1$. Luego por el TFP existe $P \in \mathrm{X}(H)$ tal que $(x \to y) \vee (y \to x) \notin P$. Consideremos los filtros $F = \langle P \cup \{x\} \rangle$ y $G = \langle P \cup \{y\} \rangle$. Supongamos que $y \in F$. Luego existe $p \in P$ tal que $y \geq p \wedge x$, es decir, $p \leq x \to y$. De esto se deduce que $x \to y \in P$, lo que es una contradicción. Luego tenemos que $y \notin F$. Del mismo modo se prueba que $x \notin G$. Luego existen $Q, Z \in \mathrm{X}(H)$ tales que $F \subseteq Q$, $G \subseteq Z$, $y \notin Q$ y $x \notin Z$. Ahora usaremos que $(\mathrm{X}(H), \subseteq)$ es un root system. Como $P \subseteq Q$ y $P \subseteq Z$, sin pérdida de generalidad podemos asumir que $Q \subseteq Z$. Como $x \in Q$ tenemos que $x \in Z$, lo cual es una contradicción. Por lo tanto H es prelineal.

¿Qué consecuencias tiene este último ejemplo? Supongamos que queremos saber si un álgebra de Heyting H es o no prelineal. Basta considerar el poset $(\mathrm{X}(H), \subseteq)$ y analizar si el mismo resulta o no un root system.

Sean $(X, \leq)$ e $(Y, \leq)$ posets, siendo el primero un root system. Si ambos posets son isomorfos entonces $(Y, \leq)$ es un root system. En consecuencia tenemos el siguiente corolario: si $(X, \leq)$ es un espacio de Esakia que resulta ser un root system entonces $\mathrm{D}(X)$ es un álgebra de Heyting prelineal. En efecto, sabemos que $X \cong \mathrm{X}(\mathrm{D}(X))$. Como X es un root system resulta que $\mathrm{X}(\mathrm{D}(X))$ es un root system, lo cual es equivalente a afirmar que $\mathrm{D}(X)$ es prelineal (notar que aquí hemos usado la dualidad de Esakia). ¿Qué nos aporta este resultado? Nos aporta, entre otras cosas, un mecanismo para construir álgebras de Heyting prelineales finitas: basta considerar el conjunto de crecientes de un root system finito dado.

Cabe destacar que una de las ventajas de trabajar con posets (o más generalmente, con ciertos espacios topológicos ordenados) radica en que muchas veces podemos intuir propiedades basándonos en la naturaleza geométrica (y topológica, si corresponde) del espacio considerado. Aunque intuir propiedades no significa haberlas demostrado. Pero sí nos ayuda a conocer el tipo de estructuras consideradas y los posibles problemas que podríamos abordar.

6.9. Ejercicios

1. Probar que si L es un retículo distributivo acotado entonces L es una cadena si y solo si $\mathrm{X}(L)$ es una cadena.

2. Sea $(X, \leq)$ un espacio topológico ordenado que satisface el axioma de separación de Priestley. Probar que para cada $x \in X$ se tiene que $\{x\}$, $[x)$ y $(x]$ son conjuntos cerrados.

3. Sea $(X, \leq, \sigma)$ un espacio de Priestley. Probar las siguientes afirmaciones:

   a) Sea A un conjunto abierto creciente. Luego existe una familia de clopens crecientes $\{A_i\}_{i \in I}$ tales que $A = \bigcup_{i \in I} A_i$.

   b) Si A es un abierto creciente y $x \in A$ entonces existe un clopen creciente B tal que $x \in B \subseteq A$.

   c) Si U es un cerrado decreciente y $x \notin U$ entonces existe un clopen decreciente V tal que $U \subseteq V$ y $x \notin V$.

   d) Si U es un cerrado creciente y $x \notin U$ entonces existe un clopen creciente V tal que $U \subseteq V$ y $x \notin V$.

   Sugerencia:

   Para probar a) bastaría probar primero la siguiente propiedad: Sea $x \in A$. Luego existe un clopen creciente V tal que $x \in V$ y $V \cap A^c = \emptyset$.

   Probemos la propiedad mencionada en el párrafo anterior. Sea $x \in A$. Supongamos que para todo clopen creciente V vale que si $x \in V$ entonces $V \cap A^c \neq \emptyset$. Definamos $\mathrm{F} = \{V \cap A^c : V \in \mathrm{D}(X) \text{ y } x \in V\}$. La familia F es una colección de conjuntos cerrados que tiene la propiedad de intersección finita (probarlo). Como (X, σ) es un espacio compacto deducimos que
   $$\bigcap_{V \in \mathrm{F}} (V \cap A^c) \neq \emptyset.$$
   Luego existe $y \in \bigcap_{V \in \mathrm{F}} (V \cap A^c)$. De este modo, $y \in A^c$ e $y \in V$ para todo V clopen creciente tal que $x \in V$. En particular, $x \leq y$ (probarlo). Como $x \in A$ y A es creciente se concluye que $y \in A$, lo cual es una contradicción.

   Finalmente notar que $a) \Rightarrow b) \Rightarrow c) \Rightarrow d)$.

4. Sea L un retículo distributivo acotado. Probar las siguientes afirmaciones:

a) Si F es un filtro de L entonces $\bigcap_{a\in F}\varphi(a)$ es un cerrado creciente de $\mathrm{X}(L)$.

b) Si U es un cerrado creciente de $\mathrm{X}(L)$ entonces $\{a \in L : U \subseteq \varphi(a)\}$ es un filtro de L.

c) Sea $\mathrm{Fil}(L)$ el conjunto de filtros de L y sea $\mathrm{Cu}(\mathrm{X}(L))$ el conjunto de cerrados crecientes de $\mathrm{X}(L)$. Probar que la función $h : \mathrm{Fil}(L) \to \mathrm{Cu}(\mathrm{X}(L))$ dada por $h(F) = \bigcap_{a\in F}\varphi(a)$ es una biyección.

Sugerencia: para ver la suryectividad de h usar el ítem d) del Ejercicio 3.

5. Sea B un álgebra de Boole B. Probar las siguientes afirmaciones:

   a) Para cada átomo a vale que $\varphi(a)$ es un conjunto unitario, cuyo único elemento será denotado como P_a. Más aún, probar que $\{P_a\}$ es un clopen en $\mathrm{X}(B)$.

   b) Sea $P \in \mathrm{X}(B)$. Probar que $\{P\}$ es un clopen en $\mathrm{X}(B)$ si y solo si $\{P\}$ es un punto aislado en $\mathrm{X}(B)$. ¿Sigue valiendo esta propiedad para $\mathrm{X}(L)$ con L un retículo distributivo acotado?

   c) La aplicación que a cada átomo a de B le hace corresponder el filtro primo P_a es una biyección entre los átomos de B y los puntos aislados de $\mathrm{X}(B)$.

6. Si $f : (X, \leq) \to (Y, \leq)$ una función monótona entonces se dice que f es un p-morfismo si para cada $x \in X$ e $y \in Y$ tales que $f(x) \leq y$ se tiene que existe $z \in X$ tal que $x \leq z$ y $f(z) = y$.

   Sea $f : (X, \leq) \to (Y, \leq)$ una función monótona. Probar que las siguientes afirmaciones son equivalentes:

   a) f es un p-morfismo.

   b) $f^{-1}((Z]) = (f^{-1}(Z)]$ para cada $Z \subseteq Y$.

   c) $f^{-1}((y]) = (f^{-1}(\{y\})]$ para cada $y \in Y$.

7. Sea Y un subconjunto cerrado de un espacio de Priestley. Probar que $[Y)$ y $(Y]$ son conjuntos cerrados. Concluir que $(X, \leq)$ es un espacio de Heyting si y solo si $(U]$ es un conjunto abierto para cada abierto U.

Bibliografía del Capítulo 6

- Balbes R. and Dwinger, P., *Distributive Lattices*. University of Missouri Press, 1974.
- Davey B.A. and Priestley H.A., *Introduction to Lattices and Order*. Cambridge University Press, 1990.
- Esakia L., *Topological Kripke models*. Soviet. Math. Dokl., 15 (1974), 147–151.
- Horn A., *Logic with truth values in a linearly ordered Heyting algebra*. J. Symbolic Logic, 34 (1969), 395–408.
- MacLane S., *Categories for the Working Mathematician*. Graduate Texts in Math., Springer-Verlag, 1971.
- Martínez G. and Priestley H., *On Priestley spaces of lattice-ordered algebraic structures*. Order, 15 (1998), 297–323.
- Monteiro A., *Sur les algébres de Heyting symétriques*. Port. Math., 39 (1980), 1–237.
- Munkres J.R., *Topología*, segunda edición. Prentice Hall, 2002.
- Priestley H.A., *Representation of distributive lattices by means of ordered Stone spaces*. Bull. London Math. Soc. 2 (1970), 186–190.
- Priestley H.A., *Ordered topological spaces and the representation of distributive lattices*. Proc. London Math. Soc. 3 (1972), no. 24, 507–530.
- Stone M.H., *The theory of representations for Boolean algebras*. Trans. Amer. Math. Soc., 40 (1936), no. 1, 37–111.

Capítulo 7

Más sobre álgebra universal

Expondremos en este capítulo algunos resultados del Álgebra Universal, especialmente los teoremas de Birkhoff, que serán necesarios para desarrollar algunos temas en capítulos posteriores.

Basándonos en lo mostrado en el Capítulo 1, Sección 3, avanzaremos en el estudio de las clases de álgebras, en particular de las variedades (ver Definición 1.3.15). Para eso es importante poder obtener información de una clase de álgebras a partir de algunos miembros distinguidos más simples. Sin embargo, esto no siempre es posible. Los candidatos a representar una clase son, generalmente, las álgebras *subdirectamente irreducibles* y también las álgebras libres. ¿Por qué son estos dos casos importantes? Porque las *ecuaciones* (ver Sección 4) que se cumplen en las álgebras subdirectamente irreducibles de una variedad se cumplen en todas las álgebras de la variedad. Lo mismo podemos decir de las álgebras libres, que además, existen en toda variedad, aunque son generalmente complicadas de describir. Hablaremos de las ecuaciones en la Sección 4.

7.1. Productos subdirectos

Vamos a definir ahora los conceptos de producto subdirecto y de álgebra subdirectamente irreducible. Las álgebras subdirectamente irreducibles son aquellas que no se pueden descomponer como productos subdirectos, son como los átomos de una clase de álgebras. Según uno de los teoremas de Birkhoff, en las variedades toda álgebra es producto subdirecto de álgebras subdirectamente irreducibles que pertenecen a la variedad. Como veremos, en algunas clases de álgebras esto es muy útil porque las subdirectamente irreducibles son álgebras fáciles de describir y en cierto modo en ellas está toda la información de la clase de álgebras considerada. Por ejemplo, tanto en los retículos distributivos como en las álgebras de Boole la única álgebra subdirectamente irreducible es **2**.

Daremos asimismo una caracterización de álgebra subdirectamente irreducible en función de sus congruencias, que en la práctica, es más aplicable que la definición.

Hemos estudiado en los Capítulos 2 y 4 las congruencias de álgebras de Boole y de álgebras de Heyting. Eso nos dio una base intuitva para demostrar en general las propiedades de las congruencias de un álgebra.

Como hemos observado en el Capítulo 1 (ver 1.3.3) a menudo denotaremos un álgebra solo por su conjunto subyacente, por abuso de notación.

Observación 7.1.1. Las siguientes propiedades se desprenden de la definición de congruencia en un álgebra.

(1) En toda álgebra $\langle A, F\rangle$ no trivial, es decir, donde A tiene más de un elemento, hay al menos dos congruencias, que llamaremos Δ y ∇. La primera es la relación de identidad, es decir que: $a\Delta b$ si y solo si $a = b$. La segunda es la que identifica todos los elementos de A, o sea que para todo par a, b de elementos de A, $a\nabla b$.

En las álgebras de Boole y de Heyting, son las que corresponden respectivamente a los filtros $\{1\}$ y A.

(2) Sea $\langle A, F\rangle$ un álgebra, $\{R_i\}_{i\in I}$ una familia de congruencias de A. Entonces la relación $R = \bigcap R_i$ es una congruencia en A, donde aRb equivale a que aR_ib para todo $i \in I$. En particular, si xRy implica $x = y$, eso significa que $R = \Delta$.

(3) Sea $\{g_i\}_{i\in I}$ una familia de homomorfismos con el mismo dominio A. Para cada $i \in I$ consideremos la congruencia R_i asociadada a g_i, es decir, la congruencia definida por: aR_ib si y solo si $g_i(a) = g_i(b)$. Entonces, las siguientes condiciones (I) y (II) son equivalentes:

(I) Para cada $a, b \in A$, si $a \neq b$ entonces existe $i \in I$ tal que $g_i(a) \neq g_i(b)$.

(II) $\bigcap R_i = \Delta$.

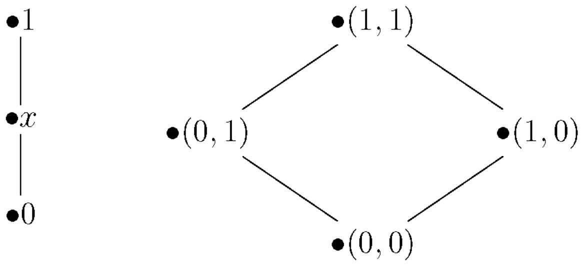
En este caso diremos que la familia $\{g_i\}_{i\in I}$ *separa puntos.*

Definición 7.1.2. Sea $\{A_s\}_{s\in S}$ una familia de álgebras del mismo tipo $\mathcal{F}$. Se dice que un álgebra A de tipo $\mathcal{F}$ es *producto subdirecto* de la familia $\{A_s\}_{s\in S}$ si existe un homomorfismo inyectivo $f : A \longrightarrow \prod A_s$ tal que, si $p_t : \prod A_s \longrightarrow A_t$ es la proyección de índice t, se verifica que $p_t \circ f$ es suryectiva.

Un álgebra no trivial $\langle A, F\rangle$ se llamará *subdirectamente irreducible* si se cumple que cada vez que A es producto subdirecto de la familia $\{A_s\}_{s\in S}$ entonces existe $t \in S$ tal que $p_t \circ f$ es un isomorfismo.

Ejemplo 7.1.3. Veamos un ejemplo simple de un retículo acotado que no es subdirectamente irreducible.

Sean $M = \{0, x, 1\}$ una cadena de tres elementos y $L = \{0, 1\}$ una cadena de dos elementos. Definimos $f : M \longrightarrow L \times L$ por $f(x) = (0, 1)$, ya que los demás elementos están determinados: $f(0) = (0, 0)$ y $f(1) = (1, 1)$.



M

$L \times L$

Entonces, f es un homomorfismo, es inyectiva y además al proyectar su imagen obtenemos L. Es decir: $(p_1 \circ f)(M) = L$ y $(p_2 \circ f)(M) = L$. Luego, M es producto subdirecto de la familia $\{L_1, L_2\}$, siendo $L_1 = L_2 = L$. Sin embargo, M no es isomorfo a L. Eso indica que existe una descomposición de M como producto subdirecto con factores no isomorfos a M, es decir, M no es subdirectamente irreducible.

Teorema 7.1.4. *Un álgebra A es producto subdirecto de una familia $\{A_i\}_{i\in I}$ si y solo si existe una familia $\{g_i\}_{i\in I}$ de homomorfismos suryectivos $g_i : A \longrightarrow A_i$ que separa puntos.*

Demostración. Dada la familia $\{g_i\}_{i\in I}$ definimos $f : A \longrightarrow \prod A_i$ por sus proyecciones: $p_i(f(a)) = g_i(a)$ para cada $i \in I$. Entonces, f es un homomorfismo por serlo todas las g_i, es inyectiva porque la familia $\{g_i\}_{i\in I}$ separa puntos y también se cumple que $p_i \circ f = g_i$ es suryectiva. Luego, A es producto subdirecto de la familia $\{A_i\}_{i\in I}$.

Recíprocamente, si A es producto subdirecto de la familia $\{A_i\}_{i\in I}$ se define para cada $i \in I$: $g_i = p_i \circ f$. Con esto $\{g_i\}_{i\in I}$ verifica las condiciones que pedimos. $\square$

Teorema 7.1.5. *Un álgebra A es subdirectamente irreducible si y solo si existe una congruencia $R_0 \neq \Delta$ tal que si $\mathcal{D} = \{R : R$ congruencia, $R \neq \Delta\}$ entonces $R_0 = \bigcap_{R\in\mathcal{D}} R$.*

Demostración. Supongamos que no existe R_0. Entonces $\bigcap_{R\in\mathcal{D}} R = \Delta$. Tomemos la familia $\{A/R\}_{R\in\mathcal{D}}$ y veamos que A es producto subdirecto de algunos de sus miembros. En efecto, por el Teorema 7.1.4 y la Observación 7.1.1 ítem (3), la familia $\{g_R\}_{R\in\mathcal{D}}$ de las aplicaciones canónicas $g_R : A \longrightarrow A/R$ cumple las condiciones. Sin embargo, $R \in \mathcal{D}$ implica que $R \neq \Delta$, con lo cual A no puede ser isomorfa a A/R para ningún $R \in \mathcal{D}$, pues de serlo cada clase de A/R sería unitaria, es decir, sería $R = \Delta$. Luego, A no es subdirectamente irreducible.

Recíprocamente, sea $R_0 = \bigcap_{R\in\mathcal{D}}$, $R_0 \neq \Delta$. Entonces existen a y b tales que $a \neq b$ y aR_0b. Llamaremos (P) a esta propiedad. Probemos que A es subdirectamente irreducible, para lo cual suponemos que A es producto subdirecto de una familia $\{A_i\}_{i\in I}$ y tomamos la familia $\{g_i\}_{i\in I}$ correspondiente. Como $a \neq b$ y los g_i separan puntos, existirá un $j \in I$ tal que $g_j(a) \neq g_j(b)$. Esto significa que, si llamamos R_j a la congruencia asociada a g_j, a no está relacionado con b por R_j. Por (P), aR_0b, luego: $R_0 \subsetneq R_j$. Luego, debe ser $R_j = \Delta$ y por lo tanto, en virtud del Teorema 1.3.20 del Capítulo 1, se tiene que existe un isomorfismo $\widetilde{g_j}$ que hace conmutar el siguiente diagrama:

$$\begin{tikzcd}
A \arrow[r, "g_j"'] \arrow[d, "p"] & A_j \\
A/\Delta \arrow[ur, "\widetilde{g_j}"'] &
\end{tikzcd}$$

Pero $A/\Delta \cong A$. Luego $A \cong A_j$ y, por lo tanto, A es un álgebra subdirectamente irreducible. $\square$

Ejemplos 7.1.6.

1. Un álgebra A es llamada *simple* si las únicas congruencias que tiene son las triviales Δ y ∇. Toda álgebra simple es subdirectamente irreducible (ejercicio).

2. El retículo **2** es subdirectamente irreducible, ya que siendo las únicas congruencias Δ y ∇, se cumple la condición del Teorema 7.1.5.

   Vamos a probar que **2** es el único retículo distributivo subdirectamente irreducible.

   Si es x un elemento de un retículo distributivo L, las siguientes relaciones R^x y R_x son congruencias en L (probarlo como ejercicio).

   uR_xv si y solo si $u \wedge x = v \wedge x$,

   uR^xv si y solo si $u \vee x = v \vee x$.

Supongamos ahora que L es subdirectamente irreducible y que $L \neq \mathbf{2}$. Entonces existirán $a, b, x \in L$ tales que $a < x < b$. Consideremos las congruencias R_x y R^x y probemos que $R_x \cap R^x = \Delta$. En efecto, si uR_xv y uR^xv entonces, aplicando el Lema 2.1.4 del Capítulo 2 tenemos que $u = v$. Como L es subdirectamente irreducible, en virtud del Teorema 7.1.5 existe una congruencia $R_0 \neq \Delta$ que es la intersección de todas las congruencias distintas de Δ. Luego, $R_0 \subseteq R_x \cap R^x = \Delta$, lo que implicaría que $R_0 = \Delta$, lo cual es un absurdo.

3. El álgebra de Boole $\mathbf{2}$ es subdirectamente irreducible por la misma razón que en el ítem 2. Veamos que es la única. Sea $\langle A, \wedge, \vee, {}^-, 0, 1\rangle$ un álgebra de Boole subdirectamente irreducible y consideremos el retículo $\langle A, \wedge, \vee\rangle$, reducto de aquella. Toda congruencia de $\langle A, \wedge, \vee, {}^-, 0, 1\rangle$ es congruencia de $\langle A, \wedge, \vee\rangle$ y también vale la recíproca, como vimos en el corolario del Lema 2.3.11 del Capítulo 2. Por lo tanto, el razonamiento que se hizo en 2 puede aplicarse aquí también. Por ende, $\mathbf{2}$ es la única álgebra de Boole subdirectamente irreducible.

4. La situación es distinta para las álgebras de Heyting. Hay "demasiadas" álgebras subdirectamente irreducibles, con lo cual una descomposición en subdirectamente irreducibles no es útil para simplificar el estudio de dichas álgebras.

   En efecto, un álgebra de Heyting H es subdirectamente irreducible si y solo si el conjunto
   $$\{x \in H : \ x \neq 1\}$$
   tiene un elemento maximal $z \neq 1$. Para probarlo, usando el Teorema 7.1.5, basta con ver que la congruencia asociada al filtro $[z)$ es la que describe ese teorema.

Vamos ahora a enunciar y delinear la demostración de uno de los importantes teoremas de Birkhoff. Recordemos que hemos definido *variedad* como una clase de álgebras $\mathcal{K}$ cerrada por subálgebras, imágenes homomorfas y productos (ver Capítulo 1, 1.3.15).

Teorema 7.1.7 (ver [6], [2] I, 9, Teorema 4)**.** *Si A es un álgebra de una variedad $\mathcal{K}$ entonces A es producto subdirecto de una familia de álgebras subdirectamente irreducibles de $\mathcal{K}$.*

Demostración. Si A fuera trivial, o sea, si tuviera solo un elemento, entonces podemos considerar que es producto subdirecto de una familia vacía de álgebras subdirectamente irreducibles.

Supongamos ahora que A no es trivial, por lo cual existirán $a, a' \in A$ tales que $a \neq a'$. Consideremos el conjunto

$$Con_{(a,a')} = \{R : \ R \text{ congruencia}, \ (a,a') \notin R\}.$$

Puede demostrarse que el conjunto que acabamos de definir tiene un elemento maximal, el cual llamaremos $R_m(a,a')$. Recordemos que a y a' no están relacionados por $R_m(a,a')$. Tomemos ahora $A/R_m(a,a')$, que está en $\mathcal{K}$ por ser imagen homomorfa de A. Entonces $A/R_m(a,a')$ tiene al menos dos elementos, pues $|a| \neq |a'|$, luego tiene alguna congruencia distinta de Δ. Sea S una de ellas y definamos una relación S' por:

$$xS'y \text{ en } A \text{ si y solo si } |x|S|y| \text{ en } A/R_m(a,a').$$

Se puede probar que S' es una congruencia y que, además, $R_m(a,a') \subseteq S'$. Por la maximalidad de $R_m(a,a')$, no puede cumplirse que $S' \in Con_{(a,a')}$, es decir que debe ser $aS'a'$. Pero esto implica $|a|S|a'|$, y esto vale para toda S no trivial en $A/R_m(a,a')$. Luego, si definimos

$$\mathcal{D}_{(a,a')} = \{S : \ S \text{ congruencia en } A/R_m(a,a'), \ S \neq \Delta\},$$

entonces $(|a|,|a'|) \in \bigcap_{S \in \mathcal{D}_{(a,a')}} S$, por lo que existe una congruencia minimal no trivial en $A/R_m(a,a')$. Esto significa, por el Teorema 7.1.5, que $A/R_m(a,a')$ es subdirectamente irreducible.

Podemos hacer esta construcción para cada par de elementos de $a, a' \in A$ con $a \neq a'$, por lo que se puede demostrar que A es producto subdirecto de la familia de álgebras de $\mathcal{K}$ subdirectamente irreducibles $\{A/R_m(a,a')\}_{a,a' \in A, a \neq a'}$.

$\square$

Observación 7.1.8. Hemos visto que la única álgebra de Boole subdirectamente irreducible es **2**. Entonces podemos mirar el Teorema de Stone de representación de las álgebras de Boole (ver 2.5.10, 4.5.5 y 4.5.8) como aplicación del Teorema 7.1.7. Volveremos sobre este tema en 7.4.15.

7.2. Términos

Conocemos desde nuestra época escolar las funciones lineales y las funciones cuadráticas con sus correspondientes gráficas en el plano real. Son funciones entre números reales que combinan las tres operaciones $+, \cdot$ y $-$. Por ejemplo, la aplicación $f : \mathbb{R} \to \mathbb{R}$ definida como $f(x) = x^2 - 3x$ es una función, la cual toma un número real x lo eleva al cuadrado y le resta tres veces x. Son operaciones que pueden llevarse a cabo en el conjunto de los números reales $\mathbb{R}$ munido de las operaciones $+, \cdot, -$, es decir, en el anillo $\langle \mathbb{R}, +, \cdot, -, 0\rangle$. La expresión "$x^2 - 3x$" es lo que llamaremos un *término* en la variable x y tiene sentido en cualquier álgebra que tenga las operaciones mencionadas. Se obtiene a partir de las variables y las constantes aplicando sucesivamente las operaciones del álgebra. Al tomar la función $f(x)$ lo que hacemos es evaluar el término en un álgebra determinada, en este caso el anillo de los números reales. Es lo que llamaremos *función término*. Esto constituye una generalización de la situación que vimos en el Capítulo 1 con respecto a los símbolos de operaciones y a las operaciones en cada álgebra.

Las congruencias de un álgebra se caracterizan por "pasar bien" a través de las operaciones. Por ejemplo, si R es una congruencia y xRy, uRv, entonces para toda operación binaria $\diamond$ se tiene que $(x \diamond u)R(y \diamond v)$. Esa propiedad se extiende a los términos (ver Teorema 7.2.5) : si se tiene que a_iRb_i para $i = 1, \ldots, k$ entonces evaluando un término en $a_1, \ldots, a_k$ obtendremos una expresión relacionada por R con el mismo término evaluado en $b_1, \ldots, b_k$.

Definición 7.2.1. Sea X un conjunto no vacío de objetos, que llamaremos *variables*. Sea $\mathcal{F}$ un tipo de álgebra, y llamemos $\mathcal{F}_n$ al conjunto de símbolos de operaciones n-arias, para $n = 0, 1, \ldots, k$. El conjunto $\mathrm{T}(X)_{\mathcal{F}}$, abreviadamente $\mathrm{T}(X)$, de los *términos de tipo $\mathcal{F}$ sobre X* se define de la siguiente manera:

(i) $X \cup \mathcal{F}_0 \subseteq \mathrm{T}(X)$, o sea: todas las variables y las constantes son términos.

(ii) Si t_1, t_2,…,t_n son términos y $f \in \mathcal{F}_n$, entonces la cadena de símbolos $f(t_1, t_2, \ldots, t_n)$ es un término.

(iii) Una cadena de símbolos es un término si y solo si se obtiene de (i) y de (ii) en un número finito de pasos.

Diremos que un término es m-ario si aparecen en el mismo a lo sumo m variables.

Ejemplos 7.2.2.

1. Consideremos el tipo de los grupos y $X = \{x, y, z\}$. Los siguientes son términos:

$$x,\ y,\ 0,\ x - 0,\ x + y,\ x - (y + x),\ ((z + y) - y) - z.$$

Observemos que cualquiera de ellos puede considerarse un término 3-ario o ternario, o sea, término en tres variables, pues tiene a lo sumo a las tres variables x, y, z.

2. Consideremos el tipo de las álgebras de Boole y $X = \{x, y\}$. Los siguientes son términos:

$$1,\ \overline{y},\ x \wedge (y \vee \overline{x}),\ y \vee \overline{y}.$$

Observemos que los términos 1 e $y \vee \overline{y}$ son distintos, aunque evaluados en cada álgebra de Boole dan lo mismo. Eso se aclarará con la siguiente definición.

Definición 7.2.3. Dado un término $t(x_1, \ldots, x_n)$ de tipo $\mathcal{F}$ sobre X y un álgebra A de tipo $\mathcal{F}$ definimos la *función término* $t^A : A^n \longrightarrow A$ como sigue:

(i) Si t es la variable x_i, entonces

$$t^A(a_1, \ldots, a_n) = a_i,$$

es decir, t^A es la proyección i-ésima,

(ii) Si t es de la forma

$$f(t_1(x_1, \ldots, x_n), \ldots, t_k(x_1, \ldots, x_n)), \quad \text{con } f \in \mathcal{F}_k,$$

entonces

$$t^A(a_1, \ldots, a_n) = f^A(t_1^A(a_1, \ldots, a_n), \ldots, t_k^A(a_1, \ldots, a_n)).$$

En particular, si $t = f \in \mathcal{F}$ entonces $t^A = f^A$.

Ejemplos 7.2.4.

1. La siguiente tabla muestra la relación entre los términos y las funciones término correspondientes al Ejemplo 1 de 7.2.2:

Término	Función término de 3 variables
x	$f(x, y, z) = x$ (primera proyección)
y	$g(x, y, z) = y$ (segunda proyección)
0	$h(x, y, z) = 0$
$x + y$	$k(x, y, z) = x + y$
$((z + y) - y) - z$	$l(x, y, z) = 0$

Observemos que la función término de una variable correspondiente al término x es la identidad, mientras que la de dos variables correspondiente a $x + y$ es la operación suma.

2. Análogamente, veamos en la siguiente tabla lo que corresponde al Ejemplo 2 de 7.2.2:

Término	Función término
1	$u(x, y) = 1$
$x \wedge (y \vee \overline{x})$	$v(x, y) = x \wedge y$
$y \vee \overline{y}$	$w(x, y) = 1$

Teorema 7.2.5 ([13, II, Teorema 10.3]). *Sean A y B álgebras de tipo $\mathcal{F}$, sea t un término n-ario de tipo $\mathcal{F}$, t^A y t^B las funciones término correspondientes.*

(a) *Sea R una congruencia en A y supongamos que $a_i R a'_i$ para $i = 1, \ldots, n$. Entonces*
$$t^A(a_1, \ldots, a_n) \; R \; t^A(a'_1, \ldots, a'_n).$$

(b) *Sea $h : A \longrightarrow B$ un homomorfismo. Entonces:*
$$h(t^A(a_1, \ldots, a_n)) = t^B(h(a_1), \ldots, h(a_n)).$$

(c) *Sea Z un subconjunto de A. El subuniverso de A generado por Z (ver Definición 1.3.8 del Capítulo 1) está dado por:*
$$Sg(Z) = \{t^A(a_1, \ldots, a_n) : t \text{ } n\text{-ario de tipo } \mathcal{F},\ n \in \mathbb{N},\ a_1, \ldots, a_n \in Z\}.$$

Demostración. Omitiremos los detalles de la demostración, dando solo una idea.

En (a) y (b), la demostración se hace por inducción de la siguiente manera: se supone, en el caso base, que t^A es una operación del álgebra. En ese caso las condiciones se cumplen por definición de congruencia y de homomorfismo respectivamente. Luego se supone que todo vale para $n = k$ y se prueba para $n = k + 1$, componiendo t^A con cada una de las operaciones y aplicando las definiciones.

El punto (c) también se demuestra por inducción. Consideramos los conjuntos
$$E^j(Z) = \{t^A(a_1, \ldots, a_n),\ t^A \text{ obtenido en } j \text{ pasos},\ a_1, \ldots, a_n \in Z\},$$

donde "obtenido en j pasos" significa lo siguiente:

- en 0 pasos, si $t^A(a_1, \ldots, a_n) \in \mathcal{F}_0 \cup Z$ (no se aplicó ninguna operación),

- en 1 paso, si $t^A(a_1, \dots, a_n)$ se obtiene aplicando una sola operación, etc.

Se prueba entonces que

$$Sg(Z) = \bigcup_{j \in \mathbb{N}} E_j(Z),$$

de donde se deduce lo pedido. $\square$

Definición 7.2.6. Se llama *función polinomial* a una aplicación de n variables $f : A^n \longrightarrow A$ obtenida de una función término reemplazando algunas de las variables por elementos del álgebra A. Dicho de otro modo, si es composición de funciones constantes con una función término.

En el Teorema 7.2.5, parte (a), vemos que las funciones término "pasan bien" a través de las congruencias. También todas las funciones constantes lo hacen. Luego, una función polinomial también cumple la condición de la parte (a) del Teorema 7.2.5.

Vamos a generalizar esta condición definiendo las funciones compatibles, que son aquellas que se comportan, podríamos decir, "como si fueran operaciones del álgebra" con respecto a las congruencias.

Definición 7.2.7. Una función de n variables $f : A^n \longrightarrow A$ se dice *compatible con una congruencia* R si cumple, para cada par de n-uplas $(a_1, \dots, a_n)$, $(a'_1, \dots, a'_n)$ de elementos de A, la siguiente condición:

Si $a_i R a'_i$ para $i = 1, \dots, n$, entonces $f(a_1, \dots, a_n) R f(a'_1, \dots, a'_n)$.

La función f se dice *compatible* si es compatible con toda congruencia R del álgebra.

Esto equivale a decir que, si agregamos f como una nueva operación al álgebra, las congruencias del álgebra "enriquecida" por f son las mismas que las del álgebra original.

Corolario 7.2.8. *Toda función polinomial es compatible.*

La pregunta que surge inmediatamente es:

¿Toda función compatible es polinomial?

Cuando en un álgebra la respuesta es positiva, es decir, si toda función compatible es polinomial, se dice que el álgebra es *afínmente completa* o *afín completa*. Si eso ocurre solo para subconjuntos finitos del álgebra, el álgebra es *localmente afín completa* (ver [66]).

Mostraremos luego que las álgebras de Boole son afín completas y que las de Heyting son solo localmente afín completas.

Veamos ahora ejemplos de aplicación de la parte (c) del Teorema 7.2.5.

Ejemplos 7.2.9.

1. Tomemos un ejemplo dado en el Capítulo 1, Definición 1.3.8.

   Sea $(\mathbb{Z}, +, -, 0)$ el grupo de los enteros. Si $Z = \{1\}$ se tiene que $Sg(Z) = \mathbb{Z}$. En efecto,

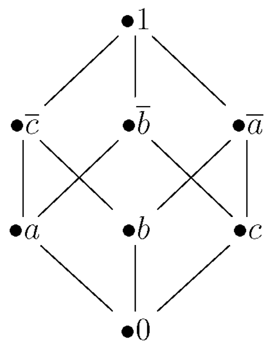
   $E_0 = \{0, 1\}$ (constante y generador),

   $E_1 = E_0 \cup \{1 + 1, -1\}$,

   $E_2 = E_1 \cup \{-2, 2 + 1\}, \ldots$

   En cada paso aplicamos una operación (tomar suma u opuesto) a los del paso anterior y así se llega a obtener todos los enteros.

2. Sea B_3 el álgebra de Boole con tres átomos a, b, c, como se muestra en la figura.

   Tomemos en primer lugar $Z = \{a\}$. Luego:

   $E_0 = \{0, 1, a\}$ (constantes y generador),

   $E_1 = E_0 \cup \{\overline{a}\}$,

   $E_2 = E_1$ y por lo tanto: $Sg(Z) = \{0, 1, a, \overline{a}\}$.

   Sea ahora $Z = \{a, b\}$ y calculemos $Sg(Z)$. Se tiene

   $E_0 = \{0, 1, a, b\}$,

   $E_1 = E_0 \cup \{\overline{a}, \overline{b}, a \wedge b, a \vee b\} = \{0, 1, a, b, \overline{a}, \overline{b}, \overline{c}\}$, pues $a \wedge b = 0$ y $a \vee b = \overline{c}$,

   $E_2 = B_3$, pues E_2 contiene el elemento $\overline{a} \wedge \overline{b}$, que es c.

   Es decir, $\{a, b\}$ genera B_3.

   Este ejemplo se puede generalizar: si B_n es el álgebra de Boole con n átomos $a_1, a_2, \ldots, a_n$, entonces basta tomar el conjunto $\{a_1, a_2, \ldots, a_{n-1}\}$ para generar B_n.

Álgebra de términos

Una vez construido el conjunto de términos podemos dotarlo de operaciones y convertirlo en un álgebra. Ya que los términos son cadenas de símbolos, expresiones bien formadas de un cierto lenguaje formal, las operaciones entre ellos serán las mismas utilizadas para construir los términos. Por ejemplo: $\overline{y}$, $x \wedge (y \vee \overline{x})$ son términos del tipo de las álgebras de Boole. Si efectuamos, por ejemplo, la operación $\wedge$ entre ellos nos queda el término $\overline{y} \wedge (x \wedge (y \vee \overline{x}))$.

Definición 7.2.10. Sea $\mathrm{T}(X) \neq \emptyset$. El *álgebra de los términos sobre* X tiene como universo a $\mathrm{T}(X)$ y como operaciones las correspondientes al tipo $\mathcal{F}$.

Ejemplos 7.2.11.

1. $(\mathrm{T}(X)_{(2,2,0,0)},\ \wedge, \vee, 0, 1)$: el álgebra de términos sobre X del tipo de los retículos acotados.

2. $(\mathrm{T}(X)_{(2,2,1,0,0)},\ \wedge, \vee, ^{-}, 0, 1)$: es el álgebra de términos sobre X del tipo de las álgebras de Boole.

3. $(\mathrm{T}(X)_{(2,0)},\ *, \top)$: es el álgebra de términos sobre X del tipo de los monoides.

4. $(\mathrm{T}(X)_{(2,1,0)},\ *, ^{-1}, 0)$: es el álgebra de términos sobre X del tipo de los grupos.

Observación 7.2.12. El álgebra de términos de tipo $\mathcal{F}$ sobre X tiene a X como conjunto de generadores: $\mathrm{T}(X) = Sg(X)$. Veremos a continuación que X es un conjunto de generadores libres de $\mathrm{T}(X)$, por lo que $\mathrm{T}(X)$ suele llamarse el álgebra *absolutamente libre* sobre X en la clase de las álgebras de tipo $\mathcal{F}$.

Teorema 7.2.13. *El álgebra de términos de tipo $\mathcal{F}$ sobre un conjunto $X \neq \emptyset$ cumple la propiedad universal de extensión de homomorfismos (ver Capítulo 1, Definición 1.3.12) con respecto a la clase de las álgebras de tipo $\mathcal{F}$.*

Demostración. Sea $k : X \longrightarrow A$, A de tipo $\mathcal{F}$. Extendemos k recursivamente a una aplicación $h : \mathrm{T}(X) \longrightarrow A$ de la siguiente manera:

$$h(f(t_1, \ldots, t_n)) = f^A(h(t_1), \ldots, h(t_n)),$$

siendo $f \in \mathcal{F}$ n-aria. Es un ejercicio de rutina ver que h es un homomorfismo. □

Álgebras libremente generadas

Hemos visto en el Capítulo 1, Sección 3.3, Definición 1.3.12 la definición de conjunto de generadores libres X de un álgebra A en una clase $\mathcal{K}$ en base a la propiedad universal de extensión de homomorfismos. Podemos ver las cosas desde otro punto de vista. Si un conjunto X genera A, se llamará libre si no hay ninguna forma de vincular entre sí los elementos de X. En el ejemplo de B_3, los elementos a y b cumplen la condición de que $a \wedge b = 0$. Por lo tanto, $\{a, b\}$ **no** es libre. De hecho, se puede probar que B_3 **no tiene** un conjunto de generadores libres.

Consideremos $\mathrm{T}_{(2,2,0,0)}(X)$ los términos en X de la clase de los retículos distributivos acotados, donde $X = \{x\}$. Entre los infinitos términos en la variable x y las constantes $0, 1$ podemos introducir una identificación muy natural: la que considera iguales a términos que lo son en todo retículo. Identificamos entonces, por ejemplo, $x \wedge x$ con x, $0 \wedge (x \vee (1 \wedge x))$ con 0, etc. Solo nos quedan como representantes los términos básicos: $0, 1, x$. Luego, el álgebra libremente generada por un elemento en la clase de los retículos distributivos acotados es la que tiene esos tres elementos. Pero ... ¿qué vínculos puede haber si hay un solo generador? Sin embargo, hay álgebras generadas por un solo generador y ese generador no es libre. Un ejemplo es el grupo $\mathbb{Z}_p$ que es generado por 1 pero no libremente, pues hay un vínculo: sumando p veces 1 obtenemos 0. Vimos el caso de $p = 3$ en el Capítulo 1.

Volveremos sobre esto próximamente.

7.3. Términos en álgebras de Boole y de Heyting

Hemos visto en el Capítulo 3, donde dimos como ejemplo el caso $n = 2$, que a cada tabla de verdad de una fórmula con n variables le corresponde una disyunción de conjunciones elementales. Esto implica que una fórmula de n variables es lógicamente equivalente a una que contiene los conectivos $\neg, \wedge, \vee$; esta última fórmula se dice que está dada en la *forma normal disyuntiva*. Por otra parte, una fórmula del CPC induce un término (pues los conectivos se corresponden con las operaciones del álgebra) y a su vez, este induce una función término en cada álgebra de Boole.

Veamos algunos ejemplos de fórmulas y sus correspondientes funciones términos.

Fórmula	Término	Función término
p $\vee$ ¬p	$x \vee \overline{x}$	$w(x, y) = 1$
p $\wedge$ (q $\vee$ ¬p)	$x \wedge (y \vee \overline{x})$	$v(x, y) = x \wedge y$

Las reflexiones anteriores nos inducen a pensar entonces que las funciones compatibles en las álgebras de Boole son exactamente las funciones término. Esto no es así, ya que si consideramos el álgebra de Boole B de cuatro elementos (siendo a y b los átomos) entonces la función $f : B \to B$ dada por $f(x) = a \vee x$ es compatible y no es una función término (ya que las funciones términos t en álgebras de Boole satisfacen que $t(0) \in \{0, 1\}$, esta afirmación se deja como ejercicio para el lector). Sin embargo, lo que sí vale es que las funciones compatibles en las álgebras de Boole son exactamente las polinomiales. Antes de probar esto, veremos una equivalencia muy útil para aplicar el concepto de función compatible en álgebras de Heyting.

Comenzaremos con una observación, que se utilizará para simplificar la prueba del lema que le sigue.

Observación 7.3.1. Sean H un álgebra de Heyting, $f : H^n \to H$ una función y $a = (a_1, \ldots, a_n) \in H^n$. Para $i = 1, \ldots, k$, definimos funciones unarias $f_i^a : H \to H$ por $f_i^a(x) := f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n)$. Luego tenemos la siguiente caracterización para funciones compatibles unarias: f es compatible si y solo si para cada $a \in H^n$ y cada $i = 1, \ldots, k$, las funciones f_i^a son compatibles.

Los resultados que veremos a continuación fueron extraídos de [17].

Lema 7.3.2. *Sean H un álgebra de Heyting y $f : H^n \to H$ una función. Las siguientes condiciones son equivalentes:*

a) $f(x_1, \ldots, x_n) \wedge y = f(x_1 \wedge y, \ldots, x_n \wedge y) \wedge y$, *para cada* $x_1, \ldots, x_n, y \in H$.

b) $\bigwedge_{i=1}^n (x_i \leftrightarrow y_i) \leq f(x_1, \ldots, x_n) \leftrightarrow f(y_1, \ldots, y_n)$ *para cada* $x_i, y_i \in H$ *con* $i = 1, \ldots, n$.

c) f *es compatible.*

Demostración. Basta demostrar el Lema para el caso en que $n = 1$. El caso general se deduce del caso unario y de la Observación 7.3.1.

$(a) \Longrightarrow (b)$. Supongamos que $f(x) \wedge y = f(x \wedge y) \wedge y$ para cada $x, y \in H$. Teniendo en cuenta que $x \wedge (x \leftrightarrow y) = y \wedge (x \leftrightarrow y)$ (ver Ejercicio 10 del Capítulo 4) tenemos que:

$$
\begin{aligned}
f(x) \wedge (x \leftrightarrow y) &= f(x \wedge (x \leftrightarrow y)) \wedge (x \leftrightarrow y) \\
&= f(y \wedge (x \leftrightarrow y)) \wedge (x \leftrightarrow y) \\
&= f(y) \wedge (x \leftrightarrow y).
\end{aligned}
$$

Luego, como $x \wedge z = y \wedge z$ si y solo si $z \leq x \leftrightarrow y$ (ver ejercicio citado), se tiene que

$$x \leftrightarrow y \leq f(x) \leftrightarrow f(y).$$

$(b) \Longrightarrow (c)$. Sean R una congruencia en H y F su filtro asociado. Sabemos que $x\ R\ y$ si y solo si $x \leftrightarrow y \in F$ (ver Lema 4.2.2 del Capítulo 4). Por hipótesis, $x \leftrightarrow y \leq f(x) \leftrightarrow f(y)$. Luego, $f(x) \leftrightarrow f(y) \in F$, de donde $f(x)\ R\ f(y)$. Es decir, f es una función compatible.

$(c) \Longrightarrow (a)$. En vista del Ejercicio 10 del Capítulo 4, basta probar que $y \leq f(x \wedge y) \leftrightarrow f(x)$. Sea R la congruencia principal generada por el par $(x, x \wedge y)$. Como f es una función compatible, $f(x)\ R\ f(x \wedge y)$. Además, por el Lema 4.2.8 del Capítulo 4, a R le corresponde el filtro principal generado por el elemento $x \leftrightarrow (y \wedge x)$. Notemos que $x \leftrightarrow (y \wedge x) = x \to y$. Por ende $f(x) \wedge (x \to y) = f(x \wedge y) \wedge (x \to y)$, de donde deducimos que

$$x \to y \leq f(x \wedge y) \leftrightarrow f(x).$$

Por lo tanto, como $y \leq x \to y$ obtenemos que

$$y \leq f(x \wedge y) \leftrightarrow f(x). \qquad \square$$

A continuación veremos que toda álgebra de Boole es afín completa. Recordemos que esto significa que si B es un álgebra de Boole y $f : B^n \to B$ es una función compatible entonces f es una función polinómica.

Teorema 7.3.3. *Toda álgebra de Boole es afín completa.*

Demostración. Vamos a probar que toda función compatible f de n variables en un álgebra de Boole coincide con una función polinomial, probando la siguiente igualdad:

$$f(x_1, \ldots, x_n) = \bigvee_{(s_1,\ldots,s_n)\in\{0,1\}^n} f(s_1, \ldots, s_n) \wedge x_1^{s_1} \wedge \cdots \wedge x_n^{s_n},$$

donde $x_i^1 = x_i$ y $x_i^0 = \overline{x}_i$. Probaremos esta afirmación solo para $n = 2$ (el caso general se prueba análogamente). Es decir, veremos que

$$\begin{aligned} f(x,y) = (f(0,0) \wedge \overline{x} \wedge \overline{y}) \vee (f(0,1) \wedge \overline{x} \wedge y) \\ \vee (f(1,0) \wedge x \wedge \overline{y}) \vee (f(1,1) \wedge x \wedge y). \end{aligned}$$

Teniendo en cuenta que $x = x \leftrightarrow 1$, $\overline{x} = x \leftrightarrow 0$ y lo visto en el Ejercicio 10 del Capítulo 4, tenemos que para $a, b \in \{0,1\}$ vale

$$f(a,b) \wedge (x \leftrightarrow a) \wedge (y \leftrightarrow b) = f(x,y) \wedge (x \leftrightarrow a) \wedge (y \leftrightarrow b). \tag{7.1}$$

Luego se tiene que

$$\begin{aligned}\bigvee_{(a,b)\in\{0,1\}^2} (f(a,b)\wedge x^a \wedge y^b) &= \bigvee_{(a,b)\in\{0,1\}^2} (f(x,y)\wedge (x^a\wedge y^b))\\ &= f(x,y)\wedge \bigvee_{(a,b)\in\{0,1\}^2} (x^a\wedge y^b).\end{aligned}$$

Por lo visto en el Ejercicio 1 del Capítulo 2 (correspondiente a álgebras de Boole) se tiene que $\bigvee_{(a,b)\in\{0,1\}^2}(x^a\wedge y^b) = 1$, por ende

$$f(x,y) = \bigvee_{(a,b)\in\{0,1\}^2} f(a,b)\wedge x^a \wedge y^b. \qquad \square$$

A continuación veremos que toda álgebra de Heyting es localmente afín completa. Recordemos que esto significa que si H es un álgebra de Heyting y $f : H^n \to H$ es una función compatible entonces f restringida a todo subconjunto finito resulta ser una función polinómica.

Teorema 7.3.4. *Toda álgebra de Heyting es localmente afín completa.*

Demostración. Sean H un álgebra de Heyting, S un subconjunto finito de H y $f : H^2 \to H$ una función compatible (consideraremos solamente este caso; el caso general es similar). Veamos que f restringida a S coincide con la siguiente función polinómica:

$$f(x,y) = \bigvee_{(a,b)\in S^2} f(a,b)\wedge (x\leftrightarrow a)\wedge (y\leftrightarrow b), \tag{7.2}$$

donde $(x,y)\in S^2$.

Por la misma razón que en (7.1) del Teorema 7.3.3 tenemos que vale la igualdad

$$f(a,b)\wedge (x\leftrightarrow a)\wedge (y\leftrightarrow b) = f(x,y)\wedge (x\leftrightarrow a)\wedge (y\leftrightarrow b).$$

Luego se tiene que

$$f(a,b)\wedge (x\leftrightarrow a)\wedge (y\leftrightarrow b) \leq f(x,y).$$

Sea $T_{(x,y)} = \{f(a,b)\wedge (x\leftrightarrow a)\wedge (y\leftrightarrow b) : (a,b)\in S^2\}$. Luego $f(x,y)$ es una cota superior de $T_{(x,y)}$, y como $f(x,y)\in T_{(x,y)}$ se concluye que $f(x,y)$ es el máximo de $T_{(x,y)}$. Por lo tanto vale (7.2). $\square$

Las funciones compatibles en álgebras de Heyting se vinculan con los conectivos intuicionistas, cuya definición semántica vimos en el Capítulo 5. En efecto, en el artículo [17] Caicedo y Cignoli dan una definición algebraica de conectivo intuicionista a través de la noción de función compatible en álgebras de Heyting. En el mencionado artículo se prueba en el Lema 2.1 (ver Lema 7.3.2) que la siguiente condición es equivalente a la compatibilidad de la función f:

$$f(x) \wedge y = f(x \wedge y) \wedge y \text{ para cada } x, y.$$

Notemos que esta condición aplicada a una función $\Phi_{\mathrm{C}} : P^{+} \longrightarrow P^{+}$, es la dada en el Capítulo 5 (Definición 5.6.8) para definir semánticamente un conectivo intuicionista unario:

$(\circ)\quad \Phi_{\mathrm{C}}(T) \cap U = \Phi_{\mathrm{C}}(T \cap U) \cap U.$

Luego, las funciones Φ_{C} que dan lugar a conectivos implícitos definidos semánticamente (por modelos de Kripke) no son otra cosa que funciones compatibles de álgebras de Heyting pg (ver Capítulo 4, Definición 4.5.2). Se exhiben en el artículo [17] ejemplos de funciones compatibles que no son polinomiales, lo que demuestra que existen álgebras de Heyting que no son afín completas.

7.4. Ecuaciones

Entendemos elementalmente una *ecuación* como un problema: calcular para qué valores numéricos de las variables se cumple la igualdad que se propone simbólicamente por medio de letras, que son las incógnitas. La resolución de ecuaciones data de los primeros siglos de la era cristiana y es la que da inicio al Álgebra. Fue Mohamed ibn Musa, apodado Al-Khwarizimi, en el siglo IX, el primero en estudiar más o menos científicamente la teoría de ecuaciones. De su nombre proviene la palabra "algoritmo" y del nombre de su obra surgió la misma palabra "álgebra", que significa pasaje de un término de un miembro a otro de una ecuación.

Mucho se ha extendido el alcance del Álgebra y mucho ha cambiado la forma de plantear los problemas desde entonces. Sin embargo, las soluciones dadas por los griegos, los hindúes y los árabes para las ecuaciones algebraicas todavía se estudian.

Veremos en esta sección la definición de ecuación o identidad en general, desde el punto de vista del Álgebra Universal, y algunas importantes consecuencias. En particular, veremos el Teorema de Birkhoff que muestra que las variedades no son otra cosa que clases de álgebras caracterizadas por ecuaciones.

Definición 7.4.1. Una *ecuación* o *identidad* de tipo $\mathcal{F}$ sobre X es una expresión de la forma

$$t \approx u,$$

siendo $t, u \in \mathrm{T}(X)$.

Diremos que un álgebra A de tipo $\mathcal{F}$ *satisface* tal ecuación para t, u términos n-arios y denotaremos $A \vDash t \approx u$ si para toda n-upla $(a_1, \ldots, a_n)$ de elementos de A se verifica $t^A(a_1, \ldots, a_n) = u^A(a_1, \ldots, a_n)$.

Diremos que una clase $\mathcal{K}$ de álgebras satisface $t \approx u$ si cada álgebra de $\mathcal{K}$ la satisface. En ese caso escribiremos: $\mathcal{K} \vDash t \approx u$.

Denotaremos $Id_{\mathcal{K}}(X)$ al conjunto de identidades que satisface la clase $\mathcal{K}$.

En lo sucesivo usaremos a menudo el signo $=$ en lugar de $\approx$.

Definición 7.4.2. Una *cuasiidentidad* es una identidad o bien es una afirmación de la forma: "si $t_1 \approx u_1, \ldots, t_n \approx u_n$ entonces $t \approx u$."

Ejemplos 7.4.3.

1. Sea $\mathcal{G}$ la clase de los grupos (ver Capítulo 1, Sección 3). Las ecuaciones que la caracterizan son:

$$\begin{aligned} x * (y * z) &= (x * y) * z, \\ x * \top &= \top * x = x, \\ x * x^{-1} &= x^{-1} * x = \top. \end{aligned}$$

   El conjunto $Id_{\mathcal{G}}(X)$ con $X = \{x, y, z, t\}$ está formado por todas las identidades obtenidas a partir de estas sustituyendo las variables x, y, z por términos en X. Por ejemplo, $(z * t) * (t^{-1} * z^{-1}) = \top$.

2. Consideremos la clase de los retículos distributivos (ver Capítulo 2, Sección 2). Las ecuaciones que la caracterizan son:

   R0 $x \vee x = x$, $x \wedge x = x$ (idempotencia),

   R1 $x \vee y = y \vee x$, $x \wedge y = y \wedge x$ (conmutatividad),

   R2 $x \vee (y \vee z) = (x \vee y) \vee z$, $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ (asociatividad),

   R3 $(x \vee y) \wedge y = y$, $(x \wedge y) \vee y = y$ (absorción),

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

El siguiente resultado afirma que las identidades se preservan por las tres operaciones que caracterizan una variedad: tomar productos, subálgebras e imágenes homomorfas. La demostración puede verse en [13, Ch. II, Sec. 11].

Teorema 7.4.4 (ver [2, I, 11, Lemma 6 y Corollary 7]). *Sea $\mathcal{K}$ una clase de álgebras del mismo tipo $\mathcal{F}$. Sea $t \approx u$ una ecuación de tipo $\mathcal{F}$ donde t, u son términos n-arios.*

(i) Sea $(A_s)_{s\in S}$ una familia de álgebras de $\mathcal{K}$ tal que $A_s \vDash t \approx u$ para todo $s \in S$. Entonces $\prod_{s\in S} A_s \vDash t \approx u$.

(ii) Sea A álgebra de $\mathcal{K}$ que satisface $t \approx u$, B subálgebra de A. Entonces $B \vDash t \approx u$.

(iii) Sea $h : A \longrightarrow B$ un homomorfismo y supongamos que $A \vDash t \approx u$. Entonces $h(A) \vDash t \approx u$.

Corolario 7.4.5. *Si las álgebras subdirectamente irreducibles de una variedad $\mathcal{K}$ satisfacen una identidad $t \approx u$ entonces toda álgebra de la clase la satisface.*

Demostración. Por el Teorema 7.1.7, toda álgebra A de una variedad es producto subdirecto de subdirectamente irreducibles. Por lo tanto existe una familia $(A_s)_{s\in S}$ de álgebras subdirectamente irreducibles y un homomorfismo inyectivo $f : A \longrightarrow \prod_{s\in S} A_s$. Por (i) del Teorema 7.4.4, $\prod_{s\in S} A_s \vDash t \approx u$. Por ser $f(A)$ subálgebra de $\prod_{s\in S} A_s$ también (por (ii)) se tiene $f(A) \vDash t \approx u$. Pero $f : A \longrightarrow f(A)$ es un isomorfismo, por lo que A es imagen de $f(A)$ por la función inversa de f, luego por (iii) se tiene que A satisface $t \approx u$. □

Corolario 7.4.6. *Sea $\mathcal{K}$ una clase de álgebras del mismo tipo $\mathcal{F}$. Sea $t \approx u$ una ecuación de tipo $\mathcal{F}$. Sea $(A_s)_{s\in S}$ una familia de álgebras de $\mathcal{K}$, A producto subdirecto de esa familia. Entonces: $A \vDash t \approx u$ si y solo si para cada $s \in S$, $A_s \vDash t \approx u$.*

Como vimos en 7.1.6, el álgebra **2** es la única álgebra de Boole subdirectamente irreducible. Aplicando el Teorema 7.1.7 a la clase de álgebras de Boole se puede concluir que toda álgebra de esta clase es producto subdirecto de copias de **2**. Se tiene, entonces, la siguiente conclusión:

Corolario 7.4.7. *Una ecuación se satisface en toda álgebra de Boole si y solo si se satisface en* **2**.

Ecuaciones y álgebras libres

Hemos dicho que, intuitivamente, un conjunto de generadores de un álgebra es *libre* si no existe "vínculo" entre sus elementos. ¿Qué clase de vínculo es ese? Un vínculo entre términos es, según acabamos de ver, una ecuación.

El ejemplo del retículo acotado distributivo libremente generado por un elemento que vimos en la sección anterior nos indicaría que una manera de obtener el álgebra libre en una clase $\mathcal{K}$ con un conjunto X de generadores es calcular todos los términos y "depurar" el conjunto $\mathrm{T}(X)$ identificando los que coinciden en todas las álgebras de la clase, o sea, viendo que las funciones término coinciden. Pero identificar elementos es lo que hacen las congruencias y de eso se trata efectivamente.

Dada una clase $\mathcal{K}$ de álgebras de tipo $\mathcal{F}$ que verifica un conjunto de ecuaciones Ω y dado X un conjunto de generadores, generamos libremente un álgebra construyendo el álgebra de términos $\mathrm{T}(X)$ y luego haciendo el cociente de $\mathrm{T}(X)$ por la intersección de todas las congruencias que se obtienen identificando términos de acuerdo a las identidades de Ω. Este proceso es posible hacerlo en cualquier clase $\mathcal{K}$ que sea una variedad.

No veremos los detalles de las demostraciones pero señalaremos los resultados.

Ejemplos 7.4.8.

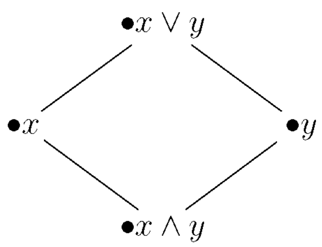
1. Sea $X = \{x, y\}$ y consideremos la clase de las álgebras de Boole, que son de tipo $(2, 2, 1, 0, 0)$.

   Se puede probar que solo hay 16 términos en X no equivalentes entre sí:

$$\{0,\ 1,\ x,\ y,\ \overline{x},\ \overline{y},\ x \wedge y,\ x \wedge \overline{y},\ \overline{x} \wedge y,\ \overline{x} \wedge \overline{y},\ (x \wedge y) \vee (\overline{x} \wedge \overline{y}),\\ (\overline{x} \wedge y) \vee (x \wedge \overline{y}),\ x \vee y,\ x \vee \overline{y},\ \overline{x} \vee y,\ \overline{x} \vee \overline{y}\}.$$

   Esta es el álgebra de Boole libre con dos generadores, que habíamos calculado ya en el Capítulo 2, Figura 2.5.

