Benemérita Universidad Autónoma de Puebla

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS
LICENCIATURA EN MATEMÁTICAS

"INTRODUCCIÓN A LAS RETÍCULAS MODULARES"

TESIS

QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN MATEMÁTICAS

PRESENTA: **GERMÁN CEJUDO CASTILLA**

DIRECTOR DE TESIS: **CÉSAR CEJUDO CASTILLA**

PUEBLA, PUE. SEPTIEMBRE 2016

A mis padres:

Ma. Eugenia Castilla y César A. Cejudo

A mi maestro y hermano César.

Agradecimientos

En la vida se presentan momentos difíciles y también buenos momentos, hay personas que hacen superar los primeros y hacen que lleguen los segundos. Quiero agradecer a mis padres César y María Eugenia por la paciencia y el apoyo, a mis hermanos Lehilani y Yeshua por su cariño y atención, a César que también ha sido mi maestro y por quien me adentré al mundo de las matemáticas, por quien recobré el gusto por ellas y quien me ha motivado para continuar.

Tampoco hubiera sido posible recorrer este camino sin la ayuda de mis amigos, aunque algunos ya no están aquí, agradezco a Sergio, Ana, Sonia, René, Beto y especialmente a Jorge Herrera por los grandes momentos, por las horas de estudio, por las discusiones filosóficas, por el conocimiento compartido y por supuesto también las tristes memorias.

Al Dr. David Villa, Dr. Fernando Vilchis y Mto. Ángel Contreras les agradezco sus aportes hechos para que este trabajo fuera mejor.

Agradezco también a la gente de la Facultad de Ciencias Físico Matemáticas que hace posible el desarrollo y mejoramiento de la misma, a los profesores que se preocupan por la educación y ven en ella la mejor opción para combatir a la máquina opresora.

En un bolsillo de Nerval

Hoy me ausentaré de mí, me excusaré de mi presencia,
diré adiós a mi envoltura
y seré más amigo de ese otro ser que me amortaja.
Hoy tengo una cita:
me encontraré con el reflejo que me busca,
con el cuchillo que me acecha;
dibujaré con más amor mi herida
para que allí anides y te pierdas.
Hoy salgo de mí, me digo adiós,
dejo mi rostro como prueba de partida,
me evaporo entre la bruma y resucito.
Camino hacia la huella que se borra,
me persigo por los senderos del bosque:
soy el ladrido y la fuga sin fin del jabalí;
también la flecha y el salto del venado.
Me encuentro en la mosca que me bebe.
Desaparezco entre un farol que agiganta la niebla
y sigo siendo la bufanda que me ahorca.
"Hoy no me esperes porque la noche será negra y blanca."

Juan Gustavo Cobo Borda

Introducción

En la primera mitad del siglo XIX, el intento de George Boole por formalizar la lógica proposicional dio lugar al concepto de álgebras booleanas.
Mientras investigaban las axiomáticas para las álgebras booleanas al final del siglo XIX, Charles S. Pierce y Ernst Schörder, encontraron útil introducir el concepto de retícula.
Independientemente, la investigación de Richard Dedekind sobre ideales de números algebraicos dio lugar al mismo concepto. De hecho, Dedekind también introdujo el concepto de modularidad, una forma debilitada de la distributividad.
A pesar de que algunos de los primeros resultados de estos matemáticos y de Edward V. Huntington son muy elegantes y lejos de ser triviales, no atrajeron la atención de la comunidad matemática.
Fue el trabajo de Garrett Birkhoff a mediados de los 30's que empezó el desarrollo general de la teoría de retículas. En una brillante serie de artículos él demostró la importancia de la teoría de retículas y también que ésta provee un marco unificador para los hasta entonces no relacionados desarrollos en muchas disciplinas matemáticas. El mismo Birkhoff, Valère Glivenko, Karl Menger, John von Neumann, Oystein Ore y otros habían desarrollado lo suficiente de este nuevo campo para que Birkhoff intentara presentarlo a la comunidad matemática en general, lo que hizo con mucho éxito en la primera edición de su *Lattice Theory*. Muchas condiciones sobre retículas y sobre elementos de ideales de retículas son formas "debilitadas" de distributividad. Por lo tanto, un conocimiento minucioso de las retículas distributivas es indispensable para el trabajo de teoría de retículas. En muchas aplicaciones la

condición de distributividad se impone sobre retículas que surgen en varias áreas de las matemáticas, especialmente el álgebra. Como hemos mencionado, la modularidad es una forma débil de distributividad que cumplen, por ejemplo, los submódulos de un módulo.
Las retículas modulares son una herramienta fundamental en la teoría general de anillos y particularmente útiles en la teoría de anillos de cocientes. Ayuda a tratar con los aspectos abstractos de la relación de inclusión entre los submódulos de un módulo. En el contexto de los anillos de cocientes, esta teoría es indispensable cuando se debe dilucidar la conexión entre submódulos de un módulo dado M y los submódulos de un módulo de cocientes de M.