2. Tomando el mismo $X = \{x, y\}$ y la clase de los retículos distributivos, que son de tipo $(2, 2)$, los términos son solamente x, y y supremos e ínfimos entre las dos variables (no hay constantes). Pero todos los términos se reducen a cuatro no equivalentes, como puede verse en el diagrama siguiente, que muestra el retículo libre con dos generadores.



Teorema 7.4.9 ([2, Theorem 4, I, 12 y resultados relacionados]). *Sea $\mathcal{K}$ una variedad que contiene al menos un álgebra no trivial. Entonces, para todo conjunto $X \neq \emptyset$ existe el álgebra libremente generada por X sobre $\mathcal{K}$.*

Teorema 7.4.10 ([13, Theorem 11.4, II, 11 y resultados relacionados]). *Sea $\mathcal{K}$ una variedad de tipo $\mathcal{F}$ que contiene al menos un álgebra no trivial. Sea $\mathbb{F}_{\mathcal{K}}(X)$ el álgebra libremente generada por X y sea $t \approx u$ una identidad. Entonces $\mathcal{K} \vDash t \approx u$ si y solo si $\mathbb{F}_{\mathcal{K}}(X) \vDash t \approx u$.*

Clases ecuacionales

Para concluir este capítulo enunciaremos un importante teorema de Birkhoff que muestra que toda variedad es una clase ecuacional y recíprocamente.

Definición 7.4.11. Sea Ω un conjunto de ecuaciones de tipo $\mathcal{F}$ y sea $M(\Omega)$ la clase de las álgebras que satisfacen todas las identidades de Ω.

Una clase $\mathcal{K}$ se llama *clase ecuacional* si existe un conjunto Ω de identidades tal que $\mathcal{K} = M(\Omega)$.

Ejemplos 7.4.12.

1. Todas las clases de álgebras que hemos visto o estudiado en capítulos anteriores son clases ecuacionales: grupos, anillos, retículos, álgebras de Boole y de Heyting.

2. Llamaremos *cuerpo* a todo anillo con unidad $\langle K, +, ., -, (\ )^{-1}, 0, 1\rangle$, tal que todo elemento distinto del cero posea inverso. Es decir que

   - $\langle K, +, -, 0\rangle$ es un grupo abeliano,

   - $\langle K', ., (\ )^{-1}, 1\rangle$ es un grupo, donde $K' = K - \{0\}$,

   - vale la propiedad distributiva: $a.(b + c) = a.b + a.c$.

   La clase de los cuerpos no es una variedad, porque la condición "todo elemento distinto de cero posee inverso" no puede darse por ecuaciones.

3. En la Sección 1 del Capítulo 9 daremos la definición de BCK-álgebra, mediante identidades y una cuasiidentidad. Fue demostrado por Wronski que las BCK-álgebras no son una variedad (es decir, que no se pueden definir por ecuaciones).

Lema 7.4.13 (ver [13, Lemma 11.8, II, 11]). *Si $\mathcal{K}$ es una variedad, entonces $\mathcal{K} = M(Id_{\mathcal{K}}(X))$, donde X es un conjunto infinito de variables.*

El siguiente teorema de Birkhoff traslada la dificultad de demostrar que una clase es cerrada por productos, subálgebras e imágenes homomorfas a la de buscar un conjunto de ecuaciones que la caracterice.

Teorema 7.4.14 (ver [5], [13, II, 11, Theorem 11.9])**.** *Una clase es ecuacional si y solo si es una variedad.*

Demostración. Sea Ω tal que $\mathcal{K} = M(\Omega)$. Veamos que $\mathcal{K}$ es cerrada por productos, subálgebras e imágenes homomorfas.

Por el Teorema 7.4.4, si A se obtiene de álgebras de $\mathcal{K}$ por cualquiera de esos tres operadores, entonces A satisface también todas las ecuaciones de Ω. Luego, $A \in \mathcal{K}$. Por lo tanto, $\mathcal{K}$ es cerrada bajo los tres operadores, es decir, es una variedad.

La recíproca sale del Lema 7.4.13. $\square$

Observación 7.4.15. En vista de este teorema, se habla indistintamente de variedades o de clases ecuacionales. Análogamente, una *cuasivariedad* es una clase de álgebras cerrada por ciertos operadores, lo que es equivalente a ser definida por cuasiidentidades (ver [13, 2.24 y 2.25]).

Podemos repensar ahora algunos resultados a la luz del Teorema 7.4.14.

En primer lugar, nos dice que las clases de los monoides, grupos, anillos, retículos, álgebras de Boole, son variedades.

Recordemos ahora algunos resultados vistos en el Capítulo 4.

En el Corolario 4.5.8 se presenta el Teorema de Stone mostrando que toda álgebra de Boole B es isomorfa a una subálgebra del producto $\prod_{P\in B^\star} A_P$, donde para todo $P \in B^\star$ es $A_P = \mathbf{2}$, o sea $\prod_{P\in B^\star} A_P = \mathbf{2}^{B^\star}$.

Llamamos f a la función que se define por: $f(x) = (a_P)_{P\in B^\star}$, donde $a_P = 1$ si y solo si $x \in P$, $pr_Q : \prod_{P\in B^\star} A_P \longrightarrow A_Q$ a la proyección y $g_Q = pr_Q \circ f$. Se tiene entonces el siguiente diagrama conmutativo:

$$\begin{tikzcd} B \arrow[r, "f"] \arrow[dr, "g_Q"'] & \mathbf{2}^{B^\star} \arrow[d, "pr_Q"] \\ & \mathbf{2} \end{tikzcd}$$

donde g_Q es obviamente suryectiva. Esto significa que toda álgebra de Boole es producto subdirecto de la familia $(A_P)_{P\in B^\star}$. Lo que estamos diciendo es que el Teorema de Stone especifica, además de lo que dice el teorema de Birkhoff, que el conjunto de índices sobre el que hay que tomar el producto de copias de $\mathbf{2}$ es el conjunto $B^\star$ de los ultrafiltros de B.

Podemos decir aún más. En el Capítulo 3, Teorema 3.5.10 mostramos, usando el Teorema de Stone, que una fórmula es válida en toda álgebra de

Boole si y solo si es válida en **2**. Es decir que el hecho de ser **2** la única álgebra de Boole subdirectamente irreducible se refleja en el hecho de que en el cálculo clásico podemos limitarnos a dos valores de verdad.

Esto nos lleva a ver cómo los teoremas importantes son vínculos entre distintos "mundos matemáticos" como el Álgebra y la Lógica y, según vimos en el Capítulo 6, también la Topología.

7.5. Ejercicios

1. Probar las afirmaciones (2) y (3) de la Observación 7.1.1.

2. Probar que toda álgebra simple es subdirectamente irreducible (usar Teorema 7.1.5).

3. Sea L un retículo distributivo. Sean R_x y R^x las relaciones dadas por:

   uR_xv si y solo si $u \wedge x = v \wedge x$, uR^xv si y solo si $u \vee x = v \vee x$.

   Probar que son congruencias (usar Corolario 2.3.10 del Capítulo 2).

4. Sea H un álgebra de Heyting, $e \in H$ un elemento tal que $x \neq 1$ implica $x \leq e$ para $x \in H$. Probar que H es subdirectamente irreducible. (Sugerencia: usar Ejercicio 11 del Capítulo 4).

5. Sea $H_3 = \{0,x,1\}$ la cadena de Heyting de tres elementos.

   a) Probar que si t es un término unario sobre H_3 entonces $t(0) \in \{0, 1\}$.

   b) Probar que la función $S : H_3 \to H_3$ dada por $S(0) = x$, $S(x) = 1$ y $S(1) = 1$ es compatible (ver la definición 7.2.7). ¿Puede ser S una función asociada a algún término unario?

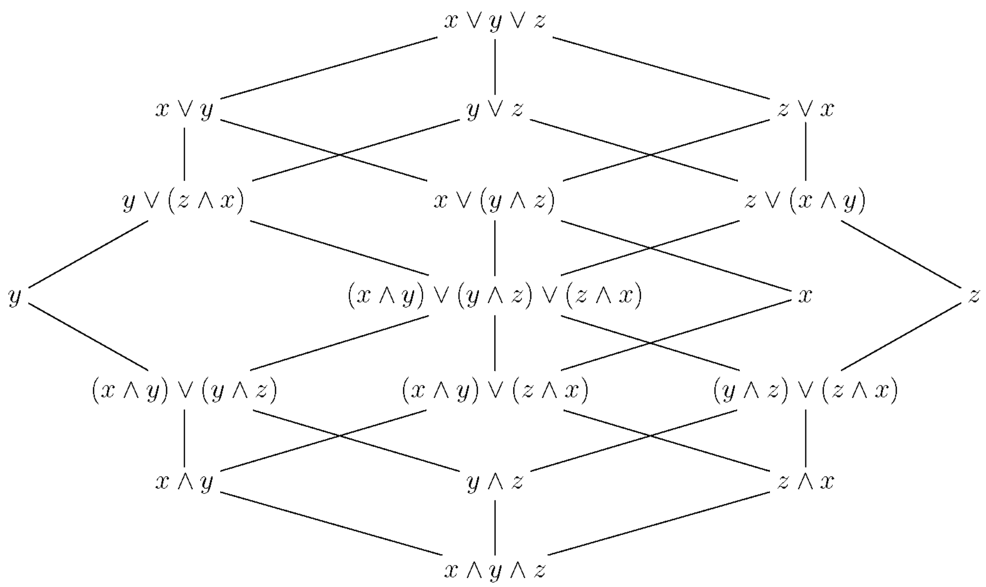
   c) Probar que la función $A : H_3 \to H_3$ dada por $A(0) = x$, $A(x) = 1$ y $A(1) = 0$ no es compatible. ¿Puede ser A una función asociada a algún término unario?

   d) Listar todas las funciones compatibles unarias sobre H_3.

6. Dar un ejemplo de una operación binaria sobre H_3 que sea no compatible.

7. Verificar que el siguiente diagrama corresponde al retículo distributivo

libre generado por $\{x, y, z\}$:



8. Probar que una función $f(x_1, \ldots, x_n)$ de n variables es compatible si y solo si lo son cada una de las n funciones de una variable $f(x_1, a_2, \ldots, a_n)$, $f(a_1, x_2, a_3, \ldots, a_n)$,..., $f(a_1, a_2, \ldots, a_{n-1}, x_n)$, siendo $a_1, \ldots, a_n$ elementos de H.

Bibliografía del Capítulo 7

- Balbes R. and Dwinger, P., *Distributive Lattices*. University of Missouri Press, 1974.
- Birkhoff G., *On the structure of abstract algebras*. Proc. Cambridge Philos. Soc., 31 (1935), 433–454.
- Birkhoff G., *Subdirect unions in universal algebra*. Bull. Amer. Math. Soc., 50 (1944), 764–768.
- Burris S. and Sankappanavar H.P., *A Course in Universal Algebra*. Springer-Verlag, 1980.
- Caicedo X., *Investigaciones acerca de los conectivos intuicionistas*. Rev. Acad. Colombiana Ciencias Exactas Físicas Naturales, 19 (1995), no. 75, 705–716.
- Caicedo X. and Cignoli R., *An algebraic approach to intuitionistic connectives*. J. Symbolic Logic, 66 (2001), no. 4, 1620–1636.
- Kaarli K. and Pixley A.F., *Polinomial Completeness in Algebraic Systems*. Chapman Hall/CRC, Boca Raton, 2001.

Capítulo 8

MV-álgebras

Las álgebras de Boole son un caso particular de MV-álgebras. Según hemos visto en el Corolario 7.4.7, para verificar que una ecuación se cumple en un álgebra de Boole cualquiera basta verificarla en **2**. Mostraremos en este capítulo el teorema de completud algebraica (Teorema 8.5.12) demostrado en primer lugar por Chang —y posteriormente de otra manera por Cignoli y Mundici— que dice esencialmente que para verificar una ecuación en las MV-álgebras basta verificarla en la MV-álgebra $\langle [0,1], \oplus, \neg, 0\rangle$ cuyas operaciones son las siguientes:

$$x \oplus y = \mathrm{mín}\{1, x+y\}, \quad \neg x = 1 - x, \quad 0 = 0.$$

La suma recién definida suele llamarse "suma truncada", ya que da por resultado $x + y$ si es menor o igual que 1 y 1 en caso contrario. La negación "refleja" a x simétricamente respecto del valor 1/2.

Trataremos la biyección entre ideales y congruencias de MV-álgebras, lo que nos dará herramientas para demostrar otro resultado importante y que se prueba con menos esfuerzo: el teorema de representación de Chang (Teorema 8.3.6), que dice que toda MV-álgebra es producto subdirecto de MV-álgebras totalmente ordenadas. De allí se deduce que una ecuación es válida en toda MV-álgebra si y solo si es válida en las MV-álgebras totalmente ordenadas.

Veremos la representación de las MV-álgebras libres, que se aplicará después al álgebra de Lindenbaum del Cálculo Ł.

8.1. Definiciones y ejemplos

Definiremos a continuación las MV-álgebras y las álgebras de Wajsberg, las cuales serán llamadas W-álgebras. Demostraremos que estas álgebras son lo que suele llamarse *definicionalmente equivalentes*. Diremos que dos variedades $\mathcal{V}$ y $\mathcal{W}$ son definicionalmente equivalentes si para cada álgebra A de $\mathcal{V}$ pueden definirse a partir de las operaciones de A otras operaciones con las cuales A resulta ser un álgebra de $\mathcal{W}$ y recíprocamente (intercambiando $\mathcal{V}$ con $\mathcal{W}$). Además se pide que en este proceso de "ida y vuelta" obtengamos en cada caso el álgebra de partida. En particular, sus correspondientes categorías son *isomorfas*. Un isomorfismo de categorías es un caso particular de equivalencia categorial (ver Sección 1 del Capítulo 6) en el cual los isomorfismos naturales ξ y σ son las respectivas identidades.

Reiterando lo dicho en 1.3.3, a veces nos referiremos a una MV-álgebra o a un álgebra de Wajsberg mencionando solo su conjunto subyacente.

Definición 8.1.1. Una MV-álgebra es un álgebra $\mathbf{A} = \langle A, \oplus, \neg, 0\rangle$ de tipo $(2, 1, 0)$ tal que satisface las siguientes condiciones para cada $x, y, z \in A$:

MV1 $x \oplus (y \oplus z) = (x \oplus y) \oplus z$,

MV2 $x \oplus y = y \oplus x$,

MV3 $x \oplus 0 = x$,

MV4 $\neg\neg x = x$,

MV5 $x \oplus \neg 0 = \neg 0$,

MV6 $\neg(\neg x \oplus y) \oplus y = \neg(\neg y \oplus x) \oplus x$.

Definimos:

$$\begin{aligned} 1 &= \neg 0, \\ x \odot y &= \neg(\neg x \oplus \neg y), \\ x \to y &= \neg x \oplus y, \\ x \ominus y &= x \odot \neg y. \end{aligned}$$

Vemos entonces que la clase $\mathcal{MV}$ de las MV-álgebras es una clase ecuacional. Luego, teniendo en cuenta el Teorema 7.4.14 que vimos en el Capítulo 7 (teorema de Birkhoff) tenemos que $\mathcal{MV}$ es una variedad.

Ejemplos 8.1.2.

1. Toda álgebra de Boole es una MV-álgebra.

   En efecto, sea $\langle A, \vee, \wedge, ^-, 0, 1\rangle$ un álgebra de Boole. Definimos:

   $$x \oplus y = x \vee y, \quad \neg x = \overline{x}, \quad 0 = 0.$$

Es sencillo mostrar que se cumplen las propiedades **MV1**,..., **MV5**. Probaremos a continuación la propiedad **MV6**.

$$\begin{aligned}
\neg(\neg x \oplus y) \oplus y &= \overline{(\overline{x} \vee y)} \vee y \\
&= (\overline{\overline{x}} \wedge \overline{y}) \vee y \\
&= (x \wedge \overline{y}) \vee y \\
&= (x \vee y) \wedge (\overline{y} \vee y) \\
&= x \vee y.
\end{aligned}$$

Análogamente,

$$\neg(\neg y \oplus x) \oplus x = y \vee x.$$

2. Veamos que, en efecto, el álgebra $\langle [0,1], \oplus, \neg, 0\rangle$ con las operaciones

$$x \oplus y = \text{mín}\{1, x+y\}, \quad \neg x = 1 - x, \quad 0 = 0,$$

es una MV-álgebra.

Probemos que valen **MV1**,...,**MV6**.

Para probar **MV1** analicemos dos casos: $x+y+z > 1$ y $x+y+z \leq 1$.

En el primer caso, si $y + z > 1$:

$$x \oplus (y \oplus z) = \text{mín}\{1, x + \text{mín}\{1, y+z\}\} = \text{mín}\{1, x+1\} = 1.$$

Si $y + z \leq 1$:

$$x \oplus (y \oplus z) = \text{mín}\{1, x + (y+z)\} = 1.$$

Análogamente, ya sea $x + y > 1$ o $x + y \leq 1$ es

$$(x \oplus y) \oplus z = 1.$$

En caso de que sea $x + y + z \leq 1$, se tiene que $x + y \leq 1$ y también $y + z \leq 1$. Por lo tanto,

$$x \oplus (y \oplus z) = \text{mín}\{1, x + \text{mín}\{1, y+z\}\} = \text{mín}\{1, x + \{y+z\}\} = x + (y+z),$$

y análogamente

$$(x \oplus y) \oplus z = \text{mín}\{1, \text{mín}\{1, x+y\} + z\} = (x+y) + z.$$

Luego $x \oplus (y \oplus z) = (x \oplus y) \oplus z$.

La propiedad **MV2** es inmediata.

Teniendo en cuenta que $0 \leq x \leq 1$ vemos que $\min\{1, x+0\} = x$, por lo que vale **MV3**.

También **MV4** y **MV5** son inmediatos, pues: $1 - (1 - x) = x$ y $\min\{1, x+1\} = 1$.

Para probar **MV6**, mostremos primero que

$$\neg(\neg x \oplus y) \oplus y = x \vee y.$$

Supongamos en primer lugar que $x \leq y$. En este caso, $\neg(\neg x \oplus y) = 1 - ((1-x) \oplus y) = 1 - \min\{1, 1-x+y\}$. Como $y - x \geq 0$, se tiene que $\min\{1, 1-x+y\} = 1$, de donde $\neg(\neg x \oplus y) = 0$. Por lo tanto, $\neg(\neg x \oplus y) \oplus y = y = x \vee y$.

Si $x > y$, $\neg(\neg x \oplus y) = 1 - \min\{1, 1-x+y\} = 1 - (1-x+y) = x - y$. Luego $\neg(\neg x \oplus y) \oplus y = \min\{1, x-y+y\} = x = x \vee y$.

Análogamente podríamos haber probado $\neg(\neg y \oplus x) \oplus x = x \vee y$, luego

$$\neg(\neg x \oplus y) \oplus y = \neg(\neg y \oplus x) \oplus x.$$

3. Mostremos un ejemplo finito. Sea

$$Ł_n = \{0, \frac{1}{n-1}, \frac{2}{n-1}, \ldots, \frac{n-2}{n-1}, 1\}.$$

Definiremos una estructura de MV-álgebra en $Ł_n$.

La negación está dada por

$$\neg\frac{k}{n-1} = \frac{n-1-k}{n-1}.$$

La suma truncada es

$$\frac{r}{n-1} \oplus \frac{s}{n-1} = \begin{cases} 1, & \text{si } r+s \geq n-1, \\ \frac{r+s}{n-1}, & \text{si } r+s < n-1. \end{cases}$$

Por ejemplo, sea $n = 4$. Las siguientes son las tablas de la negación y de la suma, omitiendo los casos obvios de la forma $x \oplus 0 = x$ y $x \oplus 1 = 1$.

x	¬ x
0	1
$\frac{1}{3}$	$\frac{2}{3}$
$\frac{2}{3}$	$\frac{1}{3}$
1	0

x	y	$x \oplus y$
$\frac{1}{3}$	$\frac{1}{3}$	$\frac{2}{3}$
$\frac{1}{3}$	$\frac{2}{3}$	1
$\frac{2}{3}$	$\frac{1}{3}$	1
$\frac{2}{3}$	$\frac{2}{3}$	1

4. En 1958 C. C. Chang introdujo la MV-álgebra totalmente ordenada **C** (ver [21]) de la siguiente manera.

   Sea $\mathbb{Z}\otimes\mathbb{Z}$ el conjunto ordenado $(\mathbb{Z}\times\mathbb{Z}, \preceq)$, donde $\preceq$ (orden *lexicográfico*) se define por (ver 1.2.1, Capítulo 1):

$$(m,n) \preceq (p,q) \begin{cases} \text{si } m < p, \text{ o bien} \\ \text{si } m = p \text{ y } n \leq q. \end{cases}$$

   Tomemos ahora el conjunto

$$C = \{(m,n) \in \mathbb{Z} \times \mathbb{Z} : \ (0,0) \leq (m,n) \leq (1,0)\}.$$

   Entonces $C \subseteq \mathbb{Z} \times \mathbb{Z}$ y podemos tomar en C el orden inducido por $\preceq$. Llamaremos $\perp = (0,0)$, $\top = (1,0)$, $e = (0,1)$. Denotaremos también $2e = (0,2)$, $3e = (0,3)$,..., y definimos:

$$\neg ne = (1,-n), \quad \neg\perp = \top, \quad \neg\top = \perp.$$

   Entonces se tiene:

$$\perp < e < 2e < \cdots < ne < \cdots < \neg ne < \neg(n{-}1)e < \cdots < \neg 2e < \neg e < \top.$$

   Esto puede verse en la Figura 8.1.

   Definimos la suma $\oplus$ como sigue:

$$re \oplus se = (r+s)e$$
$$\neg re \oplus \neg se = \top,$$
$$re \oplus \neg se = \begin{cases} \top, & \text{si } s \leq r, \\ \neg(s-r)e, & \text{si } s > r. \end{cases}$$

   Intuitivamente, si estamos en la “rama positiva”: $\perp < e < 2e < \ldots$ la suma es la usual. Si estamos en la “rama negativa” $\ldots \neg 2e < \neg e < \top$ entonces la suma siempre da $\top$. Veamos qué pasa si sumamos un elemento de la rama positiva con otro de la rama negativa. Recordemos que $re = (0,r)$ y que $\neg se = (1,-s)$. Si sumamos componente a componente: $(0,r) + (1,-s) = (1, r-s)$, que es mayor que $(1,0) = \top$ si $r - s \geq 0$, o sea, si $s \leq r$. En caso contrario, $(1, r-s) = \neg(r-s)e$.

   Definimos ahora $\mathbf{C} = \langle C, \oplus, \neg, \perp\rangle$, que resulta una MV-álgebra. Si la visualizamos horizontalmente como en la Figura 8.2 es más fácil ver que la suma es geométricamente como la suma truncada del intervalo $[0,1]$.

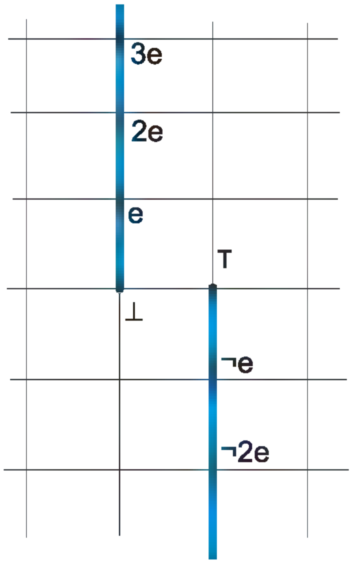


Figura 8.1: C

Figura 8.2: C horizontal

Definición 8.1.3. Un álgebra de Wajsberg, o W-álgebra para abreviar, es un sistema $\langle A, \to, \neg, 1\rangle$ tal que

W1 $1 \to x = x$,

W2 $(x \to y) \to ((y \to z) \to (x \to z)) = 1$,

W3 $(x \to y) \to y = (y \to x) \to x$,

W4 $(\neg x \to \neg y) \to (y \to x) = 1$.

Lema 8.1.4. *Sea $\langle A, \to, 1\rangle$ un álgebra en la que valen **W1**, **W2** y **W3**. Sea $\leq$ la relación definida por*

$$x \leq y \text{ si y solo si } x \to y = 1.$$

Entonces, $\leq$ es una relación de orden en A.

Demostración. Por **W2** tenemos que $(1 \to 1) \to ((1 \to x) \to (1 \to x)) = 1$.

Pero, por **W1**, $(1 \to 1) = 1$, $(1 \to x) = x$.

Luego, también usando **W1**; $1 \to (x \to x) = x \to x = 1$, de donde $x \leq x$.

Supongamos que $x \leq y$, $y \leq z$. Luego, por **W2**,

$$\begin{aligned} 1 &= (x \to y) \to ((y \to z) \to (x \to z)) \\ &= 1 \to (1 \to (x \to z)) \\ &= x \to z, \end{aligned}$$

o sea que $x \leq z$.

Veamos la antisimetría.

Si $x \leq y$, $y \leq x$, debe ser $x = y$. Se tiene, usando **W1** y **W3**:

$$\begin{aligned} x &= 1 \to x \\ &= (y \to x) \to x \\ &= (x \to y) \to y \\ &= 1 \to y \\ &= y. \end{aligned}$$

□

Lema 8.1.5. *Sea $\langle A, \to, 1\rangle$ un álgebra y supongamos que estamos en las mismas condiciones que en el Lema 8.1.4. Entonces, las siguientes propiedades valen en A:*

(i) *1 es el máximo elemento de A,*

(ii) $x \leq y \to x$,

(iii) Si $x \leq y$, *entonces* $x \to z \geq y \to z$,

(iv) $x \to (y \to z) = y \to (x \to z)$,

(v) $x \to y \leq (z \to x) \to (z \to y)$,

(vi) Si $x \leq y$, *entonces* $z \to x \leq z \to y$.

Demostración. Para probar (i) debemos ver que, para todo $x \in A$, $x \leq 1$, es decir que $x \to 1 = 1$. Veamos primero que $(x \to 1) \leq 1$ o sea que $(x \to 1) \to 1 = 1$.

Por **W3**, **W1** y el lema anterior:

$$(x \to 1) \to 1 = (1 \to x) \to x = x \to x = 1.$$

Usando esta igualdad y por **W2**:

$$\begin{aligned} 1 &= (1 \to x) \to ((x \to 1) \to (1 \to 1)) \\ &= x \to ((x \to 1) \to 1) \\ &= x \to 1. \end{aligned}$$

Demostremos (ii), usando **W2**, el hecho de que 1 es máximo y **W1**:

$$\begin{aligned} 1 &= (y \to 1) \to ((1 \to x) \to (y \to x)) \\ &= 1 \to (x \to (y \to x)) \\ &= x \to (y \to x). \end{aligned}$$

Probemos ahora (iii). Por **W2** tenemos que $x \to y \leq (y \to z) \to (x \to z)$. Por esta razón, si $x \to y = 1$ entonces $(y \to z) \to (x \to z) = 1$, es decir, $y \to z \leq x \to z$.

Para probar (iv) usaremos (ii), **W3**, (iii) y **W2**.

Por (ii), $y \leq (z \to y) \to y$, y por **W3** obtenemos: $y \leq (y \to z) \to z$.

Por (iii), de esta última desigualdad obtenemos:

$$y \to (x \to z) \geq ((y \to z) \to z) \to (x \to z).$$

Por **W2**, $x \to (y \to z) \leq ((y \to z) \to z) \to (x \to z)$.

De estas dos últimas desigualdades obtenemos:

$$x \to (y \to z) \leq y \to (x \to z).$$

La otra desigualdad se obtiene por un cambio de variables.

Probemos ahora (v).

Debemos mostrar la siguiente igualdad:

$$(x \to y) \to ((z \to x) \to (z \to y)) = 1.$$

Por (iv), el primer miembro es igual a $(z \to x) \to ((x \to y) \to (z \to y))$, que es igual a 1 por **W2**.

Por último, (vi) se deduce de (v), de manera análoga a como (iii) se deduce de **W2**. □

Lema 8.1.6. *Sea $\langle A, \to, \neg, 1\rangle$ una W-álgebra, sea $0 = \neg 1$. Valen las siguientes propiedades:*

(a) 0 *es el mínimo elemento de* A*,*

(b) $\neg x = x \to 0$*,*

(c) $\neg\neg x = x$*,*

(d) $\neg y \to \neg x = x \to y$*,*

(e) Si $x \leq y$ *entonces* $\neg y \leq \neg x$*.*

Además, $\langle A, \vee, \wedge, 0, 1\rangle$ *es un retículo acotado, siendo*

$$x \vee y = (x \to y) \to y,$$
$$x \wedge y = \neg(\neg x \vee \neg y).$$

Demostración. El ítem (a) se prueba usando **W4**, (ii) y (vi) del Lema 8.1.5. Se tiene: $0 \leq \neg x \to 0$. Además, $\neg x \to \neg 1 \leq 1 \to x = x$. Luego, $0 \leq \neg x \to 0 \leq x$.

Para probar (b) mostremos primero la igualdad

$$\neg x \to 0 = x.$$

Ya habíamos probado que

$$\text{(I)} \quad \neg x \to 0 \leq 1 \to x = x.$$

Además, por (ii) del Lema 8.1.5, es

$$\text{(II)} \quad \neg x \leq \neg 0 \to \neg x \leq x \to 0.$$

Aplicando (iii) del mismo lema a (II), y por **W3** y **W1** y usando (a):

$$\neg x \to 0 \geq (x \to 0) \to 0 = (0 \to x) \to x = 1 \to x = x,$$

de donde

$$\text{(III)}\quad \neg x \to 0 \geq x.$$

Por (I) y (III):

$$\text{(IV)}\quad \neg x \to 0 = x.$$

Finalmente, usando (IV), **W3** y (a) se tiene que:

$$x \to 0 = (\neg x \to 0) \to 0 = (0 \to \neg x) \to \neg x = \neg x.$$

El punto (c) se prueba sencillamente a partir de (b) y **W3**:

$$\neg\neg x = (x \to 0) \to 0 = (0 \to x) \to x = 1 \to x = x.$$

Probemos (d) usando **W4** y (c). En primer lugar, por **W4**,

$$\neg y \to \neg x \leq x \to y.$$

Además, por (c),

$$x \to y = \neg\neg x \to \neg\neg y \leq \neg y \to \neg x.$$

El ítem (e) se deduce de (d).

Por último, veamos que $(x \to y) \to y$ es el supremo de x e y, ya que la propiedad correspondiente al ínfimo será consecuencia de que $(x \to y) \to y = x \vee y$ usando (e).

Por (ii) del Lema 8.1.5, $y \leq (x \to y) \to y$, $x \leq (y \to x) \to x$. Veamos que $(x \to y) \to y$ es la mínima cota superior de x e y. Sea $z \geq x, y$. Por (iii) del lema citado: $x \to y \geq z \to y$. Aplicando nuevamente esta propiedad y por **W3** y **W1**:

$$\begin{aligned}(x \to y) \to y &\leq (z \to y) \to y \\ &= (y \to z) \to z \\ &= 1 \to z \\ &= z.\end{aligned}$$

□

Lema 8.1.7. *En una MV-álgebra valen las siguientes igualdades:*

(a) $\neg 1 = 0$,

(b) $\neg x \oplus x = 1$,

(c) $x \to x = 1$,

(d) $x \odot \neg y = \neg(x \to y)$,

(e) $(x \odot \neg y) \oplus y = (y \odot \neg x) \oplus x$,

(f) $(x \odot y) \to z = x \to (y \to z)$,

(g) $x \to (y \to (x \odot y)) = 1$.

Demostración. El ítem (a) es inmediato por **MV4**.

El ítem (b) se prueba usando (a) y las propiedades **MV3**, **MV2**, **MV4**, **MV5** y **MV6**:

$$\begin{aligned} \neg x \oplus x &= \neg(x \oplus 0) \oplus x \\ &= \neg((\neg 1) \oplus x) \oplus x \\ &= \neg(\neg x \oplus 1) \oplus 1 \\ &= 1. \end{aligned}$$

El ítem (c) es la traducción de (b) en términos de $\to$.

Usando **MV4** se demuestra el ítem (d).

De las propiedades **MV4** y **MV6** deducimos (e):

$$\begin{aligned} (x \odot \neg y) \oplus y &= \neg(\neg x \oplus \neg\neg y) \oplus y \\ &= \neg(\neg x \oplus y) \oplus y \\ &= \neg(\neg y \oplus x) \oplus x \\ &= (y \odot \neg x) \oplus x. \end{aligned}$$

Usando **MV1** (asociatividad de la suma), la definición de implicación y la definición del producto podemos probar (f):

$$\begin{aligned} (x \odot y) \to z &= (\neg x \oplus \neg y) \oplus z \\ &= \neg x \oplus (y \to z) \\ &= x \to (y \to z). \end{aligned}$$

Por definición de implicación y de $\odot$ y usando (b) tenemos:

$$\begin{aligned} x \to (y \to (x \odot y)) &= \neg x \oplus (\neg y \oplus (x \odot y)) \\ &= (\neg x \oplus \neg y) \oplus \neg(\neg x \oplus \neg y) \\ &= 1. \end{aligned}$$ □

Observación 8.1.8. El ítem (f) del Lema 8.1.7 nos permite probar fácilmente la siguiente propiedad de las MV-álgebras:

$$x \odot y \leq z \text{ si y solo si } x \leq y \to z \text{ (R)}.$$

Comparemos esta propiedad con la de la implicación intuicionista.

$$x \wedge y \leq z \quad \text{si y solo si} \quad x \leq y \to z.$$

Vemos que esta se obtiene de la anterior sustituyendo $\odot$ por $\wedge$.

Esa propiedad (R), llamada de **residuación**, merece una explicación más profunda, que involucra teoría de categorías. Veremos esto más adelante, en el Capítulo 12.

Teorema 8.1.9. *Sea* $\mathbf{A} = \langle A, \oplus, \neg, \mathbf{0}\rangle$ *una MV-álgebra. Si definimos*

$$x \to y = \neg x \oplus y, \quad 1 = \neg 0,$$

entonces $\langle A, \to, \neg, 1\rangle$ *es una W-álgebra.*

Demostración. Probemos **W1**, usando (a) del Lema 8.1.7 y **MV3**:

$$\begin{aligned} 1 \to x &= \neg 1 \oplus x \\ &= 0 \oplus x \\ &= x. \end{aligned}$$

Análogamente, **W4** se deduce de **MV4**, **MV2** y de (c) del Lema 8.1.7.

$$\begin{aligned} (\neg x \to \neg y) \to (y \to x) &= (\neg\neg x \oplus \neg y) \to (\neg y \oplus x) \\ &= (x \oplus \neg y) \to (x \oplus \neg y) \\ &= 1. \end{aligned}$$

Vale **W3** por ser la traducción de **MV6** en términos de $\to$.

Por último, **W2** se demuestra como sigue, usando **MV1**, **MV2**, **MV5**, (b), (d) y (e) del Lema 8.1.7:

$$\begin{aligned} (x \to y) \to ((y \to z) \to (x \to z)) &= \neg(x \to y) \oplus (\neg(y \to z) \oplus (x \to z)) \\ &= (x \odot \neg y) \oplus ((y \odot \neg z) \oplus (\neg x \oplus z)) \\ &= (x \odot \neg y) \oplus (((z \odot \neg y) \oplus y) \oplus \neg x) \\ &= ((y \odot \neg x) \oplus x) \oplus (z \odot \neg y) \oplus \neg x \\ &= (y \odot \neg x) \oplus (z \odot \neg y) \oplus (x \oplus \neg x) \\ &= ((y \odot \neg x) \oplus (z \odot \neg y)) \oplus 1 \\ &= 1. \end{aligned}$$

□

Teorema 8.1.10. *Sea* $\langle A, \to, \neg, 1\rangle$ *una W-álgebra. Si definimos*

$$x \oplus y = \neg x \to y, \quad 0 = \neg 1,$$

entonces $\mathbf{A} = \langle A, \oplus, \neg, \mathbf{0}\rangle$ *es una MV-álgebra.*

Demostración. En primer lugar, probemos que vale **MV2**, usando (c) y (d) del Lema 8.1.6.

$$\begin{aligned} x \oplus y &= \neg x \to y \\ &= \neg x \to \neg\neg y \\ &= \neg y \to x \\ &= y \oplus x. \end{aligned}$$

Para probar **MV1** se usan **MV2**, (c) y (d) del Lema 8.1.6, y (iv) del Lema 8.1.5.

$$\begin{aligned} (x \oplus y) \oplus z &= \neg(\neg x \to y) \to z \\ &= \neg z \to (\neg x \to y) \\ &= \neg x \to (\neg z \to y). \end{aligned}$$

Por otra parte:

$$\begin{aligned} x \oplus (y \oplus z) &= \neg x \to (y \oplus z) \\ &= \neg x \to (z \oplus y) \\ &= \neg x \to (\neg z \to y). \end{aligned}$$

Las igualdades **MV3** y **MV4** valen por (b) y (c) del Lema 8.1.6.

La igualdad **MV5** es consecuencia de (i) del Lema 8.1.5 y la **MV6** se deduce de **W3** y (c) del Lema 8.1.5. □

A partir de los teoremas 8.1.9 y 8.1.10 es posible probar el siguiente resultado.

Teorema 8.1.11. *Las variedades de las MV-álgebras y de las W-álgebras son definicionalmente equivalentes.*

Observación 8.1.12. En lo que sigue hablaremos de MV-álgebras, recurriendo cuando hiciera falta al 1, que es $\neg 0$ y a las operaciones de producto, implicación y diferencia como fueron definidas al principio.

Observemos que, a partir de las igualdades demostradas (ver Lema 8.1.6) se tienen las siguientes expresiones para el ínfimo y el supremo, que usaremos a lo largo de este capítulo:

$$\begin{aligned} x \vee y &= (x \odot \neg y) \oplus y, \\ x \wedge y &= x \odot (\neg x \oplus y). \end{aligned}$$

Observemos también que toda MV-álgebra tiene entonces una estructura subyacente de retículo acotado. Además, es fácil ver que

$$x \odot y \;\leq\; x \wedge y \;\leq\; x \vee y \;\leq\; x \oplus y.$$

Dado que la negación $\neg$ es una *involución* (es decir que vale **MV4**) resulta que la suma $\oplus$ y el producto $\odot$ son interdefinibles: se pasa de una propiedad de la suma a una del producto usando negaciones adecuadas. Por ejemplo, si $x \wedge y = 0$ entonces $\neg x \vee \neg y = 1$.

Veremos ahora algunas propiedades de la suma (equivalentes a sus duales del producto) que serán necesarias para demostrar teoremas posteriores.

Lema 8.1.13. *Sea $\langle A, \neg, \oplus, 0\rangle$ una MV-álgebra. La suma $\oplus$ tiene las siguientes propiedades:*

(M) Si $x \leq y$ y $t \in A$ entonces $x \oplus t \leq y \oplus t$ (monotonía),

(D) $x \oplus (y \wedge z) = (x \oplus y) \wedge (x \oplus z)$ (distributividad).

Demostración. La monotonía es consecuencia del ítem (vi) del Lema 8.1.5 tomando $t = \neg z$.

Usando la monotonía tenemos que $x \oplus (y \wedge z)$ es cota inferior de $x \oplus y$ y de $x \oplus z$. Veamos que es la máxima.

Sea $t \leq x \oplus y$ y $t \leq x \oplus z$. Probaremos que $t \leq x \oplus (y \wedge z)$.

Tenemos, por definición de $\leq$ en W-álgebras y el ítem (f) del Lema 8.1.7, que

$$\begin{aligned} t \leq x \oplus y \ \text{ si y solo si } \ & t \leq \neg x \rightarrow y \\ \text{si y solo si } \ & t \rightarrow (\neg x \rightarrow y) = 1 \\ \text{si y solo si } \ & (t \odot \neg x) \rightarrow y = 1 \\ \text{si y solo si } \ & t \odot \neg x \leq y. \end{aligned} \tag{1}$$

Análogamente, se puede probar que

$$t \leq x \oplus z \text{ si y solo si } t \odot \neg x \leq z. \tag{2}$$

Luego, de (1) y (2) resulta que $t \odot \neg x \leq y \wedge z$. Esto último es equivalente a $t \leq x \oplus (y \wedge z)$. □

Lema 8.1.14. *Para todo par de elementos de una MV-álgebra vale la siguiente igualdad:*

$$(x \ominus y) \wedge (y \ominus x) = 0.$$

Demostración. En la demostración usaremos las propiedades de asociatividad y conmutatividad de $\oplus$ y $\odot$, así como las siguientes igualdades:

$$\neg(u \ominus v) = \neg u \oplus v, \quad u \wedge v = u \odot (\neg u \oplus v) = v \odot (\neg v \oplus u), \quad u \odot \neg u = 0.$$

En particular tenemos que

$$\begin{aligned}(x \ominus y) \wedge (y \ominus x) &= (x \ominus y) \odot (\neg(x \ominus y) \oplus (y \ominus x))\\ &= (x \odot \neg y) \odot (\neg x \oplus y \oplus (y \ominus x))\\ &= x \odot (\neg y \odot (y \oplus t)),\end{aligned}$$

donde hemos llamado $t = \neg x \oplus (y \ominus x)$. Luego:

$$(x \ominus y) \wedge (y \ominus x) = x \odot (t \odot (\neg t \oplus \neg y)).$$

Como

$$x \odot t = x \odot (\neg x \oplus (y \ominus x)) = x \wedge (y \ominus x) = (y \ominus x) \odot (\neg(y \ominus x) \oplus x),$$

se tiene, por ser $\neg t = x \odot \neg(y \ominus x)$ y llamando $u = x \oplus \neg(y \ominus x)$:

$$\begin{aligned}(x \ominus y) \wedge (y \ominus x) &= ((y \ominus x) \odot (\neg(y \ominus x) \oplus x)) \odot (\neg t \oplus \neg y)\\ &= ((y \odot \neg x) \odot (x \oplus \neg(y \ominus x))) \odot (\neg t \oplus \neg y)\\ &= y \odot (\neg x \odot u) \odot (\neg t \oplus \neg y)\\ &= (\neg x \odot u) \odot (y \odot (\neg y \oplus \neg t))\\ &= (\neg x \odot u) \odot (\neg t \odot (t \oplus y))\\ &= \neg x \odot (x \odot \neg(y \ominus x)) \odot u \odot (t \oplus y)\\ &= (\neg x \odot x) \odot \neg(y \ominus x) \odot (u \odot (t \oplus y))\\ &= 0 \odot (\neg(y \ominus x) \odot (u \odot (t \oplus y)))\\ &= 0.\end{aligned}$$

□

Lema 8.1.15. *Sean A una MV-álgebra y $x, y \in A$ tales que $x \wedge y = 0$. Entonces:*

(a) Para todo z, $x \wedge (y \oplus z) = x \wedge z$,

(b) $nx \wedge ny = 0$, siendo $nx = x \oplus x \oplus \cdots \oplus x$ (n veces).

Demostración. Dejamos la prueba de (a) como ejercicio. Para probar (b) veamos en primer lugar que $nx \wedge ny = 0$ para $n = 2^k$.

Se tiene que $x = x \oplus (x \wedge y)$ y distribuyendo: $x = (x \oplus x) \wedge (x \oplus y) \geq 2x \wedge y$, pues por monotonía de la suma es $x \oplus y \geq y$. Luego: $0 = x \wedge y \geq 2x \wedge y$ y por lo tanto: $0 = 2x \wedge y$. Ahora tenemos: $y = y \oplus (2x \wedge y) = (y \oplus 2x) \wedge (y \oplus y)$ y tomando ínfimo con $2x$: $y \wedge 2x = (y \oplus 2x) \wedge 2y \wedge 2x$. Como $y \oplus 2x \geq 2x$ se deduce que: $0 = y \wedge 2x \geq 2y \wedge 2x$, de donde $0 = 2y \wedge 2x$. Análogamente se prueba $4x \wedge 4x = 0$, $8x \wedge 8x = 0$,... Finalmente, como $n \leq 2^n$ se tiene que $nx \wedge ny \leq 2^n x \wedge 2^n y = 0$, o sea $nx \wedge ny = 0$. □

8.2. Ideales, homomorfismos y congruencias

Una vez conocidas algunas propiedades básicas, demostraremos en esta sección que para toda MV-álgebra A existe una biyección entre los ideales y las congruencias de A. Mostraremos también algunas propiedades de los homomorfismos.

Definición 8.2.1. Sea $\langle A, \oplus, \neg, 0\rangle$ una MV-álgebra, I un subconjunto de A. Diremos que I es un *ideal* si se cumplen las siguientes condiciones:

(I1) $0 \in I$.

(I2) Si $x \leq y$, $y \in I$, entonces $x \in I$ (I decreciente).

(I3) Si $x, y \in I$ entonces $x \oplus y \in I$ (cerrado por suma).

En toda MV-álgebra hay al menos dos ideales: el $\{0\}$ y A. Los demás (si los hubiera) se llaman *propios*. Un ideal I se llama *primo* si es propio y si, para cada par de elementos $x, y \in A$ se tiene que $x \ominus y \in I$ o bien $y \ominus x \in I$.

Observación 8.2.2. Observemos que, considerando que toda MV-álgebra tiene estructura de retículo, la noción de ideal que acabamos de definir en general **no** coincide con la de ideal del correspondiente retículo. Por ejemplo, el subconjunto $J = (\frac{1}{3}]$ de la MV-álgebra $[0, 1]$ es un ideal del retículo pero no de la MV-álgebra, porque $\frac{1}{3} \oplus \frac{1}{3} = \frac{2}{3} \notin J$.

Pero la recíproca sí vale: todo ideal de una MV-álgebra es un ideal del retículo que ella induce. En efecto, dado un ideal I de una MV-álgebra A, el mismo es decreciente y cerrado por $\oplus$. De lo observado en la sección anterior (Observación 8.1.12), se deduce que para todo $x, y \in I$ se tiene $x \vee y \leq x \oplus y$. Luego, I es cerrado por $\vee$.

Ejemplos 8.2.3.

1. En la MV-álgebra $[0, 1]$ no hay ideales propios. En efecto, se puede probar, como en el caso de $J = (\frac{1}{3}]$, que ningún ideal es cerrado por $\oplus$.

2. En la MV-álgebra producto $[0, 1] \times [0, 1]$ los subconjuntos: $\{0\} \times [0, 1]$ y $[0, 1] \times \{0\}$ son ideales propios.

3. En el álgebra $\mathbf{C}$ de Chang, dada en la sección anterior, el conjunto $I = \{\perp, e, 2e, \ldots, ne \ldots\}$ de los elementos positivos es un ideal propio.

4. Sea A un álgebra de Boole. Hemos visto en el Capítulo 2 la biyección entre filtros y congruencias, que es equivalente a una biyección entre ideales y congruencias (ver Observación 2.3.15):

$$x \equiv_I y \text{ si y solo si } (x \wedge \overline{y}) \vee (y \wedge \overline{x}) \in I.$$

Considerando en A la estructura de MV-álgebra, podemos traducir esta condición como:

$$x \equiv_I y \text{ si y solo si } (x \odot \neg y) \oplus (y \odot \neg x) \in I.$$

Veremos en lo que sigue que esta condición puede generalizarse a una MV-álgebra cualquiera, permitiendo así establecer una biyección entre ideales y congruencias.

Observación 8.2.4. Sea $\langle A, \oplus, \neg, 0\rangle$ una MV-álgebra, R una relación de equivalencia en A. De acuerdo a lo visto en la Sección 3 del Capítulo 1, diremos que R es una *congruencia* en A si se cumple:

(C1) Si xRy entonces $\neg xR\neg y$,

(C2) Si xRy, uRv, entonces $(x \oplus u)R(y \oplus v)$.

Las operaciones definidas a partir de las dos básicas $\neg$ y $\oplus$ también se preservarán, es decir, vale lo siguiente:

Si xRy, uRv, entonces $(x \diamond u)R(y \diamond v)$, donde $\diamond$ puede ser reemplazado por $\rightarrow$, $\odot$ ó $\ominus$.

Definición 8.2.5. Dada una MV-álgebra A definimos la función *distancia* $d : A \times A \longrightarrow A$ por:

$$d(x, y) = (x \ominus y) \oplus (y \ominus x).$$

En un álgebra de Boole, como vimos, $d(x, y) = (x \wedge \overline{y}) \vee (y \wedge \overline{x})$. En el intervalo $[0, 1]$ se tiene que (¡probarlo!): $x \ominus y$ es el máximo entre $x - y$ y 0. Luego,

$$d(x,y) = \begin{cases} y - x, & \text{si } x \leq y, \\ x - y, & \text{si } x > y. \end{cases}$$

Dicho de otro modo, $d(x, y) = |x - y|$.

Lema 8.2.6. *La distancia en una MV-álgebra cumple las siguientes condiciones:*

(a) $d(x, y) = 0$ *si y solo si* $x = y$*,*

(b) $d(x, y) = d(y, x)$,

(c) $d(x, z) \leq d(x, y) \oplus d(y, z)$,

(d) $d(x, y) = d(\neg x, \neg y)$,

(e) $d(x \oplus s, y \oplus t) \leq d(x, y) \oplus d(s, t)$,

(f) $d(x, 0) = x$.

Demostración. Por la propiedad de monotonía de la suma, $d(x, y) = 0$ implica $x \ominus y = y \ominus x = 0$. Luego: $x \to y = y \to x = 1$, de donde $x \leq y, y \leq x$. Si $x = y$ entonces: $x \odot \neg y = x \odot \neg x = 0 = y \odot \neg x$, por lo que $d(x, y) = 0$. Hemos probado (a).

La simetría en la definición de d prueba (b).

Para probar (c) demostremos $\neg d(x, z) \geq \neg d(x, y) \odot \neg d(y, z)$, es decir:

$$(x \to z) \odot (z \to x) \geq (y \to x) \odot (x \to y) \odot (y \to z) \odot (z \to y).$$

Por (v) del Lema 8.1.5 y (f) del Lema 8.1.7, se tiene que:

$$(z \to y) \odot (y \to x) \leq (z \to x),$$

$$(x \to y) \odot (y \to z) \leq (x \to z).$$

Haciendo el producto miembro a miembro se obtiene lo pedido.

El punto (d) es inmediato por ser $\neg$ una involución (es decir, satisface que $\neg\neg x = x$ para todo x).

Para demostrar (e) probemos previamente las siguientes desigualdades:

$$\text{(I) } \neg(x \oplus y) \odot (s \oplus t) \leq (\neg x \odot s) \oplus (\neg y \odot t),$$

$$\text{(II) } \neg(s \oplus t) \odot (x \oplus y) \leq (\neg s \odot x) \oplus (\neg t \odot y).$$

Por la definición de $\leq$ se tiene que $a \leq b$ si y solo si $\neg a \oplus b = a \to b = 1$. Probemos entonces (I) de ese modo. Utilizaremos la propiedad $u \oplus (\neg u \odot v) = v \oplus (\neg v \odot u)$.

Comenzaremos probando (I). Primero notemos que

$$\neg(\neg(x \oplus y) \odot (s \oplus t)) \oplus (\neg x \odot s) \oplus (\neg y \odot t) = x \oplus y \oplus \neg(s \oplus t) \oplus \neg x \odot s \oplus \neg y \odot t.$$

Además,

$$\begin{aligned} x \oplus y \oplus \neg(s \oplus t) \oplus \neg x \odot s \oplus \neg y \odot t & \\ &= (x \oplus (\neg x \odot s)) \oplus (y \oplus (\neg y \odot t)) \oplus \neg(s \oplus t) \\ &= (s \oplus (\neg s \odot x)) \oplus (t \oplus (\neg t \odot y)) \oplus \neg(s \oplus t) \\ &= (\neg s \odot x) \oplus (\neg t \odot y) \oplus (s \oplus t) \oplus \neg(s \oplus t) \\ &= 1. \end{aligned}$$

Luego vale (I).

Análogamente se prueba:

$$\neg(\neg(s \oplus t) \odot (x \oplus y)) \oplus (\neg s \odot x) \oplus (\neg t \odot y) = 1,$$

lo que prueba (II). Sumando miembro a miembro (I) y (II) se obtiene lo que queríamos demostrar.

El punto (f) se deja como ejercicio. □

Si R es una congruencia en una MV-álgebra vamos a denotar por $|0|$ a la clase del 0.

Lema 8.2.7. *Sea I un ideal en una MV-álgebra A. La siguiente relación en A es una congruencia:*

$$x \equiv_I y \textit{ si y solo si } d(x,y) \in I.$$

Más aún, el ideal I es la clase del 0 de dicha congruencia.

Recíprocamente, si R es una congruencia entonces $|0|$ es un ideal. Más aún, $\equiv_{|0|}$ coincide con R.

Demostración. En la prueba nos referiremos a las propiedades (a),...,(e) del Lema 8.2.6.

Las propiedades reflexiva, simétrica y transitiva de $\equiv_I$ valen respectivamente por (a), (b) y (c).

Además, por (d) se tiene que $\equiv_I$ preserva $\neg$ y por (e) que preserva $\oplus$. Luego, $\equiv_I$ es una congruencia. El hecho de que $I = |0|$ se deduce de (f).

Probemos la recíproca. Si R es una congruencia entonces $0 \in |0|$. Veamos que $|0|$ es decreciente. Sean x, y tales que $x \leq y$, $y \in |0|$. En particular, $x \to y = \neg x \oplus y = 1$. Además, como $yR0$ y $\neg xR\neg x$ vale que $(y \oplus \neg x)R(0 \oplus \neg x)$. Es decir, $1R\neg x$, de donde se sigue que $0Rx$. Además, si $y, z \in |0|$ se tiene que $(y \oplus z) \in |0|$, es decir, $|0|$ es cerrado por $\oplus$. Hemos probado que si R es una congruencia entonces $|0|$ es un ideal.

Veamos por último que si $x, y \in A$ entonces $x \equiv_{|0|} y$ si y solo si xRy, o sea:

$$d(x,y) \in |0| \text{ si y solo si } xRy.$$

Supongamos que xRy. Como R es una congruencia tenemos que preserva $\odot$. Luego, $(x \odot \neg y)R(y \odot \neg y) = 0$, o sea, $(x \odot \neg y)R0$. Esto equivale a $(x \ominus y)R0$. Análogamente, $(y \ominus x)R0$, de donde $d(x,y)R0$.

Sea ahora $d(x,y)R0$. Entonces, $d(x,y) \oplus \neg(x \ominus y)R\neg(x \ominus y)$. Pero

$$\begin{aligned} d(x,y) \oplus \neg(x \ominus y) &= (y \ominus x) \oplus (x \ominus y) \oplus \neg(x \ominus y) \\ &= 1. \end{aligned}$$

Luego, $\neg(x \ominus y)R1$ y por lo tanto $(x \ominus y)R0$. De esto último deducimos que $y \oplus (x \ominus y) = (y \vee x)Ry$. Análogamente podemos probar que $(x \vee y)Rx$. Por ende, yRx. □

Observación 8.2.8. Sea A una MV-álgebra. Sean $\mathrm{Id}(A)$ el conjunto de los ideales de A y $\mathrm{Con}(A)$ el conjunto de las congruencias de A. El Lema 8.2.7 establece una aplicación de $\mathrm{Id}(A)$ en $\mathrm{Con}(A)$ dada por: $I \mapsto \equiv_I$. Además, se define en el mismo lema otra función de $\mathrm{Con}(A)$ en $\mathrm{Id}(A)$ por la asignación $R \mapsto |0|$. El teorema siguiente muestra que estas dos funciones son una inversa de la otra, estableciéndose entonces una biyección entre $\mathrm{Id}(A)$ y $\mathrm{Con}(A)$.

Teorema 8.2.9. *Sea A una MV-álgebra. Existe una biyección entre* $\mathrm{Id}(A)$ *y* $\mathrm{Con}(A)$.

Demostración. En el Lema 8.2.7 se probó que, dado un ideal I, $\equiv_I$ es una congruencia. Además, si tomamos la clase del 0 por dicha congruencia, ella coincide con I. Recíprocamente, se muestra que, dada una congruencia R, la clase del 0 por R, que llamamos $|0|$, es un ideal. También se prueba que la congruencia asociada a ese ideal es justamente R. □

Observación 8.2.10. Según hemos visto en los ejemplos 8.1.2, la MV-álgebra $[0,1]$ no tiene ideales propios. Luego, por el Teorema 8.2.9, es una MV-álgebra simple (ver Capítulo 7, Ejemplo 7.1.6).

Observación 8.2.11. Sean $\langle A, \oplus_A, \neg_A, 0_A \rangle$ y $\langle B, \oplus_B, \neg_B, 0_B \rangle$ MV-álgebras, $h : A \longrightarrow B$. Teniendo en cuenta lo visto en el Capítulo 1 sobre Álgebra Universal, se tiene que función h es un *homomorfismo* si preserva las operaciones $\neg$ y $\oplus$, es decir, si valen las siguientes condiciones:

(H1) $h(0_A) = 0_B$,

(H2) $h(\neg_A x) = \neg_B h(x)$,

(H3) $h(x \oplus_A y) = h(x) \oplus_B h(y)$.

Las operaciones $\rightarrow$, $\odot$ y $\ominus$, definidas a partir de las dos operaciones básicas $\neg$ y $\oplus$ también se preservarán. Como consecuencia, un homomorfismo de MV-álgebras preserva las operaciones $\wedge$ y $\vee$ del retículo subyacente a un MV-álgebra (que son también composición de operaciones). Es decir que resulta, en particular, un homomorfismo de retículos.

Llamaremos *núcleo* de h al conjunto

$$h^{-1}(\{0\}) = \{x : \ h(x) = 0\}.$$

El mismo será denotado por $\mathrm{Ker}(h)$.

Lema 8.2.12. *Sea $h : A \longrightarrow B$ un homomorfismo de MV-álgebras. Entonces valen las siguientes propiedades:*

(a) *Si J es un ideal de B entonces $h^{-1}(J) = \{x : h(x) \in J\}$ es un ideal de A. En particular,* $\mathrm{Ker}(h)$ *es un ideal de A.*

(b) *h es inyectiva si y solo si* $\mathrm{Ker}(h) = \{0\}$.

Demostración. La prueba de (a) es de rutina, teniendo en cuenta que h preserva 0, el orden y $\oplus$.

Probemos (b). Si h es inyectiva, es claro que $h(x) = 0$ implica $x = 0$. Veamos la recíproca. Sean x, y tales que $h(x) = h(y)$. Multiplicando ambos miembros de esta igualdad por $\neg h(y)$ obtenemos: $h(x) \ominus h(y) = 0$. Luego, $h(x \ominus y) = 0$. Por la hipótesis, esto implica $x \ominus y = 0$. Análogamente podemos probar que $y \ominus x = 0$, por lo que $d(x, y) = 0$. Luego, $x = y$, por (a) del Lema 8.2.6. $\square$

Lema 8.2.13. *Sea $h : A \longrightarrow B$ un homomorfismo suryectivo de MV-álgebras. Entonces valen las siguientes propiedades:*

(a) $B \cong A/\mathrm{Ker}(h)$,

(b) $\mathrm{Ker}(h)$ *es primo si y solo si B es totalmente ordenada.*

Demostración. Para demostrar (a), por el Teorema 1.3.20 visto en la sección 3.5 del Capítulo 1, basta probar que la congruencia R_h determinada por h coincide con la determinada por el ideal $\mathrm{Ker}(h)$.

$$
\begin{aligned}
xR_hy \ \text{ si y solo si } \ & hx = hy \\
\text{si y solo si } \ & hx \ominus hy = hy \ominus hx = 0 \\
\text{si y solo si } \ & h(x \ominus y) = h(y \ominus x) = 0 \\
\text{si y solo si } \ & (x \ominus y) \in \mathrm{Ker}(h),\ (y \ominus x) \in \mathrm{Ker}(h) \\
\text{si y solo si } \ & d(x, y) \in \mathrm{Ker}(h) \\
\text{si y solo si } \ & x \equiv_{\mathrm{Ker}(h)} y.
\end{aligned}
$$

$$
\begin{tikzcd}
A \arrow[r, "h"] \arrow[d, "p"'] & B \\
A/\mathrm{Ker}(h) \arrow[ur, "\widetilde{h}"'] &
\end{tikzcd}
$$

Veamos (b).

$$
\begin{aligned}
\mathrm{Ker}(h) \text{ primo} & \text{ si y solo si para todo } x, y \in A,\ x \ominus y \in \mathrm{Ker}(h) \text{ ó } y \ominus x \in \mathrm{Ker}(h)\\
& \text{ si y solo si para todo } x, y \in A,\ h(x \ominus y) = 0 \text{ ó } h(y \ominus x) = 0\\
& \text{ si y solo si para todo } x, y \in A,\ h(x) \ominus h(y) = 0 \text{ ó } h(y) \ominus h(x) = 0\\
& \text{ si y solo si para todo } x, y \in A,\ h(x) \leq h(y) \text{ ó } h(y) \leq h(x)\\
& \text{ si y solo si para todo } u, v \in B,\ u \leq v \text{ ó } v \leq u.
\end{aligned}
$$

Esto último, por ser h suryectiva. □

Llamaremos *MV-cadena* a una MV-álgebra totalmente ordenada.

8.3. Teorema de representación de Chang

En esta sección vamos a demostrar un importante teorema debido a C. C. Chang, que permite descomponer una MV-álgebra en función de MV-cadenas.

Para llegar al teorema mencionado debemos demostrar algunos resultados previos.

Teorema 8.3.1. *Una MV-álgebra A es producto subdirecto de una familia de MV-álgebras $\{A_i\}_{i\in I}$ si y solo si existe una familia de ideales $\{J_i\}_{i\in I}$ tales que*

(1) $A_i \cong A/J_i$ *para todo* i.

(2) $\bigcap_{i\in I} J_i = \{0\}$.

Demostración. Este teorema es la aplicación directa del Teorema 7.1.4 del Capítulo 7, teniendo en cuenta que la propiedad de separar puntos de la familia $(g_i)_{i\in I}$ es equivalente a que $\bigcap_{i\in I} R_i = \Delta$, siendo R_i la congruencia asociada a g_i, y también teniendo en cuenta que esta última condición equivale (en virtud del Lema 8.2.13, parte (a)) a que $\bigcap_{i\in I} \mathrm{Ker}(g_i) = \{0\}$, llamando aquí $J_i = \mathrm{Ker}(g_i)$. □

Corolario 8.3.2. *Una MV-álgebra A es producto subdirecto de una familia de MV-cadenas $\{A_i\}_{i\in I}$ si y solo si existe una familia de ideales primos $\{J_i\}_{i\in I}$ para la cual se satisfacen las condiciones (1) y (2) del Teorema 8.3.1.*

Demostración. Es consecuencia del Lema 8.2.13 de la Sección 2 y del Teorema 8.3.1. □

Lema 8.3.3. *Sea A una MV-álgebra, $\{J_s\}_{s\in S}$ una familia de ideales de A. Entonces:*

(i) *La intersección* $\bigcap_{s\in S} J_s$ *es un ideal de* A.

(ii) *Si para cada par* $s,t \in S$ *es* $J_s \subseteq J_t$ *o bien* $J_t \subseteq J_s$ *entonces* $\bigcup_{s\in S} J_s$ *es un ideal.*

(iii) *Dado un conjunto* Y *no vacío,* $Y \subseteq A$*, el conjunto*

$$[Y] = \{x \in A:\ x \leq y_1 \oplus \cdots \oplus y_n,\ \text{para } y_1, \ldots, y_n \in Y\}$$

es la intersección $\bigcap_{J\supseteq Y} J$*, es decir, el menor ideal que contiene a* Y.

Demostración. Para probar (i) observemos que $0 \in \bigcap_{s\in S} J_s$. Además, la intersección es decreciente y cerrada por $\oplus$ por serlo todos los J_s.

Veamos (ii). Es sencillo ver que la unión $\bigcup_{s\in S} J_s$ es no vacía y decreciente. Para ver que es cerrada por $\oplus$ tomemos $x, y \in \bigcup_{s\in S} J_s$. Luego, $x \in J_r$, $y \in J_t$. Supongamos sin pérdida de generalidad que $J_r \subseteq J_t$. Luego, $x, y \in J_t$ y la suma estará en J_t y por lo tanto en la unión.

Observemos, antes de probar (iii), que $\bigcap_{J\supseteq Y} J$ es efectivamente el menor ideal que contiene a Y. Por (i) es un ideal (que claramente contiene a Y). Si K es un ideal que contiene a Y entonces $K \supseteq \bigcap_{J\supseteq Y} J$.

Probemos ahora que $[Y]$ contiene a Y, que es un ideal y que es el mínimo. En efecto, para cada $y \in Y$ vale que $y \leq y$, de donde $y \in [Y]$, por lo que $[Y] \neq \emptyset$. Si $x \in [Y]$ existirán $y_1, \ldots, y_n \in Y$ tales que $x \leq y_1 \oplus \cdots \oplus y_n$; si tomamos $x' \leq x$, entonces también $x' \leq y_1 \oplus \cdots \oplus y_n$, de donde $x' \in [Y]$. Sean ahora $x, x' \in [Y]$ y veamos que $x \oplus x' \in [Y]$. Se tendrá $x \leq y_1 \oplus \cdots \oplus y_n$, $x' \leq y'_1 \oplus \cdots \oplus y'_n$ y, por monotonía de la suma, podemos sumar miembro a miembro y obtendremos: $x \oplus x' \leq (y_1 \oplus \cdots \oplus y_n) \oplus (y'_1 \oplus \cdots \oplus y'_n)$ por lo cual $x \oplus x' \in [Y]$. $\square$

Recordemos que $nx = x \oplus \ldots \oplus x$, donde x aparece n veces en la expresión del miembro derecho (ver 8.1.15).

Llamaremos a $[Y]$ el ideal *generado por* Y. En particular, puede probarse que, dados un ideal J y un elemento $z \in A$:

$$[J \cup \{z\}] = \{x \in A:\ x \leq nz \text{ para algún } n \in \mathbb{N}\}.$$

Teorema 8.3.4. *Sea* A *una MV-álgebra,* K *un ideal de* A*,* z *un elemento que no pertenece a* K. *Existe un ideal primo* P *que contiene a* K *y tal que* $z \notin P$.

Demostración. Sea $\mathcal{H} = \{J,\ J \text{ ideal},\ K \subseteq J,\ z \notin J\}$.

El conjunto $\mathcal{H}$ es no vacío, pues $K \in \mathcal{H}$.

Por (ii) del Lema 8.3.3, si se toma una cadena de ideales de $\mathcal{H}$ su unión resulta ser también un ideal de $\mathcal{H}$, luego toda cadena tiene máximo. Por el

Lema de Zorn (ver 2.6 en el Capítulo 2) resulta entonces que $\mathcal{H}$ tiene un elemento maximal P. Veamos que P es un ideal primo.

Supongamos que no lo es. Entonces existen $s, t \in A$ tales que $s \ominus t \notin P$ y $t \ominus s \notin P$. Consideremos el ideal J_1 generado por $P \cup \{s \ominus t\}$. Como vimos:

$$J_1 = \{x,\, x \leq p \oplus m(s \ominus t),\, p \in P,\, m \in \mathbb{N}\}.$$

Análogamente, sea J_2 el ideal generado por $P \cup \{t \ominus s\}$:

$$J_2 = \{x,\, x \leq q \oplus n(s \ominus t),\, q \in P,\, n \in \mathbb{N}\}.$$

Como $s \ominus t \in J_1 - P$, J_1 contiene propiamente a P y entonces también a K. Análogamente, J_2 contiene propiamente a P y a K. Por ser P maximal en $\mathcal{H}$, J_1 y J_2 no pueden estar en $\mathcal{H}$. Luego, debe ocurrir que $z \in J_1$ y $z \in J_2$. Luego, existen números naturales m y n, elementos p y q de P tales que

$$z \leq p \oplus m(s \ominus t), \quad z \leq q \oplus n(t \ominus s).$$

Si llamamos $r = p \oplus q$, $h = m + n$, se tiene que

$$z \leq r \oplus h(s \ominus t), \quad z \leq r \oplus h(t \ominus s),$$

de donde, por la distributividad (D) (ver Lema 8.1.13), se sigue que:

$$z \leq (r \oplus h(s \ominus t)) \wedge (r \oplus h(t \ominus s)) = r \oplus (h(t \ominus s) \wedge h(s \ominus t).$$

Por los lemas 8.1.14 e 8.1.15 tenemos que

$$h(t \ominus s) \wedge h(s \ominus t) = 0.$$

Luego $z \leq r$, de donde $z \in P$, lo cual es absurdo.

Por lo tanto P es primo. □

Corolario 8.3.5. *Todo ideal propio de una MV-álgebra es intersección de ideales primos.*

Demostración. Sea J ideal de A. Sea, para cada $x \notin J$, P_x el ideal primo dado por el Teorema 8.3.4. Probemos:

$$J = \bigcap_{x \notin J} P_x$$

Si $y \notin J$ entonces $y \notin P_y$, por la forma en que se eligió P_y. Luego, $y \notin \bigcap P_x$.

Recíprocamente, si $y \notin \bigcap P_x$, entonces existe $x \notin J$ tal que $y \notin P_x$. Entonces $y \notin J$, pues $J \subseteq P_x$. □

Teorema 8.3.6 (Teorema de representación de Chang)**.** *Toda MV-álgebra es producto subdirecto de MV-cadenas.*

Demostración. Dada un MV-álgebra A, tomemos el ideal $\{0\}$. Por el Corolario 8.3.5, $\{0\} = \bigcap_{x \neq 0} P_x$. Además, por el Corolario 8.3.2, A es producto subdirecto de la familia $\{A/P_x\}_{x \neq 0}$, donde cada A/P_x es una MV-cadena. □

8.4. MV-ecuaciones

Estudiaremos ahora los términos y ecuaciones en la variedad de las MV-álgebras.

Según lo visto en la Definición 7.2.1 del Capítulo 7, los MV-términos en n variables $\{x_1, \ldots, x_n\}$ son los obtenidos a partir de 0, $x_1, \ldots, x_n$, teniendo en cuenta que si t y u son términos entonces $\neg(t)$, $\neg(u)$ y $(t \oplus u)$ son términos y que todos los términos se obtienen de esa forma en un número finito de pasos. Se suprimirán paréntesis si eso no da lugar a ambigüedad. Por ejemplo, $\neg t \oplus u$ significará $(\neg(t) \oplus u)$.

Las funciones término se definen aplicando análogamente la Definición 7.2.3 del Capítulo 7. Llamaremos MV-ecuaciones a las ecuaciones de la forma $t \approx u$, para t y u MV-términos. Diremos que una MV-álgebra A satisface la ecuación $t \approx u$ si las funciones término t^A y u^A coinciden. La notación que usaremos en este caso es la siguiente: $A \vDash t \approx u$. Si toda MV-álgebra satisface la ecuación entonces escribiremos $\mathcal{MV} \vDash t \approx u$. Por ejemplo, $\mathcal{MV} \vDash \neg x \oplus x \approx \neg 0$ y $\mathcal{MV} \vDash x \oplus y \approx y \oplus x$. Hemos definido los símbolos 1, $x \to y$, $x \odot y$ como abreviaturas de, respectivamente, $\neg 0$, $\neg x \oplus y$ y $\neg(\neg x \oplus \neg y)$. Por esta razón también serán MV-ecuaciones $x \odot \neg y \approx \neg(x \to y)$ y $(x \odot \neg y) \oplus y \approx (y \odot \neg x) \oplus x$, por ejemplo. Todas las MV-ecuaciones anteriores valen en todas las MV-álgebras. También $x \wedge (y \oplus z) \approx x \wedge z$ y $x \oplus x \approx x$ son MV-ecuaciones, sin embargo no son válidas en general.

Teorema 8.4.1. *Sea A una MV-álgebra que es producto subdirecto de la familia $(A_i)_{i \in I}$ de MV-álgebras, sea $t \approx u$ una MV-ecuación. Entonces*
$A \vDash t \approx u$ si y solo si $A_i \vDash t \approx u$ para todo $i \in I$.

Demostración. Es consecuencia del Corolario 7.4.6 del Capítulo 7. □

Corolario 8.4.2. *Una MV-ecuación vale en toda MV-álgebra si y solo si vale en toda MV-cadena.*

Demostración. Se deduce del Teorema 8.3.6 de la Sección 3 (teorema de Chang). □

8.5. MV-álgebras y ℓ-grupos

En esta sección delinearemos algunos resultados que muestran la importante vinculación entre los *grupos reticulados* o ℓ-grupos munidos de un elemento distinguido llamado *unidad fuerte* con las MV-álgebras. Esta vinculación, que resulta ser un funtor (ver Sección 1 del Capítulo 6) permite optimizar el Corolario 8.4.2, demostrando el siguiente teorema de completud:

Una ecuación es válida en toda MV-álgebra si y solo si es válida en $[0,1]$.

En primer lugar, en 1959 Chang asoció a una MV-cadena un ℓ-grupo totalmente ordenado con unidad fuerte y recíprocamente. A partir de esa construcción probó un teorema de completud, que profundiza el Corolario 8.4.2. Posteriormente, en 1986, D. Mundici generalizó la construcción de Chang a ℓ-grupos con unidad fuerte y MV-álgebras, definiendo el funtor Γ entre las categorías respectivas. Para los enunciados que involucran teoría de categorías nos basaremos en las definiciones del Capítulo 6.

En 1998 R. Cignoli y D. Mundici demostraron el mencionado teorema de completud.

Recorreremos, por ser más intuitivo, el camino que llevó a Chang a demostrar su teorema de completud (sin entrar en detalles) y enunciaremos los resultados de Cignoli y Mundici.

Definición 8.5.1. Un *grupo reticulado abeliano* o *ℓ-grupo* es un álgebra $\langle G, +, -, \vee, \wedge, 0\rangle$ tal que:

(a) el reducto $\langle G, +, -, 0\rangle$ es un grupo abeliano,

(b) el reducto $\langle G, \vee, \wedge\rangle$ es un retículo,

(c) para $x, y, z \in G$ se verifica la identidad $(x \vee y) + z = (x + z) \vee (y + z)$.

En el caso particular en que el orden del retículo sea un orden total, se llamará *grupo totalmente ordenado*, abreviadamente, *o-grupo*.

A menudo denotaremos (ver Observación 1.3.3) a un ℓ-grupo mencionando solo su conjunto subyacente.

Lema 8.5.2. *En todo ℓ-grupo valen:*

$$z + (x \wedge y) = (z + x) \wedge (z + y), \tag{8.1}$$
$$z - (x \vee y) = (z - x) \wedge (z - y), \tag{8.2}$$
$$z - (x \wedge y) = (z - x) \vee (z - y). \tag{8.3}$$

Hablaremos más sobre ℓ-grupos en el Capítulo 11.

Supondremos que los ℓ-grupos de los que hablaremos son abelianos, y en adelante suprimiremos la palabra "abeliano".

Dado que está definida por ecuaciones, la clase de los ℓ-grupos constituye una variedad, que llamaremos $\mathcal{L}G$.

Sea x un elemento de un ℓ-grupo G. Denotaremos $\|x\|$ al *módulo de x*, definido por: $\|x\| = x \vee -x$.

Una *unidad fuerte* u de un ℓ-grupo G es un elemento $0 \leq u$ tal que para cada $x \in G$ existe un número natural $n \geq 0$ que verifica: $\|x\| \leq nu$, donde $nu = u + \cdots + u$ (n veces).

Un homomorfismo de ℓ-grupos o *ℓ-homomorfismo* es una aplicación que preserva las operaciones: $+, -, \vee, \wedge, 0$. Si se tiene un homomorfismo $h : G \longrightarrow H$ entre dos grupos con unidades fuertes u y v respectivamente y $h(u) = v$, decimos que h es un ℓ-homomorfismo *unital*.

Se puede probar que la clase de los ℓ-grupos con unidad fuerte no es ecuacional. Intuitivamente, esto ocurre ya que la condición de unidad fuerte no está dada por una ecuación.

Ejemplos 8.5.3.

1. El conjunto $\mathbb{Z}$ de los números enteros con su estructura de grupo y su orden es el ejemplo emblemático de ℓ-grupo, más aún, de o-grupo. ¿Por qué "emblemático"? Porque cualquier ℓ-grupo puede ser obtenido a partir de $\mathbb{Z}$ por medio de los operadores que caracterizan una variedad: tomar productos, subálgebras e imágenes homomorfas. Dicho de otra manera, $\mathbb{Z}$ *genera* la variedad $\mathcal{L}G$. Además, se prueba que todo ℓ-grupo libre es producto subdirecto de copias de $\mathbb{Z}$ (ver [1, Th. 6.1]).

2. Los conjuntos $\mathbb{Q}$ y $\mathbb{R}$ de los números racionales y reales respectivamente tienen análogamente una estructura de o-grupo. Cada uno de ellos genera también la variedad $\mathcal{L}G$.

3. El ℓ-grupo $\mathbb{Z}\times\mathbb{Z}$ es libremente generado por el único generador $(-1, 1)$.

La siguiente definición fue dada inicialmente por Chang para o-grupos y generalizada luego por Mundici (ver [23, Capítulo 2]).

Definición 8.5.4. Sea $\langle G, +, -, \vee, \wedge, 0\rangle$ un ℓ-grupo, u un elemento $u > 0$. Sea

$$[0, u] = \{x \in G : \ 0 \leq x \leq u\},$$

y definimos para cada $x, y \in [0, u]$ las siguientes operaciones:

$$x \oplus y = u \wedge (x + y), \quad \neg x = u - x.$$

Denotaremos $\Gamma(G, u) = \langle [0, u], \oplus, \neg, 0\rangle$.

Lema 8.5.5. $\Gamma(G, u)$ *es una MV-álgebra.*

Demostración. Las propiedades **MV1**,...,**MV6** se deducen de (a), (b), (c) de la Definición 8.5.1, y (8.1), (8.2) y (8.3) del Lema 8.5.2. Detallaremos la deducción de **MV6**.

$$\begin{aligned}\neg(\neg x \oplus y) \oplus y &= (u - ((u - x + y) \wedge u) + y) \wedge u \\ &= (((u - (u - x + y)) \vee (u - u)) + y) \wedge u \\ &= (((x - y) \vee 0) + y) \wedge u \\ &= (x \vee y) \wedge u \\ &= x \vee y.\end{aligned}$$

Análogamente,

$$\neg(\neg y \oplus x) \oplus x = y \vee x.$$

Luego, vale **MV6**. □

Ejemplos 8.5.6. Vamos a "reencontrar" ejemplos de MV-álgebra dados al principio, ahora bajo la forma $\Gamma(G, u)$. En realidad, como después veremos, **toda** MV-álgebra es isomorfa a una de esa forma.

1. Sean $G = \mathbb{R}$, $u = 1$. Entonces $\Gamma(\mathbb{R}, 1)$ no es otra cosa que $[0, 1]$ con la estructura de MV-álgebra que ya conocemos.

2. Dada una fracción $1/n$, para $n \in \mathbb{N}$, $n \neq 0$, podemos dotar al conjunto $\mathbb{Z}_{1/n} = \{z/n,\ z \in \mathbb{Z}\}$ de una estructura de grupo aditivo con las operaciones heredadas de los racionales. Entonces $\Gamma(\mathbb{Z}_{1/n}, 1) = \text{Ł}_{n+1}$, como es fácil comprobar.

3. Un caso particular del anterior se obtiene para $n = 1$. Se tiene $\mathbb{Z}_{1/1} = \mathbb{Z}$ y $\Gamma(\mathbb{Z}, 1) = \text{Ł}_2 = \mathbf{2}$.

Teorema 8.5.7. *Sea $\mathcal{C}_{LGu}$ la categoría cuyos objetos son los pares (G, u), donde G es un ℓ-grupo, u una unidad fuerte de G y cuyos morfismos son los ℓ-homomorfismos unitales. Sea $\mathcal{C}_{MV}$ la categoría cuyos objetos son las MV-álgebras y cuyos morfismos son los homomorfismos de MV-álgebras. Entonces, si definimos, para un ℓ-homomorfismo unital h, $\Gamma(h) = h\ |_{[0,u]}$ (h restringido a $[0, u]$), Γ es un funtor de $\mathcal{C}_{LGu}$ en $\mathcal{C}_{MV}$.*

Demostración. Las tres condiciones que debe cumplir Γ (ver Capítulo 6, Sección 1) pueden verificarse sin dificultad por ser $\Gamma(h)$ restricción de h. □

El funtor Γ determina, en realidad, una equivalencia entre las categorías $\mathcal{C}_{LGu}$ y $\mathcal{C}_{MV}$. Para ver eso, se necesita un funtor "de vuelta" de $\mathcal{C}_{MV}$ en $\mathcal{C}_{LGu}$ con los correspondientes isomorfismos naturales.

En los ejemplos que hemos visto, el grupo que consideramos para tomar Γ es un o-grupo. Ese caso fue el que consideró inicialmente Chang para mostrar que es posible recuperar el grupo mediante una construcción que consiste en "pegar bien" sucesivas copias de una MV-cadena dada A. Llamaremos G_A al grupo así obtenido, que es un o-grupo con unidad fuerte. De esta manera dado un grupo G con unidad fuerte u obtenemos $\Gamma(G, u)$ y a partir de esta el grupo $G_{\Gamma(G,u)}$ que resulta ser isomorfo a G preservando las unidades. Por otra parte, dada una MV-cadena A podemos tomar G_A con su unidad u. Si calculamos $\Gamma(G_A, u)$ obtenemos una MV-cadena isomorfa a A.

Definición 8.5.8. Sea A una MV-cadena. Definimos G_A por:

$$G_A = \{(n, x) : \; n \in \mathbb{Z}, \, x \in A - \{1\}\},$$

con el orden lexicográfico y las siguientes operaciones:

$$(m, x) + (n, y) = \begin{cases} (n + m, x \oplus y), & \text{si } x \oplus y < 1, \\ (n + m + 1, x \odot y), & \text{si } x \oplus y = 1 \end{cases}$$

$$-(n, x) = \begin{cases} (-n, 0), & \text{si } x = 0, \\ (-(n+1), \neg x), & \text{si } 0 < x < 1. \end{cases}$$

Supongamos que A es $[0, 1]$. Entonces G_A es de la forma mostrada en la Figura 8.3.

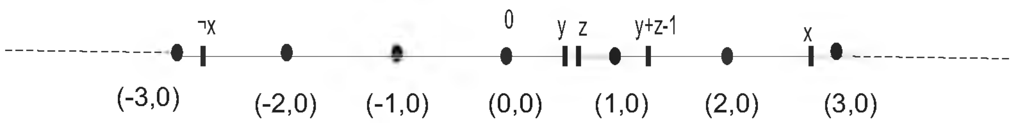


Figura 8.3: $G_{[0,1]}$

Dado $x \in G_A$, $\neg x$ es el simétrico de x respecto de $(0, 0)$. Entre $(0, 0)$ y $(1, 0)$ está la primera copia de $[0, 1]$. Si sumamos elementos de la forma $(0, x) + (0, y)$ obtendremos $(0, x + y)$, mientras $x + y < 1$. Si $x + y = 1$ obtendremos $(1, 0)$ y pasamos a la segunda copia. Si $x + y > 1$ obtendremos $(1, (x + y - 1))$, dentro de la segunda copia. Por ejemplo:

$$(0, \frac{1}{3}) + (0, \frac{1}{2}) = (0, \frac{5}{6}),$$

$$(0, \frac{1}{3}) + (0, \frac{2}{3}) = (1, 0),$$

$$(0, \frac{1}{3}) + (0, \frac{5}{6}) = (1, \frac{1}{6}).$$

Teorema 8.5.9. *Sea A una MV-cadena. Entonces, $\langle G_A, +, -, \wedge, \vee, (0,0)\rangle$ es un o-grupo con unidad fuerte $(1,0)$ y $\Gamma(G_A, (1,0))$ es isomorfa a A.*

Teorema 8.5.10. *Sea G un o-grupo con unidad fuerte u, sea $H = G_{\Gamma(G,u)}$. Entonces, $(1,0)$ es una unidad fuerte de H y existe un isomorfismo unital de G en H.*

A fin de generalizar estos resultados, como primer paso se construye el grupo G_A en el caso en que A es una MV-álgebra cualquiera (ver [23, Capítulo 2]). Esa construcción se extiende a los morfismos, quedando así definido un funtor de la categoría $\mathcal{C}_{MV}$ en la categoría $\mathcal{C}_{LGu}$ (ver [23, Capítulo 7]), que es el funtor "de vuelta" que habíamos mencionado. Se prueba que ambos funtores determinan una equivalencia categorial.

Teorema 8.5.11. *Las categorías $\mathcal{C}_{MV}$ y $\mathcal{C}_{LGu}$ son equivalentes.*

Parte de este teorema se usa para vincular MV-ecuaciones con ecuaciones en los ℓ-grupos y de esa manera se llega a demostrar el importante Teorema de Completud algebraica siguiente.

Teorema 8.5.12 (Chang, Cignoli, Mundici, [22])**.** *Una ecuación vale en $[0,1]$ si y solo si vale en toda MV-álgebra.*

8.6. MV-álgebras libres

En base al Teorema de Completud 8.5.12, vamos a mostrar en esta sección una descripción de la MV-álgebra libre $\mathbb{F}_n$ con n generadores, como subálgebra de la MV-álgebra de funciones: $[0,1]^{[0,1]^n}$. Los elementos de $\mathbb{F}_n$ son las llamadas *funciones de McNaughton*, que son funciones continuas y lineales a trozos, y cada una de las lineales tiene coeficientes enteros. Los resultados pueden generalizarse extendiendo el dominio de las funciones al producto infinito numerable del intervalo $[0,1]$ por sí mismo $[0,1]^{\mathbb{N}}$ (*cubo de Hilbert*) y considerando funciones de McNaughton con dominio en este producto; en efecto, en el Capítulo 9 probaremos que el álgebra de Lindenbaum del Cálculo Proposicional Ł de Łukasiewicz es isomorfa a la MV-álgebra de las funciones de McNaughton sobre el cubo de Hilbert.

Hemos hablado en la Sección 4 de los MV-términos sobre un conjunto de variables $X = \{x_1, \ldots, x_n\}$ y de sus correspondientes funciones término en cada MV-álgebra. Observemos que al término constante 0 corresponde la función término constante igual a 0 y a cada variable x_i la proyección i-ésima π_i. Las demás funciones término se obtienen a partir de las proyecciones aplicando sucesivamente las operaciones $\neg$ y $\oplus$. Es decir que el conjunto de proyecciones genera el conjunto de funciones término.

Consideremos ahora las funciones término de n variables en $[0,1]$. Sea

$$Proy_n^{[0,1]} = \{\pi_1, \ldots, \pi_n\}$$

el conjunto de las proyecciones y sea

$$\mathrm{T}_n^{[0,1]}(X)$$

el conjunto de las funciones término de n variables definidas en $[0,1]$. En dicho conjunto podemos definir las operaciones $\neg$ y $\oplus$ de manera de obtener una MV-álgebra.

Teorema 8.6.1. *El álgebra $T_n^{[0,1]}(X)$ es la MV-álgebra libremente generada por $Proy_n^{[0,1]}$.*

Demostración. Debemos probar que para toda MV-álgebra B y toda aplicación $f : Proy_n^{[0,1]} \longrightarrow B$ existe un homomorfismo $\widetilde{f} : \mathrm{T}_n^{[0,1]}(X) \longrightarrow B$ que extiende f.

$$\begin{tikzcd} Proy_n^{[0,1]} \arrow[r, "f"'] \arrow[d, "inc"] & B \\ \mathrm{T}_n^{[0,1]}(X) \arrow[ur, "\widetilde{f}"'] & \end{tikzcd}$$

Sean: $f(\pi_1) = b_1, \ldots, f(\pi_n) = b_n$. Para cada $t \in \mathrm{T}_n^{[0,1]}(X)$ definimos

$$\widetilde{f}(t^{[0,1]}) = t^B(b_1, \ldots, b_n).$$

Esta función está bien definida porque, usando el Teorema de Completud 8.5.12, si t y s son términos tales que sus funciones $t^{[0,1]}$ y $s^{[0,1]}$ coinciden, entonces t y s coinciden en toda MV-álgebra B. Es de rutina probar que $\widetilde{f}$ es un homomorfismo. $\square$

Veamos ahora que entre los elementos de $[0,1]^{[0,1]^n}$, las que son funciones término son exactamente las que tienen una forma determinada y “bonita”: son las funciones de McNaughton.

Definición 8.6.2. Sea $f : [0,1]^n \longrightarrow [0,1]$. Diremos que f es una *función de McNaughton* si satisface las siguientes condiciones:

(i) f es continua con respecto a la topología natural de $[0,1]$,

(ii) existen polinomios de grado 1, p_i, $i = 1, \ldots, k$,

$$p_i(x_0, \ldots, x_{n-1}) = b_i + m_{i0}x_0 + \cdots + m_{i(n-1)}x_{n-1},$$

$b_i, m_{i0}, \ldots, m_{i(n-1)} \in \mathbb{Z}$, tales que para cada elemento $(y_0, \ldots, y_{n-1}) \in [0,1]^n$ existe i para el cual vale que $f(y_0, \ldots, y_{n-1}) = p_i(y_0, \ldots, y_{n-1})$.

Definición 8.6.3. El *cubo de Hilbert* es el producto infinito numerable del intervalo $[0,1]$ por sí mismo: $[0,1]^{\mathbb{N}}$, es decir, es el conjunto de las sucesiones de números del intervalo $[0,1]$.

Denotaremos $[0,1]^\omega$ al cubo de Hilbert.

Una función $g : [0,1]^\omega \longrightarrow [0,1]$ es una *función de McNaughton sobre el cubo de Hilbert* si existe un $n \in \mathbb{N}$ y una función de McNaughton $f : [0,1]^n \longrightarrow [0,1]$ tal que $g(x) = f(x_1, \ldots x_n)$ para todo $x \in [0,1]^\omega$.

Observación 8.6.4. Se tiene que $\mathrm{T}_n^{[0,1]}(X)$ es libremente generada por las n proyecciones. Como ya hemos visto (Capítulo 1), $\mathbb{F}_n$ es entonces isomorfa a $\mathrm{T}_n^{[0,1]}(X)$, podemos decir que "es" $\mathrm{T}_n^{[0,1]}(X)$.

Teorema 8.6.5. *La MV-álgebra libre con n generadores está contenida en el conjunto de funciones de McNaughton de n variables.*

Demostración. Bastaría probar que las proyecciones y la constante 0 son funciones de McNaughton (lo que es evidente) y que el conjunto de tales funciones es cerrado por $\neg$ y por $\oplus$, lo cual no es difícil de verificar. Pero entonces la subálgebra de $[0,1]^{[0,1]^n}$ generada por las proyecciones, que es $\mathrm{T}_n^{[0,1]}(X)$, está contenida en el conjunto de funciones de McNaughton. □

La recíproca de este teorema requiere mucho trabajo técnico y solo veremos algunos detalles de la prueba para el caso $n = 1$.

El siguiente lema vale para un n cualquiera. Veremos una idea de la demostración para $n = 1$.

Lema 8.6.6 (McNaughton). *Sea g una función lineal con coeficientes enteros, o sea:*

$$g(x_0, \ldots, x_{n-1}) = b + m_0x_0 + \cdots + m_{(n-1)}x_{n-1},$$

$b, m_0, \ldots, m_{(n-1)} \in \mathbb{Z}$. *Entonces existe un término t tal que $g^\sharp = t^{[0,1]}$, siendo $g^\sharp = (g \vee 0) \wedge 1$.*

Demostración. Sea $g(x) = b + mx$, con b, m enteros.

Si $m = 0$, $g^\sharp$ será el término constante 0 o el 1.

Sea $m > 0$. Se demuestra que, si definimos $z(x) = g(x) - x$, entonces vale la siguiente igualdad:

$$(s)\ g^{\sharp} = (z^{\sharp} \oplus x) \odot (z+1)^{\sharp}.$$

A partir de ahí la demostración se hace por inducción sobre m, ya que $z = b + (m-1)x$ y $z + 1 = (b+1) + (m-1)x$.

Para $m < 0$ basta tomar $1 - g$, ya que $g^{\sharp} = 1 - (1-g)^{\sharp}$. □

Veamos algunos ejemplos de aplicación del Lema 8.6.6.

Ejemplos 8.6.7.

1. Calculemos, para un n natural, $(nx)^{\sharp}$ y $(1 - nx)^{\sharp}$.

   Si $g(x) = x$, entonces $g^{\sharp} = g$. Si $g(x) = 2x = x \oplus x$, entonces $z = z^{\sharp} = x$, $z + 1 = x + 1$, por lo que $(z+1)^{\sharp} = 1$. Reemplazando en la fórmula (s):

   $$(2x)^{\sharp} = (x \oplus x) \odot 1 = x \oplus x = 2x.$$

   A partir de esto se obtiene inductivamente: $(nx)^{\sharp} = nx$. Además, $(1-x)^{\sharp} = 1 - x^{\sharp} = \neg x$, y en general: $(1 - nx)^{\sharp} = 1 - (nx)^{\sharp} = \neg(nx)^{\sharp}$, como se ve en la Figura 8.4.

2. Veamos cuál puede ser la función g tal que $g^{\sharp} = x \odot x$.

   En $[0,1]$ se tiene que $x \odot x = 1 - ((1-x) \oplus (1-x))$. Luego, intuitivamente debe ser $(2x-1)^{\sharp} = x \odot x$. Probemos que es así. Si es $g = 2x - 1$, entonces $z = x - 1$ y por lo tanto $z^{\sharp} = 0$ y $(z+1)^{\sharp} = x$. Reemplazando en la fórmula (s):

   $$(2x-1)^{\sharp} = (0 \oplus x) \odot x = x \odot x.$$

   Análogamente se tiene que $x \odot x \odot x = 1 - ((1-x) \oplus (1-x) \oplus (1-x))$, de donde nuestro candidato para g es $3x - 2$. Nuestro z es entonces $z = 2x - 2$ de donde $z^{\sharp} = 0$ y $(z+1)^{\sharp} = (2x-1)^{\sharp} = x \odot x$. Por lo tanto:

   $$(3x-2)^{\sharp} = x \odot (x \odot x).$$

   Así siguiendo, se tiene que $x \odot \cdots \odot x = x^n = (nx - (n-1))^{\sharp}$, como se ve en la Figura 8.4.

Sigamos acercándonos a la demostración del recíproco del Teorema 8.6.5 para $n = 1$. Necesitamos conocer las siguientes definiciones.

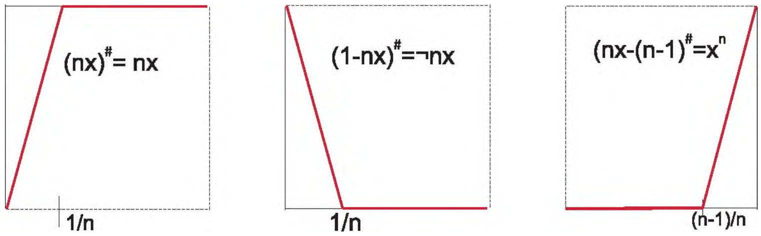


Figura 8.4: Ejemplos

Definición 8.6.8. Las *sucesiones de Farey* son conjuntos finitos de números racionales positivos y menores o iguales que 1. Se definen inductivamente a partir de la sucesión inicial $F_0 = \{0, 1\}$. Cada sucesión se obtiene a partir de la anterior intercalando entre $\frac{a}{b}$ y $\frac{c}{d}$ la fracción $\frac{a+c}{b+d}$.

Son las siguientes:

$$F_0 = \{0, 1\},$$
$$F_1 = \{0, \frac{1}{2}, 1\},$$
$$F_2 = \{0, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, 1\},$$
$$F_3 = \{0, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, 1\}, \ldots$$

Estas sucesiones tienen interesantes propiedades, como la “unimodularidad”: siendo $\frac{a}{b}$ y $\frac{c}{d}$ dos fracciones sucesivas se verifica $cb - ad = 1$. Además, cada fracción irreducible está en alguna de las sucesiones F_i.

Definición 8.6.9. Supongamos que tenemos los números de una sucesión de Farey F_k:

$$0 < d_1 < \cdots < d_{j-1} < d_j < d_{j+1} < \cdots < d_s < 1,$$

siendo $d_j = \frac{c}{d}$. Un *sombrero de Schauder* es una función h_{ki} de la forma mostrada en la Figura 8.5.

En la Figura 8.6 damos todos los sombreros de Schauder correspondientes a la sucesión de Farey F_2.

Observación 8.6.10. Cada sombrero de Schauder puede ser obtenido tomando supremos e ínfimos de a lo sumo cuatro funciones lineales con coeficientes enteros. Luego, por el Lema 8.6.6 y por ser los ínfimos y supremos expresables en función de los conectivos de la MV-álgebra (ver Observación 8.1.12), podemos ver que para cada uno de ellos existirá un término t tal que $h_{ki} = t^{[0,1]}$.

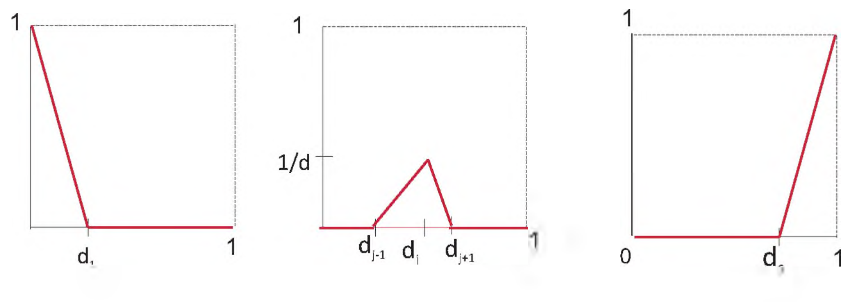


Figura 8.5: Sombreros de Schauder

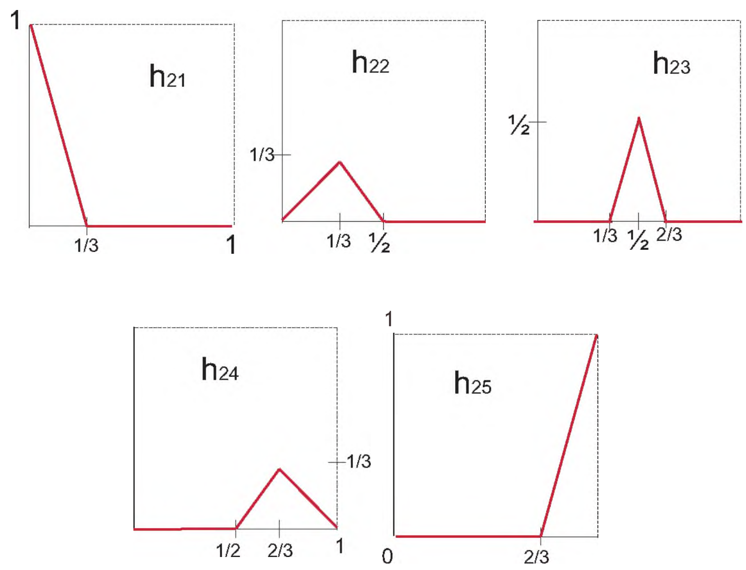


Figura 8.6: Schauder$_2$

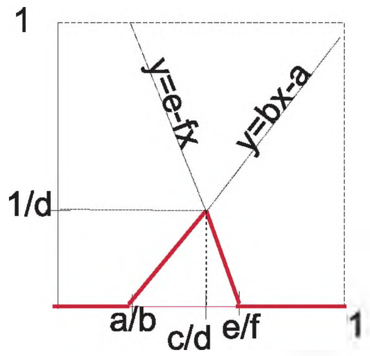


Figura 8.7: Funciones lineales

Analicemos ahora el ejemplo de la Figura 8.7.

Suponemos que $a/b, c/d$ y e/f son fracciones sucesivas de una sucesión de Farey. Por lo tanto: $cb - ad = 1$ y $ed - cf = 1$, por la unimodularidad. Teniendo en cuenta esto, la ecuación de la recta que pasa por los puntos $(a/b, 0)$ y $(c/d, 1/d)$ es $y = bx - a$ y la de la recta que pasa por $(e/f, 0)$ y $(c/d, 1/d)$ es $y = e - fx$, como se muestra en la figura. Si llamamos f_1 a la recta $y = 0$, f_2 a la de ecuación $y = bx - a$ y f_3 a $y = e - fx$ podemos comprobar que el sombrero de Schauder h de la figura verifica: $h = f_1 \vee (f_2 \wedge f_3)$.

Con los elementos que tenemos, veamos ahora una idea de la prueba de la recíproca del Teorema 8.6.5 para el caso $n = 1$.

Teorema 8.6.11. *El conjunto de funciones de McNaughton de una variable está contenido en la MV-álgebra libre con* 1 *generador.*

Demostración. Sea f una función de McNaughton de 1 variable. Existirá un conjunto finito A de fracciones irreducibles: $0 < a_1 < a_2 < \cdots < a_t < 1$ tales que f es lineal en cada intervalo $[a_r, a_{r+1}]$. Podemos tomar entonces una sucesión de Farey F_j que incluya a los elementos de A. Consideramos entonces los sombreros de Schauder h_{ji}, $i = 1, \ldots, q$ asociados a dicha sucesión. Por la observación 8.6.10 cada uno de ellos coincide con una función término $t_{ji}^{[0,1]}$ de una variable, o sea, está en el álgebra libre.

Nuestra función f es lineal en cada intervalo de los determinados por la sucesión de Farey F_j. Para cada $\frac{m_r}{n_r}$ de F_j el valor de $f(\frac{m_r}{n_r})$ debe ser racional y además, por tener f coeficientes enteros, será de la forma $f(\frac{m_r}{n_r}) = \frac{c_r}{n_r}$ para cierto entero c_r. Pero tenemos algún sombrero de Schauder h_{jr} tal que $h_{jr}(\frac{m_r}{n_r}) = \frac{1}{n_r}$. Luego, $f(x) = c_r h_{jr}(x)$, para $x = \frac{m_r}{n_r}$.

Entonces podemos ver que f resulta ser la siguiente combinación lineal:

$$f = c_1 h_{j1} + c_2 h_{j2} + \cdots + c_q h_{jq}.$$

Como $f \leq 1$ se puede sustituir la suma por la suma truncada:

$$f = (h_{j1} \oplus h_{j1} \oplus \cdots \oplus h_{j1}) \oplus (h_{j2} \oplus \cdots \oplus h_{j2}) \oplus \cdots \oplus (h_{jq} \oplus \cdots \oplus h_{jq}),$$

donde en el primer paréntesis se suma c_1 veces, en el segundo c_2 veces,... y en el último c_q veces.

Luego, sumando de esa manera los términos asociados a cada uno de los sombreros de Schauder obtenemos un término cuya función término es igual a f. $\square$

Ejemplo 8.6.12. Calculemos algunos términos correspondientes a los sombreros de Schauder de la Figura 8.6.

La recta que pasa por los puntos $(0,0)$ y $(\frac{1}{3}, \frac{1}{3})$ es $y = x$ y por los puntos $(\frac{1}{3}, \frac{1}{3})$ y $(\frac{1}{2}, 0)$ es $y = 1 - 2x$. Podemos ver que

$$h_{22} = x^\sharp \wedge (1 - 2x)^\sharp.$$

Análogamente se tiene que

$$h_{24} = (2x - 1)^\sharp \wedge (1 - x)^\sharp.$$

Veamos los términos correspondientes.

Por lo visto en los Ejemplos 8.6.7, tenemos que:

$$h_{22} = x \wedge \neg(x \oplus x), \quad h_{24} = (x \odot x) \wedge \neg x.$$

8.7. Ejercicios

1. (Ejemplo de Chang) Sea $\mathbb{Z} \times \mathbb{Z}$ el grupo producto de $\mathbb{Z}$ por sí mismo. Consideremos el ℓ-grupo totalmente ordenado $\mathbb{Z} \otimes \mathbb{Z}$ obtenido considerando sobre $\mathbb{Z} \times \mathbb{Z}$ el orden lexicográfico. Calcular $\Gamma(\mathbb{Z} \otimes \mathbb{Z}, (1, 0))$.

2. Probar lo que se afirma en la Observación 8.1.12, o sea:
   a)
   $$x \vee y = (x \odot \neg y) \oplus y,$$
   $$x \wedge y = x \odot (\neg x \oplus y).$$

   b)
   $$x \odot y \;\leq\; x \wedge y \;\leq\; x, y \;\leq\; x \vee y \;\leq\; x \oplus y.$$

3. Sean $x, y \in A$, A una MV-álgebra, tales que $x \wedge y = 0$. Probar que para todo z, $x \wedge (y \oplus z) = x \wedge z$ (parte (a) del Lema 8.1.15).

4. Probar que en la MV-álgebra $[0, 1]$ $x \ominus y$ es el máximo entre $x - y$ y 0. Deducir de allí que $d(x, y) = |x - y|$.

5. Sea $h : A \longrightarrow B$ un homomorfismo de MV-álgebras.

   Probar las siguientes afirmaciones:

   a) $h(x \wedge y) = h(x) \wedge h(y)$ y $h(x \vee y) = h(x) \vee h(y)$ para cada $x, y \in A$.

   b) La relación $\sim_h$ definida por $x \sim_h y$ si y solo si $h(x \ominus y) = h(y \ominus x) = 0$ es una MV-congruencia en A.

6. Sea $h : A \to B$ un homomorfismo de MV-álgebras, con B no trivial. Probar que $h(x) \leq h(y)$ si y solo si $x \ominus y \in \mathrm{Ker}(h)$.

7. Sea A una MV-álgebra y P un ideal de A. Probar que P es primo si y solo si A/P es una MV-cadena.

8. Probar que todo ideal propio de una MV-cadena es primo.

9. Probar que si A es una MV-cadena, si $x \oplus y = x \oplus z$ y $x \odot y = x \odot z$ entonces $y = z$.

10. Probar que todo ideal propio de una MV-álgebra que contiene un ideal primo es primo.

11. Sea A una MV-álgebra. Para cada ideal primo P e ideales I e J, probar que si $P \subseteq I$ y $P \subseteq J$ entonces $I \subseteq J$ ó $J \subseteq I$.

12. Sea A una MV-álgebra y $\mathrm{Spec}(A)$ el conjunto de ideales primos de A. Probar que si $f : A \to B$ es un homomorfismo de MV-álgebras entonces la función $\mathrm{Spec}(f) : (\mathrm{Spec}(B), \subseteq) \to (\mathrm{Spec}(A), \subseteq)$, definida como $\mathrm{Spec}(f)(P) = f^{-1}(P)$, es un p-morfismo (ver Sección 6.5 del Capítulo 6 para la definición de p-morfismo).

13. Dar los detalles de la prueba del Teorema 8.6.5.

Bibliografía del Capítulo 8

- Anderson M. and Feil T., *Lattice-Ordered Groups, an Introduction.* D. Reidel, 1988.

- Bigard A., Keimel K. and Wolfenstein S., *Groupes et Anneaux Réticulés.* Lecture Notes in Math., 608, Springer-Verlag, 1977.

- Cignoli R., D'Ottaviano I. and Mundici D., *Álgebras das Lógicas de Łukasiewicz.* Coleção CLE, vol. 12. Centro de Lógica, Epistemología e História da Ciencia, Universidade Estadual de Campinas, Campinas, San Pablo, 1994.

- Cignoli R. and Mundici D., *An elementary proof of Chang's completeness theorem for the infinite–valued calculus of Łukasiewicz.* Studia Logica, 58 (1997), no. 1, 79–97.

- Cignoli R., D'Ottaviano I. and Mundici D., *Algebraic Foundations of Many-Valued Reasoning.* Trends in Logic—Studia Logica Library, vol. 7, Kluwer Academic Publishers, 2000.

- Fuchs L., *Partially Ordered Algebraic Systems.* Addison-Wesley, Pergamon Press, 1963.

Capítulo 9

Cálculo infinitovalente de Łukasiewicz

Históricamente, el Cálculo Proposicional Trivalente de Łukasiewicz fue la primera de las lógicas que "rompieron el molde" de la lógica clásica. Posteriormente se definió el cálculo n-valente y luego el infinitovalente Ł. En estos cálculos no valen ni el *principio del tercero excluido* ni el *principio de no contradicción*. Según vimos, la fórmula $\mathrm{A} \vee \neg\mathrm{A}$ es un teorema en el CPC pero no en el CPI, mientras que $\neg(\mathrm{A} \wedge \neg\mathrm{A})$ es un teorema en ambas lógicas.

En realidad, estos principios valen "de otra manera" en este contexto. Como hemos visto, las álgebras de Boole son un caso particular de las MV-álgebras. En efecto, el supremo $\vee$ y el ínfimo $\wedge$ se generalizan a la suma $\oplus$ y el producto $\odot$ respectivamente. Si con esa idea traducimos $\mathrm{A} \vee \neg\mathrm{A}$ a la lógica Ł obtendremos $\mathrm{A} \oplus \neg\mathrm{A}$, que es, según veremos, un teorema de Ł, pues es equivalente a $\mathrm{A} \to \mathrm{A}$. Análogamente, $\neg(\mathrm{A} \wedge \neg\mathrm{A})$ se traduciría como $\neg(\mathrm{A} \odot \neg\mathrm{A})$, que es equivalente a $\neg\mathrm{A} \to \neg\mathrm{A}$, que también es un teorema de Ł.

Łukasiewicz intenta resolver el problema aristotélico de los "futuros contingentes": Aristóteles había pensado que hay ciertas proposiciones compuestas a las que no es posible asignar un valor de verdad que dependa solo del valor de verdad de sus componentes. La célebre frase *"Habrá mañana batalla en el mar"* es un ejemplo de esa situación.

En 1920, Jan Łukasiewicz introduce las lógicas polivalentes intentando caracterizar semánticamente los operadores modales posibilidad M y necesidad $\neg M \neg$. Consideró las siguientes propiedades inherentes al operador posibilidad:

1) Si no es posible p, entonces $\neg$p.

2) Si se supone $\neg$p, entonces no es posible p.

3) Para alguna p es posible p y es posible $\neg$p.

No existe una "función de verdad" clásica $f_M : \{0,1\} \longrightarrow \{0,1\}$ que verifique 1), 2) y 3). En efecto, 1) y 2) dicen que $v(\neg \mathrm{p}) = 1$ si y solo si $v(\neg M\mathrm{p}) = 1$, o sea que las tablas de verdad de $\neg\mathrm{p}$ y de $\neg M\mathrm{p}$ deben coincidir, por lo que también coincidirían las de p y Mp. Si así fuera, para que se cumpliera 3) debería existir p tal que $v(M\mathrm{p}) = v(M\neg\mathrm{p})$, pero entonces sería $v(\mathrm{p}) = v(\neg\mathrm{p})$, lo que va contra el principio de no contradicción, ya que tendríamos $v(\mathrm{p} \wedge \neg\mathrm{p}) = 1$.

Entonces Łukasiewicz introduce un tercer valor de verdad $\frac{1}{2}$ y define

$$f_M : \{0, \frac{1}{2}, 1\} \longrightarrow \{0, \frac{1}{2}, 1\}.$$

Se conviene en que el valor de verdad de la negación de p, $v(\neg\mathrm{p})$, es $\frac{1}{2}$ cuando $v(\mathrm{p}) = \frac{1}{2}$. Se define f_M de la siguiente manera y se ve que cumple las condiciones requeridas.

$v(\mathrm{p})$	$f_M(v(\mathrm{p}))$	$v(\neg\mathrm{p})$	$f_M(v(\neg\mathrm{p}))$	$v(\neg(f_M(v(\neg\mathrm{p}))))$
0	0	1	1	0
$\frac{1}{2}$	1	$\frac{1}{2}$	1	0
1	1	0	0	1

La tabla de la función f_M es la del operador posibilidad M, también denotado $\Diamond$: $v(M\mathrm{p}) = f_M(v(\mathrm{p}))$. La del operador necesidad, también denotado $\Box$, es la que figura en la última columna.

Se definen las tablas de verdad de los conectivos $\neg$ y $\rightarrow$ en $Ł_3$ por las siguientes igualdades:

$$v(\neg\mathrm{p}) = 1 - v(\mathrm{p}),$$
$$v(\mathrm{p} \rightarrow q) = \mathrm{mín}\{1, 1 - v(\mathrm{p}) + v(\mathrm{q})\}.$$

En ambos casos si nos restringimos a $\{0,1\}$ obtenemos los valores clásicos. Así queda definida la semántica del cálculo proposicional trivalente.

Esta idea se generaliza a n valores. Tomando $Ł_n = \{0, \frac{1}{n-1}, \frac{2}{n-1}, \ldots, \frac{n-2}{n-1}, 1\}$ se consideran "grados de posibilidad" s_1, s_2, ..., s_{n-1} que generalizan el operador M. Las tablas de verdad de $\neg$ y de $\rightarrow$ son regidas por las mismas igualdades.

También esas igualdades pueden extenderse al intervalo real $[0,1]$ y dar lugar así al cálculo Ł de Łukasiewicz infinitovalente cuyo estudio es el principal objetivo de este capítulo.

9.1. Sistemas formales de Łukasiewicz

Cálculo Proposicional Trivalente CP3Ł

Antes de definir el cálculo Ł veamos brevemente cuál fue el primer paso para llegar a él.

La siguiente es la axiomatización que dio Wajsberg (ver [12, Ch. 9]) para el Cálculo Proposicional Trivalente de Łukasiewicz (que hemos abreviado como CP3Ł).

Lenguaje

Está dado por las variables $\mathrm{p}_1, \ldots, \mathrm{p}_n, \ldots$ y los conectivos $\neg$ y $\rightarrow$, sujetos a las reglas de construcción habituales.

Axiomas

(A1) $\mathrm{A} \rightarrow (\mathrm{B} \rightarrow \mathrm{A})$.

(A2) $(\mathrm{A} \rightarrow \mathrm{B}) \rightarrow ((\mathrm{B} \rightarrow \mathrm{C}) \rightarrow (\mathrm{A} \rightarrow \mathrm{C}))$.

(A3) $((\mathrm{A} \rightarrow \neg\mathrm{A}) \rightarrow \mathrm{A}) \rightarrow \mathrm{A}$.

(A4) $(\neg\mathrm{A} \rightarrow \neg\mathrm{B}) \rightarrow (\mathrm{B} \rightarrow \mathrm{A})$.

Reglas

Regla Modus Ponens.

Llamemos, en correspondencia con los axiomas dados,

$$\begin{aligned}
f_1(x, y, z) &= x \rightarrow (y \rightarrow x), \\
f_2(x, y, z) &= (x \rightarrow y) \rightarrow ((y \rightarrow z) \rightarrow (x \rightarrow z)), \\
f_3(x, y, z) &= ((x \rightarrow \neg x) \rightarrow x) \rightarrow x, \\
f_4(x, y, z) &= (\neg x \rightarrow \neg y) \rightarrow (y \rightarrow x).
\end{aligned}$$

El álgebra de Lindenbaum de este cálculo es un álgebra $\langle A, \rightarrow, \neg, 1\rangle$ que verifica:

($\mathrm{W}_3 1$) $f_i(x, y, z) = 1$, para $i = 1, 2, 3, 4$,

($\mathrm{W}_3 2$) $1 \rightarrow x = 1$ implica $x = 1$,

($\mathrm{W}_3 3$) $x \rightarrow y = 1$, $y \rightarrow x = 1$ implican $x = y$.

Teorema 9.1.1 ([12, Ch. 3, Th. 3.8]). *Dada un álgebra $\langle A, \rightarrow, \neg, 1\rangle$ que verifica ($W_3$1), ($W_3$2) y ($W_3$3), si se define:*

$$\begin{aligned} x \vee y &= (x \rightarrow y) \rightarrow y, \\ x \wedge y &= \neg(\neg x \vee \neg y), \\ \nabla x &= \neg x \rightarrow x, \\ 0 &= \neg 1, \end{aligned}$$

entonces $\langle A, \vee, \wedge, \neg, \nabla, 0, 1\rangle$ es una 3Ł-álgebra (ver 5.6.21).

Recíprocamente, dada una 3Ł-álgebra, definiendo:

$$x \rightarrow y = (\nabla(\neg x) \vee y) \wedge (\nabla y \vee \neg x),$$

el álgebra $\langle A, \rightarrow, \neg, 1\rangle$ verifica ($W_3$1), ($W_3$2) y ($W_3$3).

Además, por el teorema de representación dado por Cignoli (ver [2, Ch. XI, 7, Th. 1]) se tiene que una 3Ł-álgebra es subdirectamente irreducible si y solo si es una subálgebra de la cadena $Ł_3$. Pero la única subálgebra propia es la dada por $\{0, 1\}$. Luego, la validez en una 3Ł-álgebra cualquiera puede reducirse a la validez en la cadena $Ł_3$. Es decir que vale el teorema de completud siguiente:

Teorema 9.1.2. *Una fórmula es un teorema del CP3Ł si y solo si es válida en $Ł_3$.*

A partir de CP3Ł se definió el Cálculo n-valente de Łukasiewicz, cuyos valores de verdad, como dijimos, son los de la cadena $Ł_n$. En particular, CP2Ł coincide con el CPC.

Sin embargo, las álgebras n-valentes de Łukasiewicz–Moisil (ver Teorema 5.6.21) son la correcta "contraparte algebraica" de CPnŁ solo para $n = 3, 4$ (ver [18], [12]). En efecto, si $n \geq 5$ la implicación de Łukasiewicz no puede definirse en función de los los operadores modales junto con los de retículo y la negación $(\ )'$ de De Morgan, como ocurre para $n = 3, 4$. Sin embargo, sí puede definirse para todo n la implicación intuicionista en función de dichos operadores, como hemos visto para $n = 3$.

En [20] Cignoli define las *álgebras de Łukasiewicz n-valuadas propias*, agregando algunas funciones a los operadores dados por Moisil. De esa manera se consiguen modelos apropiados para los cálculos CPnŁ para cualquier n.

Cálculo Proposicional Infinitovalente Ł

Lenguaje

Está dado por las variables $p_1, \ldots, p_n, \ldots$ y los conectivos $\neg$, $\rightarrow$ sujetos a las reglas de construcción habituales. Llamaremos $\mathcal{L}_{Ł}$ al conjunto de las fórmulas bien formadas.

Axiomas

(Ł1) $A \rightarrow (B \rightarrow A)$.

(Ł2) $(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$.

(Ł3) $((A \rightarrow B) \rightarrow B) \rightarrow ((B \rightarrow A) \rightarrow A)$.

(Ł4) $(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$.

Reglas

Modus Ponens:

$$(\mathrm{MP})\ \frac{A\ ,\ A \rightarrow B}{B}.$$

Las definiciones de deducción, consecuencia, teoría, etc. dadas en general en el Capítulo 1, Sección 4, serán aplicadas aquí en lo que sigue.

Observación 9.1.3. La lógica B-C-K ([8], [98]) tiene como único conectivo $\rightarrow$, como única regla modus ponens y los axiomas siguientes:

(**B**) $(A \rightarrow B) \rightarrow ((C \rightarrow A) \rightarrow (C \rightarrow B))$.

(**C**) $(A \rightarrow (B \rightarrow C)) \rightarrow (B \rightarrow (A \rightarrow C))$.

(**K**) $A \rightarrow (B \rightarrow A)$.

Analicemos los axiomas del sistema Ł en comparación con los del sistema $\mathbf{L}_4$ del cálculo clásico y con los de la lógica B-C-K.