El objetivo principal de ésta tesis es proporcionar un libro de texto introductorio para estudiantes de ciencias y que se tenga un mejor acceso a los cursos de álgebra, como teoría de grupos, teoría de anillos y campos y teoría de módulos.
Las retículas, aunque pueden ser estudiadas por sí solas, tienen una aplicación fundamental en el estudio de las estructuras algebraicas, ya que proporcionan información de su estructura interna y además brindan otro enfoque en el estudio de la mismas.
Muchos resultados de la teoría de retículas ayudan a demostrar resultados en cada una de las teorías de estructuras algebraicas específicas, como álgebra lineal, teoría de grupos y teoría de módulos. Otros resultados que aparecen en dichas teorías, son en realidad resultados de la teoría de retículas.
Además, al abstraer las propiedades esenciales del orden en las estructuras, las retículas son ideales para hablar de subestructuras comunes a los objetos algebraicos los cuales proporcionan una manera natural de analizar y clasificar la retícula de algún módulo, grupo, etc.

En el capítulo 1 de preliminares se habla de conjuntos parcialmente orde-

nados, morfismos de orden y algunas propiedades de éstos. Se introudce la definición de retícula y retícula completa, se dan ejemplos y se demuestran algunas porposiciones que serán auxiliares para el siguiente capítulo.
En el capítulo 2 de retículas modulares se da la definición correspondiente tomando en cuenta porpiedades que se dieron en los preliminares y, entre otras cosas se demuestra que la modularidad es una forma debilitada de la distributividad. Se definen retículas distributivas y álgebras booleanas y también, como ejemplo, se demuestra la equivalencia de las categorías $\mathbf{Set}^{\mathbf{OP}}$ y **CABool**. Para no perder la fluidez de la lectura, los conceptos necesarios para leer el ejemplo aparecen en el apéndice Categorías. Más adelante se definen conceptos con ejemplos en la teoría de módulos. Por último se estudian berevemente los operadores de cerradura y las conexiones de Galois, y como una aplicación se menciona el teorema fundamental de la teoría de Galois.

Índice general

Capítulo 1

Preliminares

1.1. Conjuntos parcialmente ordenados

Definición 1.1.1
Un sistema $(A_1, A_2, ..., A_n; R)$ con A_i, tal que $1 \leq i \leq n$, conjuntos arbitrarios y $R \subseteq A_1 \times A_2 \times ... \times A_n$ es llamado una **relación n-aria** entre los elementos de dichos conjuntos. Si $A_1 = A_2 = ... = A_n = A$ la relación $(A, ...A; R)$ es llamada **homogénea** y si $n = 2$ la relación es llamada **binaria**.

Definición 1.1.2
Una relación binaria $(A, A; R)$ es llamada:

(R) **Reflexiva**: $\forall a \in A : (a, a) \in R$.

(T) **Transitiva**: $\forall a, b, c \in A : (a, b), (b, c) \in R \Rightarrow (a, c) \in R$.

(A) **Antisimétrica**: $\forall a, b \in A : (a, b), (b, a) \in R \Rightarrow a = b$.

Es llamada **relación de orden parcial** si cumple con (R), (T) y (A). A una relación de orden parcial la denotaremos por "$\leq$".

Si X es un conjunto en el que está definida una relación de orden parcial "$\leq$", se dice que $(X, \leq)$ es un **conjunto parcialmente ordenado** (COPO).

Observación 1
Si $(A, A; R)$ es una relación binaria, la relación inversa es $(A, A; R^{-1})$ donde $R^{-1} = \{(b, a)|(a, b) \in R\}$. Esta relación también es una relación de orden parcial pues es claro que cumple con (R),(T) y (A).
<u>**Demostración:**</u>
En efecto, es claro que $\forall a \in A : (a, a) \in R^{-1}$.
Si $(a, b), (b, c) \in R^{-1}$ entonces $(b, a), (c, b) \in R$, como R es relación de orden parcial entonces $(c, a) \in R$ y por tanto $(a, c) \in R^{-1}$.
Si $(a, b), (b, a) \in R^{-1}$ entonces $(b, a), (a, b) \in R$ y ya que R es relación de orden parcial, tenemos que $a = b$. ■

A la relación inversa de "$\leq$" la denotamos por "$\geq$".