El primer axioma de Ł es (K), el mismo que aparece en $\mathbf{L}_4$ como ($L_4$1).

El axioma (Ł2) se probará que es equivalente a (**B**), pero no es equivalente a ($L_4$2). Esto hará que no pueda probarse el Teorema de la deducción válido en los cálculos clásico e intuicionista. Valdrá en este caso un teorema más débil.

También se demostrará que (**C**) se deduce de los axiomas de Ł.

Entonces vemos que la lógica de Łukasiewicz es una extensión de la lógica B-C-K, que es la que contiene solo esos tres axiomas. O sea que todo teorema de B-C-K es teorema de Ł.

Añadiendo dos axiomas a la lógica B-C-K se obtiene un sistema en el que los teoremas son los mismos que los de Ł, salvo traducción de conectivos (ver [97]). Esta vinculación es el reflejo de la que existe entre las álgebras naturalmente asociadas a ambas lógicas. La cuasivariedad de las *BCK-álgebras*, asociada a la lógica B-C-K (ver por ejemplo, [8]), está definida de la siguiente manera.

Una BCK-álgebra es un álgebra $\langle A, *, 0\rangle$ que verifica las siguientes identidades y cuasiidentidad:

- $((x * y) * (x * z)) * (z * y) = 0$,
- $(x * (x * y)) * y = 0$,
- $x * x = 0$,
- $0 * x = 0$,
- si $x * y = 0$ e $y * x = 0$ entonces $x = y$.

La operación $*$ es dual de $\to$, pues cumple $y * x = x \to y$. Puede interpretarse como la diferencia de conjuntos y 0 como $\emptyset$.

Una subclase de ellas son las *BCK-álgebras conmutativas*, que forman una variedad. Las ecuaciones que las definen son las siguientes:

(Y1) $(x * y) * z = (x * z) * y$,

(Y2) $x * (x * y) = y * (y * x)$,

(Y3) $x * x = 0$,

(Y4) $x * 0 = x$.

En particular, las *BCK-álgebras conmutativas acotadas* son las álgebras $\langle A, *, 0, 1\rangle$ que cumplen (Y1),...,(Y4) y además:

(Bo) $x * 1 = 0$.

La clase de álgebras que acabamos de definir es definicionalmente equivalente a la clase de las MV-álgebras. Como hemos visto en el caso de las W-álgebras, esto significa que son interdefinibles: dada una MV-álgebra A se pueden definir, en función de $\oplus, \neg$ y 0, operaciones $*$, 0 y 1 que dan sobre A

una estructura de BCK-álgebra acotada conmutativa y recíprocamente (ver [82]).

Trataremos una subvariedad de las BCK-álgebras conmutativas (las BCK-álgebras cónicas) en relación con los ℓ-grupos en el Capítulo 11.

Veamos ahora algunos ejemplos de teoremas que se derivan rápidamente de los axiomas.

Ejemplos 9.1.4.

1. Llamaremos, abreviadamente, $\mathrm{A} \vee \mathrm{B}$ a la fórmula $(\mathrm{A} \to \mathrm{B}) \to \mathrm{B}$. Luego, por el axioma (Ł1),
$$\vdash \mathrm{B} \to (\mathrm{A} \vee \mathrm{B}).$$
Podemos derivar de aquí una regla de deducción:
$$\frac{\mathrm{B}}{\mathrm{A} \vee \mathrm{B}}\,.$$

2. Por el axioma (Ł3),
$$\vdash (\mathrm{A} \vee \mathrm{B}) \to (\mathrm{B} \vee \mathrm{A}).$$
Por lo tanto podemos enunciar la siguiente regla:
$$\frac{\mathrm{A} \vee \mathrm{B}}{\mathrm{B} \vee \mathrm{A}}\,.$$

3. Luego, por los dos ítems anteriores,
$$\vdash \mathrm{B} \to (\mathrm{B} \vee \mathrm{A}).$$

4. Si $\Gamma = \{\mathrm{A} \to \mathrm{B}, \mathrm{B} \to \mathrm{C}\}$ entonces
$$\Gamma \vdash \mathrm{A} \to \mathrm{C};$$
la derivación es a partir del axioma (Ł2), con dos aplicaciones de (MP).

Del último ejemplo podemos obtener la siguiente regla de deducción de Silogismo Hipotético:

$$\text{(SH)}\ \frac{\mathrm{A}\to\mathrm{B}\ ,\ \mathrm{B}\to\mathrm{C}}{\mathrm{A}\to\mathrm{C}}.$$

Ejemplos 9.1.5.

1. Vamos a dar ahora una deducción de:

$$(\mathbf{C}) \quad (A \to (B \to C)) \to (B \to (A \to C)).$$

   (i) $(A \to (B \to C)) \to ((B \vee C) \to (A \to C)) = (A \to (B \to C)) \to (((B \to C) \to C)) \to (A \to C))$, por (Ł2),

   (ii) $B \to (B \vee C)$ (ya probado),

   (iii) $(B \to (B \vee C)) \to (((B \vee C) \to (A \to C)) \to (B \to (A \to C)))$, por ser instancia de (Ł2),

   (iv) $((B \vee C) \to (A \to C)) \to (B \to (A \to C))$, de (ii), (iii), por (MP),

   (v) $(A \to (B \to C)) \to (B \to (A \to C))$, por(i), (iv) y (SH).

2. A partir del ejemplo anterior podemos probar

$$\vdash A \to A.$$

   En efecto, si tomamos $C = A$, de (**C**) obtenemos:

$$(A \to (B \to A)) \to (B \to (A \to A)),$$

   que por (Ł1) y (MP) nos dan

$$B \to (A \to A).$$

   Basta ahora tomar como B una instancia de cualquier axioma y por (MP) deducimos

$$A \to A.$$

3. El axioma (**B**) de la lógica B-C-K es un teorema de Ł (ejercicio).

4. Usando (SH) podemos probar

$$B \to (\neg\neg A \to A).$$

   Esta es una deducción:

   (i) $\neg\neg A \to (\neg\neg B \to \neg\neg A)$, por (Ł1)

   (ii) $(\neg\neg B \to \neg\neg A) \to (\neg A \to \neg B)$, por (Ł4),

   (iii) $\neg\neg A \to (\neg A \to \neg B)$, por (i), (ii) y (SH),

   (iv) $(\neg A \to \neg B) \to (B \to A)$, por (Ł4),

   (v) $\neg\neg A \to (B \to A)$, por (iii), (iv) y (SH),

(vi) $B \to (\neg\neg A \to A)$, por aplicación de una instancia de (**C**) a (v) y usando (MP).

Como hicimos en el Ejemplo 2, tomamos como B una instancia de axioma, por ejemplo $(C \to (D \to C))$ y por (MP) obtenemos:

$$\neg\neg A \to A.$$

5. Se tiene:

$$\vdash (A \to \neg B) \to (B \to \neg A).$$

No daremos la deducción correspondiente (ejercicio o ver [23, Proposición 4.3.4]).

6. Probaremos a continuación que

$$\vdash A \to \neg\neg A.$$

Si cambiamos A por $\neg A$ y B por A, obtenemos la siguiente instancia del teorema del ítem 6:

$$(\neg A \to \neg A) \to (A \to \neg\neg A). \tag{1}$$

Como ya hemos probado

$$\vdash A \to A,$$

si cambiamos la variable A por $\neg A$ obtenemos

$$\vdash \neg A \to \neg A,$$

que combinado con (1), por (MP), nos da

$$\vdash A \to \neg\neg A.$$

Daremos a continuación algunas reglas de deducción que se demuestran fácilmente a partir de los axiomas y los ejemplos que vimos. Algunas de ellas ya fueron enunciadas.

Reglas derivadas de los axiomas

(R1) $\dfrac{A}{B \to A}$,

(R2) $\dfrac{A \to B}{(B \to C) \to (A \to C)}$, (R3) $\dfrac{\text{A}\vee\text{B}}{\text{B}\vee\text{A}}$,

(R4) $\dfrac{\neg\text{A}\to\neg\text{B}}{\text{B}\to\text{A}}$,

Otras Reglas

(R5) $\dfrac{\text{A}}{\text{A}\vee\text{B}}$,

(R6) $\dfrac{\text{A}}{\text{B}\vee\text{A}}$,

(R7) $\dfrac{\text{A}\to\text{B}}{(\text{C}\to\text{A})\to(\text{C}\to\text{B})}$,

(R8) $\dfrac{\text{A}\to\neg\text{B}}{\text{B}\to\neg\text{A}}$,

(R9) $\dfrac{\text{A}\to\text{B}}{\neg\text{B}\to\neg\text{A}}$,

(R10) $\dfrac{\neg\neg\text{A}}{\text{A}}$,

(R11) $\dfrac{\text{A}}{\neg\neg\text{A}}$,

(SH) $\dfrac{\text{A}\to\text{B}\ ,\ \text{B}\to\text{C}}{\text{A}\to\text{C}}$.

Observación 9.1.6. Sabemos que toda álgebra de Boole es una MV-álgebra, en la cual el producto $\odot$ es el ínfimo y la suma $\oplus$ es el supremo (ver 8.1.2). Desde el punto de vista de la lógica, podemos ver que si agregamos un axioma a los del sistema Ł obtenemos el CPC, es decir que el CPC es una extensión de Ł. Sea **(N)** el siguiente axioma:

$$(\mathbf{N})\ (\text{A} \to (\text{B} \to \text{C})) \to (\neg\text{C} \to ((\text{A} \to \text{B}) \to \neg\text{A})).$$

¿Qué dice este axioma? Que la fórmula $\text{A} \to (\text{B} \to \text{C})$ implica algo equivalente a $(\text{A} \wedge \text{B}) \to \text{C}$, traduciendo el segundo miembro en términos del ínfimo. Es decir que, teniendo en cuenta la propiedad (f) del Lema 8.1.7, estamos identificando $\wedge$ con $\odot$.

Probaremos brevemente que se tiene la siguiente "ecuación": Ł+$(\mathbf{N}) = \mathbf{L}$. Para esto basta demostrar el axioma (L2) de **L**, ya que los otros dos axiomas son comunes a Ł y **L**.

(i) $(\text{A} \to (\text{B} \to \text{C})) \to (\neg\text{C} \to ((\text{A} \to \text{B}) \to \neg\text{A}))$, por **(N)**,

(ii) $(\neg C \to ((A \to B) \to \neg A)) \to ((A \to B) \to (\neg C \to \neg A))$, por **(C)**,

(iii) $(\neg C \to \neg A) \to (A \to C)$, por (Ł4),

(iv) $((A \to B) \to (\neg C \to \neg A)) \to ((A \to B) \to (A \to C))$, por (iii) usando (R7),

(v) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$, por (i), (ii), (iv) y aplicando sucesivamente (SH).

También obtendríamos **L** si hubiéramos agregado a los axiomas de Ł simplemente el axioma (L2) en lugar de **(N)**.

9.2. Álgebra de Lindenbaum

Repetiremos aquí procesos y resultados que hemos visto en los capítulos 3 y 5. Por ejemplo, la construcción del álgebra de Lindenbaum y la demostración de que esta álgebra tiene como generadores libres las clases de las variables proposicionales. Esta repetición nos hace sospechar que debe haber un marco general que englobe estos conceptos. En ese sentido, hemos dado algunas ideas sobre Álgebra Universal en los capítulos 1 y 7. Veremos también en el Capítulo 10 los lineamientos de lo que ha dado en llamarse *Lógica Algebraica Abstracta* o AAL, debida a W. Blok y D. Pigozzi (ver [8]). Reproduciremos allí un texto de R. Lewin [72], a quien mucho agradecemos su colaboración.

En esta sección vamos a construir entonces, de la misma manera que lo hicimos para el CPC y el CPI, el álgebra de Lindenbaum del cálculo Ł de Łukasiewicz. Obtendremos en primer lugar una estructura de álgebra de Wajsberg, que, como vimos, es equivalente a una estructura de MV-álgebra.

Podemos aquí dar una visión más completa de la situación.

Vimos en el Capítulo 1 el concepto de valuación, que proporciona una interpretación de una fórmula de un cierto cálculo proposicional en un álgebra de manera que se corresponden los conectivos de la lógica y las operaciones de dicha álgebra. Pensemos en los términos $\mathrm{T}(X)$ de un cierto tipo $\mathcal{F}$ y en las fórmulas $\mathcal{L}$ de un cierto cálculo proposicional que tienen conectivos correspondientes a las operaciones de tipo $\mathcal{F}$: son esencialmente lo mismo. Por ejemplo, los términos de tipo $\mathcal{F} = \langle 2, 1, 0 \rangle$ de un álgebra de Wajsberg y las fórmulas del cálculo Ł: son las mismas, salvo el 1 (que puede ser presentado en la lógica como abreviatura de la fórmula $A \to A$) y el hecho de que uno elige letras minúsculas para representar las variables del álgebra y mayúsculas para las de la lógica.

Vimos en el Capítulo 7 que los términos de tipo $\mathcal{F}$ sobre un conjunto X de variables forman un álgebra: el álgebra absolutamente libre sobre ese conjunto de generadores. Identifiquemos mentalmente los términos con las fórmulas de la lógica correspondiente; entonces, la relación de equivalencia entre fórmulas que permite definir el álgebra de Lindenbaum (que es la que identifica dos fórmulas A y B si $\mathrm{A} \to \mathrm{B}$ y $\mathrm{B} \to \mathrm{A}$ son teoremas) se demuestra que es una congruencia de esa álgebra absolutamente libre, es decir, que, además de ser relación de equivalencia, preserva los conectivos. Eso corresonde a identificar en el álgebra de términos aquellos que se identifican por las ecuaciones que definen la clase de álgebras correspondiente. El resultado de dicha identificación, es decir, el cociente, es el álgebra "libre de identificaciones", es decir, aquella en la que todo lo identificable ya fue identificado. Lo que queda es entonces el álgebra libre con un conjunto X de generadores.

Vamos a construir ahora el álgebra de Lindenbaum del cálculo Ł.

Los dos lemas que siguen son análogos a los lemas 5.2.3 y 5.2.4 del Capítulo 5, aunque sus demostraciones son distintas.

Sea P la siguiente relación en $\mathcal{L}_{\text{Ł}}$:

$$\mathrm{A}\, P\, \mathrm{B} \quad \text{si y solo si} \quad \vdash \mathrm{A} \to \mathrm{B}.$$

Lema 9.2.1. *La relación P es un preorden.*

Demostración. En los ejemplos de la Sección 2 se probó que $\vdash \mathrm{A} \to \mathrm{A}$ y también, por (SH), que la fórmula $\mathrm{A} \to \mathrm{C}$ es consecuencia de Γ, siendo

$$\Gamma = \{\mathrm{A} \to \mathrm{B}, \mathrm{B} \to \mathrm{C}\}.$$

Luego, P es un preorden en $\mathcal{L}_{\text{Ł}}$. □

Lema 9.2.2. *La relación binaria $\equiv$ en $\mathcal{L}_{\text{Ł}}$ dada por*

$$\mathrm{A} \equiv \mathrm{B} \quad \textit{si y solo si} \quad \mathrm{A}\, P\, \mathrm{B} \ \textit{y}\ \mathrm{B}\, P\, \mathrm{A}.$$

es una relación de equivalencia.

Sea $A_{\text{Ł}} = \mathcal{L}_{\text{Ł}}/\equiv$. Sean X, $Y \in A_{\text{Ł}}$ y sea $\preceq$ la siguiente relación en $A_{\text{Ł}}$: $X \preceq Y$ si y solo si $\mathrm{A}\, P\, \mathrm{B}$ para $\mathrm{A} \in X$ y $\mathrm{B} \in Y$. Entonces, $\preceq$ está bien definida y es un orden en $A_{\text{Ł}}$.

Demostración. Sale de la Observación 1.2.7 dada en el Capítulo 1. □

Indicaremos con $|\mathrm{A}|$ los elementos de $A_{\text{Ł}}$.

Teorema 9.2.3. *La relación $\equiv$ verifica:*

Si $\mathrm{A} \equiv \mathrm{B}$ *y* $\mathrm{C} \equiv \mathrm{D}$, *entonces* $\mathrm{A} \to \mathrm{C} \equiv \mathrm{B} \to \mathrm{D}$.

Si $\mathrm{A} \equiv \mathrm{B}$*, entonces* $\neg\mathrm{A} \equiv \neg\mathrm{B}$.

Demostración. Por (R2) podemos deducir:

$$\begin{array}{lll} \mathrm{A}\,P\,\mathrm{B} & \text{implica} & (\mathrm{B} \to \mathrm{C})\,P\,(\mathrm{A} \to \mathrm{C}), \\ \mathrm{B}\,P\,\mathrm{A} & \text{implica} & (\mathrm{A} \to \mathrm{C})\,P\,(\mathrm{B} \to \mathrm{C}). \end{array}$$

Luego:

$$\mathrm{A} \equiv \mathrm{B} \quad \text{implica} \quad (\mathrm{B} \to \mathrm{C}) \equiv (\mathrm{A} \to \mathrm{C}).$$

Análogamente, usando (R7) se tiene:

$$\mathrm{C} \equiv \mathrm{D} \quad \text{implica} \quad (\mathrm{B} \to \mathrm{C}) \equiv (\mathrm{B} \to \mathrm{D}).$$

Por lo tanto,

$$\mathrm{A} \equiv \mathrm{B},\ \mathrm{C} \equiv \mathrm{D} \quad \text{implica} \quad (\mathrm{A} \to \mathrm{C}) \equiv (\mathrm{B} \to \mathrm{D}).$$

Sea ahora $\mathrm{A} \equiv \mathrm{B}$ y veamos que $\neg\mathrm{A} \equiv \neg\mathrm{B}$.

Por la regla (R11) se tiene: $\mathrm{A}\,P\,\neg\neg\mathrm{A}$. Luego, por (R7),

$$(\mathrm{B} \to \mathrm{A})\,P\,(\mathrm{B} \to \neg\neg\mathrm{A}). \tag{1}$$

Por (R8) vale

$$\vdash (\mathrm{C} \to \neg\mathrm{D}) \to (\mathrm{D} \to \neg\mathrm{C}),$$

o sea,

$$(\mathrm{C} \to \neg\mathrm{D})\,P\,(\mathrm{D} \to \neg\mathrm{C})$$

y, sustituyendo C por B y D por $\neg\mathrm{A}$, vale:

$$(\mathrm{B} \to \neg\neg\mathrm{A})\,P\,(\neg\mathrm{A} \to \neg\mathrm{B}). \tag{2}$$

De (1) y (2):

$$(\mathrm{B} \to \mathrm{A})\,P\,(\neg\mathrm{A} \to \neg\mathrm{B}),$$

o sea

$$\vdash (\mathrm{B} \to \mathrm{A}) \to (\neg\mathrm{A} \to \neg\mathrm{B}).$$

Como se tiene $\vdash (\mathrm{B} \to \mathrm{A})$, se deduce que

$$\vdash (\neg\mathrm{A} \to \neg\mathrm{B}).$$

Análogamente puede probarse que

$$\vdash (\neg\mathrm{B} \to \neg\mathrm{A}),$$

de donde

$$\neg\mathrm{A} \equiv \neg\mathrm{B}. \qquad \square$$

Hemos probado entonces que $\equiv$ es una congruencia, por lo cual podemos definir en $A_{\text{Ł}}$ las operaciones $\to$ y $\neg$. Nos falta encontrar el 1 para completar las operaciones, con lo cual podremos probar que $\langle A_{\text{Ł}}, \to, \neg, 1\rangle$ es una W-álgebra.

Denotaremos, como en los otros casos, $\Gamma^{\vdash}$ a las consecuencias de un conjunto de fórmulas Γ. En particular, $\emptyset^{\vdash}$ es el conjunto de los teoremas de Ł.

Veremos en el siguiente lema que, como en los casos del CPC y del CPI, el 1 está bien definido, siendo $1 = \emptyset^{\vdash}$.

Lema 9.2.4. *Sea* $\mathrm{A} \in \mathcal{L}_{\text{Ł}}$. *Entonces:*

$$|\mathrm{A}| = \emptyset^{\vdash} \quad \textit{si y solo si} \quad \vdash \mathrm{A}.$$

Demostración. Si $|\mathrm{A}| = \emptyset^{\vdash}$ entonces $\vdash \mathrm{A}$ porque $\mathrm{A} \in |\mathrm{A}|$.

Sea A teorema. Veamos que $|\mathrm{A}| \subseteq \emptyset^{\vdash}$, es decir que, si $\mathrm{B} \equiv \mathrm{A}$ entonces $\vdash \mathrm{B}$. En efecto, se tiene $\vdash \mathrm{A}$ y $\vdash (\mathrm{A} \to \mathrm{B})$. Luego, por (MP), $\vdash \mathrm{B}$.

Probemos ahora $|\mathrm{A}| \supseteq \emptyset^{\vdash}$. Sea C un teorema. Se tiene $\vdash \mathrm{A} \to (\mathrm{C} \to \mathrm{A})$, por (Ł1). Por ser A teorema resulta $\vdash (\mathrm{C} \to \mathrm{A})$. Análogamente tenemos que $\vdash (\mathrm{A} \to \mathrm{C})$ porque C es un teorema. Por ende concluimos que $\mathrm{C} \in |\mathrm{A}|$. □

Teorema 9.2.5. *Definimos sobre* $A_{\text{Ł}}$ *las siguientes operaciones:*

$$|\mathrm{A}| \to |\mathrm{B}| = |\mathrm{A} \to \mathrm{B}|,$$
$$\neg|\mathrm{A}| = |\neg \mathrm{A}|,$$
$$1 = \emptyset^{\vdash}.$$

Entonces, $\langle A_{\text{Ł}}, \to, \neg, 1\rangle$ *es una* W*-álgebra.*

Demostración. Ya hemos probado en los lemas 9.2.3 y 9.2.4 que las operaciones están bien definidas. Veamos que se cumplen las ecuaciones (W1), (W2), (W3) y (W4).

Para probar (W1) debemos tomar un teorema A, otra fórmula cualquiera B y demostrar que $|\mathrm{A}| \to |\mathrm{B}| = |\mathrm{B}|$, ya que $|\mathrm{A}| = 1$. Basta probar que $\mathrm{A} \to \mathrm{B} \equiv \mathrm{B}$, es decir, que $\vdash \mathrm{B} \to (\mathrm{A} \to \mathrm{B})$ y $\vdash (\mathrm{A} \to \mathrm{B}) \to \mathrm{B}$. Lo primero vale por (Ł1) y lo segundo se traduce: $\vdash \mathrm{A} \vee \mathrm{B}$, lo cual también es cierto en virtud de la regla (R5).

Lo que debemos mostrar para ver las ecuaciones (W2), (W3) y (W4) es que, respectivamente,

$$\vdash (\mathrm{A} \to \mathrm{B}) \to ((\mathrm{B} \to \mathrm{C}) \to (\mathrm{A} \to \mathrm{C})),$$
$$\vdash ((\mathrm{A} \to \mathrm{B}) \to \mathrm{B}) \to ((\mathrm{B} \to \mathrm{A}) \to \mathrm{A}),$$
$$\vdash (\neg \mathrm{A} \to \neg \mathrm{B}) \to (\mathrm{B} \to \mathrm{A}).$$

Las tres condiciones valen respectivamente por (Ł2), (Ł3) y (Ł4). □

Corolario 9.2.6. *Definimos sobre* $A_{Ł}$ *las siguientes operaciones:*

$$|\mathrm{A}| \oplus |\mathrm{B}| = |\neg\mathrm{A} \to \mathrm{B}|,$$
$$\neg|\mathrm{A}| = |\neg\mathrm{A}|,$$
$$0 = \neg\emptyset^{\vdash}.$$

Entonces, $\langle A_{Ł}, \oplus, \neg, 0\rangle$ *es una MV-álgebra, llamada el* álgebra de Lindenbaum del Cálculo Proposicional Ł.

Veremos en seguida un teorema que muestra que $A_{Ł}$ es el álgebra libre con numerables generadores. Usaremos resultados de la Sección 6 del Capítulo 8. Si bien en ese capítulo obtuvimos resultados para un número finito de generadores, puede probarse que también valen en general. Demostraremos aquí que $A_{Ł}$ es isomorfa a la MV-álgebra de las funciones de McNaughton sobre el cubo de Hilbert (ver 8.6.3).

Teorema 9.2.7. *La MV-álgebra* $A_{Ł}$ *es libremente generada por el conjunto numerable* $|\mathcal{V}|$ *de las clases de equivalencia de las variables proposicionales.*

Demostración. Basta probar que $A_{Ł}$ es isomorfa al álgebra de términos $\mathrm{T}^{[0,1]}(X)$ generada por las proyecciones π_j, $j \in \mathbb{N}$, ahora consideradas como funciones $\pi_j : [0,1]^\omega \longrightarrow [0,1]$.

Definimos la aplicación $h : A_{Ł} \longrightarrow \mathrm{T}^{[0,1]}(X)$ para las clases de las variables proposicionales por

$$h(|\mathrm{p}_j|) = \pi_j^{[0,1]},$$

(con lo cual mandamos generadores en generadores) e inductivamente:

$$h(|\neg\mathrm{A}|) = \neg h(|\mathrm{A}|),$$

$$h(|\mathrm{B} \to \mathrm{C}|) = h(|\mathrm{B}|) \to h(|\mathrm{C}|).$$

Es fácil ver entonces que para todo elemento $|\mathrm{C}|$ de $A_{Ł}$

$$h(|\mathrm{C}|) = \mathrm{C}^{[0,1]}$$

y que h es un isomorfismo. □

9.3. Valuaciones

En esta sección consideraremos las valuaciones de las fórmulas de Ł a valores en una MV-álgebra A, que son esencialmente homomorfismos de $A_{Ł}$ en A. La definición de valuación es caso particular de la dada en el Capítulo 1 y las nociones de validez, modelo y consecuencia semántica son análogas a las dadas en los Capítulos 3 y 5.

Definición 9.3.1. Dada una MV-álgebra A, una A-valuación v es una aplicación $v : \mathcal{L} \longrightarrow A$ tal que:

(V1) $v(\neg \mathrm{A}) = \neg v(\mathrm{A})$,

(V2) $v(\mathrm{A} \to \mathrm{B}) = v(\mathrm{A}) \to v(\mathrm{B})$.

En particular, la aplicación canónica $p : \mathcal{L}_{\text{Ł}} \longrightarrow A_{\text{Ł}}$ es una $A_{\text{Ł}}$-valuación.
Diremos que una fórmula C es *A-válida* y lo denotaremos $\models_A$ C, si para toda valuación v a valores en A, $v(\mathrm{C}) = 1$. La fórmula C es *válida* si es A-válida para toda MV-álgebra A. Se indica por $\models$ C. Dado un conjunto de fórmulas Σ decimos que v es un *modelo* de Σ si $v(\mathrm{C}) = 1$ para toda $\mathrm{C} \in \Sigma$. Una fórmula B es *consecuencia semántica* de un conjunto de fórmulas Σ si $v(\mathrm{B}) = 1$ para todo modelo v de Σ. Se indica $\Sigma \models \mathrm{B}$.

Como hemos dicho en la sección anterior, las fórmulas de $\mathcal{L}_{\text{Ł}}$ y los MV-términos son esencialmente la misma cosa. De esta manera, dada una fórmula, podemos considerar "abusivamente" una fórmula como un término y podemos hablar de la función término asociada a ella.

Teorema 9.3.2. *Sea* C *una fórmula con n variables* $\mathrm{p}_1, \ldots, \mathrm{p}_n$*, v una A-valuación y sea* C^A *la función término asociada a* C*. Entonces:*

$$v(\mathrm{C}) = \mathrm{C}^A(v(p_1), \ldots, v(p_n)).$$

Una fórmula B *es A-válida si y solo si A satisface la MV-ecuación* $\mathrm{B} = 1$*.*

Demostración. La primera parte se obtiene haciendo inducción sobre el número de conectivos de la fórmula. La segunda parte se deduce de la primera, teniendo en cuenta que "A satisface la MV-ecuación $\mathrm{B} = 1$" significa que B^A es la función constante igual a 1. □

En lugar de dar en detalle la prueba del teorema anterior, daremos un ejemplo.
Sea C la fórmula en las dos variables p y q $\neg(\mathrm{q} \to \neg \mathrm{p})$. Entonces:

$$\begin{aligned} v(\mathrm{C}) &= \neg v(\mathrm{q} \to \neg \mathrm{p}) \\ &= \neg(v(\mathrm{q}) \to v(\neg \mathrm{p})) \\ &= \neg(v(\mathrm{q}) \to \neg v(\mathrm{p})) \\ &= \mathrm{C}^A(v(\mathrm{p}), v(\mathrm{q})). \end{aligned}$$

Teniendo en cuenta el Teorema 8.5.12 que vimos en el Capítulo 8 y el Teorema 9.3.2 podemos demostrar el siguiente resultado.

Teorema 9.3.3. *Una fórmula* C *es* $[0,1]$*-válida si y solo si es válida.*

Demostración.

$$\begin{aligned} \models_{[0,1]} \mathrm{C} \quad & \text{si y solo si } [0,1] \text{ satisface } \mathrm{C} = 1 \\ & \text{si y solo si toda MV-álgebra satisface } \mathrm{C} = 1 \\ & \text{si y solo si } \models \mathrm{C}. \end{aligned}$$ □

Observación 9.3.4. Una valuación v a valores en $[0,1]$ está determinada por sus valores en las variables proposicionales, que son numerables. Podemos decir entonces que a una valuación le corresponde un elemento del cubo de Hilbert. Recíprocamente, a un elemento de $[0,1]^\omega$, que es de la forma $a_1, \ldots, a_n, \ldots$ con $a_i \in [0,1]$, le corresponde la valuación v definida por $v(\mathrm{p}_i) = a_i$, para $i = 1, \ldots, n, \ldots$. Esta correspondencia es una biyección, por lo que podemos pensar el cubo de Hilbert como el conjunto de las $[0,1]$-valuaciones.

9.4. Filtros y teorías

En esta sección, en primer lugar, vamos a volver un poco al álgebra.

En el Capítulo 8 estudiamos los ideales de una MV-álgebra en relación con sus congruencias. Vamos a ver ahora la noción dual de *filtro* que, así como vimos en los dos casos anteriores del CPC y CPI, está directamente ligada a la noción de *teoría* de la lógica Ł.

Definición 9.4.1. Un subconjunto F de una MV-álgebra A es un *filtro* si verifica las siguientes condiciones:

(F1) $F \neq \emptyset$.

(F2) Si $x \in F$ y $x \leq y$ entonces $y \in F$ (es decir, F es creciente).

(F3) Si $x, y \in F$ entonces $x \odot y \in F$.

La condición (F1), en presencia de (F2), puede reemplazarse por la de $1 \in F$.

Un filtro F es propio si $F \neq A$ y es maximal si es propio y no hay otro filtro propio que lo contenga propiamente.

Dado un ideal I, es fácil ver que el conjunto

$$\neg I = \{x \in A : \neg x \in F\}$$

es un filtro.

Notemos que, como ya lo observamos en el caso de los ideales en el Capítulo 8, un filtro del retículo subyacente de una MV-álgebra no es, en general, un filtro de la MV-álgebra.

Un *filtro implicativo* es un subconjunto F tal que:

(F′1) $1 \in F$,

(F′2) Si $x \in F$ y $x \to y \in F$, entonces $y \in F$.

Lema 9.4.2. *Un subconjunto de una MV-álgebra es un filtro si y solo si es un filtro implicativo.*

Demostración. Sea F un filtro. Como ya dijimos, eso implica que $1 \in F$. Sea $x \in F$, $x \to y \in F$. Luego, por (F3), $x \odot (x \to y) = x \odot (\neg x \oplus y) \in F$. Por ser $x \odot (\neg x \oplus y) = x \wedge y$ y por (F2), $y \in F$.

Recíprocamente, sea F un filtro implicativo. Trivialmente vale (F1). Sea $x \in F$, $x \leq y$. Luego, $x \to y = 1 \in F$, de donde $y \in F$, por (F′2). Sean $x, y \in F$. Por (g) del Lema 8.1.7 se tiene

$$x \to (y \to (x \odot y)) = 1,$$

por lo que aplicando dos veces (F′2) se tiene que $x \odot y \in F$. □

De la misma manera que hemos visto en otros casos, dado que toda intersección de filtros es un filtro, podemos calcular el *filtro generado* por un subconjunto X de una MV-álgebra, que es $\bigcap_{F \supseteq X} F$, el menor filtro que contiene a X.

Lema 9.4.3. *Sean A una MV-álgebra y X un subconjunto no vacío de A. Entonces $F(X)$, el filtro generado por X, tiene la siguiente forma:*

$$F(X) = \{z \in L : z \geq x_1 \odot x_2 \odot \cdots \odot x_k \text{ para ciertos } x_1, x_2, \ldots x_k \in X\}.$$

Corolario 9.4.4. *Sean A una MV-álgebra , $x \in A$ y X un subconjunto no vacío de A. Entonces:*

$$F(X \cup \{x\}) = \{z \in L : z \geq x_1 \odot \cdots \odot x_k \odot x^n \text{ para } x_1, \ldots, x_k \in X, n \in \mathbb{N}\}.$$

Corolario 9.4.5 (Teorema algebraico de la deducción)**.** *Sean A una MV-álgebra, $x, y \in A$ y X un subconjunto no vacío de A. Entonces:*

$$y \in F(X \cup \{x\}) \text{ si y solo si existe un } n \in \mathbb{N} \text{ tal que } x^n \to y \in F(X).$$

Demostración. Tenemos que $z \in F(X \cup \{x\})$ si y solo si existen $x_1, x_2, \ldots x_k$ en X y $n \in \mathbb{N}$ tales que

$$x_1 \odot x_2 \odot \cdots \odot x_k \odot x^n \leq z.$$

Por la propiedad (R) vista en el Capítulo 8, Sección 1, se tiene que lo anterior equivale a

$$x_1 \odot x_2 \odot \cdots \odot x_k \leq x^n \to z,$$

que equivale a que $x^n \to z \in F(X)$. $\square$

Estudiaremos ahora la relación entre las teorías del cálculo Ł y los filtros de la correspondiente álgebra de Lindenbaum y mostraremos que hay una biyección entre aquellas y estos. Usando esto y el Corolario 9.4.5 demostraremos un teorema de la deducción débil que vale en Ł.

Teorema 9.4.6. *Existe una biyección entre el conjunto de los filtros del álgebra de Lindenbaum $A_{Ł}$ de Ł y el conjunto de las teorías de Ł.*

Demostración. La demostración es la misma que la dada en el Teorema 3.3.1 del Capítulo 3 definiendo igualmente para cada filtro F de $A_{Ł}$ el siguiente conjunto:

$$\mathcal{T}_F = \{\mathrm{A} : |\mathrm{A}| \in F\}.$$

Por otra parte, a una teoría $\mathcal{T}$ le asociamos el conjunto

$$|\mathcal{T}| = \{|\mathrm{C}| : \mathrm{C} \in \mathcal{T}\}.$$ $\square$

Lema 9.4.7. *Sea Σ un conjunto de fórmulas de $\mathcal{L}_{Ł}$ y denotemos como $|\Sigma|$ al conjunto $\{|\mathrm{A}| : \mathrm{A} \in \Sigma\}$. Luego el filtro generado por $|\Sigma|$ en $A_{Ł}$, $F(|\Sigma|)$, es igual al filtro asociado a la teoría $\Sigma^{\vdash}$. Es decir, $F(|\Sigma|) = |\Sigma^{\vdash}|$.*

Demostración. También esta prueba es la misma que la dada en el Lema 3.3.2 del Capítulo 3. $\square$

Veamos ahora el siguiente teorema que es "de la deducción" en el sentido de que, como en el caso clásico, estipula de qué forma una hipótesis de una deducción pasa como parte del antecedente de la conclusión.

Teorema 9.4.8 (Teorema de la Deducción)**.** *Sea Σ un conjunto de fórmulas de $\mathcal{L}_{Ł}$, y sean $\mathrm{A}, \mathrm{B} \in \mathcal{L}_{Ł}$. Si $\Sigma \cup \{\mathrm{A}\} \vdash \mathrm{B}$ entonces existe un $n \in \mathbb{N}$ tal que $\Sigma \vdash \mathrm{A}^n \to \mathrm{B}$.*

Demostración. Sea $\Sigma \cup \{A\} \vdash B$. Luego, $B \in (\Sigma \cup \{A\})^{\vdash}$, de donde $|B| \in |(\Sigma \cup \{A\})^{\vdash})|$. Por el Lema 9.4.7, $|(\Sigma \cup \{A\})^{\vdash})| = F(|\Sigma| \cup \{|A|\})$. Luego, $|B| \in F(|\Sigma| \cup \{|A|\})$. Por el Teorema Algebraico de la Deducción 9.4.5, esto último implica que existe $n \in \mathbb{N}$ tal que $(|A|)^n \to |B| \in F(|\Sigma|)$. Nuevamente por el Lema 9.4.7 se tiene que $|(A)^n \to B| \in |\Sigma^{\vdash}|$. Luego, $(A)^n \to B \in \Sigma^{\vdash}$, es decir, $\Sigma \vdash (A)^n \to B$. □

9.5. Completud

Los valores de verdad clásicos 0 y 1 bastan para evaluar las proposiciones del CPC y las tablas de verdad nos dan un procedimiento efectivo y simple para decidir si una cierta proposición es o no una tautología. Eso es importante porque tenemos, además, un teorema de completud que nos dice que una fórmula es un teorema si y solo si es una tautología.

En el cálculo Ł de Łukasiewicz el papel del álgebra **2** lo juega el intervalo $[0, 1]$, como hemos ido viendo a lo largo del capítulo. Los "valores de verdad" son aquí el conjunto infinito de números reales entre 0 y 1, lo que intuitivamente significa que tendremos algo así como una "probabilidad" de que una fórmula sea verdadera o no. En este sistema, las tautologías son las proposiciones $[0, 1]$-válidas, que son las válidas en toda MV-álgebra. También existe aquí un procedimiento efectivo, aunque no tan simple, para decidir si una fórmula es o no una tautología. Y también se puede demostrar la completud del cálculo Ł: una fórmula es un teorema si y solo si es $[0, 1]$-válida. Sin embargo, la completud no es fuerte como en el caso del CPC: si bien toda consecuencia sintáctica de un conjunto de fórmulas es también consecuencia semántica, no se da la recíproca en general.

En esta sección veremos resultados relativos a la completud de Ł.

En primer lugar, se prueba por inducción que, para un conjunto Σ de fórmulas, toda consecuencia sintáctica de Σ es consecuencia semántica de Σ. Daremos aquí la prueba, ya que los teoremas análogos del CPC y del CPI no fueron demostrados en detalle.

Teorema 9.5.1. *Dados $\Sigma \subseteq \mathcal{L}_{Ł}$ y $A \in \mathcal{L}_{Ł}$, si $\Sigma \vdash A$ entonces $\Sigma \vDash A$.*

Demostración. Haremos inducción sobre el número de pasos de la prueba de A a partir de Σ.

Si la prueba de A tiene un paso, entonces A es instancia de un axioma o está en Σ. En ambos casos $v(A) = 1$ para todo modelo v de Σ.

Supongamos que $\Sigma \vDash C$ para toda fórmula C tal que puede derivarse de Σ en menos de k pasos. Sea $A_1, \ldots, A_k = A$ una prueba de A. Luego, existen $1 < i, j \leq k$ tales que $A_j = A_i \to A$. Por la hipótesis inductiva, dado un modelo v de Σ, se tiene que $v(\mathrm{A}_i) = v(\mathrm{A}_j) = 1$. Luego: $1 = 1 \to v(\mathrm{A})$, de donde $v(\mathrm{A}) = 1$. $\square$

La recíproca de este teorema no es cierta en general. Pero sí vale para $\Sigma = \emptyset$, como veremos en seguida.

Teorema 9.5.2 (Completud). *Dada* $\mathrm{A} \in \mathcal{L}_{Ł}$,

$$\vdash \mathrm{A} \;\; \textit{si y solo si} \;\; \models \mathrm{A}.$$

Demostración. En virtud del Teorema 9.5.1 deducimos que $\vdash \mathrm{A}$ implica $\models \mathrm{A}$. Sea ahora A tal que $\models \mathrm{A}$, es decir, A válida. Supongamos que $\nvdash \mathrm{A}$ y por lo tanto, $|\mathrm{A}| \neq 1$. Luego, existe una valuación que es la aplicación canónica $p : \mathcal{L}_{Ł} \longrightarrow A_{Ł}$ para la cual $p(\mathrm{A}) \neq 1$. Por lo tanto, A no es válida, lo cual es un absurdo. Por lo tanto concluimos que $\vdash \mathrm{A}$. $\square$

Enunciamos a continuación el teorema que nos dice en qué caso vale la recíproca del Teorema 9.5.1.

Teorema 9.5.3. *Sean* $\Sigma \subseteq \mathcal{L}_{Ł}$ *y* $\mathrm{A} \in \mathcal{L}_{Ł}$. *Si* $|\Sigma^{\vdash}|$ *es intersección de filtros maximales de* $A_{Ł}$, *entonces*

$$\Sigma \models \mathrm{A} \;\; \textit{implica} \;\; \Sigma \vdash \mathrm{A}.$$

9.6. Ejercicios

1. Usando una instancia de (Ł2) y aplicando (**C**) probar que (**B**) es un teorema.

2. Dar una derivación de (A → ¬B) → (B → ¬A).

3. Definimos sobre $A_Ł$ las siguientes operaciones:

$$|\mathrm{A}| \oplus |\mathrm{B}| = |\neg \mathrm{A} \to \mathrm{B}|,$$
$$\neg|\mathrm{A}| = |\neg \mathrm{A}|,$$
$$0 = \neg \emptyset^{\vdash}.$$

   Probar que $\langle A_Ł, \oplus, \neg, 0\rangle$ es una MV-álgebra.

4. Probar que las siguientes afirmaciones son equivalentes:

   a) $\mathrm{A} \in \emptyset^{\vdash}$.

   b) Para toda fórmula B vale que $\mathrm{B} \to \mathrm{A} \in \emptyset^{\vdash}$.

5. Deducir del ejercicio anterior que $|\mathrm{A}| = \emptyset^{\vdash}$ si y solo si $\vdash \mathrm{A}$.

6. Sean A una MV-álgebra y $x, y \in A$.

   a) Probar que $y \in F(\{x\})$ si y solo si existe $n \in \mathbb{N}$ tal que $x^n \to y = 1$.

   b) Dada la MV-álgebra $[0,1] \times [0,1]$ calcular el filtro generado por $\{(1/3, 1), (3/4, 1)\}$.

7. Sea α una fórmula de Ł cuyas variables son $p_1, p_2, \ldots, p_n$. Definimos recursivamente una función $f_\alpha : [0,1]^n \longrightarrow [0,1]$ del siguiente modo: a) Si $\alpha = p_i$ entonces f_α es la i-ésima proyección, es decir, $f_\alpha(a_1, a_2, \ldots, a_n) = a_i$. b) Si $\alpha = \neg\beta$ entonces $f_\alpha = 1 - f_\beta$. c) Si $\alpha = \beta \to \gamma$ entonces $f_\alpha = \mathrm{mín}(1, 1 - f_\beta + f_\gamma)$.

   Calcular f_α para las siguientes fórmulas en una variable p:

   a) p,

   b) $\neg p$,

   c) $p \to p$,

   d) $\neg p \to p$,

   e) $\neg(p \to p)$,

   f)$\neg p \to (\neg p \to p)$,

   g) $p \to \neg p$,

   h) $\neg(p \to \neg p)$.

8. Calcular las sucesiones de Farey y los sombreros de Schauder para $d = 3, 4$. Calcular los términos asociados a estos y sus fórmulas correspondientes.

Bibliografía del Capítulo 9

- Balbes R. and Dwinger, P., *Distributive Lattices.* University of Missouri Press, 1974.
- Blok W. J. and Pigozzi D., *Algebraizable Logics.* Memoirs Amer. Math. Soc., 77 (1989), no. 396.
- Boicescu V., Filipoiu A., Georgescu G. and Rudeanu, S., *Łukasiewicz–Moisil algebras.* Annals of Discrete Mathematics, vol. 49, North-Holland, 1991.
- Cignoli R., *Some algebraic aspects of many valued logics.* In: Proceedings of the Third Brazilian Conference on Mathematical Logic (Inst. Math., Fed. Univ. Pernambuco, Recife, 1979), 49–69, Soc. Brasil. Lógica, São Paulo, 1980.
- Cignoli R. and Sagastume de Gallego M., *The lattice structure of some Łukasiewicz algebras.* Algebra Universalis, 13 (1981), 315–328.
- Cignoli R., *Proper n-valued Łukasiewicz algebras as S-algebras of Łukasiewicz n-valued propositional calculi.* Studia Logica, 41 (1982), 3–16.
- Cignoli R., D'Ottaviano I. and Mundici D., *Álgebras das Lógicas de Łukasiewicz.* Coleção CLE, vol. 12. Centro de Lógica, Epistemología e História da Ciencia, Universidade Estadual de Campinas, Campinas, San Pablo, 1994.
- Lewin R., *Lógica Algebraica Abstracta.* Apuntes de un curso dictado en Chile, Colombia y Argentina, 2008. Ver Capítulo 10 del presente texto.
- Mundici D., *MV-algebras are categorically equivalent to bounded commutative BCK-algebras.* Math. Japonica, 31 (1986), no. 6, 889–894.
- Sagastume M., *Bounded commutative B-C-K logic and Łukasiewicz logic.* Manuscrito Rev. Int. Filos. (Campinas), 28(2005) no. 2, 575–583.

Capítulo 10

Lógica algebraica abstracta

En este capítulo reproducimos las notas que fueron escritas por el Profesor Renato Lewin, de la Pontificia Universidad Católica de Chile, para un cursillo dictado en la Universidad Nacional de La Plata, en junio de 2008. Están basadas en varios cursillos similares dictados previamente por dicho profesor en Chile, Colombia y Argentina.

Hemos conservado la nomenclatura original del texto, aunque la notación tiene algunas diferencias con la usada en el resto del libro.

El lector encontrará tal vez definiciones y resultados que han sido dados previamente, pero que aquí son prerrequisitos para enfocar el tema principal, la Lógica Algebraica Abstracta. De esta manera, este capítulo puede leerse independientemente de los precedentes.

10.1. Preliminares: Lógica Proposicional

Desarrollaremos aquí los conceptos básicos mínimos de lógica proposicional necesarios a modo de introducción del tema. Algunos libros que sirven como referencia en el tema son [14, 76, 92, 91, 107].

Lógicas y Sistemas Deductivos

En esta sección definiremos la relación de *derivabilidad* $\Gamma \vdash \psi$ entre fórmulas y conjunto de fórmulas, que refleje las propiedades de la relación de consecuencia lógica en el siguiente sentido:

- Debe ser una relación sintáctica, es decir, debe depender solo de la forma lógica de las oraciones y no de su significado; esta condición es la que facilita la aplicación de métodos matemáticos.

- Debe ser *correcta*, es decir, si $\Gamma \vdash \psi$, entonces $\Gamma \vDash \psi$. No debe ser posible demostrar cosas que no son consecuencia lógica de la premisas.

- Debe ser *completa*, o sea, si $\Gamma \vDash \psi$, entonces $\Gamma \vdash \psi$. Esta es la propiedad que andamos buscando, ser capaces de demostrar sintácticamente a partir de Γ todas sus consecuencias lógicas.

Como hicimos notar anteriormente, introducir un lenguaje formalizado es imprescindible para establecer la estructura lógica de las oraciones y argumentos. Es necesaria también para eliminar las ambiguedades de los lenguajes naturales. Resulta también útil para aplicarles herramientas matemáticas.

Un *lenguaje proposicional*, o simplemente un *lenguaje*, es un conjunto $\mathcal{L}$ de símbolos llamados *conectivos lógicos*. Cada conectivo está asociado con un número natural, su *aridad* (o rango). Estos definen el *tipo de similaridad* del lenguaje, una función $\rho : \mathcal{L} \longrightarrow \mathbb{N}$, que en adelante subentenderemos sin mayor mención. Las constantes son consideradas conectivos de aridad cero.

El conjunto $\mathcal{F}m_{\mathcal{L}}$ de las *fórmulas* de $\mathcal{L}$ se define recursivamente a partir de los conectivos lógicos y de un conjunto $\mathcal{P} = \{p_j : j \in \mathbb{N}\}$ de *variables proposicionales* aplicando un número finito de las reglas siguientes:

- $\mathcal{P} \subseteq \mathcal{F}m_{\mathcal{L}}$.

- Si $\omega \in \mathcal{L}$ es un conectivo n-ario y $\varphi_1, \ldots, \varphi_n \in \mathcal{F}m_{\mathcal{L}}$, entonces $\omega(\varphi_1, \varphi_2, \ldots, \varphi_n) \in \mathcal{F}m_{\mathcal{L}}$.

Si ω es un conectivo binario, usaremos la notación habitual $\varphi_1 \; \omega \; \varphi_2$, en lugar de $\omega(\varphi_1, \varphi_2)$.

Lema 10.1.1. *$\mathcal{F}m_{\mathcal{L}}$ es el menor conjunto que contiene a $\mathcal{P}$ y que es cerrado bajo todos los conectivos lógicos. Es decir, si consideramos los conectivos como funciones $\widehat{\omega} : \mathcal{F}m_{\mathcal{L}}{}^n \longrightarrow \mathcal{F}m_{\mathcal{L}}$, donde n es la aridad de ω, y $\widehat{\omega}(\varphi_1, \varphi_2, \ldots, \varphi_n) = \omega(\varphi_1, \varphi_2, \ldots, \varphi_n)$.*

Ejemplos 10.1.2.

1. El conjunto $\mathcal{F}m_{\mathcal{L}}$ contiene por lenguaje los conectivos $\mathcal{L} = \{\rightarrow, \wedge, \vee, \neg\}$ y su tipo de similaridad es $\langle 2, 2, 2, 1\rangle$.

El conjunto $\mathcal{L}$ contiene, además de las variables proposicionales, elementos de la forma $\varphi_1 \rightarrow \varphi_2$, $\varphi_1 \wedge \varphi_2$, $\varphi_1 \vee \varphi_2$ y $\neg\varphi_1$, siendo φ_1, φ_2 fórmulas.

2. El lenguaje de las lógicas modales agrega al anterior un conectivo unario $\Box$, llamado operador de necesitación de tal modo que si φ es una fórmula, $\Box\varphi$ también lo es.

Una función $s : \mathcal{P} \longrightarrow \mathcal{F}m_{\mathcal{L}}$ se puede extender recursivamente de manera única a la función $\bar{s} : \mathcal{F}m_{\mathcal{L}} \longrightarrow \mathcal{F}m_{\mathcal{L}}$ como sigue:

$$\bar{s}(\varphi(p_1, \ldots, p_n)) = \varphi(s(p_1), \ldots, s(p_n)).$$

A dicha función la llamaremos *sustitución* y la denotaremos por la misma letra s. Para cada $\Gamma \subseteq \mathcal{F}m_{\mathcal{L}}$ denotaremos $s(\Gamma)$ al conjunto de fórmulas $s(\Gamma) = \{s(\gamma) : \gamma \in \Gamma\}$.

Una *regla de inferencia* sobre $\mathcal{L}$ es un par $\langle \Gamma, \varphi \rangle$, donde $\Gamma \subseteq \mathcal{F}m_{\mathcal{L}}$, Γ es finito y $\varphi \in \mathcal{F}m_{\mathcal{L}}$.

Diremos que ψ es *directamente demostrable* a partir de Δ por la regla $\langle \Gamma, \varphi \rangle$, si existe una sustitución s tal que $s(\varphi) = \psi$ y $s(\Gamma) \subseteq \Delta$.

Un *axioma* es una regla de la forma $\langle \emptyset, \psi \rangle$. Cualquier sustitución de un axioma es directamente demostrable a partir de cualquier conjunto de fórmulas Δ. Cada sustitución será una *instancia* del axioma. Una formula tal que $\emptyset \vdash_{\mathcal{S}} \varphi$ es un *teorema* de $\mathcal{S}$ y lo denotamos simplemente $\vdash_{\mathcal{S}} \varphi$

Un *sistema deductivo* $\mathcal{S}$ sobre $\mathcal{L}$ está determinado por un conjunto de axiomas y de reglas de inferencia. Entenderemos a $\mathcal{S}$ como un par $\langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ donde $\vdash_{\mathcal{S}}$ es una relación entre conjuntos de fórmulas y fórmulas definida de la manera siguiente:

$\Delta \vdash_{\mathcal{S}} \psi$ si y solo si existe una sucesión finita $\langle \varphi_1, \varphi_2, \ldots, \varphi_n \rangle$ de fórmulas de $\mathcal{F}m_{\mathcal{L}}$, tal que $\varphi_n = \psi$ y para todo $i \leq n$, se cumple alguna de las condiciones siguientes:

- φ_i es una instancia de un axioma,
- $\varphi_i \in \Delta$,
- para ciertos $i_1, i_2, \ldots, i_k$ todos menores que i, φ_i es directamente demostrable a partir de Δ.

Esta sucesión se llama una *demostración de ψ a partir de Δ*.

Ejemplos 10.1.3.
1. El Cálculo Proposicional Clásico (Versión 2). El lenguaje $\mathcal{L} = \{\rightarrow, \neg\}$.

Axiomas:

A1 $\quad p \rightarrow (q \rightarrow p)$.

A2 $\quad (p \rightarrow q) \rightarrow ((p \rightarrow (q \rightarrow r)) \rightarrow (p \rightarrow r))$.

A3 $\quad (\neg p \rightarrow \neg q) \rightarrow (q \rightarrow p)$.

Regla:

MP $\quad p \rightarrow q\ , p \vdash_{S4} q$.

Ejemplo. Demostrar $\vdash_{CPC}\ p \to p$.

$\varphi_1 = p \to (p \to p)$, (A1),
$\varphi_2 = (p \to (p \to p)) \to ((p \to ((p \to p) \to p)) \to (p \to p))$, (A2),
$\varphi_3 = (p \to ((p \to p) \to p)) \to (p \to p)$, (MP),
$\varphi_4 = p \to ((p \to p) \to p)$, (A1),
$\varphi_5 = p \to p$, (MP).

$\langle \varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5 \rangle$ es una demostración de $p \to p$ a partir del conjunto vacío, o sea, es un teorema del CPC.

2. El sistema de lógica modal S_4 tiene el lenguaje de CPC (con o sin los conectivos para disyunción y conjunción) y el conectivo unario $\Box$.

Axiomas:

A1 Todas las tautologías del CPC son axiomas.

A2 $\Box(p \to q) \to (\Box p \to \Box q)$.

A3 $\Box p \to p$.

A4 $\Box p \to \Box\Box p$.

Reglas:

MP $p \to q\ , p \vdash_{S4}\ q$,

N $p \vdash_{S4}\ \Box p$.

3. Un sistema deductivo puede ser aún más abstracto. Consideremos el lenguaje $\mathcal{L} = \{\ \cdot\ ,\ ^{-1}, e\}$ y sobre él definamos el sistema $\mathcal{G}$.

G1 $((p \cdot q) \cdot r) \cdot (p \cdot (q \cdot r))^{-1}$,

G2 $(p \cdot e) \cdot p^{-1}$,

G3 $(e \cdot p) \cdot p^{-1}$,

G4 $p \cdot p^{-1}$,

G5 $p^{-1} \cdot p$.

Reglas:

R1 $p \cdot q^{-1} \vdash_{\mathcal{G}}\ q \cdot p^{-1}$, R2 $\quad p \cdot q^{-1} \vdash_{\mathcal{G}} p^{-1} \cdot q^{-1^{-1}}$,

R3 $\quad \{p \cdot q^{-1}\ ,\ q \cdot r^{-1}\} \vdash_{\mathcal{G}} p \cdot r^{-1}$,

R4 $\quad \{p \cdot q^{-1}\ ,\ r \cdot s^{-1}\} \vdash_{\mathcal{G}} (p \cdot r) \cdot (q \cdot s)^{-1}$,

R5 $\quad p \vdash_{\mathcal{G}} p \cdot e^{-1}$,

R6 $\quad p \cdot e^{-1} \vdash_{\mathcal{G}} p$.

El sistema deductivo del primer ejemplo está asociado a la Lógica Proposicional Clásica, en el sentido de que es un sistema correcto y completo:

$$\Gamma \vDash \varphi \quad \text{si y solo si} \quad \Gamma \vdash \varphi.$$

Si se agregan las definiciones

$$p \vee q := \neg p \to q,$$
$$p \wedge q := \neg(p \to \neg q),$$

en él se pueden probar todos los axiomas conocidos correspondientes a conjunciones y disyunciones. La demostración de la completud de los sistemas CPC se puede encontrar en [14, 76].

En el caso del sistema de lógica modal $\mathcal{S}_4$ de Lewis, no hemos desarrollado una semántica con respecto a la cual el sistema sea completo, sin embargo esta existe y se puede estudiar, por ejemplo, en [63].

La pregunta obvia aquí es: ¿A qué lógica corresponde el sistema deductivo del cuarto ejemplo?

Lema 10.1.4. *Si $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ es un sistema deductivo, entonces $\Delta \vdash_{\mathcal{S}} \psi$ si y solo si ψ pertenece al conjunto más pequeño de fórmulas que contiene a Δ, a todas las sustituciones de los axiomas y es cerrado bajo pruebas directas.*

La relación $\vdash_{\mathcal{S}}$, llamada *relación de consecuencia* de $\mathcal{S}$, satisface:

Lema 10.1.5 ([8, p. 5])**.** *Si $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ es un sistema deductivo, entonces para todo $\Gamma, \Delta \subseteq \mathcal{F}m_{\mathcal{L}}$ y $\varphi, \psi \in \mathcal{F}m_{\mathcal{L}}$ se tiene:*

1. *$\Delta \vdash_{\mathcal{S}} \varphi$, para todo $\varphi \in \Delta$.*
2. *Si $\Delta \vdash_{\mathcal{S}} \psi$ y $\Delta \subseteq \Gamma$, entonces $\Gamma \vdash_{\mathcal{S}} \psi$.*
3. *Si $\Delta \vdash_{\mathcal{S}} \psi$ y $\Gamma \vdash_{\mathcal{S}} \varphi$, para todo $\varphi \in \Delta$, entonces $\Gamma \vdash_{\mathcal{S}} \psi$.*
4. *Si $\Delta \vdash_{\mathcal{S}} \psi$, entonces existe $\Gamma \subseteq \Delta$ finito tal que $\Gamma \vdash_{\mathcal{S}} \psi$. Diremos que $\mathcal{S}$ es* finitario.

5. *Si* $\Delta \vdash_{\mathcal{S}} \psi$*, entonces* $s(\Delta) \vdash_{\mathcal{S}} s(\psi)$*, para toda sustitución* s*. Diremos que* $\mathcal{S}$ *es* estructural.

Cualquier relación que satisfaga 1–5 es la relación de consecuencia de algún sistema deductivo. Podemos así definir un sistema deductivo como un par $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$, donde $\vdash_{\mathcal{S}}$ es una relación entre conjuntos de fórmulas y fórmulas que verifica 1–5. Nótese que esta definición no hace alusión alguna a reglas de inferencia ni a axiomas.

10.2. Preliminares: Álgebra Universal

El Álgebra Universal es la rama del álgebra que estudia propiedades comunes a distintos tipos de álgebras. En esta sección veremos algunos conceptos elementales que son necesarios para el desarrollo posterior. Para un estudio más profundo se puede consultar [13, 75].

Álgebras

Dado un lenguaje $\mathcal{L} = \{\omega_1, \omega_2, \ldots, \omega_n\}$, una *$\mathcal{L}$-álgebra* es una estructura $\mathbf{A} = \langle A; {\omega_1}^{\mathbf{A}}, {\omega_2}^{\mathbf{A}}, \ldots, {\omega_n}^{\mathbf{A}} \rangle$, donde A es un conjunto no vacío llamado el *universo* de $\mathbf{A}$ y para cada $i \in \{1, \ldots, n\}$, ${\omega_i}^{\mathbf{A}}$ es una operación sobre A de la misma aridad que ω_i, i.e., una función ${\omega_i}^{\mathbf{A}} : A^n \longrightarrow A$, donde n es la aridad de ω_i. Para toda esta sección se puede consultar el excelente libro [13].

Obsérvese que mientras ω_i es un símbolo lingüístico, su asociada ${\omega_i}^{\mathbf{A}}$ es una función con un dominio y un rango bien determinados. Sin embargo, para aliviar la notación, generalmente omitimos el superíndice $\mathbf{A}$, si se subentiende el álgebra de la que se está hablando y no hay riesgo de confusión.

Ejemplos 10.2.1.

1. En general, la mayoría de las estructuras estudiadas en un curso de Álgebra Abstracta son álgebras: grupos anillos, espacios vectoriales, retículos, álgebras de Boole, etc. Una excepción son los cuerpos: en ellos el inverso multiplicativo no es una operación ya que no está definida para 0. Llamamos a este tipo de estructura *álgebras parciales* y su teoría es mucho más compleja que la de las álgebras.

2. Un ejemplo importante para nosotros es el álgebra $\boldsymbol{\mathcal{F}m_{\mathcal{L}}}$, cuyo universo es el conjunto $\mathcal{F}m_{\mathcal{L}}$ de las fórmulas de un lenguaje proposicional $\mathcal{L}$ y cuyas operaciones se definen de la manera obvia: para cada conectivo n-ario $\omega \in \mathcal{L}$ y fórmulas $\varphi_1, \ldots, \varphi_n$,

$$\omega^{\boldsymbol{\mathcal{F}m_{\mathcal{L}}}}(\varphi_1, \ldots, \varphi_n) = \omega(\varphi_1, \ldots, \varphi_n).$$

$\mathcal{Fm}_{\mathcal{L}}$ es conocida también como el *álgebra fórmulas de* $\mathcal{L}$ o el álgebra *totalmente libre sobre el conjunto* $\mathcal{P}$ de las variables proposicionales.

3. Análogamente, dados un lenguaje algebraico $\mathcal{L}$ y un conjunto X de *variables*, construimos el conjunto $Term(X)$ de los *términos sobre* X de la misma manera como construimos las fórmulas de la lógica. Con este conjunto como universo construimos en el álgebra totalmente libre de términos $\mathbf{Term}(\mathbf{X})$ de una manera similar a las de las fórmulas del ejemplo anterior.

Construcciones Básicas

A partir de un conjunto de álgebras del mismo tipo se puede construir otras. Tres son las construcciones más elementales: subálgebras, productos directos e imágenes homomorfas. Todas ellas han sido estudiadas por el lector en algún curso de estructuras algebraicas o similar, por lo que no es necesario dar ejemplos.

Sean $\mathbf{A} = \langle A; {\omega_1}^{\mathbf{A}}, {\omega_2}^{\mathbf{A}}, \ldots, {\omega_n}^{\mathbf{A}} \rangle$ y $\mathbf{B} = \langle B; {\omega_1}^{\mathbf{B}}, {\omega_2}^{\mathbf{B}}, \ldots, {\omega_n}^{\mathbf{B}} \rangle$ dos álgebras. $\mathbf{B}$ es *subálgebra* de $\mathbf{A}$, lo que denotamos $\mathbf{B} \leq \mathbf{A}$, si $B \subseteq A$ es no vacío y cada operación ${\omega_i}^{\mathbf{B}}$ de $\mathbf{B}$ es la restricción a B de la operación correspondiente de $\mathbf{A}$.

Si $B \subseteq A$, para que exista una subálgebra con universo B, basta que este sea no vacío y cerrado bajo todas las operaciones de $\mathbf{A}$.

Un *homomorfismo* entre dos álgebras $\mathbf{A}$ y $\mathbf{B}$ del mismo tipo es una función $f : A \longrightarrow B$ tal que para cada operación n-aria ω

$$f(\omega^{\mathbf{A}}(a_1, a_2, \ldots, a_n)) = \omega^{\mathbf{B}}(f(a_1), f(a_2), \ldots, f(a_n)).$$

Es inmediato que $f(A)$ es no vacío y cerrado bajo las operaciones de $\mathbf{B}$, por lo tanto existe una subálgebra de $\mathbf{B}$ cuyo universo es $f(A)$. Esta se llama la *imagen homomorfa de* $\mathbf{A}$ y la denotamos $f(\mathbf{A})$.

Un homomorfismo biyectivo es un *isomorfismo*. En tal caso, $f(\mathbf{A}) = \mathbf{B}$ y decimos que $\mathbf{A}$ y $\mathbf{B}$ son *isomorfas*, lo que denotamos $\mathbf{A} \cong \mathbf{B}$. Si bien lo presentamos como un caso particular, el concepto de isomorfismo es más elemental que el de homomorfismo. Dos álgebras isomorfas son *iguales* en todo sentido algebraico, solo difieren en sus elementos y los símbolos usados para denotar sus operaciones.

Dada una familia $\langle \mathbf{A}_i : i \in I \rangle$ de álgebras del mismo tipo, su *producto directo* $\mathbf{A} = \prod_{i \in I} \mathbf{A}_i$ es el álgebra cuyo universo es el conjunto de todas las funciones

$$f : I \longrightarrow \bigcup_{i \in I} A_i$$

tales que para cada $i \in I$, $f(i) \in A_i$ y para cada operación n-aria ω, y $f_1, f_2, \ldots, f_n$ elementos de A,

$$\omega^{\mathbf{A}}(f_1, f_2, \ldots, f_n) \,:\, I \longrightarrow \bigcup_{i\in I} \mathbf{A}_i$$

esta definida por

$$\omega^{\mathbf{A}}(f_1, f_2, \ldots, f_n)(i) = \omega^{\mathbf{A}_i}(f_1(i), f_2(i), \ldots, f_n(i)).$$

Abusando un poco de la nomenclatura, podemos considerar I como el conjunto de las coordenadas de los elementos de A, de tal manera que cada coordenada de un elemento de A pertenece al (universo del) álgebra correspondiente y las operaciones se hacen coordenada a coordenada. De hecho, si I es finito, el producto directo de $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ es isomorfo al producto cartesiano $\mathbf{A}_1 \times \mathbf{A}_2 \times \cdots \times \mathbf{A}_n$.

Una *variedad* es una clase de álgebras cerrada bajo imágenes homomorfas, subálgebras y productos directos.

Ecuaciones

Una $\mathcal{L}$-*ecuación* (o simplemente *ecuación*) ([8, p. 13]) es una expresión de la forma $\varphi \approx \psi$, donde $\varphi, \psi \in \mathit{Term}(X)$. Denotaremos al conjunto de las ecuaciones de $\mathcal{L}$ por $Eq_{\mathcal{L}}$.

En el Álgebra Abstracta se estudian clases de álgebras, de un tipo de similaridad dado, definidas por ciertas propiedades o axiomas. Para nosotros revisten especial importancia aquellas clases de álgebras que satisfacen ciertas ecuaciones, o *clases ecuacionales*. Un importante teorema demostrado por Birkhoff dice que una clase de álgebras es ecuacional si y solo si es una variedad (ver [13, p. 75]).

Ejemplos 10.2.2. La mayoría de las clases de álgebras conocidas por el lector, por ejemplo, retículos, álgebras de Boole, anillos, grupos, ℓ-grupos, etc., son variedades por poder axiomatizarse por ecuaciones.

Algunos Resultados sobre Retículos

En esta sección veremos algunas propiedades de los retículos que serán usadas más adelante.

Un retículo $\mathbf{L}$ se dice *completo* si para todo $A \subseteq L$, existen el supremo y el ínfimo de A, denotados por $\bigvee A$ y $\bigwedge A$, respectivamente. En particular, $\bigvee L = 1$ y $\bigwedge L = 0$.

Ejemplos 10.2.3.

1. El retículo $\langle \mathcal{P}(X); \cup, \cap \rangle$ de todos los subconjuntos de un conjunto X, es completo.

2. Los retículos $\langle \mathcal{SU}(\mathbf{G}); \vee, \wedge \rangle$ y $\langle \mathcal{SUN}(\mathbf{G}); \vee, \wedge \rangle$ de todos los subgrupos y de todos los subgrupos normales de un grupo $\mathbf{G}$, respectivamente, son completos. En ambos caso las operaciones son $\mathbf{H} \vee \mathbf{K} = \langle H \cup K \rangle$ y $\mathbf{H} \wedge \mathbf{K} = \mathbf{H} \cap \mathbf{K}$, donde $\langle A \rangle$ es el subgrupo (normal, en el segundo caso) generado por A.

3. $\mathbb{Q}$ y $\mathbb{R}$ con sus ordenes habituales no son retículos completos. Si a $\mathbb{R}$ le agregamos un punto final $+\infty$ y un punto inicial $-\infty$, entonces $\overline{\mathbb{R}}$ es completo.

Lema 10.2.4. *Un retículo es completo si y solo si es cerrado bajo supremos. Lo mismo ocurre si es cerrado bajo ínfimos.*

Un elemento c de un retículo $\mathbf{L}$ es *compacto* si toda vez que $c \leq \bigvee A$ (obsérvese que esto presupone que tal supremo existe), hay un subconjunto finito $B \subseteq A$ tal que $c \leq \bigvee B$.

Un retículo es *algebraico* si es completo, y todos sus elementos son el supremo de un conjunto de elementos compactos.

Ejemplos 10.2.5.

1. El retículo $\mathcal{P}(X)$ es algebraico. Los elementos compactos son los subconjuntos finitos de X.

2. Los retículos $\mathcal{SU}(\mathbf{G})$ y $\mathcal{SUN}(\mathbf{G})$ son algebraicos. En ambos casos los elementos compactos son los subgrupos finitamente generados.

3. $\overline{\mathbb{R}}$ no es un retículo algebraico. De hecho, no tiene elementos compactos.

Relaciones de Equivalencia y Congruencias

Una relación binaria ϑ sobre un conjunto A es *de equivalencia* si es reflexiva, simétrica y transitiva.

Una relación de equivalencia ϑ particiona al conjunto en *clases de equivalencia*, vale decir, conjuntos formados por elementos relacionados entre sí. Más técnicamente, la *clase de equivalencia de a módulo ϑ* es el conjunto

$$[a]_\vartheta = \{x \in A : x\vartheta a\}.$$

El conjunto de todas las clases de equivalencia módulo ϑ se denomina *cociente* de A módulo ϑ.

Desde el punto de vista algebraico es interesante hacer notar que el par $\langle E(A), \subseteq\rangle$, de todas las relaciones de equivalencia sobre A ordenado por inclusión, es un retículo distributivo completo. Las operaciones de supremo e ínfimo sobre $E(A)$ están dadas por:

$$\vartheta_1 \wedge \vartheta_2 = \vartheta_1 \cap \vartheta_2,$$
$$\vartheta_1 \vee \vartheta_2 = \bigcap\{\vartheta : \vartheta_1 \cup \vartheta_2 \subseteq \vartheta\}.$$

Hay también una forma constructiva de definir el supremo:

$$\vartheta_1 \vee \vartheta_2 = \{\langle a, b\rangle : \text{ existen } c_0, \ldots, c_n \text{ tales que } c_0 = a,\ c_n = b \text{ y para cada } i,\ c_i\vartheta_1 c_{i+1} \text{ o bien } c_i\vartheta_2 c_{i+1}\}.$$

La completud del retículo $E(A)$ se obtiene porque dada una familia de relaciones de equivalencia sobre A, su intersección también lo es, es decir, si para cada $i \in I$, ϑ_i es una relación de equivalencia sobre A, entonces $\bigcap_{i\in I} \vartheta_i$ es una relación de equivalencia sobre A. Por otra parte, notemos que tanto la identidad, denotada por $\triangle_A$, como la relación trivial ∇_A, son relaciones de equivalencia sobre A. Tenemos que

$$\bigwedge_{i\in I} \vartheta_i = \bigcap_{i\in I} \vartheta_i.$$

Una relación de equivalencia sobre (el universo de) un álgebra $\mathbf{A}$ es una *congruencia sobre* $\mathbf{A}$ si es compatible con todas las operaciones del álgebra, vale decir, para cada operación n-aria ω y elementos a_i, $b_i \in A$, si $a_i\vartheta b_i$ para $i \leq n$, se verifica

$$\omega^{\mathbf{A}}(a_1, \ldots, a_n)\vartheta\omega^{\mathbf{A}}(b_1, \ldots, b_n).$$

La condición de compatibilidad nos dice que si escogemos representantes de ciertas clases de equivalencia y los operamos, la clase a la que pertenece el resultado no depende de los elementos particulares que se usaron, sino de las clases de las que fueron tomados. Esto es lo que nos permite definir una estructura algebraica sobre el conjunto cociente de la siguiente manera:

$$\mathbf{A} \mid \vartheta = \langle A \mid \vartheta, {\omega_1}^{\mathbf{A}|\vartheta}, {\omega_2}^{\mathbf{A}|\vartheta}, \ldots, {\omega_n}^{\mathbf{A}|\vartheta} \rangle,$$

donde dadas las clases $[a_1]_\vartheta, \ldots, [a_n]_\vartheta$, la operación

$$\omega^{\mathbf{A}|\vartheta}([a_1]_\vartheta, \ldots, [a_n]_\vartheta) = [\ \omega_i^{\mathbf{A}}(a_1, \ldots, a_n)\ ]_\vartheta.$$

La compatibilidad garantiza que esta está bien definida. $\mathbf{A} \mid \vartheta$ se denomina el *álgebra cociente de* $\mathbf{A}$ *por* ϑ.

Para los efectos de estas Notas, lo más interesante es que el conjunto de todas las congruencias sobre un álgebra $\mathbf{A}$, ordenado por inclusión, es un retículo distributivo y algebraico al que denotamos $Con(\mathbf{A})$. Los elementos compactos son las congruencias finitamente generadas.

Ejemplos 10.2.6.

1. Si $\mathbf{G}$ es un grupo y $\mathbf{N}$ un subgrupo normal de $\mathbf{G}$, entonces la relación $x\vartheta y$ si y solo si $x\,y^{-1} \in \mathbf{N}$ es una congruencia. El grupo cociente $\mathbf{G} \mid \vartheta$ es por supuesto el mismo que el grupo cociente $\mathbf{G} \mid \mathbf{N}$ que el lector ha estudiado en sus cursos de álgebra abstracta. Un caso particular interesante es cuando el grupo es $\mathbb{Z}$ y el subgrupo es $n\mathbb{Z}$. En este caso, la relación anterior es la conocida congruencia módulo n de la teoría de números, de donde se ha tomado prestado el nombre.

2. Sobre el retículo de cuatro elementos $0 < a < b < 1$, considere la congruencia que identifica 0 con a y 1 con b. El retículo cociente tiene dos elementos $[0] < [1]$.

Operadores de Clausura

(Ver por ejemplo [13, Cap. 1, §4 y §5]).

Un *operador de clausura* sobre un conjunto A es una función $\mathbf{C} : \mathcal{P}(A) \longrightarrow \mathcal{P}(A)$ que satisface lo siguiente:

(C1) $X \subseteq \mathbf{C}(X)$.

(C2) $\mathbf{C}(\mathbf{C}(X)) \subseteq \mathbf{C}(X)$.

(C3) $X \subseteq Y$ implica $\mathbf{C}(X) \subseteq \mathbf{C}(Y)$.

Si además $\mathbf{C}$ verifica:

(C4) $\mathbf{C}(X) = \bigcup\{\mathbf{C}(Y) : Y \subseteq X \text{ e } Y \text{es finito}\}$,

decimos que $\mathbf{C}$ es un operador de clausura *algebraico*.

Ejemplos 10.2.7.

1. En un espacio topológico $X \longmapsto \overline{X}$ es un operador de clausura sobre X, donde recordemos que $\overline{X}$ significa la clausura de X.

2. La identidad es un operador de clausura sobre cualquier conjunto.

3. Si $\mathbf{G}$ es un grupo, entonces la función $X \longmapsto \langle X \rangle$ que envía cualquier subconjunto de G en el (universo del) subgrupo que genera, es un operador de clausura sobre G.

Teorema 10.2.8. *Sea* $\mathbf{C}$ *un operador de clausura sobre un conjunto* A*. Entonces el conjunto* $L_{\mathbf{C}} = \{X \subseteq A : \mathbf{C}(X) = X\}$ *dotado de las operaciones*

$$\bigvee_{i\in I} \mathbf{C}(A_i) = \mathbf{C}\left(\bigcup_{i\in I} A_i\right) \qquad y \qquad \bigwedge_{i\in I} \mathbf{C}(A_i) = \bigcap_{i\in I} \mathbf{C}(A_i)$$

es un retículo completo. Los elementos de $L_{\mathbf{C}}$ *se llaman* conjuntos cerrados.

Si además $\mathbf{C}$ *es un operador algebraico,* $\mathbf{L}_{\mathbf{C}}$ *es un retículo algebraico en el que los elementos compactos son los subconjuntos cerrados* $\mathbf{C}(B)$*, para algún* B *finito.*

Teorema 10.2.9. *Todo retículo algebraico es isomorfo al retículo de los subconjuntos cerrados de algún conjunto dotado de un operador de clausura algebraico.*

Idea de la demostración. Sea $\mathbf{L}$ un retículo algebraico y C el conjunto de sus elementos compactos. Para $X \subseteq L$ definimos

$$\mathbf{C}(X) = \{c \in C : c \leq \bigvee X\}.$$

Entonces $\mathbf{C}$ es un operador de clausura algebraico. La función

$$\begin{aligned} f \,:\, \mathbf{L} &\longrightarrow \mathcal{P}(C) \\ x &\longmapsto \{c \in C : c \leq x\}, \end{aligned}$$

es un isomorfismo. □

Un Ejemplo Importante

Sea $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ un sistema deductivo. Si definimos

$$\mathcal{C}n_{\mathcal{S}}(\Delta) = \{\varphi \in \mathcal{F}m_{\mathcal{L}} \,:\, \Delta \vdash_{\mathcal{S}} \varphi\},$$

$\mathcal{C}n_{\mathcal{S}}$ define un operador

$$\mathcal{C}n_{\mathcal{S}} \,:\, \mathcal{P}(\mathcal{F}m_{\mathcal{L}}) \longrightarrow \mathcal{P}(\mathcal{F}m_{\mathcal{L}})$$

sobre el conjunto de las fórmulas, llamado *operador de consecuencia de* $\mathcal{S}$. Las propiedades 1–5 de $\vdash_{\mathcal{S}}$ que aparecen en el Lema 10.1.5, implican que $\mathcal{C}n_{\mathcal{S}}$ es un operador de clausura algebraico. Se puede hacer el estudio de sistemas deductivos a partir de operadores de consecuencia (ver [8, p. 6]), pero no lo haremos en estas Notas.

Los conjuntos cerrados bajo este operador se llaman $\mathcal{S}$-*teorías*. En otras palabras, una teoría es un conjunto T de fórmulas que es cerrado bajo $\vdash_{\mathcal{S}}$:

$$\text{Si } T \vdash_{\mathcal{S}} \varphi \text{ entonces } \varphi \in T.$$

El conjunto de los teoremas $\mathcal{S}$ (aquellas fórmulas φ tales que $\vdash_{\mathcal{S}} \varphi$, o equivalentemente, aquellas fórmulas directamente demostrables a partir de cualquier conjunto Δ de fórmulas), es la menor $\mathcal{S}$-teoría. Por otra parte, $\mathcal{F}m_{\mathcal{L}}$ es la mayor $\mathcal{S}$-teoría. Observemos que $\mathcal{C}n_{\mathcal{S}}(\Delta)$ es la menor $\mathcal{S}$-teoría que contiene a Δ.

El conjunto de todas las $\mathcal{S}$-teorías se denota $Th\mathcal{S}$ ([8, p. 7]). Sobre este conjunto definimos las operaciones $\wedge^{\mathcal{S}}$ y $\vee^{\mathcal{S}}$, que son respectivamente, la intersección usual de conjuntos y la teoría generada por la unión conjuntista de teorías, es decir, para $T, U \in Th\mathcal{S}$,

$$T \wedge^{\mathcal{S}} U = T \cap U \quad \text{y} \quad T \vee^{\mathcal{S}} U = \mathcal{C}n_{\mathcal{S}}(T \cup U).$$

Observemos que la intersección arbitraria de teorías es una teoría y como $\mathcal{F}m_{\mathcal{L}}$ es la mayor $\mathcal{S}$-teoría, el retículo $\mathbf{Th}\mathcal{S} = \langle Th\mathcal{S}, \wedge^{\mathcal{S}}, \vee^{\mathcal{S}} \rangle$ es un retículo completo. El siguiente lema se desprende fácilmente de las propiedades de los operadores de clausura algebraicos.

Lema 10.2.10 ([8, Lema 1.1])**.** *Sea* $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ *un sistema deductivo.*

1. *Los elementos compactos de* $\mathbf{Th}\mathcal{S}$ *son las* $\mathcal{S}$*-teorías finitamente generadas.*

2. *El retículo* $\mathbf{Th}\mathcal{S}$ *el algebraico.*

3. $Th\mathcal{S}$ *es cerrado bajo uniones dirigidas.*

La Lógica de las Ecuaciones

Lema 10.2.11. *Sean* $\sigma(x_1, x_2, \ldots, x_n) \in Term(X)$ *y* $\mathbf{A}$ *una* $\mathcal{L}$*-álgebra. Una función* $I : X \longrightarrow A$*, definida por* $x_i \longmapsto a_i$ *,* $i \in \omega$*, se extiende de manera única a*

$$\begin{aligned} \bar{I} \, : \, \mathcal{F}m_{\mathcal{L}} &\longrightarrow A \\ \sigma(x_1, x_2, \ldots, x_n) &\longmapsto \sigma^{\mathbf{A}}(a_1, \ldots, a_n). \end{aligned}$$

I se llama una *interpretación* de las variables en $\mathbf{A}$. Por ejemplo, una sustitución s de las letras proposicionales $\mathcal{P}$ es una interpretación de $\mathcal{P}$ en el álgebra $\boldsymbol{\mathcal{F}m}_{\mathcal{L}}$ definida más arriba.

Sea $\mathcal{K}$ una clase de $\mathcal{L}$-álgebras. Definimos la relación $\models_{\mathcal{K}}$ entre un conjunto de ecuaciones y una ecuación de la manera siguiente ([8, p. 13]):

$\Gamma \models_{\mathcal{K}} \sigma \approx \tau$ si y solo si para toda $\mathbf{A} \in \mathcal{K}$ y para toda interpretación $\bar{a} = (a_1, a_2, \ldots, a_n)$ de las variables de $\Gamma \cup \{ \sigma \approx \tau \}$ se tiene:

$$\xi^{\mathbf{A}}(\bar{a}) = \eta^{\mathbf{A}}(\bar{a}) \text{ , para } \xi \approx \eta \in \Gamma \text{ entonces } \sigma^{\mathbf{A}}(\bar{a}) = \tau^{\mathbf{A}}(\bar{a}).$$

Esta relación es llamada *relación de consecuencia ecuacional determinada por* $\mathcal{K}$.

Es fácil ver que la única propiedad de $\vdash_{\mathcal{S}}$ que $\models_{\mathcal{K}}$ no tiene necesariamente es la finitud. Por ejemplo, directamente de la definición se observa que $\models_{\mathcal{K}}$ es estructural.

Lema 10.2.12 ([8, Lema 3.1]). *Si $\mathcal{K}$ es una clase de álgebras entonces para conjuntos de ecuaciones $\Gamma, \Delta \subseteq Eq(X)$ y toda ecuación $\sigma \approx \tau$ se tiene:*

1. $\Delta \models_{\mathcal{K}} \delta \approx \varepsilon$, *para todo* $\delta \approx \varepsilon \in \Delta$.

2. *Si* $\Delta \models_{\mathcal{K}} \sigma \approx \tau$ *y* $\Delta \subseteq \Gamma$, *entonces* $\Gamma \models_{\mathcal{K}} \sigma \approx \tau$.

3. *Si* $\Delta \models_{\mathcal{K}} \sigma \approx \tau$ *y* $\Gamma \models_{\mathcal{K}} \delta \approx \varepsilon$, *para todo* $\delta \approx \varepsilon \in \Delta$, *entonces* $\Gamma \models_{\mathcal{K}} \sigma \approx \tau$.

4. *Si* $\Delta \models_{\mathcal{K}} \sigma \approx \tau$, *entonces* $s(\Delta) \models_{\mathcal{K}} s(\sigma) \approx s(\tau)$, *para toda sustitución* s. *Es decir,* $\models_{\mathcal{K}}$ *es siempre* estructural.

Podemos definir el concepto de operador de clausura $\mathcal{C}n_{\mathcal{K}}$, el de *teoría ecuacional* y el retículo $\mathbf{Th}\mathcal{K}$ de todas las teorías ecuacionales respecto de $\models_{\mathcal{K}}$. El lector interesado puede consultar [13, Cap. 2, §14].

10.3. Lógica Algebraica Abstracta

Lógica Algebraica

Incluso antes del nacimiento de la lógica matemática, George Boole, a mediados del siglo XIX, propuso ciertas “reglas del pensamiento” que anticipaban lo que más tarde se conocería como Álgebras de Boole. Él hizo notar que los conectivos lógicos obedecen a leyes similares a las que rigen a los números y las operaciones algebraicas.

Durante el siglo XX muchos autores contribuyeron a profundizar estas ideas. Probablemente los más importantes son Adolf Lindenbaum y Alfred Tarski. Los trabajos de Tarski, o más precisamente del grupo de Varsovia, (ver [104]) en los años 20 y 30 del siglo pasado son el punto de partida del estudio de los sistemas deductivos en general y de la lógica algebraica tal como se la entiende hoy. En [103] (una versión en inglés aparece en [104]), Tarski introduce el álgebra de fórmulas del cálculo proposicional y define la relación

$$\varphi \sim \psi \quad \text{si y solo si} \quad \vdash_{CPC} \varphi \leftrightarrow \psi.$$

Enseguida muestra que esta es lo que hoy llamamos una congruencia y que el álgebra cociente, que ahora es conocida como el *álgebra de Lindenbaum–Tarski del cálculo proposicional clásico*, es un álgebra de Boole. Recíprocamente, indica cómo construir un sistema deductivo a partir de una axiomatización de las álgebras de Boole.

Conocida esta relación entre el Cálculo Proposicional Clásico y las álgebras de Boole, el método se aplicó a otras lógicas, representadas por otros sistemas deductivos, a los que les corresponden otras clases de álgebras. Entre los principales están:

Lógica Proposicional Clásica	Álgebras de Boole
Lógica Prop. Intuicionista	Álgebras de Heyting
Lógicas Multivaluadas	Álgebras de Wajsberg, MV-álgebras
Lógicas Modales	Álgebras Modales
Lógica de Primer Orden	Álgebras Cilíndricas, Álgebras Poliádicas
etc.	etc-álgebras

¿Qué condiciones debe satisfacer un sistema deductivo para contar con una clase de álgebras asociada? De la misma manera podemos plantearnos la pregunta inversa. Dada una clase de álgebras, ¿corresponde esta a un cierto sistema deductivo?

En los dos importantes libros de Helena Rasiowa y Roman Sikorski [91] y H. Rasiowa [92] se reúnen varias décadas de resultados en esta línea. El tratamiento dado en estos libros se aplica a sistemas con ciertas particularidades, por ejemplo, presupone la existencia de una implicación con ciertas propiedades estándar (ver los ejemplos de la Sección 10.4). Por lo tanto muchos sistemas no son en este sentido algebrizables simplemente porque no cuentan con una implicación, o porque la que tienen no goza de las propiedades adecuadas.

En la década de los '80 Willem Blok y Don Pigozzi decantaron en [8] el trabajo de muchos investigadores en el tema proponiendo una definición general y precisa del concepto de algebrizabilidad. Basados en una generalización del proceso de Lindenbaum–Tarski, ellos proponen un tratamiento más general o "abstracto" del problema, uno que no dependa del lenguaje subyacente del sistema ni de la presencia de ciertos axiomas o reglas predeterminados. Naturalmente, hay muchos sistemas que tampoco son algebrizables en este sentido, sin embargo, no lo son por motivos más profundos y generales que el lenguaje en el que se expresan. ¿Qué tan buena es esta noción de algebrizabilidad? Esta pregunta solo podrá responderse al ver las aplicaciones que la teoría tenga, especialmente, el uso de técnicas del álgebra universal en las clases de álgebras para obtener resultados sobre las lógicas asociadas. En el último tiempo se ha llamado Lógica Algebraica Abstracta al estudio de sistemas deductivos usando herramientas del álgebra universal.

Varios autores han perfeccionado, extendido o modificado estos conceptos iniciales. Ver por ejemplo [9, 31, 30, 41, 59, 60].

Por último, recordemos lo que Paul Halmos nos hace notar en [54]. En matemática es frecuente que se inicie un estudio con un cierto objetivo en mente, por ejemplo una aplicación a la física, pero luego dicho estudio adquiere un interés puramente matemático. La teoría se generaliza y entra en contacto con otras ramas de la matemática y eventualmente se establece como una nueva área de estudio. Esta nueva rama no pretende en general resolver los problemas que le dieron origen. Algo de esto ha pasado con la lógica algebraica, la que ha desarrollado temas y problemas muy distintos de aquellos de la lógica formal, quien le diera origen.

Lógicas Algebrizables

Intuitivamente, un sistema deductivo $\mathcal{S}$ es algebrizable si existe una clase $\mathcal{K}$ de álgebras del mismo tipo y existe una correspondencia entre fórmulas de $\mathcal{F}m_{\mathcal{L}}$ y ecuaciones de $Eq_{\mathcal{L}}$ tal que las relaciones $\vdash_{\mathcal{S}}$ y $\models_{\mathcal{K}}$ sean "equivalentes". Es decir, dada una fórmula α existe una ecuación $\widehat{\alpha}$ y dada una ecuación $s \approx \tau$ existe una fórmula $\widetilde{s \approx \tau}$ tales que:

1. $\Gamma \vdash_{\mathcal{S}} \alpha$ si y solo si $\widehat{\Gamma} \models_{\mathcal{K}} \widehat{\alpha}$,
2. $\Sigma \models_{\mathcal{K}} s \approx \tau$ si y solo si $\widetilde{\Sigma} \vdash_{\mathcal{S}} \widetilde{s \approx \tau}$,
3. $\alpha \dashv\vdash_{\mathcal{S}} \widetilde{\widehat{\alpha}}$,
4. $s \approx \tau \mathrel{=\!\!|\!\!\models}_{\mathcal{K}} \widehat{\widetilde{s \approx \tau}}$.

Por ejemplo, si $\mathcal{S}$ es CPC y $\mathcal{K}$ es la variedad de las álgebras de Boole, definiendo

- $\widehat{\alpha} := \alpha \approx \top$

- $\widetilde{s \approx \tau} := s \leftrightarrow \tau$,

como sabemos, se verifican las cuatro condiciones de arriba.

Semánticas Algebraicas Equivalentes

Formalizaremos aquí las ideas intuitivas del párrafo anterior.

Definición 10.3.1 ([8, Def. 2.2]). Sea $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ un sistema deductivo y $\mathcal{K}$ una clase de $\mathcal{L}$-álgebras. $\mathcal{K}$ es una *semántica algebraica* para $\mathcal{S}$ si $\vdash_{\mathcal{S}}$ puede ser interpretado en $\models_{\mathcal{K}}$ de la manera siguiente. Existe un conjunto finito $\delta_i(p) \approx \varepsilon_i(p)$, para $i < n$, de ecuaciones en una variable p, tal que para $\Gamma \cup \{\varphi\} \subseteq \mathcal{F}m_{\mathcal{L}}$ para cada $j < n$:

(1) $\Gamma \vdash_{\mathcal{S}} \varphi$ si y solo si
$\{\delta_i(\psi) \approx \varepsilon_i(\psi) \ : i < n, \psi \in \Gamma\} \models_{\mathcal{K}} \delta_j(\varphi) \approx \varepsilon_j(\varphi)\ ; \quad j < n.$

$\delta_i \approx \varepsilon_i$ son llamadas *ecuaciones de definición* para $\mathcal{S}$ y $\mathcal{K}$.

Definición 10.3.2 ([8, Def. 2.4]). $\mathcal{K}$ es una semántica algebraica *equivalente* para un sistema deductivo $\mathcal{S}$ si existe un conjunto finito $\Delta_j(p,q)$, para $j < m$, de fórmulas con dos variables tal que para todo $\varphi \approx \psi \in Eq_{\mathcal{L}}$ se tiene:

(2) $\varphi \approx \psi \dashv\models_{\mathcal{K}} \delta_i(\varphi \Delta_j \psi) \approx \varepsilon_i(\varphi \Delta_j \psi)\ ; \quad i < n,\ j < m.$

El conjunto de fórmulas $\Delta_j(p,q)$ es llamado *sistema de fórmulas de equivalencia* para $\mathcal{S}$ y $\mathcal{K}$. Abreviaremos $\delta \approx \varepsilon$ para el sistema de ecuaciones de definición y $\Delta(p,q)$ para el sistema de fórmulas de equivalencia.

Lema 10.3.3 ([8, Lema 2.9]). *Sea $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ un sistema deductivo y $\mathcal{K}$ una semántica algebraica equivalente con ecuaciones de definición $\delta \approx \varepsilon$ y fórmulas de equivalencia $\Delta(p,q)$. Entonces para todo $\Sigma \subseteq Eq_{\mathcal{L}}$ y toda ecuación $\varphi \approx \psi$,*

(3) $\Sigma \models_{\mathcal{K}} \varphi \approx \psi$ *si y solo si* $\{\xi \Delta \eta : \xi \approx \eta \in \Sigma\} \vdash_{\mathcal{S}} \varphi \Delta \psi$,

y para cada $\theta \in \mathcal{F}m_{\mathcal{L}}$,

(4) $\theta \dashv\vdash_{\mathcal{S}} \delta(\theta) \Delta \varepsilon(\theta)$.

Recíprocamente, si existen fórmulas Δ y ecuaciones $\delta \approx \varepsilon$ que satisfagan (3) y (4), entonces $\mathcal{K}$ es una semántica algebraica equivalente para $\mathcal{S}$.

Definición 10.3.4. Un sistema deductivo $\mathcal{S}$ se dice *algebrizable* si tiene una semántica algebraica equivalente.

A continuación veremos que, esencialmente, todo sistema algebrizable tiene una única semántica equivalente.

Lema 10.3.5 ([8, Cor. 2.11])**.** *Si $\mathcal{K}$ es una semántica algebraica para $\mathcal{S}$, entonces $\mathcal{K}$ es una semántica algebraica equivalente si y solo si $\mathcal{K}^Q$, la cuasivariedad generada por $\mathcal{K}$, lo es.*

Demostración. Basta ver que para Σ finito,

$$\Sigma \models_{\mathcal{K}} \rho \approx \tau \text{ si y solo si } \Sigma \models_{\mathcal{K}^Q} \rho \approx \tau,$$

y que esto es inmediato porque $\mathcal{K}$ y $\mathcal{K}^Q$ satisfacen las mismas cuasi-identidades. □

Teorema 10.3.6 ([8, Teo. 2.15])**.** *Sean $\mathcal{S}$ un sistema deductivo algebrizable, $\mathcal{K}$ y $\mathcal{K}'$ dos semánticas algebraicas equivalentes. Entonces $\mathcal{K}$ y $\mathcal{K}'$ generan la misma cuasivariedad.*

Idea de la demostración. (a) Usando el Lema 8 y las propiedades de $\approx$, se demuestra que $\vdash_{\mathcal{S}} x\Delta y$ define una relación de congruencia sobre $\mathcal{F}m_{\mathcal{L}}$.

(b) $x\,, x\Delta y \vdash_{\mathcal{S}} y$.

$$\begin{array}{lr}
\text{(i)}\quad x \approx y\,,\ \delta(x) \approx \varepsilon(x) \models_{\mathcal{K}} \delta(y) \approx \varepsilon(y)\,, & \text{prop. de } \approx, \\
\text{(ii)}\ x \approx y \ =\!\mid\models_{\mathcal{K}} \delta(x\Delta y) \approx \varepsilon(x\Delta y)\,, & (2), \\
\text{(iii)}\ \delta(x\Delta y) \approx \varepsilon(x\Delta y)\,, \delta(x) \approx \varepsilon(x) \models_{\mathcal{K}} \delta(y) \approx \varepsilon(y)\,, & \text{(i), (ii)}, \\
\text{(iv)}\ x\Delta y\,, x \vdash_{\mathcal{S}} y & (1).
\end{array}$$

Sean $\mathcal{K}$ y $\mathcal{K}'$ dos semánticas algebraicas equivalentes al sistema $\mathcal{S}$ y sean $x\Delta y$ y $x\Delta' y$ sus respectivas fórmulas de equivalencia.

(c) $x\Delta y \dashv\vdash_{\mathcal{S}} x\Delta' y$.

Consideramos $\alpha(p) = x\Delta' p$. Entonces

$$\begin{array}{lr}
x\Delta y \vdash_{\mathcal{S}} \alpha(x)\Delta\alpha(y)\,, & \text{(a)}, \\
x\Delta y \vdash_{\mathcal{S}} (x\Delta' x)\Delta(x\Delta' y)\,, & \text{def.}, \\
x\Delta y \vdash_{\mathcal{S}} (x\Delta' y)\,, & \text{(a), (b)}.
\end{array}$$

Similarmente probamos en la otra dirección.

(d) $\mathcal{K}^Q = \mathcal{K}'^Q$.

$$\begin{array}{lllr}
\Sigma \models_{\mathcal{K}} \varphi \approx \psi & \text{si y solo si} & \{\alpha\Delta\beta : \alpha \approx \beta \in \Sigma\} \vdash_{\mathcal{S}} \varphi\Delta\psi\,, & (3), \\
\Sigma \models_{\mathcal{K}} \varphi \approx \psi & \text{si y solo si} & \{\alpha\Delta'\beta : \alpha \approx \beta \in \Sigma\} \vdash_{\mathcal{S}} \varphi\Delta'\psi\,, & \text{(c)}, \\
\Sigma \models_{\mathcal{K}} \varphi \approx \psi & \text{si y solo si} & \Sigma \models_{\mathcal{K}'} \varphi \approx \psi\,, & (3).
\end{array}$$

□

El recíproco de este teorema es falso. Existen sistemas deductivos distintos que tienen la misma semántica algebraica equivalente (ver [8, Sec. 5.2.4]).

Semánticas Matriciales

Una *$\mathcal{L}$-matriz* ([8, p. 8]) es un par $\mathcal{A} = \langle \mathbf{A}, F\rangle$, donde $\mathbf{A}$ es una $\mathcal{L}$-álgebra y F es un subconjunto del universo de $\mathbf{A}$, los elementos de F son llamados *elementos designados de $\mathcal{A}$*. Para una clase de matrices $\mathcal{M}$ definimos la relación $\models_{\mathcal{M}}$ entre un conjunto de fórmulas y una fórmula de la manera siguiente:

$\Gamma \models_{\mathcal{K}} \varphi$ si y solo si para toda $\mathcal{A} \in \mathcal{M}$ y para toda interpretación $\bar{a}$ de las variables de $\Gamma \cup \{\varphi\}$,

$$\psi^{\mathbf{A}}(\bar{a}) \in F, \quad \text{para todo } \psi \in \Gamma \ \Rightarrow \varphi^{\mathbf{A}}(\bar{a}) \in F.$$

Una matriz $\mathcal{A}$ es un *modelo matricial* de $\mathcal{S}$ si

$$\Gamma \vdash_{\mathcal{S}} \varphi \ \Rightarrow \Gamma \models_{\{\mathcal{A}\}} \varphi,$$

en tal caso F se denomina un *$\mathcal{S}$-filtro*.

Observemos que si T es una $\mathcal{S}$-teoría, entonces $\langle \boldsymbol{\mathcal{F}m}_{\mathcal{L}}, T\rangle$ es un modelo matricial de $\mathcal{S}$. Estas matrices se llaman *matrices de Lindenbaum* para $\mathcal{S}$.

Definición 10.3.7. Sea $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}}\rangle$ un sistema deductivo. Una clase de matrices $\mathcal{M}$ es una *semántica matricial* de $\mathcal{S}$ si para todo $\Gamma \cup \{\varphi\} \subseteq \mathcal{F}m_{\mathcal{L}}$ se tiene

$$\Gamma \vdash_{\mathcal{S}} \varphi \quad \text{si y solo si} \quad \Gamma \models_{\mathcal{M}} \varphi.$$

Por ejemplo, la clase de todas las matrices de Lindenbaum para $\mathcal{S}$ y la clase de todos los modelos matriciales de $\mathcal{S}$ son semánticas matriciales.

El Operador de Leibniz

Definición 10.3.8 ([8, Def. 1.4])**.** Sean $\mathbf{A}$ una $\mathcal{L}$-álgebra y $F \subseteq A$. Definimos la relación binaria sobre A:

$$\boldsymbol{\Omega}_{\mathbf{A}} F = \left\{ \begin{array}{rl} \langle a, b\rangle : & \varphi^{\mathbf{A}}(a, \bar{c}) \in F \iff \varphi^{A}(b, \bar{c}) \in F, \text{ para todo} \\ & \varphi(p, q_1, \ldots, q_n) \in \mathcal{F}m_{\mathcal{L}} \text{ y todo } \bar{c} \in A^n \end{array} \right\}.$$

La relación $\boldsymbol{\Omega}_{\mathbf{A}}$ se llama la *relación de Leibniz en* $\mathbf{A}$ *sobre* F. El operador sobre las partes de A, que denotaremos $\boldsymbol{\Omega}_{\mathbf{A}}$, es llamado *operador de Leibniz sobre* A. Si $\mathbf{A}$ es el álgebra de fórmulas $\boldsymbol{\mathcal{F}m}_{\mathcal{L}}$, el operador de Leibniz se denota simplemente $\boldsymbol{\Omega}$.

De la definición anterior se desprende inmediatamente que $\boldsymbol{\Omega}_{\mathbf{A}}$ es una congruencia sobre $\mathbf{A}$. Intuitivamente, nos dice que $\boldsymbol{\Omega}_{\mathbf{A}}$ identifica todos aquellos elementos de A que el álgebra $\mathbf{A}$ no puede distiguir relativamente a un conjunto F. Evidentemente esta definición es inmanejable desde el punto de vista práctico: difícilmente podremos calcular $\mathbf{\Omega_A}$ en un caso particular a partir de ella. Un par de teoremas nos ayudarán en esto.

Una congruencia Θ de $\mathbf{A}$ se dice *compatible* con el subconjunto F de A, si para todo $a, b \in A$, si $a \in F$ y $\langle a\,,\, b\rangle \in \Theta$ entonces $b \in F$.

Teorema 10.3.9 ([8, Teo. 1.5]). *Para toda álgebra $\mathbf{A}$ y cualquier $F \subseteq A$, $\mathbf{\Omega_A} F$ es la mayor congruencia compatible con F.*

Teorema 10.3.10 ([8, Teo. 1.6]). *Sea $\mathbf{A}$ un álgebra y $F \subseteq A$. Sea Θ una relación binaria sobre A que es elementalmente definible sobre la matriz $\langle \mathbf{A}, F\rangle$ con parámetros y sin igualdad:*

(i) Si Θ es reflexiva, entonces $\mathbf{\Omega_A} F \subseteq \Theta$.

(ii) Si además Θ es una congruencia compatible con F, entonces $\mathbf{\Omega_A} F = \Theta$.

Los Retículos de Teorías de $\mathcal{S}$ y de $\mathcal{K}$

La esencia de la teoría de algebrización desarrollada por Blok y Pigozzi, está en el siguiente teorema. Daremos su demostración porque ilustra cómo las ecuaciones de definición y las fórmulas de equivalencia aparecen más o menos naturalmente.

Teorema 10.3.11 ([8, Teo. 3.7]). *Sea $\mathcal{S}$ un sistema deductivo y $\mathcal{K}$ una cuasivariedad. Entonces $\mathcal{K}$ es la semántica algebraica equivalente de $\mathcal{S}$ si y solamente si existe un isomorfismo entre $\mathbf{Th}\mathcal{S}$ y $\mathbf{Th}\mathcal{K}$ que conmuta con sustituciones.*

Idea de la demostración. Supongamos que $\mathcal{K}$ es la semántica algebraica equivalente de $\mathcal{S}$. Entonces

$$\begin{aligned} \Omega_{\mathcal{K}} \;:\; \mathbf{Th}\mathcal{S} &\longrightarrow \mathbf{Th}\mathcal{K} \\ T &\longmapsto \mathcal{C}n_{\mathcal{K}}\{\delta(\varphi) \approx \varepsilon(\varphi) \;:\; \varphi \in T\} \end{aligned}$$

preserva el orden y las uniones dirigidas. De ahí es fácil demostrar que $\Omega_{\mathcal{K}}$ es un isomorfismo de retículos que conmuta con sustituciones.

Por otro lado, supongamos que $h \;:\; \mathbf{Th}\mathcal{S} \longrightarrow \mathbf{Th}\mathcal{K}$ es un isomorfismo que conmuta con sustituciones.

Consideramos la $\mathcal{S}$-teoría $T = \mathcal{C}n_{\mathcal{S}}\{p\}$. Como T es compacta, su imagen $\theta = h(T)$ también lo es y por lo tanto, es finitamente generada (ver Lema 5). O sea,

$$\theta = \mathcal{C}n_{\mathcal{K}}\{\kappa_i(p, r_1, \ldots, r_k) \approx \tau_i(p, r_1, \ldots, r_k) \;:\; i < n\}.$$

Sea s una sustitución tal que

$$\begin{aligned} s(p) &\approx p \\ s(r_j) &\approx p, \qquad \text{para } j \leq k. \end{aligned}$$

Usando el hecho de que h conmuta con sustituciones, se demuestra que

$$s(T) = \mathcal{C}n_{\mathcal{S}}\{s(p)\} = T,$$

luego (con un abuso de notación),

$$\begin{aligned} \theta = h(T) = h(s(T)) &= s(h(T)) \\ &= s(\mathcal{C}n_{\mathcal{K}}\{\kappa_i(p, r_1, \ldots, r_k) \approx \tau_i(p, r_1, \ldots, r_k) \,:\, i < n\} \\ &= \mathcal{C}n_{\mathcal{K}}\{\kappa_i(p, p, \ldots, p) \approx \tau_i(p, p, \ldots, p) \,:\, i < n\}. \end{aligned}$$

Hagamos $\delta_i(p) = \kappa_i(p, p, \ldots, p)$ y $\varepsilon_i(p) = \tau_i(p, p, \ldots, p)$, para $i \leq n$. Entonces

$$\begin{aligned} \Gamma \vdash_{\mathcal{S}} \varphi \quad &\text{ssi} \quad \mathcal{C}n_{\mathcal{S}}\{\varphi\} \subseteq \mathcal{C}n_{\mathcal{S}}T \\ &\text{ssi} \quad h(\mathcal{C}n_{\mathcal{S}}\{\varphi\}) \subseteq h(\mathcal{C}n_{\mathcal{S}}T) \\ &\text{ssi} \quad \mathcal{C}n_{\mathcal{K}}\{\delta(\varphi) \approx \varepsilon(\varphi)\} \subseteq \mathcal{C}n_{\mathcal{K}}\{\delta(\gamma) \approx \varepsilon(\gamma) \,:\, \gamma \in \Gamma\} \\ &\text{ssi} \quad \{\delta(\gamma) \approx \varepsilon(\gamma) \,:\, \gamma \in \Gamma\} \models_{\mathcal{K}} \delta(\varphi) \approx \varepsilon(\varphi). \end{aligned}$$

Similarmente, $\theta = \mathcal{C}n_{\mathcal{K}}\{p \approx q\}$ es una $\mathcal{K}$-teoría compacta, luego $h^{-1}(\theta)$ también lo es y por lo tanto, es generada por un conjunto finito de fórmulas $\{\varphi_j(p, q, r_1, \ldots, r_k)\} \,:\, j < m$.

Haciendo $\Delta(p, q) = \varphi(p, q, p, \ldots, p)$, se cumple

$$p \approx q \;\;=\!\mid\models_{\mathcal{K}}\;\; \delta(p\Delta q) \approx \varepsilon(p\Delta q),$$

completando la demostración del teorema. □

El isomorfismo $\Omega_{\mathcal{K}}T$ del teorema puede encontrarse de la siguiente manera.

Lema 10.3.12 ([8, Lema 3.8])**.** *Sea $\mathcal{S}$ algebrizable y $\mathcal{K}$ su semántica algebraica equivalente. Sea Δ el sistema de equivalencias para $\mathcal{K}$. Entonces para $T \in Th\mathcal{S}$,*

$$\Omega_{\mathcal{K}}T = \{\varphi \approx \psi : \varphi \,\Delta\, \psi \in T\}.$$

Criterios de Algebrizabilidad

Hay dos importantes caracterizaciones para los sistemas algebrizables.

Algebrizabilidad y el Operador de Leibniz

Lema 10.3.13 ([8, Teo. 4.1]). *Sea $\mathcal{S}$ algebrizable y $\mathcal{K}$ su semántica algebraica equivalente $\mathcal{K}$. Entonces para cada $T \in Th\mathcal{S}$*

$$\boldsymbol{\Omega} T = \{\langle\varphi, \psi\rangle : \varphi \approx \psi \in \Omega_{\mathcal{K}} T\} = \{\langle\varphi, \psi\rangle : \varphi\Delta\psi \in T\}.$$

Teorema 10.3.14 ([8, Teo. 4.2]). *Un sistema deductivo $\mathcal{S}$ es algebrizable si y solo si el operador de Leibniz sobre $\mathcal{F}m_{\mathcal{L}}$ cumple las condiciones:*

(i) $\boldsymbol{\Omega}$ *es inyectivo y preserva el orden de* $\mathbf{Th}\mathcal{S}$.

(ii) $\boldsymbol{\Omega}$ *preserva uniones de subconjuntos dirigidos en* $\mathbf{Th}\mathcal{S}$.

Idea de la demostración. Se define

$$\mathcal{K} = \{\boldsymbol{\mathcal{F}m}_{\mathcal{L}}/\theta \ : \ \theta \in \boldsymbol{\Omega} Th\mathcal{S}\}$$

y se demuestra que $\boldsymbol{\Omega}$ es un isomorfismo entre $\mathbf{Th}\mathcal{S}$ y $\mathbf{Th}\mathcal{K}$. Aplicamos entonces el Teorema 10.3.11. □

Algebrizabilidad y Términos

Teorema 10.3.15 ([8, Teo. 4.7]). *Un sistema deductivo $\mathcal{S}$ es algebrizable si y solo si existen un sistema de fórmulas de equivalencia Δ y un sistema de ecuaciones de definición $\delta \approx \varepsilon$ que satisfacen las condiciones siguientes para $\varphi\,,\psi\,,\theta\, \in \mathcal{F}m_{\mathcal{L}}$:*

(i) $\vdash_{\mathcal{S}} \ \varphi\,\Delta\,\varphi$,

(ii) $\{\varphi\,\Delta\,\psi\} \vdash_{\mathcal{S}} \ \psi\,\Delta\,\varphi$,

(iii) $\{\varphi\,\Delta\,\psi\,,\psi\,\Delta\,\theta\} \vdash_{\mathcal{S}} \ \varphi\,\Delta\,\theta$,

(iv) *Para todo conectivo n-ario ω de $\mathcal{L}$,*
$\{\varphi_1\,\Delta\,\psi_1, \ldots, \varphi_n\,\Delta\,\psi_n\} \vdash_{\mathcal{S}} \ \omega(\varphi_1, \varphi_2, \ldots, \varphi_n)\,\Delta\,\omega(\psi_1, \psi_2, \ldots, \psi_n)$,

(v) $\theta \ \dashv\vdash_{\mathcal{S}} \ \delta(\theta)\,\Delta\,\varepsilon(\theta)$.

Demostración. Definimos

$$\Omega_{\Delta} T = \{\langle\varphi, \psi\rangle : \varphi\,\Delta\,\psi \in T\}$$

entonces (i)-(iv) demuestran que $\Omega_{\Delta} T$ es una congruencia.

Para ver que $\Omega_{\Delta} T$ es compatible con T demostramos que

$$\varphi\,,\,\varphi\Delta\psi \vdash_{\mathcal{S}} \ \psi\,.$$

En efecto, consideremos la teoría $U = Cn\{\varphi\,,\,\varphi\Delta\psi\}$. Entonces por (v), $\varphi \vdash_{\mathcal{S}} \delta(\varphi)\Delta\varepsilon(\varphi)$, luego por definición,

$$\delta(\varphi) \approx \varepsilon(\varphi) \in \Omega_{\Delta}U. \qquad (*)$$

Como además $\langle\varphi, \psi\rangle \in \Omega_{\Delta}U$, podemos sustituir φ por ψ en $(*)$ y por lo tanto $\langle\delta(\psi), \varepsilon(\psi)\rangle \in \Omega_{\Delta}U$, es decir,

$$\varphi\,,\,\varphi\Delta\psi \vdash_{\mathcal{S}} \delta(\psi) \approx \varepsilon(\psi)\,.$$

Aplicamos (v) en la otra dirección para obtener lo que queremos. Como $\boldsymbol{\Omega}$ es la mayor congruencia compatible con T, $\Omega_{\Delta}(T) \subseteq \boldsymbol{\Omega}(T)$.

Para demostrar la otra dirección, sea $\langle\varphi, \psi\rangle \in \boldsymbol{\Omega}$. Entonces usamos la fórmula $\gamma(x) = \varphi\Delta x$ y la definición de $\boldsymbol{\Omega}(T)$ para obtener

$$\varphi\Delta\varphi \in \Omega_{\Delta}(T) \;\text{ si y solo si }\; \varphi\Delta\psi \in \Omega_{\Delta}(T)\,,$$

pero la primera vale por hipótesis, luego $\langle\varphi, \psi\rangle \in \Omega_{\Delta}(T)$.

Esto demuestra que $\Omega_{\Delta} = \boldsymbol{\Omega}$. □

Corolario 10.3.16 ([8, Cor. 4.8])**.** *Una condición suficiente para que un sistema deductivo $\mathcal{S}$ sea algebrizable es que exista un sistema Δ de fórmulas de equivalencia que satisfaga las condiciones (i)–(iv) del teorema anterior y adicionalmente las condiciones*

(vi) $\{\varphi\,,\varphi\,\Delta\,\psi\} \vdash_{\mathcal{S}} \psi$, *(conocida como regla de corte).*

(vii) $\{\varphi\,,\psi\} \vdash_{\mathcal{S}} \varphi\,\Delta\,\psi$, *(conocida como regla G, por Gödel). En este caso la ecuación de definición es $p \approx p\,\Delta\,p$.*

Algebrizabilidad y Matrices

Existe una conexión estrecha entra las semánticas algebraicas y las semánticas matriciales de un sistema deductivo algebrizable.

El siguiente teorema es muy útil, especialmente para verificar que un sistema no es algebrizable. Dada una cuasivariedad $\mathcal{K}$ y una $\mathcal{L}$-álgebra $\mathbf{A}$, diremos que una congruencia Θ de $\mathbf{A}$ es una $\mathcal{K}$-*congruencia* si el cociente $\mathbf{A}/\Theta \in \mathcal{K}$.

Teorema 10.3.17 ([8, Cor. 5.1])**.** *Sea $\mathcal{S}$ algebrizable y $\mathcal{K}$ una cuasivariedad. Entonces $\mathcal{S}$ es algebrizable con semántica algebraica equivalente $\mathcal{K}$ si y solo si para toda $\mathcal{L}$-álgebra $\mathbf{A}$, el operador de Leibniz $\boldsymbol{\Omega}_{\mathbf{A}}$ es un isomorfismo entre los retículos de $\mathcal{S}$-filtros y de $\mathcal{K}$-congruencias de $\mathbf{A}$.*

Lema 10.3.18 ([8, Lema 5.2]). *Sea $\mathcal{S}$ algebrizable y sea Δ un sistema de fórmulas de equivalencia. Entonces para toda $\mathcal{L}$-álgebra $\mathbf{A}$ y todo $\mathcal{S}$-filtro $F \subseteq A$*

$$\mathbf{\Omega_A} F = \{\langle \varphi, \psi \rangle : \varphi \, \Delta^{\mathbf{A}} \, \psi \in F\}.$$

Una matriz $\langle \mathbf{A}, F \rangle$ se dice *reducida* si $\mathbf{\Omega_A} F = I_{\mathbf{A}}$, la identidad sobre A. La matriz cociente $\langle \mathbf{A}/\mathbf{\Omega_A} F, F/\mathbf{\Omega_A} F \rangle$ es una matriz reducida.

Teorema 10.3.19 ([8, Cor. 5.3]). *Sean $\mathcal{S}$ algebrizable, $\mathcal{K}$ la cuasivariedad que es su semántica algebraica equivalente y $\mathcal{M}^*$ la clase de todas las $\mathcal{S}$-matrices reducidas. Entonces $\mathcal{K}$ es la clase de los reductos algebraicos de $\mathcal{M}$, es decir,*

$$\mathcal{K} = \{\mathbf{A} : \langle \mathbf{A}, F \rangle \in \mathcal{M}^*, \text{ para algún } \mathcal{S}\text{-filtro } F\}.$$

Axiomatización

Si podemos demostrar que un sistema deductivo es algebrizable usando el Teorema 10.3.15, la teoría nos proporciona una manera de encontrar la cuasi-variedad asociada.

Teorema 10.3.20. *Sea S un sistema deductivo definido por un conjunto Σ de axiomas y un conjunto RI de reglas de inferencia. Suponga que S es algebrizable mediante las fórmulas de equivalencia Δ y ecuaciones de definición $\delta \approx \varepsilon$. Entonces la (única) cuasivariedad que es semántica equivalente para S está axiomatizada por las identidades*

1. $\delta(\varphi) \approx \varepsilon(\varphi)$,
2. $\delta(p\Delta p) \approx \varepsilon(p\Delta p)$,

para cada axioma φ y las cuasi-identidades

3. $\delta(\psi_1) \approx \varepsilon(\psi_1), \ldots, \delta(\psi_n) \approx \varepsilon(\psi_n) \ \Rightarrow \ \delta(\varphi) \approx \varepsilon(\varphi)$,
4. $\delta(p\Delta q) \approx \varepsilon(p\Delta p) \ \Rightarrow \ p \approx q$. □

10.4. Ejemplos

Sistemas implicativos estándar

Como dijimos en la introducción, H. Rasiowa y R. Sikorski llevaron el método de Lindenbaum–Tarski a su mayor generalidad. Su teoría se aplica a los cálculos implicativos estándar (SIC), es decir, (i) el lenguaje $\mathcal{L}$ tiene un número finito de conectivos de rango 0, 1 y 2, pero no superiores. (ii) $\mathcal{L}$ contiene un conectivo binario que verifica

SIC1 $\vdash A \to A$,

SIC2 $A, A \to B \vdash B$,

SIC3 $A \to B\,,\, B \to C \vdash A \to C$,

SIC4 $A \vdash B \to A$,

SIC5 $A \to B\,,\, B \to A \vdash A^\sharp \to B^\sharp$,
para toda operación unaria $\sharp$.

SIC5 $A \to B\,,\, B \to A,\, C \to D\,,\, D \to C \vdash (A * C) \to (B * D)$,
para toda operación binaria $*$.

Los cálculos proposicionales clásico, intuicionista, las lógicas modales normales, las lógicas multivaluadas y gran parte de sus fragmentos son sistemas implicativos estándar y pueden algebrizarse con una ecuación $A \approx A \to A$ y fórmulas de equivalencia $\Delta = \{A \to B\,,\, B \to A\}$.