Para un COPO podemos escribir las propiedades (R), (T) y (A) de la siguiente forma:

Sea $(A, \leq)$ un COPO, entonces se cumple que:

(R) $\forall a \in A : a \leq a$.

(T) $\forall a, b, c \in A : a \leq b, b \leq c \Rightarrow a \leq c$.

(A) $\forall a, b \in A : a \leq b, b \leq a \Rightarrow a = b$.

Si $a \leq b$ decimos que a es **menor que** b o que b es **mayor que** a.

Ejemplo 1

1.- $(\mathbb{N}, \leq)$ es un conjunto parcialmente ordenado.

2.- $(\mathbb{N}, |)$ es un conjunto parcialmente ordenado donde "$|$" es la relación "divide a".

3.- Si X es un conjunto entonces $(\mathcal{P}(X), \subseteq)$ es un conjunto parcialmente ordenado.

4.- Los subespacios de un espacio vectorial son un conjunto parcialmente ordenado con la relación de orden parcial dada por la inclusión.

5.- $(\mathbb{Z}, |)$ no es un COPO ya que la relación "$|$" no es de orden parcial en $\mathbb{Z}$ pues no cumple con la propiedad antisimétrica ya que $3| -3$ y $-3|3$ pero $3 \neq -3$.

Definición 1.1.3

Un subconjunto B de un COPO $(A, \leq)$ es llamado **subCOPO** si es parcialmente ordenado por restricción de la relación, es decir,

$$\forall a, b \in B \subseteq A : a \leq_B b \Leftrightarrow a \leq_A b.$$

Definición 1.1.4

En un COPO decimos que dos propiedades son **duales** si una se obtiene de la otra mediante la permutación de la relación de orden parcial dada.

Notación 1

En un COPO $(A, \leq)$ y $a, b \in A$ si $a \leq b$ y $a \neq b$ escribimos $a < b$.

Definición 1.1.5

1.- Dos elementos a, b en un COPO $(A, \leq)$ son llamados **comparables** si $a \leq b$ o $b \leq a$. En caso contrario son llamados **incomparables** y esto se denota por $a \| b$.

2.- Si $(A, \leq)$ es un COPO y $C \subseteq A$ entonces C es un **conjunto totalmente ordenado, cadena o COTO** si cualesquiera dos de sus elementos son comparables.

Definición 1.1.6
Sea $(A, \leq)$ un COPO :

1.- El **elemento mayor (menor)** de un subconjunto X de A es un elemento $m \in X$ tal que $\forall x \in X : x \leq m$ (respectivamente $m \leq x$).

2.- Un elemento $m \in X$ es llamado **máximo (mínimo)** en X si no existe elemento en X mayor (menor) que m, es decir, $\forall x \in X : m \leq x$ (respectivamente $x \leq m$) entonces $m = x$.

Observación 2

1.- Si el elemento mayor (menor) existe, es único.

Demostración:

En efecto, supongamos que m_1 y m_2 son elementos mayores de $X \subseteq A$, donde $(A, \leq)$ es un COPO. Como m_1 es elemento mayor entonces $m_2 \leq m_1$, pero también m_2 es elemento mayor, así que $m_1 \leq m_2$. Como ambos elementos pertenecen a un COPO, se cumple la propiedad antisimétrica y por tanto $m_1 = m_2$. Dualmente se demuestra el caso para elemento menor. ■

2.- Si el elemento mayor (menor) existe, es siempre máximo (mínimo) pero los elementos máximos (mínimos) pueden existir sin que exista un elemento mayor (menor).

Ya que, por ejemplo, si $A = \{\{n\} : n \in \mathbb{N}\}$ entonces para cada $n \in \mathbb{N}$: $\{n\}$ es máximo pues si existe $\{m\}$ tal que $\{n\} \subseteq \{m\}$ entonces $m = n$ y por tanto $\{n\} = \{m\}$.

Otro ejemplo: Tomemos el conjunto de ideales propios de $\mathbb{Z}$. Si p es primo entonces $p\mathbb{Z}$ es máximo pues sólo lo contienen $\mathbb{Z}$ y él mismo. Pero es claro que no hay un elemento mayor, pues no existe ideal no trivial que contenga a todos los ideales propios de $\mathbb{Z}$.

Proposición 1.1.1

Cualquier cadena tiene a lo más un elemento máximo (mínimo). Notar que puede no tener elemento máximo (mínimo), pero en caso de tenerlo, es único.