El sistema modal $S5^G$ (Gödel)

El sistema

Axiomas

$S5^G1$ Todas las tautologías,

$S5^G2$ $\Box(A \to B) \to (\Box A \to \Box B)$,

$S5^G3$ $\Box A \to A$,

$S5^G4$ $\Diamond A \to \Box\Diamond A$.

Reglas de Inferencia

MP $A, A \to B \vdash B$,

G $A \vdash \Box A$.

$S5^G$ es algebrizable

El sistema $S5^G$ es SIC, luego algebrizable.

El sistema modal $S5^C$ (Carnap)

El sistema

Axiomas

$S5^C1$ $\quad \Box A$, para toda tautología A,

$S5^C2$ $\quad \Box(\,\Box(A \to B) \to (\Box A \to \Box B)\,)$,

$S5^C3$ $\quad \Box(\,\Box A \to A\,)$,

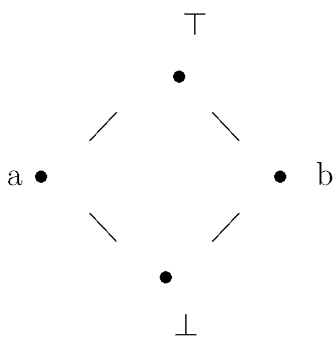
$S5^C4$ $\quad \Box(\,\Diamond A \to \Box\Diamond A\,)$.

Reglas de Inferencia

MP $\quad A,\, A \to B \,\vdash\, B$.

$S5^C$ no es algebrizable

Considérese el álgebra $\langle\{\bot, a, b, \top\}, \to, \neg, \Box, \bot, \top\rangle$, donde $\langle\{\bot, a, b, \top\}, \to, \neg, \bot, \top\rangle$ es el álgebra de Boole del próximo diagrama y $\Box$ se define en la tabla siguiente.



	$\Box x$
$\top$	$\top$
a	$\bot$
b	$\bot$
$\bot$	$\bot$

Entonces $F_1 = \{a, \top\}$ y $F_2 = \{b, \top\}$ son filtros ya que todos los axiomas toman valor $\top$ y ambos conjuntos son cerrados bajo la regla de inferencia. Como $\mathbf{A}$ es simple, no hay congruencias más que las triviales y $\mathbf{\Omega_A}(F_1) = \mathbf{\Omega_A}(F_2) = Id$, luego $\mathbf{\Omega_A}$ no es inyectiva.

El sistema P^1 de Sette

El sistema

Axiomas

$P^1 1$ $A \to (B \to A)$,

$P^1 2$ $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$,

$P^1 3$ $(\sim A \to \sim B) \to ((\sim A \to \sim\sim B) \to A)$,

$P^1 4$ $\sim (A \to \sim\sim A) \to A$,

$P^1 5$ $(A \to B) \to \sim\sim (A \to B)$.

Regla de Inferencia Modus Ponens

P^1 es algebrizable

Las ecuaciones de definición son

$$\delta(A) = (A \to A) \to A,$$
$$\varepsilon(A) = A \to A.$$

y las fórmulas de equivalencia son

$$\Delta_1(A, B) = A \to B,$$
$$\Delta_2(A, B) = B \to A,$$
$$\Delta_3(A, B) = \sim A \to \sim B,$$
$$\Delta_4(A, B) = \sim B \to \sim A.$$

Sette Algebras (P^1 Álgebras)

Las álgebras de Sette (introducidas como P^1-álgebras en Lewin et al. [71] y en Pynko [90]) son estructuras

$$\mathbf{A} = \langle A; \to, ', \mathbf{1} \rangle$$

que verifican los axiomas siguientes:

A1. $x \to (y \to x) = \mathbf{1}$,

A2. $(x \to (y \to z)) \to ((x \to y) \to (x \to z)) = \mathbf{1}$,

A3. $(x' \to y') \to ((x' \to y'') \to x) = \mathbf{1}$,

A4. $(x \to x'')' \to x = \mathbf{1}$,

A5. $(x \to y) \to (x \to y)'' = \mathbf{1}$,

y las cuasi-identidades:

Q1. $x \to y = \mathbf{1}$ y $(x \to x) \to x = \mathbf{1} \implies (y \to y) \to y = \mathbf{1}$.

Q2. $x \to y = \mathbf{1}$, $y \to x = \mathbf{1}$, $x' \to y' = \mathbf{1}$ y $y' \to x' = \mathbf{1} \implies x = y$.

La semántica algebraica equivalente es una cuasi-variedad propia generada por el álgebra

$$\mathbf{A} = \langle \{0, a, 1\}; \to, \,', 1\rangle,$$

donde $\langle \{0,1\}; \to, '\rangle$ es el álgebra de Boole de dos elementos y las operaciones $\to$ y $'$ están definidas por:

$\to$	0	a	1
0	1	1	1
a	0	1	1
1	0	1	1

	$'$
0	1
a	1
1	0

Dos lógicas con la misma semántica algebraica equivalente

$$\mathbf{A} = \langle \{0, \frac{1}{2}, 1\}; \rightarrowtail, \sim\rangle$$

$\rightarrowtail$	0	$\frac{1}{2}$	1
0	1	1	1
$\frac{1}{2}$	0	1	1
1	0	1	1

	$\sim$
0	1
$\frac{1}{2}$	$\frac{1}{2}$
1	0

$$\text{Ł}_3 = \langle \mathbf{A}, \{1\}\rangle \qquad \text{y} \qquad \mathbf{J}_3 = \langle \mathbf{A}, \{\frac{1}{2}, 1\}\rangle$$

Estas matrices dan origen a dos lógicas diferentes con la misma semántica algebraica equivalente.

Ecuación de definición y formulas de equivalencia para $\mathbf{Ł}_3$:

$$p \approx \top$$

$$\Delta(p,q) = \{p \rightarrowtail q, q \rightarrowtail p\}$$

Ecuación de definición y formulas de equivalencia para $\mathbf{J}_3$:

$$(\sim p \rightarrowtail p) \rightarrowtail p \approx \top$$

$$\Delta(p,q) = \{p \rightarrowtail q, q \rightarrowtail p, \sim p \rightarrowtail \sim q, \sim q \rightarrowtail \sim p\}$$

El Sistema C_1 de da Costa

Axiomas

$C_1 1$ $\quad A \to (B \to A)$,

$C_1 2$ $\quad (A \to (B \to C)) \to ((A \to B) \to (A \to C))$,

$C_1 3$ $\quad (A \wedge B) \to A$ y $(A \wedge B) \to B$,

$C_1 4$ $\quad (A \to B) \to ((A \to C) \to (A \to (B \wedge C)))$,

$C_1 5$ $\quad A \to (A \vee B)$ y $B \to (A \vee B)$,

$C_1 6$ $\quad (A \to C) \to ((B \to C) \to ((A \vee B) \to C))$,

$C_1 7$ $\quad A \vee \neg A$,

$C_1 8$ $\quad \neg\neg A \to A$,

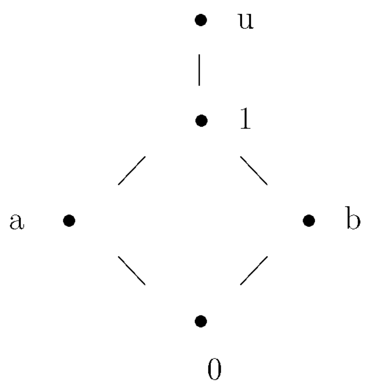
$C_1 9$ $\quad B^\circ \to ((A \to B) \to ((A \to \neg B) \to \neg A))$,

$C_1 10$ $\quad (A^\circ \wedge B^\circ) \to ((A \wedge B)^\circ \wedge (A \vee B)^\circ \wedge (A \to B)^\circ)$
donde $A^\circ := \neg(A \wedge \neg A)$.

Regla de Inferencia Modus Ponens.

C_1 no es algebrizable

Considere la matriz $\langle \mathbf{A}, \{1, u\} \rangle$ definida por el retículo:



con las operaciones siguientes:

$\to$	u	1	a	b	0	$\neg x$	$\neg\neg x$	$x^\circ = \neg(x \wedge \neg x)$
u	u	u	a	b	0	1	0	0
1	u	1	a	b	0	0	1	1
a	u	1	1	b	b	b	a	1
b	u	1	a	1	a	a	b	1
0	u	1	1	1	1	1	0	1

La mayor congruencia compatible con los filtros

$$F_1 = \{a, 1, u\} \quad \text{y} \quad F_2 = \{b, 1, u\}$$

es la identidad, esto es, $\mathbf{\Omega_A}$ no es inyectiva.

Bibliografía del Capítulo 10

- Blok W. J. and Pigozzi D., *Algebraizable Logics.* Memoirs Amer. Math. Soc., 77 (1989), no. 396.
- Blok W.J. and Pigozzi D., *Protoalgebraic logics.* Studia Logica, 45 (1986), 337–369.
- Blok W.J. and Pigozzi D., *Algebraic semantics for universal Horn logic without equality.* In: Universal Algebra and Quasigroup Theory (Jadwisin, 1989), 1–56, Heldermann, Berlin, 1992.
- Burris S. and Sankappanavar H.P., *A Course in Universal Algebra.* Springer-Verlag, 1980.
- Caicedo X., *Elementos de Lógica y Calculabilidad.* Una Empresa Docente, Bogotá, 1990.
- Czelakowski J., *Consequence Operations. Foundational Studies.* Reports of the Research Project: Theories, Models, Cognitive Schemata, Institute of Philosophy and Sociology, Polish Academy of Sciences, Warszawa, 1992.
- Czelakowski J., *Equivalential logics I, II.* Studia Logica, 40 (1981), 227–236 and 335–372.
- Czelakowski J., *Reduced products of logical matrices.* Studia Logica, 39 (1980), 19–43.
- Czelakowski J., *Protoalgebraic Logics.* Kluwer Academic Pub., 2001.
- Da Costa N.C.A., *On the theory of inconsistent formal systems.* Notre Dame J. Formal Logic, 15 (1974), 497–510.
- Enderton H.B., *A Mathematical Introduction to Logic.* Academic Press, 1972.
- Epstein R.L., *Five Ways of Saying "Therefore".* Wadsworth Group, 2002.
- Font J. and Jansana R., *A General Algebraic Semantics for Sentential Logics.* Lecture Notes in Logic, vol. 7, Springer-Verlag, 1996.
- Halmos P., *Algebraic Logic.* Chelsea Pub. Co., 1962.

- Herrmann B., *Equivalential and algebraizable logics.* Studia Logica, 57 (1997), 419–436.
- Herrmann B., *Characterizing equivalential and algebraizable logics by the Leibniz operator.* Studia Logica, 58 (1997), 305–323.
- Hughes G.E. and Cresswell M.J., *Introducción a la Lógica Modal.* Tecnos, Madrid, 1973.
- Lewin R., Mikenberg I. and Schwarze M.G., *Algebraization of paraconsistent logic P1*, J. Non-Classical Logic 7 (1990), no. 1-2, 79–88.
- Lewin R., Mikenberg I. and Schwarze M.G., *C1 is not algebraizable*, Notre Dame J. Formal Logic, 32 (1991), 609–611.
- Lewin R.A., Mikenberg I.F. and Schwarze M.G., *P1 algebras*, Studia Logica, 53 (1994), no. 1, 21–28.
- McKenzie R.N., McNulty G.F. and Taylor W.F., *Algebras, Lattices, Varieties.* Wadsworth, 1987.
- Mendelson E., *Introduction to Mathematical Logic.* Fourth Ed., Chapman & Hall, 1997.
- Mortensen C., *Every quotient algebra for C1 is trivial.* Notre Dame J. Formal Logic, 21 (1980), 694–700.
- Pynko A.P., *Algebraic study of Sette's maximal paraconsistent logic*, Studia Logica, vol. 54, 89–128 (1995).
- Rasiowa R., *An Algebraic Approach to Non-Classical Logics.* North-Holland, Amsterdam, 1974.
- Rasiowa R. and Sikorski R., *The Mathematics of Metamathematics.* Polska Akademia Nauk, Warsawa, 1963.
- Sette A.M., *On the propositional calculus* P^1, Math. Japon., 18 (1973), 173–180.
- Tarski A., *Grundzüge des Systemenkalküls. Erster Teil.* Fundamenta Mathematicae, 25 (1935), 503–526.
- Tarski A., *Logic, Semantics, Metamathematics. Papers from 1923 to 1938.* Hackett, Indianapolis, IN, 1983.
- Wójcicki R., *Theory of Logical Calculi.* Kluwer Academic Publishers, 1988.

Capítulo 11

ℓ-grupos y su lógica

Hemos visto en el Capítulo 8 la definición de ℓ-grupo y la equivalencia categorial entre los ℓ-grupos con unidad fuerte y las MV-álgebras. Nos detendremos aquí en estudiar propiedades de ℓ-grupos a fin de conocer un poco más sobre esta variedad. Supondremos siempre que los grupos considerados son abelianos.

Con esta base estaremos en condiciones de tratar el aspecto lógico. Definiremos dos lógicas: el sistema $\mathcal{B}al$, cuya semántica algebraica equivalente (usando el lenguaje del Capítulo 10) es una variedad de álgebras definicionalmente equivalente a la variedad de los ℓ-grupos, y el sistema $\mathcal{B}al^o$, equivalente al anterior, cuya álgebra de Lindenbaum es un ℓ-grupo. El primer sistema nos proporcionará un ejemplo de aplicación de la teoría de Block y Pigozzi vista en el Capítulo 10. El segundo nos permitirá ver un aspecto lógico de la equivalencia categorial entre los ℓ-grupos y sus conos de elementos positivos.

Nos basaremos principalmente en [1], [42], [47] y [96].

11.1. ℓ-grupos

Un ℓ-grupo es un caso particular de *grupo ordenado* o *grupo parcialmente ordenado* o *p.o.grupo*. Observemos que, sin embargo, un p.o.grupo no es un álgebra.

Un p.o.grupo es un sistema $\langle G, \leq, +, -, 0\rangle$ tal que:

- $\langle G, +, -, 0\rangle$ es un grupo,

- $(G, \leq)$ es un conjunto ordenado,

- Vale la propiedad:

  (M) Si $x \leq y$ entonces $x + z \leq y + z$.

Propiedades

El siguiente teorema nos dice que el orden en un grupo está determinado por el conjunto de sus elementos positivos.

Teorema 11.1.1. *Sea $\langle G, +, -, 0\rangle$ un grupo, $P \subseteq G$. Sea $\leq$ la relación definida por:*

$$x \leq y \text{ si y solo si } y - x \in P.$$

La relación $\leq$ verifica (M) y es tal que $P = \{x \in G : x \geq 0\}$. Además, $\leq$ es un orden si y solo si valen las siguientes condiciones

(1) *P es cerrado por $+$. Abreviadamente, $P + P \subseteq P$.*

(2) *Si $x \in P$ y $-x \in P$, entonces $x = 0$. Abreviadamente, $P \cap -P = \{0\}$.*

Demostración. Veamos que vale (M). Sea $x \leq y$, es decir que $y - x \in P$ y veamos que, para todo $z \in G$, $x+z \leq y+z$. Luego $y+z-(x+z) = y-x \in P$. Por definición de $\leq$, se tiene que $x \geq 0$ si y solo si $x \in P$.

Sea $\leq$ un orden. Entonces, se cumple (1): si $x \geq 0$, $y \geq 0$ entonces, por (M), $x + y \geq 0$. Por propiedades de grupo, si $x \geq 0$ y $-x \geq 0$ entonces es $x = 0$, luego vale también (2).

Recíprocamente, supongamos que P cumple (1) y (2). Veamos que $\leq$ es un orden. Se tiene que $x - x = 0 \in P$, luego $x \leq x$ para todo x. Sean $x \leq y$, $y \leq x$. Luego, $y - x \in P$, $x - y = -(y - x) \in P$. Luego, por (2), $y - x = 0$, de donde $y = x$. Veamos la transitividad. Sean $x \leq y$, $y \leq z$. Luego tenemos que $y - x \in P$ y $z - y \in P$. Por la condición (1) deducimos que $(y - x) + (z - y) = z - x \in P$, es decir, $x \leq z$. □

Llamaremos *cono positivo* de un ℓ-grupo G al conjunto de sus elementos positivos:

$$G^+ = \{x \in G : x \geq 0\}.$$

Veamos ahora una condición necesaria y suficiente para que un grupo ordenado sea un ℓ-grupo.

Teorema 11.1.2. *Un p.o.grupo es un ℓ-grupo si y solo si existe $x \vee 0$, para todo $x \in G$.*

Demostración. Mostremos que existe el supremo para todo par de elementos x, y, dado por

$$x \vee y = ((x - y) \vee 0) + y.$$

En primer lugar, por (M), $(x - y) \vee 0 \geq 0$ implica $((x - y) \vee 0) + y \geq y$. Además, $(x - y) \vee 0 \geq x - y$, por lo que $((x - y) \vee 0) + y \geq x - y + y = x$, luego, es cota superior de x, y. Sea $c \geq x, y$. Luego, $c - y \geq 0$ y $c - y \geq x - y$, por lo cual $c - y \geq (x - y) \vee 0$ y entonces se tiene que $c \geq ((x - y) \vee 0) + y$. □

Veamos ahora una propiedad que vamos a usar repetidamente.

Lema 11.1.3. *Para todo par de elementos x, y de un ℓ-grupo:*

$$x - (x \wedge y) + y = x \vee y.$$

Demostración. Hemos visto en el Lema 8.5.2 del Capítulo 8 que en todo ℓ-grupo vale la siguiente propiedad:

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

De allí deducimos:

$$x - (x \wedge y) = 0 \vee (x - y) = (y - y) \vee (x - y),$$

de donde, distribuyendo:

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

Luego,

$$x - (x \wedge y) + y = x \vee y. \qquad \square$$

En particular, si x e y son *disjuntos*, es decir, si $x \wedge y = 0$, se tiene que

$$x + y = x \vee y. \tag{Di}$$

Teorema 11.1.4. *Todo elemento x de un ℓ-grupo admite una única descomposición como la diferencia de dos elementos positivos disjuntos.*

Demostración. Dado un elemento x, sean

$$x^+ = x \vee 0, \quad x^- = (-x) \vee 0.$$

Veamos que $x = x^+ - x^-$. En efecto, $x + x^- = x + ((-x) \vee 0) = 0 \vee x = x^+$. Probemos ahora que $x^+ \wedge x^- = 0$.

Tenemos que

$$\begin{aligned} x^+ \wedge x^- &= (x + x^-) \wedge (0 + x^-) \\ &= (x \wedge 0) + x^- \\ &= -x^- + x^- \\ &= 0. \end{aligned}$$

Veamos que la descomposición es única.

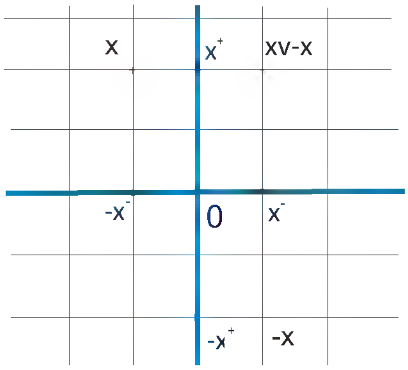


Figura 11.1: $\mathbb{Z} \times \mathbb{Z}$

Sea $x = a - b$, con $a, b \geq 0$, $a \wedge b = 0$. Entonces, por ser $a \vee b = a + b$,

$$\begin{aligned} x^+ &= x \vee 0 \\ &= (a - b) \vee 0 \\ &= (a - b) \vee (b - b) \\ &= (a \vee b) - b \\ &= (a + b) - b \\ &= a. \end{aligned}$$

Usando esto,

$$x^- = x^+ - x = a - (a - b) = b.$$ □

Hemos definido en el Capítulo 8 el módulo de un elemento x por:

$$\|x\| = x \vee -x.$$

En la Figura 11.1 observamos en el ℓ-grupo $\mathbb{Z} \times \mathbb{Z}$ el elemento $x = (-1, 2)$ para el cual $-x = (1, -2)$, $x^+ = (0, 2)$, $x^- = (1, 0)$ y su módulo $\|x\| = x \vee -x = (1, 2)$.

Veamos algunas de las propiedades del módulo.

Lema 11.1.5. *En un ℓ-grupo G se verifica:*

(1) $\|x\| \geq 0$,

(2) $x = \|x\|$ *si y solo si* $x \geq 0$,

(3) $\|x\| = x^+ \vee x^-$,

(4) $\|x\| = x^+ + x^-$,

(5) $\|x + y\| \leq \|x\| + \|y\|$ *(desigualdad triangular).*

Demostración. 1) Se tienen las siguientes igualdades:

$$x + (x \vee -x) = 2x \vee 0,$$
$$-x + (x \vee -x) = 0 \vee -2x.$$

Sumando miembro a miembro obtenemos:

$$x \vee -x = (2x \vee 0) + (-2x \vee 0).$$

Luego, por ser suma de dos elementos positivos, es $x \vee -x \geq 0$.

2) Si $x \geq 0$, entonces $-x \leq 0$; luego, $-x \leq 0 \leq x$, de donde $\|x\| = x$. La recíproca es obvia.

3) Tenemos:

$$\begin{aligned} x \vee -x &= (x \vee -x) \vee 0 \\ &= (x \vee 0) \vee (-x \vee 0) \\ &= x^+ \vee x^-. \end{aligned}$$

4) Como x^+ y x^- son disjuntos, por (Di):

$$x^+ + x^- = x^+ \vee x^-.$$

5) Veamos en primer lugar que

$$(x + y) \vee 0 \leq (x \vee 0) + (y \vee 0).$$

En efecto, por (M), $x + y \leq (x \vee 0) + (y \vee 0)$. Además, $0 \leq (x \vee 0) + (y \vee 0)$. Luego,

$$(x + y) \vee 0 \leq (x \vee 0) + (y \vee 0).$$

Por lo tanto:

$$\begin{aligned} \|x + y\| &= ((x + y) \vee 0) + (-(x + y) \vee 0) \\ &\leq (x \vee 0) + (y \vee 0) + (-x \vee 0) + (-y \vee 0) \\ &= \|x\| + \|y\|. \end{aligned}$$ □

Veamos ahora que un ℓ-grupo tiene propiedades especiales en cuanto a su estructura subyacente de retículo y también en cuanto a la de grupo.

Un grupo se llama *libre de torsión* si solo puede darse que $nx = 0$, siendo $n \neq 0$ un número natural, para $x = 0$.

Teorema 11.1.6. *Sea* $\langle G, \vee, \wedge, +, -, 0\rangle$ *un* ℓ*-grupo. Entonces:*

(1) $\langle G, \vee, \wedge\rangle$ *es distributivo,*

(2) $\langle G, +, -, 0\rangle$ *es libre de torsión.*

Demostración. Para probar (1) vamos a usar el Teorema 2.1.8 visto en el Capítulo 2. Sean x, y elementos de G y supongamos que existe z tal que:

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

Probemos que $x = y$. Se tiene, por el Lema 11.1.3, que

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

Luego,

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

Probemos (2). Sea x tal que $nx = 0$ para cierto n. Distribuyendo obtenemos:

$$\begin{aligned} n(x \vee 0) &= (x \vee 0) + (x \vee 0) + \cdots + (x \vee 0) \quad (n \text{ veces}) \\ &= nx \vee ((n-1)x) \vee \cdots \vee x \vee 0 \\ &= ((n-1)x) \vee \cdots \vee x \vee 0 \\ &= (n-1)(x \vee 0). \end{aligned}$$

Luego,

$$n(x \vee 0) - (n-1)(x \vee 0) = 0,$$

de donde

$$x \vee 0 = x^+ = 0.$$

Análogamente podemos obtener

$$n(-x \vee 0) - (n-1)(-x \vee 0) = 0,$$

lo que implica

$$-x \vee 0 = x^- = 0.$$

Luego

$$x = 0.$$

□

Congruencias y ℓ-subgrupos convexos

Vamos a referirnos a los homomorfismos de ℓ-grupos, a sus congruencias asociadas y a aquellos subconjuntos del universo de un ℓ-grupo que están en correspondencia con ellas. El tema será visto con más generalidad en el capítulo próximo.

Recordemos que un *homomorfismo* de un ℓ-grupo G en un ℓ-grupo H es una función $h : G \longrightarrow H$ que preserva las operaciones de grupo: $+$, $-$, 0 y las de retículo: $\vee$, $\wedge$.

Lema 11.1.7. *h es un homomorfismo si y solo si valen las siguientes propiedades:*

(i) *h es homomorfismo de grupos,*

(ii) $h(x \vee 0) = h(x) \vee 0$.

Demostración. Probemos que, si valen (i) y (ii), h es homomorfismo de retículos.

En primer lugar, observemos que vale la siguiente igualdad:

$$u \vee v = u + (0 \vee (v - u)).$$

Usando esto y el hecho de que h es homomorfismo de grupos, se tiene que

$$h(x \vee y) = h(x) \vee h(y).$$

Análogamente demostramos que

$$h(x \wedge y) = h(x) \wedge h(y).$$

La recíproca es obvia. □

En el Capítulo 1, Teorema 1.3.20, hemos visto que la relación R_h asociada a un homomorfismo $h : A \longrightarrow B$ es una congruencia y que, si h es suryectivo, A/R_h es isomorfo a B.

Llamaremos *núcleo* de h al conjunto $\mathrm{Ker}(h) = h^{-1}(0)$. Ya dimos una definición análoga para homomorfismo de MV-álgebras en el Capítulo 8.

Como se puede probar fácilmente, R_h puede definirse en función del núcleo de h de la siguiente manera.

Lema 11.1.8. *Dado $h : G \longrightarrow H$ homomorfismo, vale:*

$$xR_hy \ \text{ si y solo si } \ x - y \in \mathrm{Ker}(h).$$

Definición 11.1.9. Un subconjunto S de un ℓ-grupo G se llama *convexo* si dados $x, y, z \in G$ tales que $x, z \in S$, $x \leq y \leq z$ se tiene que $y \in S$. Si el subconjunto es, además, un ℓ-subgrupo, es decir, un subgrupo y un subretículo de G, entonces se llama *ℓ-ideal*.

Lema 11.1.10. *Un ℓ-subgrupo K de G es convexo si y solo si se cumple la siguiente condición:*

(Conv) *Si $z \in K$ y $x \in G$ es tal que $\|x\| \leq \|z\|$, entonces $x \in K$.*

Demostración. Supongamos que K es un ℓ-subgrupo convexo, es decir, un ℓ-ideal. Veamos que vale (Conv).

Sean $k \in K$ y $x \in G$ tales que $\|x\| \leq \|k\|$. Como K es un ℓ-subgrupo tenemos que $0 \in K$, $k^+ \in K$ y $k^- \in K$. En consecuencia, $\|k\| \in K$. Luego, como $0 \leq \|x\| \leq \|k\|$ y por convexidad tenemos que $\|x\| \in K$. Luego $0 \leq x^+ \leq \|x\|$ implica que $x^+ \in K$. Análogamente se tiene que $x^- \in K$, de donde se sigue que $x = x^+ - x^- \in K$.

Recíprocamente, supongamos que K es un ℓ-subgrupo que cumple (Conv). Veamos que es convexo.

Sean $h, k \in K$, $x \in G$ tales que $h \leq x \leq k$. Entonces, $h \vee 0 \leq x \vee 0 \leq k \vee 0$. Por ser elementos positivos, se tiene, por (2) del Lema 11.1.5, que $t^+ = \|t^+\|$, $t^- = \|t^-\|$ para $t = h, x, k$. Además, $k^+ \in K$ y $x^+ \leq k^+$. Por (Conv), $x^+ \in K$. Análogamente, por ser $x^- \leq h^-$, se tiene $x^- \in K$. Luego, $x = x^+ - x^- \in K$. $\square$

Se prueba ([1]) que la intersección de ℓ-ideales es un ℓ-ideal. Luego existe $I(E)$, el mínimo ℓ-ideal que contiene a un conjunto no vacío E (el *ideal generado por* E), que es la intersección de todos los ℓ-ideales K tales que $K \supseteq E$:

$$I(E) = \bigcap_{K \supseteq E} K.$$

En particular, denotamos $I(x)$ al ℓ-ideal generado por el conjunto $\{x\}$, que es llamado ℓ-ideal *principal*.

Lema 11.1.11. *Sea G un ℓ-grupo, J un ℓ-ideal de G.*

(a) *Para todo x en G: $x \in J$ si y solo si $\|x\| \in J$.*

(b) *Sean $E \neq \emptyset$, $E' = \{\|e\|, e \in E\}$. Entonces $I(E) = I(E')$.*

(c) *Si E es un conjunto finito no vacío, entonces $I(E)$ es principal.*

Demostración. Probemos (a). Si $x \in J$, entonces, por (Conv), $\|x\| \in J$. Por otra parte, también usando (Conv), $\|x\| \in J$ implica que $x^+ \in J$, pues $\|x^+\| = x^+ \leq \|x\|$. Análogamente $x^- \in J$. Luego, por ser J subgrupo, $x^+ - x^- = x \in J$.

Para probar (b), veamos previamente que para todo ℓ-ideal K de G, $K \supseteq E$ si y solo si $K \supseteq E'$. Pero eso se deduce de (a). Luego,

$$\bigcap_{K \supseteq E} K = \bigcap_{K \supseteq E'} K,$$

o sea, $I(E) = I(E')$, como queríamos probar.

Supongamos ahora que $E = \{e_1, \ldots, e_n\}$. Para ver (c), probemos que existe x tal que $I(E) = I(x)$. Sea $x = \|e_1\| \vee \cdots \vee \|e_n\|$. Se tiene que $x \in I(E)$, pues cada $\|e_i\| \in I(E)$ e $I(E)$ es cerrado por $\vee$. Luego, $I(x) \subseteq I(E)$, por ser $I(x)$ el mínimo ℓ-ideal que contiene a x. Por otra parte, por (Conv), $\|e_i\| \leq \|x\| = x$ implica $e_i \in I(x)$, para $i = 1, \ldots, n$. Luego, $E \subseteq I(x)$ y por minimalidad de $I(E)$: $I(E) \subseteq I(x)$. Por lo tanto, $I(E) = I(x)$. □

Lema 11.1.12. *Dados un ℓ-grupo G y un conjunto $E \neq \emptyset$, el ℓ-ideal generado por E tiene la siguiente forma:*

$$I(E) = \{z : \ \|z\| \leq \|e_1\| + \cdots + \|e_n\|, \ e_1, \ldots, e_n \in E, \ n \text{ natural}\}.$$

Demostración. Debemos probar que: $I(E) \supseteq E$, que es un subgrupo de G, que es un subretículo de G, que es convexo y que es el mínimo ℓ-ideal que contiene a E. Es fácil ver que $I(E) \supseteq E$ y que $I(E)$ es subgrupo, usando propiedades del módulo (se deja como ejercicio). Probemos que es subretículo.

Sean z y t en $I(E)$. Luego, por ser $I(E)$ subgrupo, $z - t \in I(E)$. Luego, $(z-t)^+ \in I(E)$, pues por (a) del Lema 11.1.11 se tiene que $\|z - t\| \in I(E)$. Por la demostración del Teorema 11.1.2 sabemos que, para todo $x, y \in G$,

$$x \vee y = ((x - y) \vee 0) + y.$$

Luego,

$$z \vee t = (z - t)^+ + t.$$

Como $(z-t)^+ \in I(E)$ y $t \in I(E)$, tenemos que $z \vee t \in I(E)$. Por otra parte, por el Lema 11.1.3, $z \wedge t = (z + t) - (z \vee t)$, de donde, por ser $I(E)$ cerrado por suma, resulta $z \wedge t \in I(E)$.

El resto de la prueba se deja como ejercicio. □

Corolario 11.1.13. *El ideal principal generado por un elemento x (ver [1, Teorema 1.2.3]) está dado por*

$$I(x) = \{z : \ \|z\| \leq n\|x\|, \ n \text{ natural}\}.$$

Teorema 11.1.14. *Sea $h : G \longrightarrow H$ un homomorfismo suryectivo. Entonces:*

(a) $\operatorname{Ker}(h)$ *es un ℓ-ideal,*

(b) $G/\operatorname{Ker}(h)$ *es isomorfo a H.*

Demostración. Probemos (a), ya que (b) se deduce del Teorema 1.3.20. Es de rutina ver que $\operatorname{Ker}(h)$ es ℓ-subgrupo. Mostremos que es convexo. Sean $s \leq x \leq t$, $s, t \in \operatorname{Ker}(h)$. Como h preserva ínfimos y supremos, es monótona. Por esta razón $h(s) = 0 \leq h(x) \leq h(t) = 0$. Por ende, $h(x) = 0$, o sea, $x \in \operatorname{Ker}(h)$. □

Observación 11.1.15. Hemos visto en el Capítulo 1 las congruencias módulo p en el grupo $\mathbb{Z}$ de los enteros: $x \equiv_p y$ si y solo si $x - y$ es múltiplo de p, es decir, si $x - y \in p\mathbb{Z}$, llamando $p\mathbb{Z}$ al conjunto de múltiplos de p. El conjunto $p\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$. La relación $\equiv_p$ se define entonces por medio de este subgrupo.

En general, en un grupo abeliano, las congruencias están en correspondencia con los subgrupos: Dado G y una congruencia R, la aplicación canónica $p_R : G \longrightarrow G/R$ es un homomorfismo de grupos cuyo núcleo $\operatorname{Ker}(p_R)$ es un subgrupo. Recíprocamente, dado un subgrupo H de G, la siguiente relación $\sim_H$ es una congruencia en G:

$$x \sim_H y \text{ si y solo si } x - y \in H.$$

Las asignaciones $R \mapsto \operatorname{Ker}(p_R)$ y $H \mapsto \sim_H$ son una inversa de la otra, estableciéndose entonces una biyección entre congruencias y subgrupos.

Veremos ahora que en ℓ-grupos, la correspondencia se establece entre congruencias y ℓ-ideales.

Teorema 11.1.16. *Sea J un ℓ-ideal de G. Entonces, $G/{\sim_J}$ tiene estructura de ℓ-grupo, donde hemos llamado $\sim_J$ a la congruencia de grupos asociada al subgrupo J.*

Demostración. Por lo visto en el Capítulo 1, 1.3.18, $G/{\sim_J}$ tiene estructura de grupo con las operaciones:

$$\begin{aligned} 0 &= |0| \\ -|x| &= |-x| \\ |x+y| &= |x| + |y|. \end{aligned}$$

Para mostrar que $G/{\sim_J}$ tiene estructura de retículo, empecemos por definir un orden en $G/{\sim_J}$.

Consideremos la relación

$$|x| \preceq |y| \quad \text{si y solo si} \quad y - x \leq j, \;\; j \in J.$$

Veamos que $\preceq$ está bien definida. Sea $|x| \preceq |y|$ y sean $x' \sim_J x$, $y' \sim_J y$, es decir que existen $i, j, k \in J$ tales que $x - x' = i$, $y - y' = j$, $y - x \leq k$. Entonces:

$$y' - x' = (x - x') + (y - x) + (y' - y) \leq i + k - j \in J.$$

Luego $|x'| \preceq |y'|$.

Se verifica fácilmente que $\preceq$ es reflexiva y transitiva. Probemos la antisimetría. Sean x, y tales que $|x| \preceq |y|$, $|y| \preceq |x|$. Existen $j, k \in J$ tales que $y - x \leq j$, $x - y \leq k$. Luego,

$$x \leq y + k \leq x + j + k.$$

Restando x obtenemos

$$0 \leq y - x + k \leq j + k.$$

Como $0 \in J$, $j + k \in J$, por convexidad de J resulta $y - x + k = u \in J$, de donde $y - x = u - k \in J$. Luego

$$|x| = |y|.$$

Vamos a demostrar ahora que $|x \vee y|$ es el supremo de $|x|$ e $|y|$. Se tiene, en primer lugar: $x \leq (x \vee y) + 0$, como $0 \in J$ es $|x| \preceq |x \vee y|$ y análogamente, $|y| \preceq |x \vee y|$. Sea $|z| \succeq |x|, |y|$. Se tiene entonces que existen $j, k \in J$ tales que

$$\begin{aligned} x &\leq z + j \\ y &\leq z + k, \text{ de donde} \\ x \vee y &\leq (z + j) \vee (z + k), \text{ luego} \\ x \vee y &\leq z + (j \vee k). \end{aligned}$$

Como J es un subretículo tenemos que $j \vee k \in J$, de donde resulta $|x \vee y| \preceq |z|$ y por lo tanto

$$|x \vee y| = |x| \vee |y|.$$

Por el Lema 8.5.2 del Capítulo 8 sabemos que $u \wedge v = -(-u \vee -v)$. Por esto también existe el ínfimo de dos clases dadas. La propiedad de distributividad de la suma en el supremo y el ínfimo salen de lo demostrado hasta aquí. $\square$

Corolario 11.1.17. *En las condiciones del teorema anterior, $\sim_J$ es una congruencia de ℓ-grupos.*

Teorema 11.1.18. *Dado un ℓ-grupo G, existe una biyección entre el conjunto $LID(G)$ de ℓ-ideales de G y el conjunto $CON(G)$ de ℓ-congruencias en G.*

Demostración. La correpondencia $LID(G) \longrightarrow CON(G)$ (respectivamente $CON(G) \longrightarrow LID(G)$) se define por $J \mapsto \sim_J$ (respectivamente por $R \mapsto |0|$).

La segunda correspondencia está bien definida, porque $|0| = \mathrm{Ker}(p_R)$, siendo $p_R : G \longrightarrow G/R$ la aplicación canónica.

Es sencillo mostrar que estas funciones son una inversa de la otra. En primer lugar, la clase del 0 por la congruencia $\sim_J$ es claramente J. En segundo lugar, y teniendo en cuenta que xRy si y solo si $(x - y)R0$, se tiene que $\sim_{|0|}= R$. □

11.2. La lógica $\mathcal{B}al$

Vamos a definir ahora el sistema deductivo $\mathcal{B}al$, cuya semántica algebraica equivalente es la cuasivariedad BAL. Probaremos luego que es, en realidad, una variedad. Sea $\mathcal{L}G$ la variedad de los ℓ-grupos. Veremos que las variedades $\mathcal{L}G$ y BAL son definicionalmente equivalentes. Nos basaremos en [47] y en resultados del Capítulo 10.

Lenguaje

El conjunto de conectivos es $\{\rightarrow, ^+\}$.

Consideramos numerables variables proposicionales y se construyen las fórmulas como es habitual.

Intuitivamente, $\rightarrow$ simboliza la diferencia: en las álgebras de BAL $x \rightarrow y$ será $y - x$, así como el conectivo $^+$ simboliza "la parte positiva de x" o sea x^+.

Axiomas

(B) $\quad$ (A $\rightarrow$ B) $\rightarrow$ ((C $\rightarrow$ A) $\rightarrow$ (C $\rightarrow$ B)).

(C) $\quad$ (A $\rightarrow$ (B $\rightarrow$ C)) $\rightarrow$ (B $\rightarrow$ (A $\rightarrow$ C)).

(N) $\quad$ ((A $\rightarrow$ B) $\rightarrow$ B) $\rightarrow$ A.

(P) $\quad$ $\mathrm{A}^{++} \rightarrow \mathrm{A}^{+}$.

(O) $((\mathrm{B} \to \mathrm{A})^+ \to (\mathrm{A} \to \mathrm{B})^+) \to (\mathrm{A} \to \mathrm{B})$.

Reglas de Inferencia

$$(\mathrm{MP}) \qquad \frac{\mathrm{A}\ ,\ \mathrm{A} \to \mathrm{B}}{\mathrm{B}}\,, \qquad (\mathrm{G}) \qquad \frac{\mathrm{A},\ \mathrm{B}}{\mathrm{A} \to \mathrm{B}}\,,$$

$$(\mathrm{PI}) \qquad \frac{\mathrm{A}}{\mathrm{A}^+}\,, \qquad (\mathrm{MI}) \qquad \frac{(\mathrm{A} \to \mathrm{B})^+}{(\mathrm{A}^+ \to \mathrm{B}^+)^+}\,.$$

Como es usual, diremos que A es consecuencia de un conjunto de fórmulas Γ si hay una sucesión de fórmulas $\mathrm{B}_1, \dots, \mathrm{B}_k$ tales que para cada $i = 1, \dots, k$, B_i es instancia de un axioma, pertenece a Γ o se obtiene de las anteriores por aplicación de alguna de las reglas.

Los axiomas (B) y (C) son conocidos; el axioma (N) podemos interpretarlo como $\neg_B\neg_B\mathrm{A} \to \mathrm{A}$, tomando $\neg_B\mathrm{A}$ como $\mathrm{A} \to \mathrm{B}$ (negación relativa a B). El axioma (P) nos dice, intuitivamente, que la parte positiva de un elemento positivo es él mismo.

Si interpretamos $x \to y$ como $y - x$ y x^+ como $x \vee 0$, el axioma (O) podría interpretarse de la siguiente manera: $y - x = ((y - x) \vee 0) - ((x - y) \vee 0)$, o sea que $y - x = (y - x)^+ - (y - x)^-$.

Si pensamos que "la verdad" en esta lógica, según veremos, es el 0, afirmar $(x \to y)^+$ significa decir que $(y - x) \vee 0 = 0$. Por lo tanto, sería $y - x \leq 0$, es decir que $y \leq x$. La última regla, (MI), dice entonces que $y \leq x$ implica $y^+ \leq x^+$.

Se puede probar que los siguientes son teoremas de $\mathcal{B}al$:

(i) $\vdash \mathrm{A} \to \mathrm{A}\,,$

(ii) $\vdash (\mathrm{A} \to \mathrm{B}) \to ((\mathrm{B} \to \mathrm{C}) \to (\mathrm{A} \to \mathrm{C}))\,,$

(iii) $\mathrm{A} \to \mathrm{B} \vdash \mathrm{B} \to \mathrm{A}\,,$

(iv) $\mathrm{A} \to \mathrm{B}\ ,\ \mathrm{C} \to \mathrm{D}\ \vdash\ (\mathrm{A} \to \mathrm{C}) \to (\mathrm{B} \to \mathrm{D})\,,$

(v) $\mathrm{A} \to \mathrm{B} \vdash \mathrm{A}^+ \to \mathrm{B}^+$.

$\mathcal{B}al$ es algebrizable

El siguiente teorema es una aplicación del Teorema 10.3.15 y del Corolario 10.3.16 del Capítulo 10. Los números en la demostración se refieren a los teoremas de $\mathcal{B}al$ recién mencionados.

Teorema 11.2.1. *El sistema $\mathcal{B}al$ es algebrizable por medio de la única ecuación de definición* $\mathrm{A} \approx \mathrm{A} \to \mathrm{A}$ *y la única fórmula de equivalencia* $\mathrm{A} \to \mathrm{B}$.

Demostración.

1. Por (i) tenemos que $\vdash \mathrm{A} \to \mathrm{A}$.

2. Por (iii) se tiene que $\mathrm{A} \to \mathrm{B} \vdash \mathrm{B} \to \mathrm{A}$.

3. En virtud de (ii) y de (MP) obtenemos que $\mathrm{A} \to \mathrm{B}\,,\, \mathrm{B} \to \mathrm{C} \vdash \mathrm{A} \to \mathrm{C}$.

4. Por (iv) vale que $\mathrm{A}_1 \to \mathrm{B}_1\ ,\ \mathrm{A}_2 \to \mathrm{B}_2\ \vdash\ (\mathrm{A}_1 \to \mathrm{A}_2) \to (\mathrm{B}_1 \to \mathrm{B}_2)$, y por (v) deducimos que $\mathrm{A} \to \mathrm{B} \vdash \mathrm{A}^+ \to \mathrm{B}^+$.

   Por lo tanto $\to$ define una congruencia en el álgebra de las fórmulas de $\mathcal{B}al$.

Por el Corolario 10.3.16 tenemos que el sistema $\mathcal{B}al$ es algebrizable puesto que valen las reglas de Gödel y modus ponens. □

Teorema 11.2.2. *Sea $\mathcal{F}_{\mathcal{B}al}$ el conjunto de las fórmulas de $\mathcal{B}al$. Sea $\equiv$ la relación binaria definida por*

$$\mathrm{A} \equiv \mathrm{B} \ \textit{ si y solo si } \ \vdash_{\mathcal{S}} \mathrm{A} \to \mathrm{B}.$$

Entonces $\equiv$ es una congruencia en el álgebra $\langle \mathcal{F}_{\mathcal{B}al}, {}^+, \to \rangle$.

Demostración. Es consecuencia del Teorema 11.2.1. □

Notación: Para toda fórmula A denotaremos $|\mathrm{A}|$ su clase de equivalencia. La clase de equivalencia de $\mathrm{B} \to \mathrm{B}$ será denotada $\mathbb{O}$.

Asimismo, definimos ahora las siguientes abreviaturas:

$$\begin{aligned} \mathbf{0} &:= x \to x \\ -x &:= x \to \mathbf{0} \\ x \,\&\, y &:= -x \to y = (x \to \mathbf{0}) \to y. \end{aligned}$$

Conviene marcar que, por el hecho de ser BAL la semántica equivalente de $\mathcal{B}al$, se tiene que:

$$\vdash x \to y \quad \text{si y solo si} \quad \models_{\mathsf{BAL}} x \approx y.$$

Tenemos el siguiente teorema, cuya demostración omitiremos. La idea es que por cada axioma a de $\mathcal{B}al$ hay una identidad $\delta(a) = \varepsilon(a)$ en BAL, en nuestro caso, será $a \approx \mathbf{0}$. Una cuasiidentidad será asociada a cada regla.

Una identidad extra se agrega al proceso, que en nuestro caso es:

$$\text{(AA)} \quad x \to x \approx (x \to x) \to (x \to x).$$

Hay también una cuasiidentidad que proviene del proceso de algebrización, que es aquí:

$$\text{(AQ)} \quad x \to y \approx \mathbf{0} \text{ implica } x \approx y.$$

Teorema 11.2.3. *La semántica equivalente a $\mathcal{B}al$ es la cuasivariedad* BAL *definida por las siguientes identidades y cuasiidentidad:*

$$\begin{array}{ll}
\mathsf{BAL}_{\text{(AA)}} & (x \to x) \approx \mathbf{0}\,, \\
\mathsf{BAL}_{\text{(B)}} & (x \to y) \approx (z \to x) \to (z \to y)\,, \\
\mathsf{BAL}_{\text{(C)}} & x \to (y \to z) \approx y \to (x \to z)\,, \\
\mathsf{BAL}_{\text{(N)}} & (x \to y) \to y \approx x\,, \\
\mathsf{BAL}_{\text{(P)}} & x^{++} \approx x^{+}\,, \\
\mathsf{BAL}_{\text{(O)}} & (y \to x)^{+} \to (x \to y)^{+} \approx x \to y\,, \\
\mathsf{BAL}_{\text{(MP)}} & \mathbf{0} \to x \approx x\,, \\
\mathsf{BAL}_{\text{(PI)}} & \mathbf{0}^{+} \approx \mathbf{0}\,, \\
\mathsf{BAL}_{\text{(AQ)}} & x \,\&\, (x \to y) \approx y\,, \\
\mathsf{BAL}_{\text{(MI)}} & (x \to y)^{+} \approx \mathbf{0} \Rightarrow (x^{+} \to y^{+})^{+} \approx \mathbf{0}.
\end{array}$$

El siguiente teorema describe al álgebra de Lindenbaum de $\mathcal{B}al$.

Teorema 11.2.4. *El sistema $\mathcal{F}/_{\equiv} = \langle \mathcal{F}_{\mathcal{B}al}/_{\equiv}\,; \to, ^{+} \rangle$ es un álgebra en* BAL*, donde $\to$ y $^{+}$ se definen por*

$$|x| \to |y| = |x \to y|$$
$$|x|^{+} = |x^{+}|.$$

El álgebra $\mathcal{F}/_{\equiv}$ es libre en BAL *con el conjunto de generadores libres $\{|X_1|, |X_2|, \ldots\}$, donde $X_1, X_2, \ldots$ son las variables proposicionales.*

La variedad BAL es definicionalmente equivalente a $\mathcal{L}G$

Se puede probar ahora que a partir de las operaciones $^+$ y $\to$ sobre un universo A de un álgebra de BAL pueden definirse operaciones de ℓ-grupo sobre A y recíprocamente. Describibirmos los pasos que llevan a ese resultado.

En primer lugar, se prueba que $\langle A, \&, -, \mathsf{0}\rangle$ es un grupo abeliano. Luego, usando el Teorema 11.1.1, se prueba que es un p.o.grupo cuyo cono positivo es

$$P = \{a \in A : a^+ = a\}.$$

Además, se demuestra usando 11.1.2 que $a^+ = a \vee \mathsf{0}$, con lo que se pueden definir $\vee$ y $\wedge$.

Finalmente se prueba que la cuasiidentidad (BAL_{MI}) puede reemplazarse por la identidad

$$((y \to x)^+ \to (y^+ \to x^+)^+)^+ \;\approx\; \mathsf{0}.$$

Luego, BAL es una variedad.

Se obtiene entonces el siguiente teorema.

Teorema 11.2.5. *La variedad* BAL *es definicionalmente equivalente a la variedad* $\mathcal{L}G$*. Para cada álgebra* $\langle A, \to, ^+\rangle$ *de* BAL *se definen sobre* A *las siguientes operaciones de* ℓ*-grupo:*

$$\begin{aligned}
\mathsf{0} &:= x \to x\\
-x &:= x \to \mathsf{0}\\
x \,\&\, y &:= (x \to \mathsf{0}) \to y\\
x \vee y &:= (x \to y)^+ \,\&\, x\\
x \wedge y &:= -(-x \vee -y).
\end{aligned}$$

Recíprocamente, para cada ℓ*-grupo* $\langle G, +, -, 0, \vee, \wedge\rangle$ *se definen sobre* G *las siguientes operaciones que le dan una estructura de álgebra de* BAL*:*

$$\begin{aligned}
x \to y &:= y - x\\
x^+ &:= x \vee 0\,.
\end{aligned}$$

Teorema de la deducción en $\mathcal{B}al$

Una vez demostrada la relación entre BAL y $\mathcal{L}G$, veremos, como hemos hecho en otros cálculos proposicionales, que las teorías de $\mathcal{B}al$ se corresponden con los filtros de $\mathcal{F}/_{\equiv}$, resultado que nos conducirá al teorema de la deducción. Indicaremos los pasos hacia ese resultado. Las demostraciones están en [47].

Un filtro en un álgebra $\mathbb{A} = \langle A, \rightarrow, ^+ \rangle$ de BAL es un subconjunto F de A que contiene todas las interpretaciones de los axiomas de $\mathcal{B}al$ y es cerrado por todas las reglas.

Sea $\mathbb{A}^* = \langle A, \&, -, \mathsf{0}\rangle$ el ℓ-grupo asociado a $\mathbb{A}$. Se tiene el siguiente resultado:

Teorema 11.2.6. *Sea $F \subseteq A$. Entonces: F es un filtro de $\mathbb{A}$ si y solo si es un ℓ-ideal de $\mathbb{A}^*$.*

Una *teoría* de $\mathcal{B}al$ es un subconjunto de fórmulas que contiene a todas las instancias de axiomas y es cerrado por todas las reglas.

Sea $F_\omega(\mathsf{BAL})$ el álgebra libre con numerables generadores, que es isomorfa al álgebra de Lindenbaum de $\mathcal{B}al$.

Es de rutina probar a partir de los resultados previos el siguiente teorema:

Teorema 11.2.7. *Existe un isomorfismo entre la clase de los filtros de $F_\omega(\mathsf{BAL})$ y la clase de las teorías de $\mathcal{B}al$.*

Teniendo en cuenta la relación entre BAL y $\mathcal{L}G$, el filtro $I(E)$ generado por un conjunto E de elementos positivos de $F_\omega(\mathsf{BAL})$ toma la siguiente forma:

$$\begin{array}{l} z \in I(E) \text{ si y solo si existen } e_1, \ldots, e_t \text{ tales que} \\ z^+ \leq e_1 \,\&\, \ldots \,\&\, e_t \quad \text{y} \quad z^- \leq e_1 \,\&\, \ldots \,\&\, e_t. \end{array}$$

En base a estas últimas consideraciones y al Teorema 11.2.7 se llega finalmente al teorema de la deducción:

Teorema 11.2.8. *Sea $\Gamma \subseteq \mathcal{F}_{\mathcal{B}al}$, A una fórmula tal que $\Gamma \vdash \mathrm{A}$. Entonces existen fórmulas $\mathrm{B}_1 \ldots, \mathrm{B}_k \in \Gamma$ tales que*

$$\vdash ((\mathrm{B}_1 \,\&\, \ldots \,\&\, \mathrm{B}_k) \rightarrow \mathrm{A}^+)^+ \quad y \quad \vdash ((\mathrm{B}_1 \,\&\, \ldots \,\&\, \mathrm{B}_k) \rightarrow \mathrm{A}^-)^+.$$

Completud

La variedad de los ℓ-grupos está generada por $\mathbb{F}$, siendo $\mathbb{F} = \mathbb{Z}$, o bien $\mathbb{F} = \mathbb{Q}$ o bien $\mathbb{F} = \mathbb{R}$. Es decir que cualquier ℓ-grupo puede ser obtenido tomando productos, subálgebras e imágenes homomorfas de $\mathbb{Z}$. Lo mismo ocurre con $\mathbb{Q}$ o con $\mathbb{R}$.

En $\mathcal{B}al$ puede demostrarse la completud tomando valuaciones en $\mathbb{F}$, siendo $\mathbb{F} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$. Sin embargo, no vale la completud fuerte en $\mathcal{B}al$.

Definición 11.2.9. Una $\mathbb{F}$-valuación es una función $v : \mathcal{F}_{\mathcal{B}al} \longrightarrow \mathbb{F}$ tal que:

1. $v(\mathrm{A} \rightarrow \mathrm{B}) = v(\mathrm{B}) - v(\mathrm{A})$,

2. $v(-\mathrm{A}) = -v(\mathrm{A})$,

3. $v(\mathrm{A}^+) = \max\{v(\mathrm{A}), 0\}$.

Como es usual, diremos que una fórmula A es:

- satisfecha por v, o que v satisface A, si $v(\mathrm{A}) = 0$,

- $\mathbb{F}$-válida si $v(\mathrm{A}) = 0$ para toda $\mathbb{F}$-valuación,

- $\mathbb{F}$-consecuencia de un conjunto de fórmulas Γ si toda valuación que satisface a todas las fórmulas de Γ satisface también a A. Lo denotamos: $\Gamma \models_{\mathbb{F}} \mathrm{A}$.

El siguiente es un teorema de corrección cuya demostración es de rutina:

Teorema 11.2.10. *Sean* $\Gamma \subseteq \mathcal{F}_{\mathcal{B}al}$, $\mathrm{A} \in \mathcal{F}_{\mathcal{B}al}$. *Entonces, para* $\mathbb{F} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$,

$$\Gamma \vdash \mathrm{A} \quad \textit{implica} \quad \Gamma \models_{\mathbb{F}} \mathrm{A}.$$

La recíproca, es decir, la completud, vale para el caso en que Γ es finito (en particular, vacío).

Teorema 11.2.11. *Sea* $\Gamma \cup \{\mathrm{A}\}$ *un conjunto finito de fórmulas de* $\mathcal{B}al$. *Entonces, para* $\mathbb{F} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$,

$$\Gamma \vdash \mathrm{A} \quad \textit{si y solo si} \quad \Gamma \models_{\mathbb{F}} \mathrm{A}.$$

11.3. Conos, ℓ-grupos y sus lógicas

Hemos visto cómo el cono positivo de un ℓ-grupo determina su orden. La relación entre conos y ℓ-grupos es más profunda. Dado un cono P, podemos obtener un ℓ-grupo G tal que $G^+ = P$. Dado un ℓ-grupo, obviamente sus elementos positivos determinan un cono. De hecho, podemos extender la correspondencia entre conos y ℓ-grupos de manera de obtener una equivalencia categorial. Pero ¿qué es, en realidad, un cono? El cono "emblemático" está dado por los números naturales con las operaciones de suma y diferencia truncada, según veremos. Podemos caracterizar los conos de ℓ-grupos como *BCK-álgebras cónicas*, que definiremos en seguida. Estas álgebras son también conocidas como *hoops cancelativos* (ver [24]).

Definición 11.3.1. Una *BCK-álgebra cónica* es un sistema $\langle M, *, \circ, 0\rangle$ que satisface las siguientes identidades:

(Y3) $x * x = 0$

(Y4) $x * 0 = x$

(Is) $(x * y) * z = x * (y \circ z)$

(P1) $x \circ (y * x) = y \circ (x * y)$

(P2) $x = (x \circ y) * y$

Se puede probar que para cada y fijo, la operación $f(u) = y \circ u$ es adjunta de $g(v) = v * y$, es decir que

$$x \leq y \circ z \quad \text{si y solo si} \quad x * y \leq z.$$

En cada BCK-álgebra cónica valen:

(Y1) $(x * y) * z = (x * z) * y$

(Y2) $x * (x * y) = y * (y * x)$.

Dado que se cumplen (Y1), ..., (Y4), el reducto $\langle M, *, 0\rangle$ de toda BCK-álgebra cónica es una BCK-álgebra conmutativa (ver 9.1.3 en el Capítulo 9). Luego, puede probarse que tiene un orden con primer elemento 0 dado por

$$x \leq y \quad \text{si y solo si} \quad x * y = 0$$

y existe el ínfimo de cada par de elementos.

Además, una BCK-álgebra cónica es un monoide conmutativo con respecto a la operación $\circ$. Es también un retículo con las operaciones $\vee$, $\wedge$ dadas por:

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

La operación $\circ$ preserva el orden.

Observación 11.3.2. La variedad de las BCK-álgebras cónicas está generada por $\langle \mathbb{N}, *, \circ, 0\rangle$, donde las operaciones son:

$$x * y := (x - y) \vee 0, \quad x \circ y := x + y, \quad 0 := 0.$$

Existe una equivalencia categorial entre la categoría de las BCK-álgebras cónicas y la categoría de los ℓ-grupos (ver [28, Thm. 2.1]).

La equivalencia puede definirse, por ejemplo, de la manera que se muestra en los siguientes teoremas (ver [96]). Llamaremos $c\mathcal{BCK}$ y $\mathcal{L}G$ a las categorías de BCK-álgebras cónicas y de ℓ-grupos respectivamente.

Teorema 11.3.3. *Sea* $\langle M, *, \circ, 0\rangle$ *una BCK-álgebra cónica. Sea*

$$K(M) = \{(x, y) \in M \times M : \ \ x \wedge y = 0\}$$

y definamos en $K(M)$ *las siguientes operaciones:*

$$\begin{aligned}
(x, y) + (u, v) &:= ((x \circ u) * (y \circ v), (y \circ v) * (x \circ u)),\\
-(x, y) &:= (y, x),\\
0 &:= (0, 0),\\
(x, y) \vee (z, t) &:= (x \vee z, y \wedge t),\\
(x, y) \wedge (z, t) &:= (x \wedge z, y \vee t).
\end{aligned}$$

Entonces, el sistema $\langle K(M), +, \vee, \wedge, -, 0\rangle$ *es un* ℓ*-grupo. Dado un morfismo* $f : M \longrightarrow N$*,* $K(f)$ *es un morfismo de* ℓ*-grupos* $K(f) : K(M) \longrightarrow K(N)$*, siendo* $K(f)$ *la restricción a* $K(M)$ *de* $f \times f$*. Entonces,* K *es un funtor c*$\mathcal{BCK}$ *en* $\mathcal{L}G$*.*

Teorema 11.3.4. *La correspondencia* $(\ )^+$ *que asigna a cada* ℓ*-grupo* G *su cono positivo y a cada morfismo de* ℓ*-grupos su restricción al cono positivo es un funtor de* $\mathcal{L}G$ *en c*$\mathcal{BCK}$*. Los funtores* K *y* $(\ )^+$ *determinan una equivalencia categorial dada por las equivalencias naturales*

$$s : \mathbf{1}_{c\mathcal{BCK}} \approx (\ )^+ \circ K, \quad t : K \circ (\ )^+ \approx \mathbf{1}_{\mathcal{L}G}$$

definidas, para cada BCK-álgebra cónica M *y cada* ℓ*-grupo* G*, por:*

$$s(M)(x) = (x, 0), \quad t(G)(x, y) = x - y.$$

La Lógica cónica

Definiremos ahora la B-C-K-lógica cónica $\mathcal{C}o$ asociada a los conos.

Lenguaje

Los conectivos son $\rightarrow$ y $\circ$.

Axiomas

(B) (A → B) → ((C → A) → (C → B)).

(C) (A → (B → C)) → (B → (A → C)).

(K) A → (B → A).

(S1) $A \to (B \to (A \circ B))$.

(S1') $(B \to (A \circ B)) \to A$.

(S2) $(A \to (B \to C)) \to ((A \circ B) \to C)$.

(S2') $((A \circ B) \to C) \to (A \to (B \to C))$.

(Su) $(A \circ (A \to B)) \to (B \circ (B \to A))$.

Reglas

La única regla es Modus Ponens.

Teorema 11.3.5. *El sistema $\mathcal{C}o$ es algebrizable y la variedad de las BCK-álgebras cónicas es su semántica algebraica equivalente.*

Teorema 11.3.6. *Sea $\mathcal{F}_{\mathcal{C}o}$ el conjunto de las fórmulas de $\mathcal{C}o$, sea la relación $\equiv$ definida en $\mathcal{F}_{\mathcal{C}o}$ por*

$$A \equiv B \ \textit{si y solo si} \ \vdash A \to B \ , \vdash B \to A.$$

El sistema $\mathcal{F}_{\mathcal{C}o}/_{\equiv} = \langle \mathcal{F}_{\mathcal{C}o}/_{\equiv}; *, \circ, \mathbb{O} \rangle$ es una BCK-álgebra cónica, siendo

$$|A| \circ |B| = |A \circ B|, \quad |A| * |B| = |B \to A|, \quad \mathbb{O} = |A \to A|.$$

Definiendo $\mathbb{N}$-valuaciones de la manera usual, obtenemos el siguiente teorema de completud.

Teorema 11.3.7. $\vdash A$ *si y solo si* $\models_{\mathbb{N}} A$.

Otra lógica para los ℓ-grupos

Vamos a definir ahora el sistema deductivo $\mathcal{B}al^o$ equivalente a $\mathcal{B}al$ y cuyas fórmulas positivas satisfacen los axiomas de $\mathcal{C}o$. El conectivo adicional $\circ$ representa la suma. Este hecho, junto con los axiomas correspondientes hace que el álgebra de Lindenbaum de $\mathcal{B}al^o$ sea un grupo. Además, los axiomas (S1) y (S2) describen la adjunción entre $\to$ (diferencia) y $\circ$ (suma). Los axiomas (In^o) y (Su^o) nos permiten definir respectivamente el ínfimo y el supremo, lo que nos completa la estructura de ℓ-grupo en $\mathcal{F}_{\mathcal{B}al^o}/\equiv$, siendo $\mathcal{F}_{\mathcal{B}al^o}$ el conjunto de fórmulas de $\mathcal{B}al^o$.

Lenguaje

El lenguaje de $\mathcal{B}al^o$ está dado por los conectivos $\to, \circ, ^+$.

Axiomas

(B) $(A \to B) \to ((C \to A) \to (C \to B))$.

(C) $(A \to (B \to C)) \to (B \to (A \to C))$.

(N) $((A \to B) \to B) \to A$.

(K^o) $(B \to (A^+ \to B))^+$.

(In^o) $((A \to B)^+ \to B) \to ((B \to A)^+ \to A)$.

(S1) $A \to (B \to (A \circ B))$.

(S2) $(A \to (B \to C)) \to ((A \circ B) \to C)$.

(Su^o) $((A \to B)^+ \circ A) \to ((B \to A)^+ \circ B)$.

Reglas

(MP) $\dfrac{A\ ,\ A \to B}{B}$, (G) $\dfrac{A,\ B}{A \to B}$,

(PI) $\dfrac{A}{A^+}$, (MI) $\dfrac{(A \to B)^+}{(A^+ \to B^+)^+}$.

En primer lugar, si traducimos $A \circ B := (A \to \mathbf{0}) \to B$, siendo la abreviatura $\mathbf{0} = C \to C$, podemos probar que $\mathcal{B}al$ y $\mathcal{B}al^o$ tienen los mismos teoremas.

Teorema 11.3.8. *Todo teorema de $\mathcal{B}al$ es un teorema de $\mathcal{B}al^o$ y recíprocamente.*

Veamos los resultados respecto al álgebra de Lindenbaum de $\mathcal{B}al^o$.

Teorema 11.3.9. *El sistema $\langle \mathcal{F}_{\mathcal{B}al^o}/_{\equiv}, +, -, \mathbb{O}\rangle$ es un grupo abeliano, con operaciones definidas por:*

$$|A| + |B| = |A \circ B|$$
$$\mathbb{O} = |\mathbf{0}|$$
$$-|A| = |A \to \mathbf{0}|.$$

Teorema 11.3.10. *El sistema* $\langle \mathcal{F}_{\mathcal{B}al^o}/_\equiv, +, -, \mathbb{O}, \preceq \rangle$ *es un grupo ordenado, donde* $\preceq$ *se define por*

$$|\mathrm{A}| \preceq |\mathrm{B}| \text{ si y solo si } \vdash (\mathrm{B} \to \mathrm{A})^+.$$

Teorema 11.3.11. *El sistema* $\langle \mathcal{F}_{\mathcal{B}al^o}/_\equiv, +, -, \mathbb{O}, \vee, \wedge \rangle$ *es un* ℓ*- grupo, siendo*

$$|\mathrm{A}| \vee |\mathrm{B}| = |(\mathrm{A} \to \mathrm{B})^+| + |\mathrm{A}|$$
$$|\mathrm{A}| \wedge |\mathrm{B}| = |(\mathrm{A} \to \mathrm{B})^+| \to |\mathrm{A}|.$$

Inmersión de $\mathcal{C}o$ en $\mathcal{B}al^o$

Vamos a mostrar que la lógica cónica $\mathcal{C}o$ puede ser sumergida en la lógica $\mathcal{B}al^o$ de manera que los teoremas de $\mathcal{C}o$ sean teoremas de $\mathcal{B}al^o$, siempre que la implicación en $\mathcal{C}o$ sea interpretada en $\mathcal{B}al^o$ por la implicación positiva $\xrightarrow{+}$ y la "suma" $\circ$ de $\mathcal{C}o$ sea interpretada por el conectivo $\bullet$. En particular se prueban los axiomas de $\mathcal{C}o$.

Lema 11.3.12. *Los siguientes son teoremas de* $\mathcal{B}al^o$*, siendo* $\mathrm{A} \xrightarrow{+} \mathrm{B}$ *una abreviatura de* $(\mathrm{A}^+ \to \mathrm{B}^+)^+$ *y* $\mathrm{A} \bullet \mathrm{B}$ *una abreviatura de* $(\mathrm{A}^+ \circ \mathrm{B}^+)^+$*:*

(C$^+$) $(\mathrm{A} \xrightarrow{+} (\mathrm{B} \xrightarrow{+} \mathrm{C})) \xrightarrow{+} (\mathrm{B} \xrightarrow{+} (\mathrm{A} \xrightarrow{+} \mathrm{C}))$.

(B$^+$) $(\mathrm{A} \xrightarrow{+} \mathrm{B}) \xrightarrow{+} ((\mathrm{B} \xrightarrow{+} \mathrm{C}) \xrightarrow{+} (\mathrm{A} \xrightarrow{+} \mathrm{C}))$.

(K$^+$) $\mathrm{A} \xrightarrow{+} (\mathrm{B} \xrightarrow{+} \mathrm{A})$.

(S1$^+$) $\mathrm{A} \xrightarrow{+} (\mathrm{B} \xrightarrow{+} (\mathrm{A} \bullet \mathrm{B}))$.

(S1'$^+$) $(\mathrm{B} \xrightarrow{+} (\mathrm{A} \bullet \mathrm{B})) \xrightarrow{+} \mathrm{A}$.

(S2$^+$) $(\mathrm{A} \xrightarrow{+} (\mathrm{B} \xrightarrow{+} \mathrm{C})) \xrightarrow{+} ((\mathrm{A} \bullet \mathrm{B}) \xrightarrow{+} \mathrm{C})$.

(S2'$^+$) $((\mathrm{A} \bullet \mathrm{B}) \xrightarrow{+} \mathrm{C}) \xrightarrow{+} (\mathrm{A} \xrightarrow{+} (\mathrm{B} \xrightarrow{+} \mathrm{C}))$.

(Su$^+$) $(\mathrm{A} \bullet (\mathrm{A} \xrightarrow{+} \mathrm{B})) \xrightarrow{+} (\mathrm{B} \bullet (\mathrm{B} \xrightarrow{+} \mathrm{A}))$.

Además, la siguiente es una regla de $\mathcal{B}al^o$*:*

$$(MP^+) \qquad \frac{\mathrm{A}^+ \ , \ \mathrm{A} \xrightarrow{+} \mathrm{B}}{\mathrm{B}^+}.$$

Definición 11.3.13. Sea A una fórmula de $\mathcal{C}o$. La $'$-traducción A' de A es una fórmula de $\mathcal{B}al^o$ definida recursivamente como sigue:

1. Si A es una variable proposicional p, entonces A$'$ es p^+.

2. Si A es de la forma B $\to$ C, entonces A$'$ es B$'$ $\xrightarrow{+}$ C$'$.

3. Si A es de la forma B $\circ$ C, entonces A$'$ es B$'$ $\bullet$ C$'$.

De manera similar definimos la $''$-traducción de una fórmula A de $\mathcal{C}o$, cambiando p^+ por $(p \to 0)^+$ en el ítem 1 y $'$ por $''$ en los lugares apropiados.

Observemos que la $'$-traducción del axioma (X) de $\mathcal{C}o$ es el teorema (X$^+$) de $\mathcal{B}al^o$.

Una fórmula A de $\mathcal{B}al^o$ se llamará *positiva* si A $\equiv$ A$^+$.

En el siguiente teorema llamaremos Γ^+ al siguiente conjunto de teoremas de $\mathcal{B}al^o$: (B$^+$), (C$^+$),..., (Su$^+$).

Teorema 11.3.14. *Sea* A *una fórmula de* $\mathcal{C}o$. *Si* $\vdash_{\mathcal{C}o}$ A *entonces* $\Gamma^+ \vdash_{\mathcal{B}al^o}$ A$'$. *Sea* B *una fórmula de* $\mathcal{B}al^o$ *tal que* $\Gamma^+ \vdash_{\mathcal{B}al^o}$ B. *Entonces existe una deducción de* B *que usa solo (MP$^+$). En particular, si* B *es de la forma* A$'$, *entonces* $\vdash_{\mathcal{C}o}$ A.

Descomposición de fórmulas de $\mathcal{B}al^o$ en fórmulas de $\mathcal{C}o$

Se puede probar que para una fórmula B de $\mathcal{B}al^o$ existen fórmulas de $\mathcal{C}o$ que determinan B.

Descibiremos la situación para el caso más simple que es el de fórmulas de una variable. En ese caso, el álgebra de Lindenbaum $\mathcal{F}_{\mathcal{B}al^o}/_{\equiv}$ está libremente generada por $|p|$.

Se sabe que el ℓ-grupo libre con un generador g es isomorfo a $\mathbb{Z} \times \mathbb{Z}$ y el isomorfismo está dado por: $g \mapsto (1, -1)$. En la Figura 11.2 se muestra este grupo. Puede verse allí que todo elemento t del cono positivo es de la siguiente forma: $t = rg^+ \vee sg^- = rg^+ + sg^-$, con r, s positivos. Luego, todo elemento x del grupo puede descomponerse como: $x = x^+ - x^- = (rg^+ \vee sg^-) - (mg^+ \vee ng^-)$, con r, s, m, n positivos. Esta intuición se ve confirmada por el siguiente resultado.

Teorema 11.3.15. *Sea* G_g *el* ℓ*-grupo libre con un generador* g. *Entonces, para todo* $t \in G_g$ *existen enteros* r, s *tales que* $t = rg^+ + sg^- = rg^+ \vee sg^-$. *La descomposición es única. Si* $t \geq 0$, *entonces* $r, s \geq 0$.

Teorema 11.3.16. *Dada una fórmula* A *de* $\mathcal{B}al^o$ *con una variable* p *existen enteros* r, s *tales que* A *es equivalente a* $r\ p^+ \circ s\ (p \to 0)^+$. *Si* A *es equivalente a* $u\ p^+ \circ v\ (p \to 0)^+$ *entonces* $r = u$ *y* $s = v$.

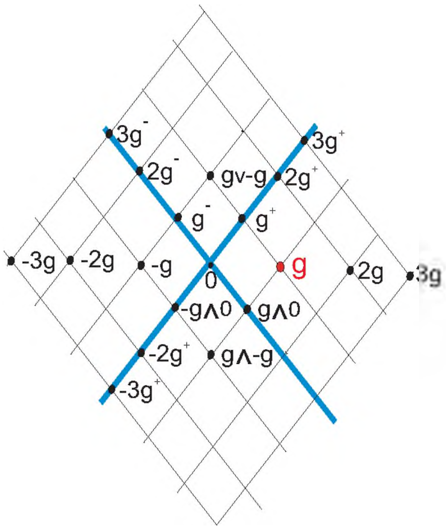


Figura 11.2: ℓ-grupo libre con 1 generador

Demostración. Es consecuencia del Teorema 11.3.15 aplicado a $\mathcal{F}_{\mathcal{B}al^o}/_{\equiv}$. $\square$

Debido a la equivalencia categorial entre los ℓ-grupos y las BCK-álgebras cónicas (ver Teorema 11.3.4), $\mathcal{F}_{\mathcal{B}al^o}/_{\equiv}$ es isomorfo a $K((\mathcal{F}_{\mathcal{B}al^o}/_{\equiv})^+)$. Entonces, todo elemento de $\mathcal{F}_{\mathcal{B}al^o}/_{\equiv}$ puede ser pensado como un par de elementos positivos $(|\mathrm{B}|, |\mathrm{C}|)$ tales que $|\mathrm{B}| \wedge |\mathrm{C}| = 0$. Es decir que toda la información acerca del ℓ-grupo $\mathcal{F}_{\mathcal{B}al^o}/_{\equiv}$ está contenida en su cono positivo. Luego, es suficiente focalizar nuestra atención en las fórmulas positivas de $\mathcal{B}al^o$.

Corolario 11.3.17. *Sea* A *una fórmula positiva de* $\mathcal{B}al^o$ *con una variable. Existen dos fórmulas* B *y* C *de* $\mathcal{C}o$ *con una variable tal que* A *es equivalente a* $\mathrm{B}' \circ \mathrm{C}''$*, siendo* B' *la* $'$*-traducción de* B *y* C'' *la* $''$*-traducción de* C*. Además,* $|\mathrm{B}'| \wedge |\mathrm{C}''| = \mathbb{O}$.

Bibliografía del Capítulo 11

- Anderson M. and Feil T., *Lattice-Ordered Groups, an Introduction.* D. Reidel, 1988.
- Bigard A., Keimel K. and Wolfenstein S., *Groupes et Anneaux Réticulés.* Lecture Notes in Math., 608, Springer-Verlag, 1977.
- Cignoli R. and Torrens A., *Free cancelative hoops.* Algebra Universalis, 43 (2000), 213–216.
- Cornish W., *Lattice-ordered groups and BCK-algebras.* Math. Japonica, 4 (1980), no. 4, 471–476.
- Fuchs L., *Partially Ordered Algebraic Systems.* Addison-Wesley, Pergamon Press, 1963.
- Galli A., Lewin R. and Sagastume M., *The logic of equilibrium and abelian lattice ordered groups.* Arch. Math. Logic, 43 (2004), no. 2, 141–158.
- Sagastume M., *Conical logic and l-groups logic.* J. Appl. Non-Classical Logics 15 (2005), no. 3, 265–283.

Capítulo 12

Retículos residuados conmutativos

En este capítulo veremos que las álgebras que hemos estudiado en capítulos anteriores pueden ponerse en un marco común. Las álgebras de Boole, las álgebras de Heyting, las MV-álgebras y los l-grupos se pueden pensar como casos particulares de álgebras que se denominan *retículos residuados conmutativos*. Vamos a estudiar algunas de sus propiedades, en particular daremos una descripción de las congruencias. Nuestra intención es hacer una introducción elemental a la teoría de retículos residuados conmutativos. Para este propósito nos basaremos principalmente en el artículo [58] de Constantine Tsinakis.

En las primeras tres secciones abordaremos resultados generales. En la cuarta sección nos referiremos al aspecto lógico desde la perspectiva de las lógicas subestructurales. Como ejemplo importante, en la quinta y última sección trataremos la lógica básica, sus álgebras asociadas (las BL-álgebras) y su relación con las MV-álgebras.

12.1. Introducción y resultados básicos

Comenzaremos dando la definición de *retículo residuado conmutativo*.

Como en otros casos, a menudo denotaremos (ver Observación 1.3.3) a un retículo residuado conmutativo mencionando solo su conjunto subyacente.

Definición 12.1.1. Un *retículo residuado conmutativo*, c.r.l. para abreviar, es un álgebra $\langle A, \wedge, \vee, \cdot, \rightarrow, e\rangle$ de tipo $(2, 2, 2, 2, 0)$ tal que satisface las siguientes condiciones:

1. $\langle A, \cdot, e\rangle$ es un monoide conmutativo.

2. $\langle A, \wedge, \vee \rangle$ es un retículo.

3. Para cada $x, y, z \in A$ vale que $x \cdot y \leq z$ si y solo si $x \leq y \to z$.

La operación $\cdot$ se llama *multiplicación*, y la operación $\to$ se llama *implicación*. Si el poset asociado al retículo $\langle A, \wedge, \vee \rangle$ tiene último elemento 1, siendo $1 = e$, se dice que el c.r.l. es *integral*. También se dice que la implicación es el *residuo* de la multiplicación con respecto al orden asociado al retículo $\langle A, \wedge, \vee \rangle$. Además se verifica la siguiente condición:

$$x \leq y \text{ si y solo si } e \leq x \to y.$$

Si el c.r.l. considerado es integral, entonces tenemos que

$$x \leq y \text{ si y solo si } x \to y = 1.$$

Casi todas las álgebras que hemos considerado en este libro pueden pensarse como casos particulares de retículos residuados conmutativos, por ejemplo:

(i) Si $\langle A, \wedge, \vee, \to, 0, 1 \rangle$ es un álgebra de Heyting, definiendo $\cdot = \wedge$ tenemos que $\langle A, \wedge, \vee, \cdot, \to, 1 \rangle$ es un c.r.l. integral. En particular, toda álgebra de Boole es un c.r.l. integral.

(ii) Si $\langle A, \oplus, \neg, 0 \rangle$ es una MV-álgebra, $\langle A, \wedge, \vee, \odot, \to, 1 \rangle$ es un c.r.l. integral, en donde las operaciones de ínfimo y supremo son las asociadas al orden parcial definido sobre MV-álgebras. De manera alternativa, si $\langle A, \to, 1 \rangle$ es una W-álgebra entonces $\langle A, \wedge, \vee, \odot, \to, 1 \rangle$ es un c.r.l., en donde como antes las operaciones de ínfimo y supremo se definen a partir del orden parcial definido en la W-álgebra.

(iii) Sea $\langle G, +, -, \vee, \wedge, 0 \rangle$ un l-grupo. Definimos $\cdot = +$, y $\to$ como $x \to y = y - x$. Luego $\langle A, \wedge, \vee, \cdot, \to, 0 \rangle$ es un c.r.l. (no necesariamente integral).

Podríamos hacernos la siguiente pregunta:

¿Qué nos dice la condición $x \cdot y \leq z$ si y solo si $x \leq y \to z$ para cada x, y, z?

Más específicamente, ¿puede esta condición ser expresada de un modo distinto? La respuesta es afirmativa, y es lo que haremos a continuación.

Si $\cdot$ es una operación binaria conmutativa sobre un poset $(A, \leq)$ entonces definimos al conjunto $E_{x,y} = \{z \in A : x \cdot z \leq y\}$.

Teorema 12.1.2. *Supongamos que tenemos un poset $(A, \leq)$ y una operación binaria $\cdot$ que es conmutativa. Las siguientes condiciones son equivalentes:*

(I) *Existe una operación binaria* $\to$ *que cumple la condición* $x \cdot y \leq z$ *si y solo si* $x \leq y \to z$ *para todo* $x, y, z \in A$.

(II) *Valen las siguientes dos condiciones:*

   (a) *La operación* $\cdot$ *es monótona. Es decir, si* $x, y, z \in A$ *y* $x \leq y$ *entonces* $x \cdot z \leq y \cdot z$.

   (b) *Para cada* $x, y \in A$ *existe el máximo del conjunto* $E_{x,y}$*, siendo* $x \to y = \text{máx}\, E_{x,y}$.

Demostración. Supongamos primero que existe una operación binaria $\to$ que satisface $x \cdot y \leq z$ si y solo si $x \leq y \to z$ para todo $x, y, z \in A$. Sean $x, y, z \in A$ tales que $x \leq y$. Luego $y \leq z \to (y \cdot z)$ porque $y \cdot z \leq y \cdot z$. Luego se sigue que $x \leq z \to (y \cdot z)$. De esto se deduce que $x \cdot z \leq y \cdot z$. Luego vale la condición **(a)**. Para probar la otra condición, notemos primero que $x \cdot (x \to y) \leq y$ porque $x \to y \leq x \to y$. Luego $x \to y \in E_{x,y}$. Veamos ahora que $x \to y$ es el máximo de este conjunto. Sea $z \in E_{x,y}$, es decir, $z \cdot x \leq y$. Luego $z \leq x \to y$. Por ende, $x \to y = \text{máx}\, E_{x,y}$, que es la condición **(b)**.

Recíprocamente, supongamos que se cumple que $\cdot$ es monótona y que para cada $x, y \in A$ existe el máximo de $E_{x,y}$. Definamos $\to$ como $x \to y = \text{máx}\, E_{x,y}$. Sean $x, y, z \in A$ tales que $x \cdot y \leq z$. Luego $x \in E_{y,z}$. Como $y \to z$ es el máximo de $E_{y,z}$ tenemos que $x \leq y \to z$. Finalmente asumamos que $x \leq y \to z$. Luego $x \cdot y \leq y \cdot (y \to z)$. Como $y \to z \in E_{y,z}$ tenemos que $y \cdot (y \to z) \leq z$. Por lo tanto $x \cdot y \leq z$. □

Notemos que en el caso de retículos se cumple que si $x \leq y$ entonces $x \wedge z \leq y \wedge z$. Luego, dado un retículo tenemos que la condición $x \wedge y \leq z$ si y solo si $x \leq y \to z$ para todo x, y, z es equivalente a que para todo x, y exista el máximo del conjunto $\{z : z \wedge x \leq y\}$, siendo $x \to y = \text{máx}\{z \in A : x \leq y \to z\}$. En particular, recuperamos la caracterización que dimos en el Capítulo 3 para las álgebras de Heyting.

Corolario 12.1.3. *Sea* $\langle A, \wedge, \vee, \cdot, \to, e\rangle$ *un álgebra de tipo* $(2, 2, 2, 2, 0)$. *Luego* $\langle A, \wedge, \vee, \cdot, \to, e\rangle$ *es un c.r.l. si y solo si* $\langle A, \wedge, \vee\rangle$ *es un retículo,* $\langle A, \cdot, e\rangle$ *es un monoide conmutativo,* $\cdot$ *es monótona y para cada* $x, y \in A$ *existe el máximo de* $E_{x,y}$*, siendo* $x \to y = \text{máx}\, E_{x,y}$.

La condición $x \cdot y \leq z$ si y solo si $x \leq y \to z$ para todo $x, y, z \in A$ también puede ser reemplazada por ecuaciones, como veremos a continuación.

Teorema 12.1.4. *Sea* $\langle A, \wedge, \vee, \cdot, \to, e\rangle$ *un álgebra de tipo* $(2, 2, 2, 2, 0)$ *tal que* $\langle A, \cdot, e\rangle$ *es un monoide conmutativo y* $\langle A, \wedge, \vee\rangle$ *es un retículo.*

Luego la condición $x \cdot y \leq z$ *si y solo si* $x \leq y \to z$ *para cada* $x, y, z \in A$ *equivale a que se cumplan las siguientes condiciones para cada* $x, y, z \in A$*:*

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

(b) $x \to (y \wedge z) = (x \to y) \wedge (x \to z)$,

(c) $x \cdot (x \to y) \leq y$,

(d) $y \leq x \to (x \cdot y)$.

Demostración. Supongamos primero que $x \cdot y \leq z$ si y solo si $x \leq y \to z$ para cada $x, y, z \in A$. Es inmediato que se satisfacen los ítems **(c)** y **(d)**. Para probar **(a)**, sean $x, y, z \in A$. Debemos ver que $x \cdot (y \vee z)$ es el supremo de $\{x \cdot y, x \cdot z\}$. Usando que $\cdot$ es monótona, que $y \leq y \vee z$ y que $z \leq y \vee z$ obtenemos que $x \cdot y \leq x \cdot (y \vee z)$ y $x \cdot z \leq x \cdot (y \vee z)$. Luego $x \cdot (y \vee z)$ es cota superior de $\{x \cdot y, x \cdot z\}$. Para probar que es la menor cota superior de dicho conjunto, sea $w \in A$ tal que $x \cdot y \leq w$ y $x \cdot z \leq w$. Luego $y \leq x \to w$ y $z \leq x \to w$. Por esto, $y \vee z \leq x \to w$, es decir, $x \cdot (y \vee z) \leq w$. Luego $x \cdot (y \vee z) = (x \cdot y) \vee (x \cdot z)$ y por ende vale la condición **(a)**. La condición **(b)** se prueba análogamente.

Recíprocamente, supongamos que se cumplen los ítems **(a)**, **(b)**, **(c)** y **(d)**. Notemos que **(a)** implica que $\cdot$ es monótona, y **(b)** implica la siguiente propiedad, a la cual llamaremos (PI): si $x \leq y$ entonces $z \to x \leq z \to y$. Veamos que si $x \cdot y \leq z$ entonces $x \leq y \to z$. Sea $x \cdot y \leq z$. Luego por **(d)** y por (PI) deducimos que $x \leq y \to (x \cdot y) \leq y \to z$, por lo cual $x \leq y \to z$. Supongamos ahora que $x \leq y \to z$. Luego por **(c)** tenemos que $x \cdot y \leq y \cdot (y \to z) \leq z$. Por lo tanto, $x \cdot y \leq z$. □

Corolario 12.1.5. *La clase de retículos residuados conmutativos es una variedad.*

Observación 12.1.6. La variedad de álgebras de Heyting puede pensarse como una subvariedad de la variedad de c.r.l.s (abreviación para referirnos a los retículos residuados conmutativos) si consideramos a un álgebra de Heyting como un álgebra: $\langle A, \wedge, \vee, \wedge, \to, 1 \rangle$. Podemos proceder análogamente para los casos de MV-álgebras (o W-álgebras) y l-grupos. Resumiendo: la variedad de álgebras de Boole, la variedad de álgebras de Heyting, la variedad de MV-álgebras (o W-álgebras) y la variedad de l-grupos pueden pensarse como subvariedades de la variedad de los c.r.l.s. Estas no son las únicas subvariedades de la variedad de c.r.l.s., aunque no abordaremos ese problema en este libro. El lector interesado puede consultar, por ejemplo, el libro [43].

A continuación enunciaremos un lema cuya demostración se deja como ejercicio para el lector.

Lema 12.1.7. *En cada c.r.l. valen las siguientes propiedades:*

1. $e \to x = x$.

2. *Si* $x \leq y$ *entonces* $x \cdot z \leq y \cdot z$, $z \to x \leq z \to y$, $y \to z \leq x \to z$.

3. $(x \cdot y) \to z = x \to (y \to z) = y \to (x \to z)$.

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

5. $(x \to y) \cdot (y \to z) \leq x \to z$.

6. *Si el c.r.l. considerado es integral entonces* $x \cdot y \leq x$ *y* $x \cdot y \leq x \wedge y$.

Residuos como adjunciones

A continuación daremos la explicación que prometimos en el Capítulo 8, 8.1.8. La misma puede ampliarse consultando [50] o [73].

Consideremos dos categorías $\mathcal{C}$ y $\mathcal{D}$, y dos funtores $F : \mathcal{C} \longrightarrow \mathcal{D}$ y $G : \mathcal{D} \longrightarrow \mathcal{C}$. Sean X un objeto de $\mathcal{C}$ e Y un objeto de $\mathcal{D}$. Luego $F(X)$ es un objeto en $\mathcal{D}$ y $G(Y)$ es un objeto en $\mathcal{C}$.

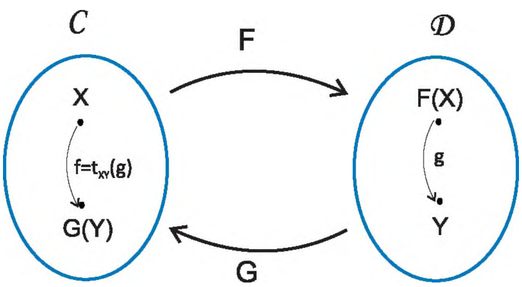


Figura 12.1: Adjunción

La adjunción se da entre F y G cuando a cada morfismo $g : F(X) \longrightarrow Y$ le corresponde un y solo un morfismo $f : X \longrightarrow G(Y)$ y recíprocamente, es decir, si para cada X y para cada Y hay una biyección t_{XY} entre el conjunto $\mathcal{D}(F(X), Y)$ de morfismos en $\mathcal{D}$ de $F(X)$ en Y y el conjunto $\mathcal{C}(X, G(Y))$ de morfismos en $\mathcal{C}$ de X en $G(Y)$:

$$t_{XY} : \mathcal{D}(F(X), Y) \longrightarrow \mathcal{C}(X, G(Y)). \qquad (1)$$

Se pide además que la biyección t_{XY} sea "natural en X y en Y", es decir, que, para cada X fijo (respectivamente para cada Y fijo), t_{XY} sea una transformación natural. Se dice entonces que F es *adjunto a izquierda de* G (notación:

$F \dashv G$) y que G es *adjunto a derecha de* F (notación: $G \vdash F$). Se indica también esta situación esquemáticamente como:

$$\frac{F(X) \longrightarrow Y}{X \longrightarrow G(Y)}.$$

Podemos explicitar la condición de que, para cada Y fijo, sea t_{XY} "natural en X" de la siguiente manera. Dado un morfismo $h : X' \longrightarrow X$, se tiene el siguiente diagrama conmutativo:

$$\begin{tikzcd} F(X') \arrow[d, "F(h)"'] \arrow[dr, "g \circ F(h)"] & \\ F(X) \arrow[r, "g"'] & Y \end{tikzcd}$$

La condición de naturalidad mencionada se traduce entonces diciendo que el siguiente diagrama también debe ser conmutativo:

$$\begin{tikzcd} X' \arrow[d, "h"'] \arrow[dr, "t_{X'Y}(g \circ F(h))"] & \\ X \arrow[r, "t_{XY}(g)"'] & G(Y) \end{tikzcd}$$

O sea, debe ser:

$$t_{X'Y}(g \circ F(h)) = t_{XY}(g) \circ h.$$

Se tiene una condición análoga para la naturalidad en Y con un X fijo.

Interesa en particular la situación en (1) cuando $Y = F(X)$ y el morfismo considerado es la identidad en $F(X)$. A esta le corresponde un morfismo $\eta_X : X \longrightarrow G(F(X))$ (llamado la *unidad* de la adjunción en X) que cumple la siguiente propiedad universal: Dado $g : X \longrightarrow G(Y)$ existe un único $f : F(X) \longrightarrow Y$ tal que $G(f) \circ \eta_X = g$. Esto dice que η es una transformación natural de $\mathbf{1}_{\mathcal{C}}$ en $G \circ F$.

En forma dual, si tomamos $X = G(Y)$ obtendremos la *counidad* ε que tiene la propiedad universal: para toda $f : F(X) \longrightarrow Y$ hay exactamente un morfismo $g : X \longrightarrow G(Y)$ tal que $\varepsilon_Y \circ F(g) = f$.

Las transformaciones naturales η y ε relacionan los funtores $\mathbf{1}_{\mathcal{C}}$ con $G \circ F$ y $F \circ G$ con $\mathbf{1}_{\mathcal{D}}$ respectivamente. Si cada η_X y cada ε_Y es un isomorfismo, entonces la adjunción es lo que hemos visto en el Capítulo 6 como *equivalencia categorial*.

Ejemplos 12.1.8.

1. El funtor “de olvido” (el que se olvida de la estructura), por ejemplo de la categoría de grupos en la categoría de conjuntos, es adjunto del funtor “de libertad”, que asocia a cada conjunto la estructura libre generada por él.

2. Es particularmente importante el ejemplo de funtores adjuntos entre categorías constituidas por conjuntos ordenados.

   Un conjunto ordenado $(P, \leq)$ puede ser considerado una categoría, tomando como objetos los elementos de P. Diremos que existe un morfismo entre los elementos p_1 y p_2 de P si $p_1 \leq p_2$. Dado otro conjunto ordenado $(Q, \leq)$, un funtor de P en Q se define como una función que preserva el orden. Entonces, una función $g : Q \longrightarrow P$ es adjunta a derecha de una $f : P \longrightarrow Q$ si se cumple que

   $$\frac{p \longrightarrow g(q)}{f(p) \longrightarrow q},$$

   es decir si para todo $p \in P$, $q \in Q$:

   $$p \leq g(q) \text{ si y solo si } f(p) \leq q.$$

3. Como caso particular del anterior tenemos la adjunción entre una operación binaria $*$ y su residuo, según se detalla a continuación.

   En general, se dice que una operación binaria conmutativa $* : A \times A \to A$ definida sobre un conjunto ordenado $(A, \leq)$ se dice que es *residuada*, si existe una operación binaria $\to: A \times A \to A$ para la cual

   $$a * b \leq c \text{ si y solo si } b \leq a \to c.$$

   En tal caso diremos que $(A, \leq)$ es un *conjunto ordenado residuado* bajo la multiplicación $*$, y la operación $\to$ será su residuo . Además, para cada $x, y \in A$, tenemos que se verifica que $x \to y = \max\{z \in A : z * x \leq y\}$.

   Las funciones que intervienen en la adjunción (que se da para cada elemento a) son $f_a(b) = a * b$, $\quad g_a(c) = a \to c$. Es decir que:

   $$\frac{b \longrightarrow g_a(c)}{f_a(b) \longrightarrow c},$$

   o también

   $$\frac{b \leq g_a(c)}{f_a(b) \leq c}.$$

12.2. Congruencias

Ya hemos visto, a lo largo de este libro, que para ciertas variedades concretas es muy importante tener una descripción de las congruencias de sus miembros ya que esto es útil para obtener información importante sobre dicha variedad. Muchos de los resultados que vimos que involucran a las congruencias pueden ser dados para variedades arbitrarias. Surge naturalmente la siguiente pregunta:

¿Qué podemos decir acerca de las congruencias de un c.r.l. dado?

Antes de responder a esa pregunta, recordemos lo que sucede con las álgebras que venimos estudiando. En el caso de las álgebras de Heyting, las congruencias están en correspondencia con los filtros, lo mismo que sucede para el caso de las álgebras de Boole.

Sea $\langle A, \wedge, \vee, \cdot, \rightarrow, e\rangle$ un c.r.l. En este contexto (y en lo que sigue) diremos que un subconjunto no vacío F de A es un *filtro* si F es creciente y para cada $x, y \in F$ tenemos que $x \cdot y \in F$. Notemos que esta definición extiende la noción de filtro que dimos para el caso de álgebras de Heyting.

En el caso de una MV-álgebra, vimos que las congruencias están en correspondencia con los ideales (según la definición de ideales que dimos para las MV-álgebras). A su vez, los ideales están en correspondencia con los filtros. Es decir, las congruencias de una MV-álgebra están en correspondencia con los filtros. La biyección entre ideales y filtros está dada por $I \mapsto \neg I$, donde $\neg I$ lo definimos como $\{\neg x : x \in I\}$ (probarlo).

En el caso de ℓ-grupos ya se encuentran algunas diferencias: en este caso las congruencias van a estar en correspondencia con los ℓ-subgrupos convexos o ℓ-ideales, como fue probado en el Teorema 11.1.18 del Capítulo 11.

Veremos que en el caso de un c.r.l. arbitrario las congruencias están en correspondencia con las subálgebras convexas.

Definición 12.2.1. Un subconjunto H de un c.r.l. A es una *subalgebra* de A si H es cerrado con respecto a las operaciones definidas en A (ver Capítulo 1, Sección 3). Diremos que un subconjunto H de A es *convexo* si se verifica que para $x, y, z \in A$ tales que $x, z \in H$ y $x \leq y \leq z$ vale que $y \in H$. Diremos que H es una *subálgebra convexa* de A si H es una subálgebra y H es convexo. Escribiremos $\mathrm{Sub_C(A)}$ para el conjunto de subálgebras convexas de A. Escribiremos $\mathrm{Con}(A)$ para el conjunto de congruencias de A.

En esta sección veremos que hay una biyección entre $\mathrm{Con}(A)$ y $\mathrm{Sub_C(A)}$. Para llegar a nuestro objetivo debemos probar antes algunos lemas técnicos que involucran congruencias y subálgebras convexas.

Lema 12.2.2. *Sea A un retículo y θ una congruencia. Para cada $x \in A$ el conjunto x/θ es convexo. Más aún, si A es un c.r.l. entonces el conjunto e/θ es una subálgebra convexa.*

Demostración. Sean A un retículo e $y, z \in x/\theta$. Supongamos que $y \leq w \leq z$, para $w \in A$. Como $(y, z) \in \theta$ tenemos que $(y \vee w, z \vee w) \in \theta$. Pero $w = y \vee w$ y $z = w \vee z$. Luego $(w, z) \in \theta$. Por simetría y transitividad de θ se tiene que $w \in x/\theta$. Supongamos ahora que A es un c.r.l. Por lo que acabamos de demostrar sabemos que e/θ es un conjunto convexo. Es inmediato probar que e/θ es subálgebra de A. $\square$

Sean $x, y \in A$. Definimos

$$s(x, y) = (x \to y) \wedge (y \to x) \wedge e.$$

Lema 12.2.3. *Sean A un c.r.l. y $\theta \in \mathrm{Con}(A)$. Luego*

$$(s(x, y), e) \in \theta \text{ si y solo si } ((x \to y) \wedge e, e) \in \theta \text{ y } ((y \to x) \wedge e, e) \in \theta.$$

Demostración. Supongamos que $(s(x, y), e) \in \theta$. Luego

$$(s(x, y) \vee ((x \to y) \wedge e) \in \theta,$$
$$((x \to y) \wedge e) \vee e) \in \theta.$$

Pero $s(x, y) \vee ((x \to y) \wedge e) = (x \to y) \wedge e$ y $((x \to y) \wedge e) \vee e = e$, por lo cual $((x \to y) \wedge e, e) \in \theta$. Por la misma razón se tiene que $((y \to x) \wedge e, e) \in \theta$. La recíproca es inmediata. $\square$

Sabemos que en cada c.r.l. vale que $x \leq y$ si y solo si $e \leq x \to y$. Esta propiedad implica que

$$x = y \quad \text{si y solo si} \quad s(x, y) = e.$$

Este hecho se puede generalizar, cambiando la congruencia dada por la relación $=$ por una congruencia arbitraria. Esto es justamente lo que haremos a continuación.

Lema 12.2.4. *Sean A un c.r.l. y $\theta \in \mathrm{Con}(A)$. Luego $(x, y) \in \theta$ si y solo si $(s(x, y), e) \in \theta$.*

Demostración. Supongamos que $(x, y) \in \theta$. Luego $(x \to x, x \to y) \in \theta$ y $(y \to x, y \to y) \in \theta$. De esto se deduce que $(s(x, y), (x \to x) \wedge (y \to y) \wedge e) \in \theta$. Pero $e \leq x \to x$ y $e \leq y \to y$. Luego $(s(x, y), e) \in \theta$.

Recíprocamente, supongamos que $(s(x, y), e) \in \theta$. Luego $(x \cdot s(x, y), x) \in \theta$, $(y \cdot s(x, y), y) \in \theta$. Sean $a = x \cdot s(x, y)$ y $b = y \cdot s(x, y)$. Es inmediato que $a \leq y$ y $b \leq x$, es decir, $a = a \wedge y$ y $b = b \wedge x$. Pero $(a, x) \in \theta$ y $(b, y) \in \theta$, por lo cual $(a \wedge y, x \wedge y) \in \theta$ y $(b \wedge x, y \wedge x) \in \theta$, es decir, $(a, x \wedge y) \in \theta$ y $(b, x \wedge y) \in \theta$. Por lo tanto $(a, b) \in \theta$, y por ende $(x, y) \in \theta$. $\square$

Sea A un c.r.l. y $H \in \mathrm{Sub_C(A)}$. Definimos

$$\theta_H = \{(x,y) \in A \times A : x \cdot z \leq y \text{ y } y \cdot z \leq x \text{ para cierto } z \in H\}.$$

Para cada $x \in A$ y $n \in \mathbb{N}$ definimos $x^0 = e$ y $x^{n+1} = x \cdot x^n$.

Lema 12.2.5. *Sean A un c.r.l. y $H \in \mathrm{Sub_C(A)}$. Luego $\theta_H \in \mathrm{Con}(A)$.*

Demostración. Es sencillo probar que θ_H es una relación de equivalencia. Veamos que θ es una congruencia. Sean $(x,y) \in \theta_H$ y $(z,w) \in \theta_H$. Luego existen $a, b \in H$ tales que $x \cdot a \leq y$, $y \cdot a \leq x$, $z \cdot b \leq w$ y $w \cdot b \leq z$. Sea $c = a \wedge b$. Este elemento pertenece a H y verifica que $x \cdot c \leq y$, $y \cdot c \leq x$, $z \cdot c \leq w$ y $w \cdot c \leq z$. Notemos también que $c^2 \in H$. Luego $(x \cdot z) \cdot c^2 \leq y \cdot w$, $(y \cdot w) \cdot c^2 \leq x \cdot z$, $(x \vee z) \cdot c \leq y \vee w$ e $(y \vee w) \cdot c \leq x \vee z$. Por esta razón se tiene que $(x \cdot z, y \cdot w) \in \theta_H$ y $(x \vee z, y \vee w) \in \theta_H$. Para probar que $(x \wedge z, y \wedge w) \in \theta_H$, notemos que $x \leq c \to y$ y $z \leq c \to w$. Luego

$$x \wedge z \leq (c \to y) \wedge (c \to w) = c \to (y \wedge w).$$

De igual modo obtenemos que $y \wedge w \leq c \to (x \wedge z)$. Es decir, $(x \wedge z) \cdot c \leq y \wedge w$, $(y \wedge w) \cdot c \leq x \wedge z$. De este modo tenemos que $(x \wedge z, y \wedge w) \in \theta_H$. Solo resta probar que $(x \to z, y \to w) \in \theta_H$. Como $y \cdot c \leq x$ tenemos que $(y \cdot c) \cdot (x \to z) \leq z$. Luego $(y \cdot c^2) \cdot (x \to z) \leq w$, es decir, $c^2 \cdot (x \to z) \leq y \to w$. De igual modo tenemos que $c^2 \cdot (y \to w) \leq x \to z$. Por lo tanto concluimos que $(x \to z, y \to w) \in \theta_H$. □

El siguiente lema nos da formas alternativas de describir al conjunto θ_H.

Lema 12.2.6. *Sean A un c.r.l. y $H \in \mathrm{Sub_C(A)}$. Luego $(x,y) \in \theta_H$ si y solo si $(x \to y) \wedge e \in H$ e $(y \to x) \wedge e \in H$ si y solo si $s(x,y) \in H$.*

Demostración. Sea $(x,y) \in \theta_H$. Luego existe $z \in H$ tal que $x \cdot z \leq y$, $y \cdot z \leq x$. Es decir, tenemos que $z \leq x \to y$, $z \leq y \to x$. Luego $z \wedge e \leq (x \to y) \wedge e \leq e$, $z \wedge e \leq (y \to x) \wedge e \leq e$. Como $z \wedge e \in H$ y $e \in H$, tenemos que $(x \to y) \wedge e \in H$ e $(y \to x) \wedge e \in H$, por convexidad de H. Recíprocamente, supongamos que $(x \to y) \wedge e \in H$ e $(y \to x) \wedge e \in H$. Sea $a = (x \to y) \wedge e$ y $b = (y \to x) \wedge e$. En particular tenemos que $a \in H$ y $b \in H$. El elemento $c = a \wedge b$ también pertenece a H. Es inmediato probar que $x \cdot c \leq y$ y que $y \cdot c \leq x$. Por lo tanto $(x,y) \in \theta_H$.

Supongamos ahora que $(x \to y) \wedge e \in H$ e $(y \to x) \wedge e \in H$. Luego $s(x,y) \in H$ porque H es cerrado por ínfimos. Recíprocamente, sea $s(x,y) \in H$. Como $s(x,y) \leq (x \to y) \wedge e \leq e$ y $s(x,y) \leq (y \to x) \wedge e \leq e$, por convexidad de H concluimos que $(x \to y) \wedge e \in H$ e $(y \to x) \wedge e \in H$. □

Lema 12.2.7. *Sean A un c.r.l., $H \in \mathrm{Sub_C(A)}$ y $\theta \in \mathrm{Con}(A)$. Luego $H = e/\theta_H$ y $\theta = \theta_{e/\theta}$.*

Demostración. Primero notemos que por los lemas 12.2.2 y 12.2.5 tenemos que e/θ es una subálgebra convexa y que θ_H es una congruencia. La igualdad $\theta = \theta_{e/\theta}$ es consecuencia del Lema 12.2.4. Veamos que $H = e/\theta_H$. Para ello consideremos primero $x \in e/\theta_H$, es decir, $(x, e) \in \theta_H$. Luego existe $z \in H$ tal que $x \cdot z \leq e$ y $e \cdot z \leq x$. Es decir, $z \leq x \leq z \to e$. Como $z, z \to e \in H$ y H es un conjunto convexo, resulta que $x \in H$. Recíprocamente, sea $x \in H$. Definamos $z = x \wedge (x \to e)$, que es un elemento de H. Luego $x \cdot z \leq e$ y $z \cdot e \leq x$, por lo cual $x \in e/\theta_H$. Por lo tanto hemos probado que $H = e/\theta_H$. $\square$

Los lemas anteriores de esta sección nos conducen al siguiente resultado.

Teorema 12.2.8. *Sea A un c.r.l. La función $F : \mathrm{Con}(A) \to \mathrm{Sub_C(A)}$ dada por $F(\theta) = e/\theta$ es biyectiva.*

Hemos establecido una biyección entre las congruencias y las subálgebras convexas de un c.r.l. dado. El conjunto de congruencias es un conjunto ordenado si tomamos como orden la inclusión, lo mismo ocurre con las subálgebras convexas. En realidad se puede probar que la biyección de la que hablamos es un isomorfismo de orden, es decir, que F y su función inversa preservan el orden. Más aún, se puede probar que estos posets forman retículos distributivos con propiedades interesantes desde la perspectiva del Álgebra Universal. Para más detalles sobre esto ver [58].

12.3. Producto no conmutativo

Podríamos tratar de extender las ideas que trabajamos en el capítulo a partir de la siguiente pregunta:

¿Podemos generalizar la definición de c.r.l. sin pedir que la operación producto sea necesariamente conmutativa?

Como es de esperar la respuesta es sí, solo que en ese caso vamos a tener dos implicaciones. Las álgebras que se obtienen se denominan *retículos residuados.*

Definición 12.3.1. Un álgebra $\langle A, \wedge, \vee, \cdot, \backslash, /, e\rangle$ de tipo $(2, 2, 2, 2, 2, 0)$ es un *retículo residuado*, r.l. para abreviar, si satiface las siguientes condiciones:

1. $\langle A, \wedge, \vee\rangle$ es un retículo.

2. $\langle A, \cdot, e\rangle$ es un monoide.

3. $\backslash$ y $/$ son operaciones binarias para las cuales las equivalencias

$$x \cdot y \leq z \text{ si y solo si } x \leq z/y \text{ si y solo si } y \leq x\backslash z$$

valen para cada $x, y, z \in A$.

Las operaciones $\backslash$ y $/$ son llamadas el *residuo a derecha* y a *izquierda* de $\cdot$, respectivamente. Se sigue de la definición que $\cdot$ es *residuado* (es decir, residuado a derecha y a izquierda) si y solo si preserva el orden en cada argumento, y para cada $x, y, z \in A$, la desigualdad $x \cdot y \leq z$ tiene un elemento máximo para x (llamado z/y) y para y (llamado $x\backslash z$). Se deja como ejercicio probar esta afirmación, es la generalización al caso no necesariamente conmutativo de la Propiedad 12.1.2.

Observación 12.3.2. La clase de retículos residuados es una variedad, como ocurría en el caso de retículos residuados conmutativos.

Surge naturalmente la siguiente pregunta:

¿Qué podemos decir sobre las congruencias de un r.l. dado?

Antes de contestar a la pregunta daremos una definición. Se dice que C es una *subálgebra convexa normal* de A si C es una subálgebra convexa de A tal que para cada $a \in A$ y $b \in C$ vale que $\rho_a(b)$ y $\lambda_a(b)$ pertenecen a C, donde ρ_a y λ_a son funciones unarias definidas como $\rho_a(b) = ((a \cdot b)/a) \wedge e$ y $\lambda_a(b) = (a\backslash(b \cdot a)) \wedge e$.

Si A es un r.l., las congruencias de A están en biyección con las subálgebras convexas normales de A.

Los resultados anteriormente mencionados en esta sección (junto con sus pruebas) pueden hallarse en [11], [65] y [43].

12.4. Lógicas subestructurales

Aunque los retículos residuados ya vienen siendo estudiados desde 1930, es bastante reciente su estudio como estructuras algebraicas asociadas a las llamadas *lógicas subestructurales*. Daremos una visión sobre este tema, basándonos principalmente en las notas del curso *Algebraic aspects of substructural logics*, dictado en Campinas por Roberto Cignoli en el marco de la Escuela de Lógica dependiente de la XIV SLALM que se celebró en mayo de 2008 en Paraty, Brasil [27]. Otro texto consultado es el de Ono [84].

Sistema LK de secuentes para el Cálculo Proposicional Clásico

En 1934, Gentzen (ver [49, 84]) adoptó el *cálculo de secuentes* para tratar los cálculos clásico e intuicionista. Les llamó sistemas **LK** y **LJ**. Para introducir las lógicas subestructurales comenzaremos por dar en esta forma el CPC y el CPI, que nosotros hemos visto en los capítulos 3 y 5 respectivamente en forma axiomática, que suele llamarse "al estilo de Hilbert".

El lenguaje se define como lo hemos venido haciendo habitualmente a partir de numerables variables proposicionales y conectivos $\vee, \wedge, \rightarrow, \neg$.

Un *secuente* es una expresión de la forma $\alpha_1, \ldots, \alpha_n \vdash \beta$, donde $\alpha_1, \ldots,$ α_n y β son fórmulas. Los secuentes de la forma $\alpha \vdash \alpha$ se llaman *iniciales*. Aquí aparecen en la regla "Axioma".

Usaremos la siguiente notación: letras griegas minúsculas $\alpha, \beta \ldots$, para las fórmulas proposicionales y letras griegas mayúsculas $\Delta, \Lambda, \Gamma, \Sigma, \Theta, \Pi \ldots$ para las listas de fórmulas proposicionales (que pueden ser vacías).

Se definen las siguientes reglas.

Reglas estructurales:

Atenuación:

$$\text{(ai)} \quad \frac{\Gamma, \Sigma \vdash \Delta}{\Gamma, \alpha, \Sigma \vdash \Delta} \qquad \text{(ad)} \quad \frac{\Gamma \vdash \Lambda, \Theta}{\Gamma \vdash \Lambda, \alpha, \Theta}$$

Contracción:

$$\text{(ci)} \quad \frac{\Gamma, \alpha, \alpha, \Sigma \vdash \Delta}{\Gamma, \alpha, \Sigma \vdash \Delta} \qquad \text{(cd)} \quad \frac{\Gamma \vdash \Lambda, \alpha, \alpha, \Theta}{\Gamma \vdash \Lambda, \alpha, \Theta}$$

Intercambio:

$$\text{(ii)} \quad \frac{\Gamma, \alpha, \beta, \Sigma \vdash \Delta}{\Gamma, \beta, \alpha, \Sigma \vdash \Delta} \qquad \text{(id)} \quad \frac{\Gamma \vdash \Lambda, \alpha, \beta, \Theta}{\Gamma \vdash \Lambda, \beta, \alpha, \Theta}$$

Regla de corte:

$$\frac{\Gamma \vdash \alpha, \Theta \qquad \Sigma, \alpha, \Pi \vdash \Delta}{\Sigma, \Gamma, \Pi \vdash \Delta, \Theta}$$

Axioma:

$$\frac{}{\alpha \vdash \alpha}$$

Reglas para los conectivos proposicionales

Implicación:

$$(\to \text{ i}) \quad \frac{\Gamma \vdash \alpha, \Theta \qquad \Pi, \beta, \Sigma \vdash \Delta}{\Pi, \alpha \to \beta, \Gamma, \Sigma \vdash \Delta, \Theta} \qquad (\to \text{ d}) \quad \frac{\Gamma, \alpha \vdash \beta, \Theta}{\Gamma \vdash \alpha \to \beta, \Theta}$$

Conjunción:

$$(\wedge \text{ i1}) \quad \frac{\Gamma, \alpha, \Sigma \vdash \Delta}{\Gamma, \alpha \wedge \beta, \Sigma \vdash \Delta} \qquad (\wedge \text{ i2}) \quad \frac{\Gamma, \beta, \Sigma \vdash \Delta}{\Gamma, \alpha \wedge \beta, \Sigma \vdash \Delta}$$

$$(\wedge \text{ d}) \quad \frac{\Gamma \vdash \Lambda, \alpha, \Theta \qquad \Gamma \vdash \Lambda, \beta, \Theta}{\Gamma \vdash \Lambda, \alpha \wedge \beta, \Theta}$$

Disyunción:

$$(\vee \text{ i}) \quad \frac{\Gamma, \alpha, \Sigma \vdash \Delta \qquad \Gamma, \beta, \Sigma \vdash \Delta}{\Gamma, \alpha \vee \beta, \Sigma \vdash \Delta}$$

$$(\vee \text{ d1}) \quad \frac{\Gamma \vdash \Lambda, \alpha, \Theta}{\Gamma \vdash \Lambda, \alpha \vee \beta, \Theta} \qquad (\vee \text{ d2}) \quad \frac{\Gamma \vdash \Lambda, \beta, \Theta}{\Gamma \vdash \Lambda, \alpha \vee \beta, \Theta}$$

Negación:

$$(\neg \text{ i}) \quad \frac{\Gamma \vdash \alpha, \Theta}{\neg\alpha, \Gamma \vdash \Theta} \qquad (\neg \text{ d}) \quad \frac{\Gamma, \alpha \vdash \Theta}{\Gamma \vdash \neg\alpha, \Theta}.$$

Una prueba o derivación del secuente $\Gamma \vdash \beta$ consiste en una sucesión finita de aplicaciones de reglas a las fórmulas de Γ, mediante las cuales podemos al final obtener β.

Ejemplo 12.4.1. Veamos la prueba del principio del tercero excluido.

$$\begin{aligned} &\alpha \vdash \alpha \text{ (Ax)} \\ &\ \vdash \neg\alpha, \alpha \ (\neg \text{ d}) \\ &\ \vdash \neg\alpha \vee \alpha, \alpha \ (\vee \text{ d1}) \\ &\ \vdash \neg\alpha \vee \alpha,\ \neg\alpha \vee \alpha \ (\vee \text{ d2}) \\ &\ \vdash \neg\alpha \vee \alpha \text{ (cd)} \end{aligned}$$

Sistema LJ de secuentes para el Cálculo Proposicional Intuicionista

Las mismas reglas definen el CPI, pero con la restricción de que a la derecha de $\vdash$ puede haber **a lo sumo una fórmula**.

El sistema quedaría entonces de la siguiente forma:

Atenuación:

$$\frac{\Gamma, \Sigma \vdash \varphi}{\Gamma, \alpha, \Sigma \vdash \varphi}, \qquad \frac{\Gamma \vdash}{\Gamma \vdash \alpha},$$

Contracción:

$$\frac{\Gamma, \alpha, \alpha, \Sigma \vdash \varphi}{\Gamma, \alpha, \Sigma \vdash \varphi},$$

Intercambio:

$$\frac{\Gamma, \alpha, \beta, \Sigma \vdash \varphi}{\Gamma, \beta, \alpha, \Sigma \vdash \varphi}$$

Regla de corte:

$$\frac{\Gamma \vdash \varphi \qquad \Sigma, \varphi, \Pi \vdash \psi}{\Sigma, \Gamma, \Pi \vdash \psi}$$

Axioma:

$$\frac{}{\alpha \vdash \alpha}$$

Implicación:

$$\frac{\Gamma \vdash \alpha \qquad \Pi, \beta, \Sigma \vdash \gamma}{\Pi, \alpha \to \beta, \Gamma, \Sigma \vdash \gamma} \qquad \frac{\Gamma, \alpha \vdash \beta}{\Gamma \vdash \alpha \to \beta}$$

Conjunción:

$$\frac{\Gamma, \alpha, \Sigma \vdash \varphi}{\Gamma, \alpha \wedge \beta, \Sigma \vdash \varphi} \qquad \frac{\Gamma, \alpha, \Sigma \vdash \varphi}{\Gamma, \beta \wedge \alpha, \Sigma \vdash \varphi}$$

$$\frac{\Gamma \vdash \varphi \qquad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}$$

Disyunción:

$$\frac{\Gamma, \alpha, \Sigma \vdash \varphi \qquad \Gamma, \beta, \Sigma \vdash \varphi}{\Gamma, \alpha \vee \beta, \Sigma \vdash \varphi}$$

$$\frac{\Gamma \vdash \alpha}{\Gamma \vdash \alpha \vee \beta} \qquad \frac{\Gamma \vdash \alpha}{\Gamma \vdash \beta \vee \alpha}$$

Negación:

$$\frac{\Gamma \vdash \alpha}{\neg\alpha, \Gamma \vdash} \qquad \frac{\Gamma, \alpha \vdash}{\Gamma \vdash \neg\alpha}.$$

Observemos que la prueba del Ejemplo 12.4.1 no puede darse aquí, ya que no se tiene ni (c d) ni (¬ d).

Las reglas de atenuación y de contracción permiten probar la equivalencia de los secuentes

$$\alpha, \beta \vdash \gamma$$

y

$$\alpha \wedge \beta \vdash \gamma$$

en **LJ** y **LK**.

En forma análoga, y utilizando otra vez atenuación y contracción, se prueba la equivalencia de

$$\alpha \vdash \beta, \gamma$$

y

$$\alpha \vdash \beta \vee \gamma,$$

pero solo en **LK**.

Se puede probar entonces el siguiente teorema.

Teorema 12.4.2. *En el CPC el secuente $\alpha_1, \ldots, \alpha_p \vdash \beta_1, \ldots, \beta_q$ es demostrable si y solo si lo es $\alpha_1 \wedge \cdots \wedge \alpha_p \vdash \beta_1 \vee \cdots \vee \beta_q$. Esto también resulta cierto para el CPI si nos restringimos a $q = 1$.*

Como consecuencia de este resultado, las comas a la izquierda de un secuente deben interpretarse como conjunciones (y en el caso clásico, las de la derecha como disyunciones).