Demostración:

Si una cadena C no tiene elemento máximo, se cumple la proposición. Supongamos que existen en C elementos máximos m_1 y m_2. Como C es cadena, todos sus elementos son comparables, así $m_1 \leq m_2$ o $m_2 \leq m_1$. Sin pérdida de generalidad supongamos que se cumple $m_1 \leq m_2$, pero como m_1 es máximo esto implica que $m_1 = m_2$. Dualmente para el caso de elemento mínimo.

■

Definición 1.1.7

Sean $(A, \leq)$ un COPO y $X \subseteq A$:

1.- Un elemento $a \in A$ es una **cota superior (inferior)** de X si $\forall x \in X : x \leq a$ (respectivamente $a \leq x$).

Denotamos como $X^{\uparrow} = \{a \in A : a \text{ es cota superior de } X\}$ y a $X_{\downarrow} = \{a \in A : a \text{ es cota inferior de X}\}$.

2.- Un elemento $a \in A$ es llamado **supremo o yunta** de X si es el elemento menor de $X^{\uparrow}$. Es decir, a es la menor de las cotas superiores (si $c \in A$ es cota superior entonces $a \leq c$). Al supremo lo denotamos por $\sup X$ o $\bigvee X$.

Dualmente definimos al **ínfimo o cuña** como el elemento mayor de $X_{\downarrow}$. Lo denotamos por $\inf X$ o $\bigwedge X$.

Como caso particular $\sup\{a, b\} = a \vee b$ y $\inf\{a, b\} = a \wedge b$.

Observación 3

El supremo y el ínfimo en caso de existir son únicos.

Para lo siguiente asumiremos el axioma de elección y por tanto sus equivalencias, en particular el Lema de Zorn.

Lema de Zorn (LZ): Si toda cadena no vacía C de un COPO $(A, \leq)$ tiene una cota superior en C, entonces A tiene al menos un elemento máximo.

Definición 1.1.8
Un COPO con la propiedad de que cada subconjunto no vacío contiene al menos un elemento máximo (mínimo) es llamado **noetheriano (artiniano)**.

Definición 1.1.9
Un COPO $(A, \leq)$ satisface la **condición de la cadena ascendente (descendente)** (CCA y respectivamente CCD) si para cada sucesión infinita $a_1 \leq a_2 \leq ... \leq a_n \leq ...$ (respectivamente $a_1 \geq a_2 \geq ... \geq a_n \geq ...$) existe un elemento $k \in \mathbb{N}$ tal que $a_k = a_{k+1} = ...$, es decir la sucesión es estacionaria.

Teorema 1.1.1
Un COPO $(A, \leq)$ es noetheriano (artiniano) si y sólo si cumple cumple con la CCA (respectivamente CCD).
Demostración:
[$\Rightarrow$] Supongamos que A es noetheriano. El conjunto de elementos de una sucesión no decreciente debe de tener un elemento máximo y es claro que la sucesión se estaciona en ese elemento.
[$\Leftarrow$] Sea $T \subseteq A$ tal que $T \neq \emptyset$. Haciendo uso del axioma de elección, escogemos $x_1 \in T$. Si x_1 es máximo, terminamos. En otro caso escogemos $x_2 \in T$ tal que $x_1 < x_2$, si x_2 es máximo, terminamos. Siguiendo este proceso podemos construir una sucesión estrictamente creciente de elementos de T, lo que contradice la CCA, a menos que encontremos un elemento máximo. ■

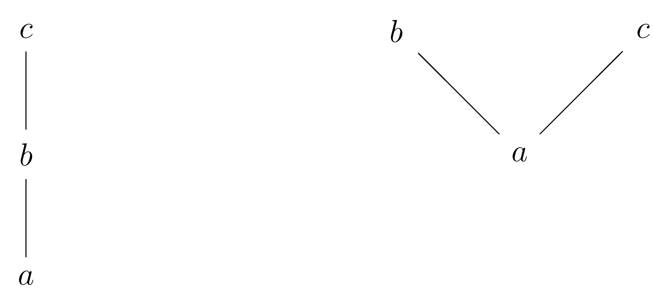
Definición 1.1.10
Si $a < b$ en un COPO $(A, \leq)$ y no existe elemento $c \in A$ tal que $a < c < b$,

decimos que a **es cubierto por** b y lo denotamos por $a \prec b$.

Muchos conjuntos parcialmente ordenados, especialmente los finitos, pueden ser representados mediante un diagrama. A continuación definiremos un grafo dirigido asociado a un COPO.