Reglas estructurales

La regla de intercambio a izquierda nos permite usar las hipótesis en cualquier orden.

La regla de atenuación a izquierda (ai) nos permite agregar hipótesis redundantes. Sin esta regla, para deducir un secuente $\Gamma \vdash \Sigma$ cada hipótesis (esto es, cada fórmula listada en Γ), debe ser utilizada **al menos una vez** en la demostración.

La regla de contracción a izquierda (ci) nos permite utilizar cada hipótesis más de una vez. Si falta esta regla, para deducir un secuente cada hipótesis debe ser usada **a lo sumo una vez** en la demostración.

En ausencia de ambas reglas ((ai) y (ci)), en la deducción de $\Gamma \vdash \Sigma$ cada fórmula de Γ deberá ser utilizada **una y solo una vez** en la demostración.

Esta propiedad expresa que la lógica es "sensible a los recursos" ("resourse sensitive").

Las reglas estructurales son, entonces, las que nos permiten usar las hipótesis cualquier número de veces (tal vez ninguna) y en cualquier orden.

Una lógica se dice *subestructural*, en general, cuando no satisface alguna de las reglas estructurales. Por ejemplo, en las *lógicas relevantes* no se permiten las reglas de atenuación. Luego, cada hipótesis debe ser usada al menos una vez, esto es, no se permite asumir hipótesis que sean "irrelevantes" para demostrar algo. En la lógica B-C-K y en la lógica Ł de Łukasiewicz faltan las reglas de contracción.

En nuestro contexto, es decir, estudiar una lógica cuya contraparte algebraica sea la variedad de los retículos residuados conmutativos e integrales, supondremos que no valen las reglas de contracción pero sí valen las de atenuación y de intercambio (esta última es la que corresponde a la conmutatividad de la estructura algebraica asociada).

En esta suposición, tenemos ciertas reglas que en **LK** o en **LJ** son equivalentes a las de $\wedge$ pero que aquí ya no lo son. Ellas definen un conectivo binario diferente, que suele llamarse *fusión* y que denotaremos con $*$. Las reglas que corresponden a $*$ son las siguientes:

$$(*\ \mathrm{i}) \qquad \frac{\Gamma, \alpha, \beta, \Sigma \vdash \Delta}{\Gamma, \alpha * \beta, \Sigma \vdash \Delta}$$

$$(*\ \mathrm{d}) \qquad \frac{\Gamma \vdash \Lambda, \alpha, \Theta \qquad \Sigma \vdash \Lambda, \beta, \Theta}{\Gamma, \Sigma \vdash, \Lambda, \alpha * \beta, \Theta}$$

Se prueba entonces el siguiente teorema.

Teorema 12.4.3. *En un sistema de secuentes que tenga fusión y la regla de corte un secuente $\alpha_1, \ldots, \alpha_n \vdash \beta$ es demostrable si y solo si el secuente $\alpha_1 * \cdots * \alpha_n \vdash \beta$ es demostrable.*

Denotaremos por FL_{ew} (cálculo completo de Lambek con intercambio y atenuación) al sistema de secuentes obtenido de **LJ** suprimiendo las reglas de contracción y agregando las reglas para $*$.

Las siguientes fórmulas son demostrables en FL_{ew}:

(B) $(\alpha \to \beta) \to ((\beta \to \gamma) \to (\alpha \to \gamma))$,

(C) $(\alpha \to (\beta \to \gamma)) \to (\beta \to (\alpha \to \gamma))$,

(K) $\alpha \to (\beta \to \alpha)$,

(Res1) $(\alpha \to (\beta \to \gamma)) \to ((\alpha * \beta) \to \gamma)$,

(Res2) $((\alpha * \beta) \to \gamma) \to (\alpha \to (\beta \to \gamma))$,

(M) $((\alpha \to \gamma) \wedge (\beta \to \gamma)) \to ((\alpha \wedge \beta) \to \gamma)$,

(J) $(\alpha \to \gamma) \to ((\beta \to \gamma) \to ((\alpha \vee \beta) \to \gamma))$.

Al sistema FL_{ew} se le asocia el sistema axiomático HFL_{ew}. Se prueba que toda fórmula deducible del sistema axiomático HFL_{ew} es deducible del sistema de secuentes FL_{ew}.

Sistema axiomático $\mathbf{HFL}_{ew}$

Lenguaje

Está dado por las variables $\mathrm{p}_1, \ldots, \mathrm{p}_n, \ldots$ y los conectivos $\neg$, $\wedge$, $\vee$, $*$, $\to$ y constante $\overline{0}$ sujetos a las reglas de construcción habituales.

Axiomas

(B) $(\mathrm{A} \to \mathrm{B}) \to ((\mathrm{B} \to \mathrm{C}) \to (\mathrm{A} \to \mathrm{C}))$.

(C)$(\mathrm{A} \to (\mathrm{B} \to \mathrm{C})) \to (\mathrm{B} \to (\mathrm{A} \to \mathrm{C}))$.

(K) $\mathrm{A} \to (\mathrm{B} \to \mathrm{A})$.

(Res1) $(\mathrm{A} \to (\mathrm{B} \to \mathrm{C})) \to ((\mathrm{A} * \mathrm{B}) \to \mathrm{C})$.

(M) $((\mathrm{A} \to \mathrm{C}) \wedge (\mathrm{B} \to \mathrm{C})) \to ((\mathrm{A} \wedge \mathrm{B}) \to \mathrm{C})$.

(J) $(\mathrm{A} \to \mathrm{C}) \to ((\mathrm{B} \to \mathrm{C}) \to ((\mathrm{A} \vee \mathrm{B}) \to \mathrm{C}))$.

(N1) $\mathrm{A} \to (\mathrm{B} \to (\mathrm{A} * \mathrm{B}))$.

(N2) $\overline{0} \to \mathrm{A}$.

($\mathrm{L}_4$3) $(\mathrm{A} \wedge \mathrm{B}) \to \mathrm{A}$.

($\mathrm{L}_4$4) $(\mathrm{A} \wedge \mathrm{B}) \to \mathrm{B}$.

($\mathrm{L}_4$5) $\mathrm{A} \to (\mathrm{B} \to (\mathrm{A} \wedge \mathrm{B}))$.

($\mathrm{L}_4$6) $\mathrm{A} \to (\mathrm{A} \vee \mathrm{B})$.

($\mathrm{L}_4$7) $\mathrm{B} \to (\mathrm{A} \vee \mathrm{B})$.

donde ($\mathrm{L}_4$3),..., ($\mathrm{L}_4$7) son los dados en el Capítulo 3 (que también son los axiomas (LI3),...,(LI7) de **LI** en el Capítulo 5).

Reglas

Modus Ponens.

Valuaciones

Dado este sistema, consideramos valuaciones en retículos residuados acotados.

Un *retículo residuado acotado* es un álgebra $\langle A, \wedge, \vee, \cdot, \rightarrow, \bot, \top\rangle$ tal que $\langle A, \wedge, \vee, \cdot, \rightarrow, \top\rangle$ es un retículo residuado conmutativo integral y $\bot$ es el mínimo elemento de A.

Sea *Form* el conjunto de fórmulas de HFL_{ew}.

Sea A un retículo residuado acotado. Una valuación v en A es una función $v : Form \longrightarrow A$ tal que:

$$v(\mathrm{A} \rightarrow \mathrm{B}) = v(\mathrm{A}) \rightarrow v(\mathrm{B}),$$

$$v(\mathrm{A} * \mathrm{B}) = v(\mathrm{A}) \cdot v(\mathrm{B}),$$

$$v(\mathrm{A} \vee \mathrm{B}) = v(\mathrm{A}) \vee v(\mathrm{B}),$$

$$v(\mathrm{A} \wedge \mathrm{B}) = v(\mathrm{A}) \wedge v(\mathrm{B}),$$

$$v(\neg \mathrm{A}) = \neg v(\mathrm{A}) = v(\mathrm{A}) \rightarrow \bot.$$

Diremos, como es habitual, que una fórmula A es válida o verdadera en A si $v(\mathrm{A}) = \top$ para toda valuación en A. Diremos que A es válida (o verdadera) si para todo retículo residuado acotado A la fórmula es verdadera para toda valuación en A.

Completud

No es difícil probar por inducción el siguiente teorema, que es "la mitad" de la completud que buscamos.

Teorema 12.4.4. *Toda fórmula demostrable en* HFL_{ew} *es verdadera.*

Definiendo la relación $\mathrm{A} \equiv \mathrm{B}$ si y solo si $\vdash \mathrm{A} \rightarrow \mathrm{B}$ y $\vdash \mathrm{B} \rightarrow \mathrm{A}$ se pueden demostrar los siguientes resultados:

Teorema 12.4.5. *Form*$/\equiv$ *munido de las operaciones definidas naturalmente en el cociente es un retículo residuado acotado, llamado el álgebra de Lindenbaum de* HFL_{ew}.

Teorema 12.4.6. *Una fórmula* A *es demostrable en* HFL_{ew} *si y solo si se verifica* $|\mathrm{A}| = 1$, *siendo* $|\mathrm{A}|$ *la clase de equivalencia de* A *en Form*$/\equiv$.

Teorema 12.4.7 (Completud). *Una fórmula es demostrable en HFL_{ew} si y solo si es verdadera.*

Idea de la demostración. El Teorema 12.4.4 prueba una parte. Para probar la recíproca basta ver que la aplicación canónica es una valuación. Luego, dada una fórmula verdadera A debe ser $|\mathrm{A}| = 1$, pero eso implica, por el Teorema 12.4.6, que A es demostrable. □

12.5. Lógica básica y BL-álgebras

Vamos a exponer aquí algunos aspectos de la *lógica básica* definida por Hájek (ver [52, Capítulo 2]) y de su estructura algebraica asociada, las *BL-álgebras*. Las BL-álgebras son una subvariedad de los retículos residuados y las MV-álgebras son a su vez una subvariedad de las BL-álgebras.

El conjunto de los valores de verdad o "grados de verdad" de la lógica básica es el intervalo $[0, 1]$ al que se le asocia una estructura de BL-álgebra. Se estudian las llamadas *t-normas* (t de "true"), que son funciones de verdad de dos variables en el intervalo $[0, 1]$. Ellas son funciones semánticas correspondientes a una cierta "conjunción" de la lógica, denotada $\overline{\wedge}$, que generaliza la conjunción clásica. A diferencia de las modalidades, que hemos visto en el Capítulo 3, las t-normas conservan una propiedad de los conectivos clásicos: son "funcionales-de-verdad", en el sentido de que el valor de verdad de una proposición compuesta depende solo del valor de verdad de sus componentes.

Para definir la t-norma o función de verdad de esta conjunción generalizada, reflexionamos sobre cómo debería comportarse. En consonancia con lo que sucede con la tabla de verdad de la conjunción clásica, parece natural suponer que para grados de verdad "grandes" de las componentes, el valor de verdad de la conjunción debe ser también "grande". Luego, pedimos que la t-norma sea monótona en ambas variables, además de conservar los valores clásicos en los pares (x, y), con $x, y \in \{0, 1\}$.

Definición 12.5.1. Una *t-norma* es una función $t : [0, 1] \times [0, 1] \longrightarrow [0, 1]$ denotada por $t(x, y) = x * y$ que cumple las siguientes condiciones:

(Co-As) $*$ es conmutativa y asociativa:

$$x * y = y * x,$$
$$x * (y * z) = (x * y) * z.$$

(Mon) $*$ es monótona en ambos argumentos:

$$x_1 \leq x_2 \text{ implica } x_1 * y \leq x_2 * y$$
$$y_1 \leq y_2 \text{ implica } x * y_1 \leq x * y_2.$$

(0-1) $1 * x = x$ y $0 * x = 0$.

Una *t-norma continua* es aquella que es continua respecto de la topología usual de $[0, 1]$.

Ejemplos 12.5.2. Los que siguen son los ejemplos más importantes de t-normas. Es fácil verificar que valen las condiciones (Co-As), (Mon) y (0-1). La definición de $x*y$ de Łukasiewicz coincide con la de $x \odot y$ en la MV-álgebra de universo $[0, 1]$.

1. t-norma de Łukasiewicz, definida por: $x * y = \text{máx}(0, x + y - 1)$,
2. t-norma de Gödel, definida por: $x * y = \text{mín}(x, y)$,
3. t-norma producto, definida por: $x * y = x \cdot y$ (producto de reales).

Se trata ahora de definir una función de verdad para la implicación. En el CPC, el valor de verdad de A $\rightarrow$ B es grande (es 1) cuando el valor de verdad de A, $v(\mathrm{A})$, no es mayor que el de B. En general, un valor de verdad "grande" de A $\rightarrow$ B debería ocurrir cuando $v(\mathrm{A})$ no sea mucho más grande que $v(\mathrm{B})$. Esto nos lleva a pedir que la función de verdad de A $\rightarrow$ B, que denotaremos $x \Rightarrow y$, para $x = v(\mathrm{A})$, $y = v(\mathrm{B})$, sea decreciente en x y creciente en y. Otras consideraciones hacen que se tome $x \Rightarrow y$ como el supremo del conjunto $\{z : x * z \leq y\}$. Se tiene entonces el siguiente resultado:

Lema 12.5.3. *Sea $*$ una t-norma continua. Entonces existe una única operación $\Rightarrow$ que verifique la condición*

$$x * z \leq y \quad \textit{si y solo si} \quad z \leq x \Rightarrow y.$$

Demostración. Para cada $x, y \in [0, 1]$, sea

$$x \Rightarrow y = \sup\{z : x * z \leq y\},$$

siendo $\sup\{z : x * z \leq y\}$ el supremo del conjunto $\{z : x * z \leq y\}$. Sea, para un z fijo, $f(x) = x * z$. Luego, f es continua y creciente, por lo que conmuta con supremos. Luego:

$$x * (x \Rightarrow y) = x * \sup\{z : x * z \leq y\} = \sup\{x * z : x * z \leq y\} \leq y.$$

Luego, $x \Rightarrow y = \text{máx}\{z : x * z \leq y\}$. La unicidad es obvia. $\square$

La operación $x \Rightarrow y$ es entonces el residuo de la t-norma $*$.

Teorema 12.5.4. *Los siguientes son los residuos de las tres t-normas del Ejemplo 12.5.2. En los tres casos: $x \Rightarrow y = 1$ si $x \leq y$. Si $x > y$:*

1. *Implicación de Łukasiewicz:* $x \Rightarrow y = 1 - x + y$,

2. *Implicación de Gödel:* $x \Rightarrow y = y$,

3. *Implicación de Goguen:* $x \Rightarrow y = y/x$.

En lo que sigue consideraremos el álgebra

$$L(*) = \langle [0,1], *, \cap, \cup, \Rightarrow, 0, 1 \rangle,$$

donde $\cap$ =mínimo, $\cup$ =máximo, $*$ es una t-norma y $\Rightarrow$ es su residuo. El orden en $L(*)$ es el usual en $[0,1]$.

Puede demostrarse, usando propiedades de las funciones continuas en $[0,1]$, que las operaciones $\cap$ y $\cup$ pueden ser definidas en función de $*$ y $\Rightarrow$:

$$x \cap y = x * (x \Rightarrow y),$$

$$x \cup y = ((x \Rightarrow y) \Rightarrow y) \cap ((y \Rightarrow x) \Rightarrow x).$$

Se observa que la implicación de Łukasiewicz es continua, pero las de Gödel y de Goguen no lo son. Sin embargo, puede probarse que el residuo de una t-norma continua es continuo a izquierda en la primer variable y continuo a derecha en la segunda.

El residuo define el *precomplemento*, que es la futura función de verdad de la negación, por:

$$-x = x \Rightarrow 0.$$

Lógica básica LB

Lenguaje

Está dado por las variables $\mathrm{p}_1, \ldots, \mathrm{p}_n, \ldots$ y los conectivos $\overline{\wedge}$, $\rightarrow$ y constante $\overline{0}$ sujetos a las reglas de construcción habituales. Además:

$$\begin{array}{rcl}
\mathrm{A} \wedge \mathrm{B} & \text{es} & \mathrm{A} \mathbin{\overline{\wedge}} (\mathrm{A} \rightarrow \mathrm{B}) \\
\mathrm{A} \vee \mathrm{B} & \text{es} & ((\mathrm{A} \rightarrow \mathrm{B}) \rightarrow \mathrm{B}) \wedge ((\mathrm{B} \rightarrow \mathrm{A}) \rightarrow \mathrm{A}) \\
\neg \mathrm{A} & \text{es} & \mathrm{A} \rightarrow \overline{0} \\
\mathrm{A} \equiv \mathrm{B} & \text{es} & (\mathrm{A} \rightarrow \mathrm{B}) \mathbin{\overline{\wedge}} (\mathrm{B} \rightarrow \mathrm{A}).
\end{array}$$

Axiomas

(A1) $(\mathrm{A} \to \mathrm{B}) \to ((\mathrm{B} \to \mathrm{C}) \to (\mathrm{A} \to \mathrm{C}))$.

(A2) $(\mathrm{A} \,\overline{\wedge}\, \mathrm{B}) \to \mathrm{A}$.

(A3) $(\mathrm{A} \,\overline{\wedge}\, \mathrm{B}) \to (\mathrm{B} \,\overline{\wedge}\, \mathrm{A})$.

(A4) $(\mathrm{A} \,\overline{\wedge}\, (\mathrm{A} \to \mathrm{B})) \to (\mathrm{B} \,\overline{\wedge}\, (\mathrm{B} \to \mathrm{A}))$.

(A5a) $(\mathrm{A} \to (\mathrm{B} \to \mathrm{C})) \to ((\mathrm{A} \,\overline{\wedge}\, \mathrm{B}) \to \mathrm{C})$.

(A5b) $((\mathrm{A} \,\overline{\wedge}\, \mathrm{B}) \to \mathrm{C}) \to (\mathrm{A} \to (\mathrm{B} \to \mathrm{C}))$.

(A6) $((\mathrm{A} \to \mathrm{B}) \to \mathrm{C})) \to (((\mathrm{B} \to \mathrm{A}) \to \mathrm{C})) \to \mathrm{C})$.

(A7) $\overline{0} \to \mathrm{A}$.

Reglas

Modus Ponens.

Observación 12.5.5. Veamos qué significan los axiomas.

El axioma (A1) expresa la transitividad de la implicación, y es el mismo que el axioma $Ł_2$ del sistema Ł de Łukasiewicz; (A2) dice que de la nueva conjunción $\overline{\wedge}$ se deduce su primera componente y (A3) dice que $\overline{\wedge}$ es conmutativa; (A4) expresa que $\wedge$ es conmutativa; (A5) expresa la residuación; (A6) dice que si una fórmula C se deduce de $\mathrm{A} \to \mathrm{B}$ y también se deduce de $\mathrm{B} \to \mathrm{A}$, entonces C es un teorema. Finalmente (A7) dice que $\overline{0}$ implica cualquier fórmula.

Valuaciones

Consideraremos valuaciones a valores en el álgebra $L(*)$, para $*$ una t-norma continua.

Sea $Form_{LB}$ el conjunto de fórmulas de la lógica básica.

Una valuación v es una función $v : Form_{LB} \longrightarrow [0,1]$ tal que:

$$v(\overline{0}) = 0,$$

$$v(\mathrm{A} \to \mathrm{B}) = v(\mathrm{A}) \Rightarrow v(\mathrm{B}),$$

$$v(\mathrm{A} \,\overline{\wedge}\, \mathrm{B}) = v(\mathrm{A}) * v(\mathrm{B}).$$

Se prueba que para toda valuación se cumple:

$$v(\mathrm{A} \wedge \mathrm{B}) = \mathrm{mín}(v(\mathrm{A}), v(\mathrm{B})),$$

$$v(\mathrm{A} \vee \mathrm{B}) = \mathrm{máx}(v(\mathrm{A}), v(\mathrm{B})).$$

Diremos que una fórmula A es una *1-tautología* si $v(\mathrm{A}) = 1$ para toda valuación.

Se demuestra que todos los axiomas son 1-tautologías y que, si A y A $\rightarrow$ B son 1-tautologías entonces B es 1-tautología. Luego, se tiene el siguiente teorema de corrección.

Teorema 12.5.6. *Todo teorema de* **LB** *es una 1-tautología en* $L(*)$*, para toda t-norma continua* $*$.

Lema 12.5.7. *Los siguientes son teoremas en* **LB***:*

$$\text{(B)} \quad (\mathrm{A} \rightarrow \mathrm{B}) \rightarrow ((\mathrm{C} \rightarrow \mathrm{A}) \rightarrow (\mathrm{C} \rightarrow \mathrm{B})),$$

$$\text{(C)} \quad (\mathrm{A} \rightarrow (\mathrm{B} \rightarrow \mathrm{C})) \rightarrow (\mathrm{B} \rightarrow (\mathrm{A} \rightarrow \mathrm{C})),$$

$$\text{(K)} \quad \mathrm{A} \rightarrow (\mathrm{B} \rightarrow \mathrm{A}),$$

$$\text{(I)} \quad \mathrm{A} \rightarrow \mathrm{A}$$

$$(\neg\neg_1) \quad \mathrm{A} \rightarrow \neg\neg\mathrm{A}.$$

Demostración. En primer lugar, podemos ver que la regla del Silogismo Hipotético vale en **LB** porque podemos probarlo de la misma manera que lo hicimos para la lógica Ł. Luego, la aplicaremos libremente.

La fórmula (C) se prueba de la siguiente manera. Aplicamos (A1) tomando como A y B respectivamente las fórmulas $\mathrm{A} \mathbin{\overline{\wedge}} \mathrm{B}$ y $\mathrm{B} \mathbin{\overline{\wedge}} \mathrm{A}$. Luego obtenemos $\vdash ((\mathrm{A} \mathbin{\overline{\wedge}} \mathrm{B}) \rightarrow \mathrm{C}) \rightarrow ((\mathrm{B} \mathbin{\overline{\wedge}} \mathrm{A}) \rightarrow \mathrm{C})$. Aplicando luego sucesivamente (A5a) y (A5b) obtenemos $\vdash (\mathrm{A} \rightarrow (\mathrm{B} \rightarrow \mathrm{C})) \rightarrow (\mathrm{B} \rightarrow (\mathrm{A} \rightarrow \mathrm{C}))$.

De (A1) y (C) se obtiene $\vdash (\mathrm{A} \rightarrow \mathrm{B}) \rightarrow ((\mathrm{C} \rightarrow \mathrm{A}) \rightarrow (\mathrm{C} \rightarrow \mathrm{B}))$.

De (A2) y (A5b) obtenemos $\vdash \mathrm{A} \rightarrow (\mathrm{B} \rightarrow \mathrm{A})$.

De (K) y (C) se obtiene: $\vdash \mathrm{B} \rightarrow (\mathrm{A} \rightarrow \mathrm{A})$, de donde, sustituyendo B por un teorema cualquiera, obtenemos $\vdash \mathrm{A} \rightarrow \mathrm{A}$.

Por último, la fórmula $(\neg\neg_1)$ se obtiene aplicando (I) a $\mathrm{A} \rightarrow \overline{0}$ y luego aplicando (C). □

Observación 12.5.8. Vemos entonces que la lógica **LB** es una *extensión* de la lógica B-C-K, en el sentido de que todo teorema de B-C-K es teorema de **LB**.

BL-álgebras

Mostraremos aquí que las BL-álgebras proveen una adecuada semántica para la lógica **LB**. En efecto, se verifican varias propiedades fundamentales: el álgebra $L(*)$ tiene estructura de BL-álgebra, el álgebra de Lindenbaum-Tarski de **LB** es una BL-álgebra y puede demostrarse un teorema de completud de **LB**: una fórmula es un teorema de **LB** si y solo si es una tautología con respecto a cada álgebra de la forma $L(*)$, para $*$ t-norma continua.

Definición 12.5.9. Una BL-álgebra es un sistema $\langle L, \wedge, \vee, *, \to, 0, 1\rangle$ tal que

- $\langle L, \wedge, \vee, *, \to, 0, 1\rangle$ es un c.r.l. acotado integral.
- valen las siguientes identidades:

$$x \wedge y = x * (x \to y),$$

$$(x \to y) \vee (y \to x) = 1.$$

Como vemos, las BL-álgebras pueden ser definidas por ecuaciones, por lo que constituyen una variedad.

Por ser c.r.l., en una BL-álgebra $\to$ es el residuo de $*$. El orden es el definido por: $x \leq y$ si y solo si $x \to y = 1$.

La demostración del siguiente lema puede verse en [26, Lemma 1.1].

Lema 12.5.10. *Las siguientes propiedades valen en toda BL-álgebra:*

(a) $\neg\neg 0 = 0$,

(b) $\neg\neg(x * y) = \neg\neg x * \neg\neg y$,

(c) $\neg\neg(x \to y) = \neg\neg x \to \neg\neg y$.

Valuaciones en BL-álgebras

Dada una BL-álgebra L, una L-valuación v es una función $v : Form_{LB} \longrightarrow L$ tal que:

$v(\overline{0}) = 0$,

$v(\mathrm{A} \to \mathrm{B}) = v(\mathrm{A}) \to v(\mathrm{B})$,

$v(\mathrm{A} \mathbin{\overline{\wedge}} \mathrm{B}) = v(\mathrm{A}) * v(\mathrm{B})$.

Diremos que una fórmula A de **LB** es una L-tautología, si $v(\mathrm{A}) = 1$, para toda L-valuación v.

Puede probarse entonces el teorema de corrección siguiente:

Teorema 12.5.11 ([52, Th. 2.3.9]). *Todo teorema de* **LB** *es una L-tautología, para toda BL-álgebra L.*

Trabajando técnicamente con la teoría de las BL-álgebras Hájek obtiene el teorema de completud siguiente:

Teorema 12.5.12 ([52, Th. 2.3.19]). *Dada una fórmula* A *de* **LB**, *son equivalentes las siguientes aserciones:*

(i) $\vdash \mathrm{A}$,

(ii) A *es una L-tautología, para toda BL-álgebra totalmente ordenada L,*

(iii) A *es una L-tautología, para toda BL-álgebra L.*

Posteriormente, en [53] y [25] se probó el siguiente teorema, que permite restringir a las BL-álgebras de la forma $L(*)$ la verificación de las fórmulas que son tautologías.

Teorema 12.5.13. *Dada una fórmula* A *de* **LB**,

$\vdash \mathrm{A}$ *si y solo si* A *es una $L(*)$-tautología, para toda t-norma continua $*$.*

Relación entre LB y Ł

Daremos ahora una breve exposición sobre la relación entre los dos sistemas lógicos y también entre las variedades de álgebras asociadas a ellos. Nos basaremos en [25] y en [52].

El resultado principal es que la lógica Ł puede ser obtenida como extensión de la lógica **LB** si agregamos el axioma siguiente:

$(\neg\neg_2)$ $\quad \neg\neg\mathrm{A} \to \mathrm{A}$.

Es fácil ver que si se extiende el sistema **LI** del cálculo intuicionista con este mismo axioma se obtiene el sistema $\mathbf{L}_4$ del cálculo clásico. Además, como vimos, el teorema de Glivenko permite "traducir" una fórmula A aplicándole la doble negación, de manera que $\vdash \mathrm{A}$ en **LI** implica $\vdash \neg\neg\mathrm{A}$ en $\mathbf{L}_4$ y recíprocamente. Veremos que resultados análogos se obtienen para las lógicas **LB** y Ł.

Desde el punto de vista algebraico, se tienen varias propiedades interesantes. Por ejemplo, que una MV-álgebra es una estructura definicionalmente equivalente a la de una BL-álgebra en la cual se cumple además:

$$(x \to 0) \to 0 = x.$$

Teorema 12.5.14. *Sea $\langle A; \oplus, \neg, 0\rangle$ una MV-álgebra. Definimos:*

$$\begin{aligned} x \to y &= \neg x \oplus y, \\ x * y &= \neg(\neg x \oplus \neg y), \\ 1 &= \neg 0, \\ x \vee y &= (x \to y) \to y, \\ x \wedge y &= \neg(\neg x \vee \neg y). \end{aligned}$$

Entonces, $\langle A, \wedge, \vee, *, \to, 0, 1\rangle$ es una BL-álgebra que verifica la ecuación

$$x = \neg\neg x.$$

Demostración. Debemos probar entonces que $\langle A, \wedge, \vee, *, \to, 0, 1\rangle$ es un retículo residuado acotado (ver 12.4) y que se cumplen

$$x \wedge y = x * (x \to y),$$

$$(x \to y) \vee (y \to x) = 1.$$

Por la Observación 8.1.8 del Capítulo 8, se sabe que $\to$ es el residuo de $*$. Por las propiedades de conmutatividad, asociatividad y existencia de neutro de la operación $\oplus$ en MV-álgebras, se deduce por dualidad que $\langle A, *, 1\rangle$ es un monoide conmutativo. También hemos visto en el Capítulo 8 que $\langle A, \wedge, \vee, 0, 1\rangle$ es un retículo acotado.

De la Observación 8.1.12 del Capítulo 8 obtenemos que: $x \wedge y = x * (\neg x \oplus y)$, o sea: $x \wedge y = x * (x \to y)$.

Aplicando $\neg$ al resultado dado en el Lema 8.1.14 del Capítulo 8, como es fácil ver, obtenemos la igualdad dual: $(x \to y) \vee (y \to x) = 1$, con lo cual hemos probado que $\langle A, \wedge, \vee, *, \to, 0, 1\rangle$ es una BL-álgebra, que obviamente cumple $\neg\neg x = x$. □

Teorema 12.5.15. *Sea $\langle A, \wedge, \vee, *, \to, 0, 1\rangle$ una BL-álgebra que verifica la ecuación*

$$x = \neg\neg x,$$

siendo $\neg x = x \to 0$. Definimos:

$$x \oplus y = \neg x \to y.$$

Entonces, $\langle A; \oplus, \neg, 0\rangle$ es una MV-álgebra.

Demostración. Veamos la conmutatividad de $\oplus$. En 12.5.7 se demostró

$$\vdash (\mathrm{A} \to (\mathrm{B} \to \mathrm{C})) \to (\mathrm{B} \to (\mathrm{A} \to \mathrm{C})).$$

Luego, vale en toda BL-álgebra $(u \to (v \to w)) \to (v \to (u \to w)) = 1$, o sea, $u \to (v \to w) \leq v \to (u \to w)$ y $v \to (u \to w) \leq v \to (u \to w)$. En particular, si tomamos $u = \neg x$, $v = \neg y$ y $z = 0$, se tiene

$$\neg x \to (\neg y \to 0) = \neg y \to (\neg x \to 0),$$

de donde, por ser $x = \neg\neg x$, $y = \neg\neg y$, se tiene $\neg x \to y = \neg y \to x$, o sea:

$$x \oplus y = y \oplus x.$$

Para probar la asociatividad, usamos también la igualdad $\neg x \to y = \neg y \to x$. Se tiene:

$$x \oplus (y \oplus z) = \neg x \to (\neg y \to z) = \neg x \to (\neg z \to y).$$

Por otra parte,

$$(x \oplus y) \oplus z) = \neg(\neg x \to y) \to z = \neg z \to \neg\neg(\neg x \to y) = \neg z \to (\neg x \to y),$$

esto último por la propiedad de la doble negación. Luego, conmutando $\neg x$ y $\neg z$ se tiene

$$x \oplus (y \oplus z) = (x \oplus y) \oplus z.$$

La propiedad $x \oplus 0 = x$ sale por doble negación, mientras que $x \oplus \neg 0 = \neg 0$ se deduce del hecho de que $0 \leq x$.

Debemos probar ahora: $\neg(\neg x \oplus y) \oplus y = \neg(\neg y \oplus x) \oplus x$, o sea:

$$(x \to y) \to y = (y \to x) \to x.$$

Por 3 de 12.1.7, se tiene, en particular:

$$(u * v) \to 0 = u \to (v \to 0) = v \to (u \to 0),$$

o sea

$$\neg(u * v) = u \to \neg v = v \to \neg u.$$

Luego, usando doble negación, tenemos:

$$\neg((x \to y) \to y) = (x \to y) * \neg y.$$

Además, es fácil ver que $x \to y = \neg y \to \neg x$. Luego:

$$\begin{aligned} \neg((x \to y) \to y) &= (x \to y) * \neg y \\ &= (\neg y \to \neg x) * \neg y \\ &= \neg y \wedge \neg x, \end{aligned}$$

esto último por la ecuación $u * (u \to v) = u \wedge v$.

Luego, $\neg((x \to y) \to y) = \neg y \wedge \neg x = \neg((y \to x) \to x)$, de donde:

$$(x \to y) \to y = (y \to x) \to x. \qquad \square$$

Se tiene también el siguiente “Glivenko algebraico”, donde los elementos regulares son (como en el caso intuicionista) aquellos x para los cuales $x = \neg\neg x$.

Teorema 12.5.16 (ver [26, Th. 1.2]). *Sea A una BL-álgebra, sea $MV(A)$ el conjunto de sus elementos regulares. Entonces, $MV(A)$ es el universo de una subálgebra de A que tiene estructura de MV-álgebra y la aplicación $r : x \mapsto \neg\neg x$ de A en $MV(A)$ es un homomorfismo suryectivo, que restringido a $MV(A)$ da la identidad.*

Demostración. El resultado se deduce de las propiedades vistas en el Lema 12.5.10 y de la igualdad: $\neg\neg\neg\neg x = \neg\neg x$. $\square$

Recordemos que, dada una fórmula A de la lógica **LB**, ella (considerada como término) determina una función-término A^B para cada BL-álgebra B y que A es B-tautología o B-válida si B satisface la ecuación $\mathrm{A} = 1$. Análogamente para la lógica Ł y una MV-álgebra C (ver Teorema 9.3.2 del Capítulo 9).

Con estos resultados estamos en condiciones de probar el siguiente teorema “de Glivenko” relativo a la relación entre **LB** y Ł.

Teorema 12.5.17. *Sea* A *una fórmula de* **LB**. *Entonces:*

$$\vdash \mathrm{A} \text{ en Ł si y solo si} \vdash \neg\neg\mathrm{A} \text{ en } \mathbf{LB}.$$

Demostración. Sea $\vdash$ A en la lógica Ł. Luego, para toda MV-álgebra C, A es C-tautología, es decir que $\mathrm{A}^C = 1$. En particular, para una BL-álgebra B, A es $MV(B)$-tautología, es decir que $\mathrm{A}^{MV(B)}(a_1, \ldots, a_n) = 1$. Pero entonces, por el Teorema 12.5.16 $\neg\neg\mathrm{A}^B(\neg\neg a_1, \ldots, \neg\neg a_n) = 1$. Debido a las propiedades del Lema 12.5.10, se puede probar por inducción que $\neg\neg\mathrm{A}^B(\neg\neg a_1, \ldots, \neg\neg a_n) = \neg\neg\mathrm{A}^B(a_1, \ldots, a_n)$. Por lo tanto, $\neg\neg\mathrm{A}^B(a_1, \ldots, a_n) = 1$. Como esto ocurre para toda BL-álgebra, por el Teorema de completud 12.5.12, se tiene que $\vdash \neg\neg$A en **LB**.

La recíproca se deduce fácilmente del hecho de que toda MV-álgebra es BL-álgebra y que la función término $\neg\neg\mathrm{A}^C$ coincide con A^C en toda MV-álgebra C. $\square$

Para terminar, mencionaremos otros resultados interesantes.

Consideremos la siguiente ecuación en BL-álgebras:

$$x \wedge \neg x = 0.$$

Las BL-álgebras que satisfacen esta ecuación se llaman *pseudocomplementadas* o SBL-álgebras. Dos subvariedades importantes de SBL-álgebras son las

PL-álgebras asociadas a la *lógica producto* y las *álgebras de Heyting prelineales* (ver Ejemplo 4, 6.8 en el Capítulo 6) también conocidas como *álgebras de Gödel*. Estas álgebras son las asociadas a la extensión obtenida del CPI agregando el axioma: $(\mathrm{A} \to \mathrm{B}) \vee (\mathrm{B} \to \mathrm{A})$. Esta lógica tiene los mismos teoremas que la extensión de **LB** que se obtiene agregando un axioma que expresa la idempotencia de la conjunción.

12.6. Ejercicios

1. Supongamos que tenemos un poset $(A, \leq)$ y una operación binaria $\to$. Probar que las siguientes condiciones son equivalentes:

   1) Existe una operación binaria y conmutativa $\cdot$ que cumple la condición $x \cdot y \leq z$ si y solo si $x \leq y \to z$ para todo $x, y, z \in A$.
   2) Se satisfacen las siguientes condiciones:
      (a) La operación $\to$ es monótona en la primer coordenada. Es decir, si $x, y, z \in A$ con $x \leq y$ entonces $z \to x \leq z \to y$.
      (b) Para cada $x, y \in A$ existe el mínimo del conjunto $\{z \in A : x \leq y \to z\}$, siendo $x \cdot y = \text{mín}\{z \in A : x \leq y \to z\}$ y $\cdot$ una operación conmutativa.

2. Probar el Lema 12.1.7.

3. Consideremos el intervalo real $[0, 1]$ con las operaciones de retículos usuales, el producto usual de números reales y $\to$ dada por $x \to y = (\frac{y}{x}) \wedge 1$ si $0 \neq 0$, y $x \to y = 1$ si $x = 0$. Probar que $\langle [0, 1], \wedge, \vee, \to, \cdot, e\rangle$ es un c.r.l.

   (a) ¿Es un álgebra de Heyting el álgebra $\langle A, \wedge, \vee, \to, 0, 1\rangle$?
   (b) ¿Es una W-álgebra el álgebra $\langle A, \to, 1\rangle$?
   (c) ¿Es un l-grupo el álgebra $\langle A, +, -, \vee, \wedge, 1\rangle$, donde $+$ es el producto usual de números reales y $-$ se define por $-x = x \to 0$?

4. Sean A un c.r.l. y $H \in \text{Sub}_{\text{C}}(\text{A})$. Probar que θ_H es una relación de equivalencia.

5. Sea A un c.r.l. integral. Probar que el conjunto de subálgebras convexas de A coincide con el conjunto de filtros de A. Si A es un álgebra de Heyting (pensada como un c.r.l.), ¿qué nos dice el resultado anterior con respecto a las congruencias de A? Misma pregunta si A es una MV-álgebra.

6. Probar que la biyección dada en el Teorema 12.2.8 es un isomorfismo de orden. Sugerencia: probar primero que si f es una función biyectiva entre dos posets, entonces decir que f es un isomorfismo de orden es equivalente a decir que para cada x, y, $x \leq y$ si y solo si $f(x) \leq f(y)$.

7. Sea A un c.r.l. Para cada $x, y \in A$ definimos

$$t(x, y) = ((x \to y) \wedge e) \cdot ((y \to x) \wedge e).$$

Probar que si $\theta \in \mathrm{Con}(A)$ entonces $(x, y) \in \theta$ si y solo si $(t(x, y), e) \in \theta$.

8. Si A es un c.r.l. y S es un subconjunto de A, escribiremos $C[S]$ para referirnos a la menor subálgebra convexa (con respecto a la inclusión) que contiene a S, y escribiremos $\langle S\rangle$ para referirnos al submonoide de $\langle A, \cdot, e\rangle$ generado por S. Si $S = \{x\}$ escribiremos $C[x]$ en lugar de $C[\{x\}]$ y $\langle x\rangle$ en lugar de $\langle\{x\}\rangle$.

   (a) Probar que $C[S] = \{x \in A : y \leq x \leq y \to e$ para cierto $y \in \langle S\rangle\}$.

   (b) Probar que $y \in \langle x\rangle$ si y solo si $y = x^n$ para cierto $n \in \mathbb{N}$.

   (c) Mostrar que $C[x] = \{y \in A : y^n \leq x \leq y^n \to e$ para cierto $n \in \mathbb{N}\}$.

   (d) Mostrar que $C[x] \cap C[y] = C[x \vee y]$.

   (e) Sean $x, y \in A$ y $\theta(x, y)$ la congruencia principal generada por (x, y), es decir, la menor congruencia que contiene a (x, y). Mostrar que valen las igualdades $e/\theta(x, y) = C[s(x, y)] = C[t(x, y)]$.

   (f) Probar que $(z, w) \in \theta(x, y)$ si y solo si existe $n \in \mathbb{N}$ tal que $s(x, y)^n \leq s(z, w)$.

9. Construir un ejemplo de un r.l. no conmutativo.

10. Probar que en cada r.l. valen las ecuaciones

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

11. Probar que el residuo de la t-norma de Gödel es $x \Rightarrow y = y$.

12. Con referencia al Ejercicio 3, probar que $\langle [0, 1], \wedge, \vee, \to, \cdot, 0, 1\rangle$ es una BL-álgebra.

13. Probar que una cadena residuada es una BL-álgebra si y solo si se cumple: $x \wedge y = x * (x \to y)$. Deducir de allí que $L(*)$ es una BL-álgebra para toda t-norma continua.

14. Probar que la cadena $A = \{0, a, b, 1\}$ con las siguientes operaciones es una BL-álgebra y no es MV-álgebra:

$\cdot$	0	a	b	1
0	0	0	0	0
a	0	0	a	a
b	0	a	b	b
1	0	a	b	1

$\to$	0	a	b	1
0	1	1	1	1
a	a	1	1	1
b	0	a	1	1
1	0	a	b	1

15. Con referencia al Teorema 12.5.15, probar la asociatividad y la propiedad $x \oplus 0 = x$.

Bibliografía del Capítulo 12

- Blount K. and Tsinakis C., *The structure of residuated lattices.* Internat. J. Algebra Comput., 13 (2003), no. 4, 437–461.
- Cignoli R., Esteva F., Godo Ll. and Torrens A., *Basic logic is the logic of continuous t-norms and their residua.* Soft Computing, 4 (2000), 106–112.
- Cignoli R. and Torrens A., *Hájek basic fuzzy logic and infinite-valued Łukasiewicz logic.* Arch. Math. Logic, 42 (2003), 361–370.
- Cignoli R., D'Ottaviano I. and Mundici D., *Algebraic Foundations of Many-Valued Reasoning.* Trends in Logic—Studia Logica Library, vol. 7, Kluwer Academic Publishers, 2000.
- Cignoli R., *Algebraic aspects of substructural logics.* Logic School UNICAMP, 2008.
- Galatos N., Jipsen P., Kowalski T. and Ono M., *Residuated Lattices: An Algebraic Glimpse at Substructural Logics.* Studies in Logic and the Foundations of Mathematics, vol. 151, Elsevier, 2007.
- Gentzen G., *Untersuchungen über das logische Schliessen.* Mathematische Zeitschrift, 39 (1934), 176–210 and 405–413.
- Goldblatt R., *Topoi: The Categorial Analysis of Logic.* 2nd edition. North-Holland, 1984.
- Hájek P., *Metamathematics of Fuzzy Logic.* Kluwer, Dordrecht, 1998.
- Hájek P., *Basic fuzzy logic and BL-algebras.* Soft Computing, 2 (1998), 124–128.
- Hart J., Raftery L. and Tsinakis C., *The structure of commutative residuated lattices.* Internat. J. Algebra Comput., 12 (2002), 509–524.
- Jipsen P. and Tsinakis C., *A Survey of Residuated Lattices.* Ordered algebraic structures, 19–56, Dev. Math., 7, Kluwer Acad. Publ., Dordrecht, 2002.
- MacLane S., *Categories for the Working Mathematician.* Graduate Texts in Math., Springer-Verlag, 1971.

- Ono H., *Substructural Logics and Residuated Lattices—An Introduction.* In: Trends in Logic, 193–228, Trends Log. Stud. Log. Libr. vol. 21, Kluwer Acad. Publ., Dordrecht, 2003.

Bibliografía general

[1] Anderson M. and Feil T., *Lattice-Ordered Groups, an Introduction.* D. Reidel, 1988.

[2] Balbes R. and Dwinger, P., *Distributive Lattices.* University of Missouri Press, 1974.

[3] Bell J.L. and Slomson A.B., *Models and Ultraproducts.* North-Holland, 1969.

[4] Bigard A., Keimel K. and Wolfenstein S., *Groupes et Anneaux Réticulés.* Lecture Notes in Math., 608, Springer-Verlag, 1977.

[5] Birkhoff G., *On the structure of abstract algebras.* Proc. Cambridge Philos. Soc., 31 (1935), 433–454.

[6] Birkhoff G., *Subdirect unions in universal algebra.* Bull. Amer. Math. Soc., 50 (1944), 764–768.

[7] Blok W.J. and Pigozzi D., *Protoalgebraic logics.* Studia Logica, 45 (1986), 337–369.

[8] Blok W. J. and Pigozzi D., *Algebraizable Logics.* Memoirs Amer. Math. Soc., 77 (1989), no. 396.

[9] Blok W.J. and Pigozzi D., *Algebraic semantics for universal Horn logic without equality.* In: Universal Algebra and Quasigroup Theory (Jadwisin, 1989), 1–56, Heldermann, Berlin, 1992.

[10] Blok W.J. and Pigozzi D., *Abstract algebraic logic and the deduction theorem*, preprint, 2001. `http://orion.math.iastate.edu/dpigozzi`

[11] Blount K. and Tsinakis C., *The structure of residuated lattices.* Internat. J. Algebra Comput., 13 (2003), no. 4, 437–461.

[12] Boicescu V., Filipoiu A., Georgescu G. and Rudeanu, S., *Łukasiewicz–Moisil algebras.* Annals of Discrete Mathematics, vol. 49, North-Holland, 1991.

[13] Burris S. and Sankappanavar H.P., *A Course in Universal Algebra.* Springer-Verlag, 1980.

[14] Caicedo X., *Elementos de Lógica y Calculabilidad.* Una Empresa Docente, Bogotá, 1990.

[15] Caicedo X., *Investigaciones acerca de los conectivos intuicionistas.* Rev. Acad. Colombiana Ciencias Exactas Físicas Naturales, 19 (1995), no. 75, 705–716.

[16] Caicedo X., *Conectivos intuicionistas sobre espacios topológicos.* Rev. Acad. Colombiana Ciencias Exactas Físicas Naturales, 21 (1997), no. 81, 521–534.

[17] Caicedo X. and Cignoli R., *An algebraic approach to intuitionistic connectives.* J. Symbolic Logic, 66 (2001), no. 4, 1620–1636.

[18] Cignoli R., *Some algebraic aspects of many valued logics.* In: Proceedings of the Third Brazilian Conference on Mathematical Logic (Inst. Math., Fed. Univ. Pernambuco, Recife, 1979), 49–69, Soc. Brasil. Lógica, São Paulo, 1980.

[19] Cignoli R. and Sagastume de Gallego M., *The lattice structure of some Łukasiewicz algebras.* Algebra Universalis, 13 (1981), 315–328.

[20] Cignoli R., *Proper n-valued Łukasiewicz algebras as S-algebras of Łukasiewicz n-valued propositional calculi.* Studia Logica, 41 (1982), 3–16.

[21] Cignoli R., D'Ottaviano I. and Mundici D., *Álgebras das Lógicas de Łukasiewicz.* Coleção CLE, vol. 12. Centro de Lógica, Epistemología e História da Ciencia, Universidade Estadual de Campinas, Campinas, San Pablo, 1994.

[22] Cignoli R. and Mundici D., *An elementary proof of Chang's completeness theorem for the infinite–valued calculus of Łukasiewicz.* Studia Logica, 58 (1997), no. 1, 79–97.

[23] Cignoli R., D'Ottaviano I. and Mundici D., *Algebraic Foundations of Many-Valued Reasoning.* Trends in Logic—Studia Logica Library, vol. 7, Kluwer Academic Publishers, 2000.

[24] Cignoli R. and Torrens A., *Free cancelative hoops.* Algebra Universalis, 43 (2000), 213–216.

[25] Cignoli R., Esteva F., Godo Ll. and Torrens A., *Basic logic is the logic of continuous t-norms and their residua.* Soft Computing, 4 (2000), 106–112.

[26] Cignoli R. and Torrens A., *Hájek basic fuzzy logic and infinite-valued Łukasiewicz logic.* Arch. Math. Logic, 42 (2003), 361–370.

[27] Cignoli R., *Algebraic aspects of substructural logics.* Logic School UNICAMP, 2008.

[28] Cornish W., *Lattice-ordered groups and BCK-algebras.* Math. Japonica, 4 (1980), no. 4, 471–476.

[29] Czelakowski J., *Reduced products of logical matrices.* Studia Logica, 39 (1980), 19–43.

[30] Czelakowski J., *Equivalential logics I, II.* Studia Logica, 40 (1981), 227–236 and 335–372.

[31] Czelakowski J., *Consequence Operations. Foundational Studies.* Reports of the Research Project: Theories, Models, Cognitive Schemata, Institute of Philosophy and Sociology, Polish Academy of Sciences, Warszawa, 1992.

[32] Czelakowski J., *Protoalgebraic Logics.* Kluwer Academic Pub., 2001.

[33] Da Costa N.C.A., *On the theory of inconsistent formal systems.* Notre Dame J. Formal Logic, 15 (1974), 497–510.

[34] Daigneault A., *Freedom in polyadic algebras and two theorems of Beth and Craig.* Michigan Math. J., 11 (1964), no. 2, 129–135.

[35] Davey B.A. and Priestley H.A., *Introduction to Lattices and Order.* Cambridge University Press, 1990.

[36] Enderton H.B., *A Mathematical Introduction to Logic.* Academic Press, 1972.

[37] Epstein R.L., *Five Ways of Saying "Therefore".* Wadsworth Group, 2002.

[38] Esakia L., *Topological Kripke models.* Soviet. Math. Dokl., 15 (1974), 147–151.

[39] Fidel M., *Un cálculo modal correspondiente a las álgebras de Moisil de orden n.* Manuscrito inédito.

[40] Fitting M.C., *Intuitionistic Logic, Model Theory and Forcing.* North-Holland, 1969.

[41] Font J. and Jansana R., *A General Algebraic Semantics for Sentential Logics.* Lecture Notes in Logic, vol. 7, Springer-Verlag, 1996.

[42] Fuchs L., *Partially Ordered Algebraic Systems.* Addison-Wesley, Pergamon Press, 1963.

[43] Galatos N., Jipsen P., Kowalski T. and Ono M., *Residuated Lattices: An Algebraic Glimpse at Substructural Logics.* Studies in Logic and the Foundations of Mathematics, vol. 151, Elsevier, 2007.

[44] Galli A. and Sagastume M., *Kripke models for 3-valued Lukasiewicz algebras.* Notas de la Sociedad de Matemática de Chile, XV (1996), no. 1, 135–140.

[45] Galli A. and Sagastume M., *Symmetric-intuitionistic connectives.* In: Models, Algebras and Proofs (Bogotá, 1995), 267–277, Lecture Notes in Pure and Appl. Math., 203, Dekker, New York, 1999.

[46] Galli A. and Sagastume M., *Some operators in Kripke models with an involution.* J. Applied Non-Classical Logics, 8 (1999), no. 1-2, 107–121.

[47] Galli A., Lewin R. and Sagastume M., *The logic of equilibrium and abelian lattice ordered groups.* Arch. Math. Logic, 43 (2004), no. 2, 141–158.

[48] Gentile E.R., *Notas de Álgebra I*, Ediciones Previas, Eudeba, Buenos Aires, 1976. Versión digitalizada

[49] Gentzen G., *Untersuchungen über das logische Schliessen.* Mathematische Zeitschrift, 39 (1934), 176–210 and 405–413.

[50] Goldblatt R., *Topoi: The Categorial Analysis of Logic.* 2nd edition. North-Holland, 1984.

[51] González Asenjo F., *Introducción a la Teoría de Modelos.* Universidad de Zaragoza, Departamento de Álgebra y Fundamentos, 1978.

[52] Hájek P., *Metamathematics of Fuzzy Logic.* Kluwer, Dordrecht, 1998.

[53] Hájek P., *Basic fuzzy logic and BL-algebras.* Soft Computing, 2 (1998), 124–128.

[54] Halmos P., *Algebraic Logic.* Chelsea Pub. Co., 1962.

[55] Halpern J.D., *The independence of the axiom of choice from the Boolean prime ideal theorem.* Fund. Math., 55 (1964), 57–66.

[56] Halpern J.D. and Levy A., *The Boolean prime ideal theorem does not imply the axiom of choice.* In: Axiomatic Set Theory (Proc. Sympos. Pure Math., Vol. 18, Part I, Univ. California, Los Angeles, Calif., 1967) 83–134, Amer. Math. Soc., 1971.

[57] Hamilton A.G., *Logic for Mathematicians.* Cambridge University Press, 1978.

[58] Hart J., Raftery L. and Tsinakis C., *The structure of commutative residuated lattices.* Internat. J. Algebra Comput., 12 (2002), 509–524.

[59] Herrmann B., *Equivalential and algebraizable logics.* Studia Logica, 57 (1997), 419–436.

[60] Herrmann B., *Characterizing equivalential and algebraizable logics by the Leibniz operator.* Studia Logica, 58 (1997), 305–323.

[61] Hofstadter D., *Gödel, Escher, Bach,* Tusquets, Barcelona, 1987.

[62] Horn A., *Logic with truth values in a linearly ordered Heyting algebra.* J. Symbolic Logic, 34 (1969), 395–408.

[63] Hughes G.E. and Cresswell M.J., *Introducción a la Lógica Modal.* Tecnos, Madrid, 1973.

[64] Iturrioz L., *Łukasiewicz and symmetrical Heyting algebras.* Z. Math. Logik Grundlagen Math., 23 (1977), 131–136.

[65] Jipsen P. and Tsinakis C., *A Survey of Residuated Lattices.* Ordered algebraic structures, 19–56, Dev. Math., 7, Kluwer Acad. Publ., Dordrecht, 2002.

[66] Kaarli K. and Pixley A.F., *Polinomial Completeness in Algebraic Systems.* Chapman Hall/CRC, Boca Raton, 2001.

[67] Klimovsky G., *El teorema de Zorn y la existencia de filtros e ideales en los reticulados distributivos.* Revista de la UMA, 18 (1958), 160–164.

[68] Kneale M. y Kneale W., *El Desarrollo de la Lógica*, Tecnos, Madrid, 1980.

[69] Lewin R., Mikenberg I. and Schwarze M.G., *Algebraization of paraconsistent logic P1*, J. Non-Classical Logic 7 (1990), no. 1-2, 79–88.

[70] Lewin R., Mikenberg I. and Schwarze M.G., *C1 is not algebraizable*, Notre Dame J. Formal Logic, 32 (1991), 609–611.

[71] Lewin R.A., Mikenberg I.F. and Schwarze M.G., *P1 algebras*, Studia Logica, 53 (1994), no. 1, 21–28.

[72] Lewin R., *Lógica Algebraica Abstracta.* Apuntes de un curso dictado en Chile, Colombia y Argentina, 2008. Ver Capítulo 10 del presente texto.

[73] MacLane S., *Categories for the Working Mathematician.* Graduate Texts in Math., Springer-Verlag, 1971.

[74] Martínez G. and Priestley H., *On Priestley spaces of lattice-ordered algebraic structures.* Order, 15 (1998), 297–323.

[75] McKenzie R.N., McNulty G.F. and Taylor W.F., *Algebras, Lattices, Varieties.* Wadsworth, 1987.

[76] Mendelson E., *Introduction to Mathematical Logic.* Fourth Ed., Chapman & Hall, 1997.

[77] Miraglia F., *Cálculo Proposicional: uma Interação da Álgebra e a Lógica.* Universidade Estadual de Campinas, Centro de Lógica, Epistemologia e História de Ciência, Campinas, 1987.

[78] Monteiro A., *Álgebras de Łukasiewicz trivalentes.* Notas de Lógica Matemática, no. 21, 1–20, Universidad Nacional del Sur, 1964.

[79] Monteiro A., *Sur les algébres de Heyting symétriques.* Port. Math., 39 (1980), 1–237.

[80] Monteiro L., *Álgebras de Boole.* Informe Técnico Interno nº 66, Instituto de Matemática de Bahía Blanca, Universidad Nacional del Sur, 1998, revisado en 2000, 2001, 2002.

[81] Mortensen C., *Every quotient algebra for C1 is trivial.* Notre Dame J. Formal Logic, 21 (1980), 694–700.

[82] Mundici D., *MV-algebras are categorically equivalent to bounded commutative BCK-algebras.* Math. Japonica, 31 (1986), no. 6, 889–894.

[83] Munkres J.R., *Topología*, segunda edición. Prentice Hall, 2002.

[84] Ono H., *Substructural Logics and Residuated Lattices—An Introduction.* In: Trends in Logic, 193–228, Trends Log. Stud. Log. Libr. vol. 21, Kluwer Acad. Publ., Dordrecht, 2003.

[85] Oubiña L., *Introducción a la Teoría de Conjuntos.* Eudeba, 1965.

[86] Oubiña L., *Estructuras Algebraicas.* Editorial Exacta, La Plata, 1994.

[87] Pitts A.M., *Amalgamation and interpolation in the category of Heyting algebras.* J. Pure Appl. Algebra, 29 (1983), 155–165.

[88] Priestley H.A., *Representation of distributive lattices by means of ordered Stone spaces.* Bull. London Math. Soc. 2 (1970), 186–190.

[89] Priestley H.A., *Ordered topological spaces and the representation of distributive lattices.* Proc. London Math. Soc. 3 (1972), no. 24, 507–530.

[90] Pynko A.P., *Algebraic study of Sette's maximal paraconsistent logic*, Studia Logica, vol. 54, 89–128 (1995).

[91] Rasiowa R. and Sikorski R., *The Mathematics of Metamathematics.* Polska Akademia Nauk, Warsawa, 1963.

[92] Rasiowa R., *An Algebraic Approach to Non-Classical Logics.* North-Holland, Amsterdam, 1974.

[93] Rubin H. and Rubin J. *Equivalents of the Axiom of Choice.* Studies in Logic and the foundations of mathematics, North Holland, 1963.

[94] Sagastume de Gallego M. *Um exemplo de modelo intensional.* Cadernos de Estudos Linguísticos, 12 (1987), 25–41.

[95] Sagastume M., *Sobre la Gramática de Montague.* Manuscrito inédito.

[96] Sagastume M., *Conical logic and l-groups logic.* J. Appl. Non-Classical Logics 15 (2005), no. 3, 265–283.

[97] Sagastume M., *Bounded commutative B-C-K logic and Łukasiewicz logic.* Manuscrito Rev. Int. Filos. (Campinas), 28(2005) no. 2, 575–583.

[98] Sagastume M., *Conectivos intuicionistas.* Rev. Educación Matemática (UMA), 24 (2009), no. 3, 3–21.

[99] Sarrión Morillo E., Hernández Antón I., *Extensiones de la Lógica Clásica, Introducción a la Lógica Modal*, 2012.

[100] Sette A.M., *On the propositional calculus* P^1, Math. Japon., 18 (1973), 173–180.

[101] Shannon C., *A symbolic analysis of relay and switching circuits*, Trans. AIEE, 57 (1938), no. 12, 713–723.

[102] Stone M.H., *The theory of representations for Boolean algebras.* Trans. Amer. Math. Soc., 40 (1936), no. 1, 37–111.

[103] Tarski A., *Grundzüge des Systemenkalküls. Erster Teil.* Fundamenta Mathematicae, 25 (1935), 503–526.

[104] Tarski A., *Logic, Semantics, Metamathematics. Papers from 1923 to 1938.* Hackett, Indianapolis, IN, 1983.

[105] Thomason R., *Formal Philosophy: Selected Papers of R. Montague.* Editado por R. Thomason, New Haven and London, Yale University Press, 1974.

[106] Van Dalen D., *Intuitionistic Logic.* In: Handbook of Philosophical Logic, Synthese Library, vol. 166, 225–339, D. Reidel, 1986.

[107] Wójcicki R., *Theory of Logical Calculi.* Kluwer Academic Publishers, 1988.

Índice alfabético