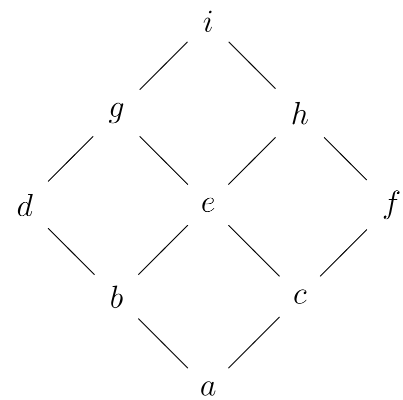
Definición 1.1.11
El **Diagrama de Hasse** de un conjunto parcialmente ordenado $(A, \leq)$ es un grafo dirigido cuyos vértices son los elementos de A, y si $x < y$ y no existe z tal que $x < z < y$ entonces existe una arista de x a y.
Para construir el Diagrama de Hasse de un COPO $(A, \leq)$ dibujamos un punto (o escribimos el elemento) por cada elemento de A de tal manera que si $a \leq b$ entonces el punto asociado con el elemento b esté arriba del punto relacionado con el elemento a. Por otra parte si $a \prec b$ conectamos a los puntos asociados con una línea vertical (de ser posible).

Ejemplo 2
Este ejemplo representa dos órdenes distintos sobre conjuntos iguales de tres elementos.



Ejemplo 3
Si $A = \{a, b, c, d, e, f, g, h, i\}$, el orden lo podemos definir con el siguiente

diagrama.



Donde podemos observar que, por ejemplo, se tiene que $a \leq b$, $b \leq e$, $e \leq h$ y $h \leq i$.

Para precisar el concepto de cuándo dos órdenes son iguales comenzaremos por la siguiente definición:

Definición 1.1.12

1.- Una función $f : (A, \leq) \longrightarrow (B, \leq)$ entre dos COPO's es llamado **morfismo de orden** si $\forall a, b \in A : a \leq b \Rightarrow f(a) \leq f(b)$.

2.- Un morfismo de orden inyectivo será llamado **morfismo de orden estricto**.

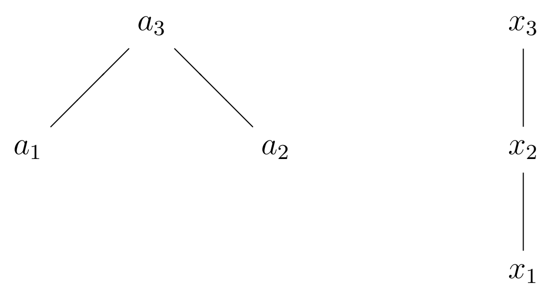
3.- Un **isomorfismo de orden** es un morfismo de orden biyectivo tal que su inversa también es un morfismo de orden.

Observación 4

La inversa de un morfismo de orden biyectivo no necesariamente es un morfismo de orden, es decir, un morfismo de orden biyectivo no siempre es isomorfismo de orden.

Demostración:

Sean $A = \{a_1, a_2, a_3\}$ y $X = \{x_1, x_2, x_3\}$ dos conjuntos parcialmente ordenados donde su orden está dado por:



Definimos $\alpha : A \longrightarrow X$ tal que para toda i con $1 \leq i \leq 3 : \alpha(a_i) = x_i$. Es claro que α es una biyección pues A y X tienen la misma cantidad de elementos.

Para ver que α es morfismo de orden notemos que:

$$a_1 \leq a_3 \text{ y } \alpha(a_1) = x_1 \leq x_3 = \alpha(a_3)$$

$$a_2 \leq a_3 \text{ y } \alpha(a_2) = x_2 \leq x_3 = \alpha(a_3)$$

Por tanto α preserva orden.

Observamos que $\alpha^{-1} : X \longrightarrow A$ está dada por $\alpha^{-1}(x_i) = a_i$ y además $x_1 \leq x_2$ y notamos que $\alpha^{-1}(x_1) = a_1$ y $\alpha^{-1}(x_2) = a_2$. Pero a_1 y a_2 son incomparables por lo que no ocurre que $\alpha^{-1}(x_1) = a_1 \leq a_2 = \alpha^{-1}(x_2)$. ■

Observación 5

Dos conjuntos parcialmente ordenados finitos son isomorfos si y sólo si son representados por el mismo diagrama.

Proposición 1.1.2

En un COPO si $\text{ínf}\{\text{ínf}\{a, b\}, c\}$ existe, entonces existe $\text{ínf}\{a, b, c\}$ y son iguales.

<u>**Demostración:**</u>

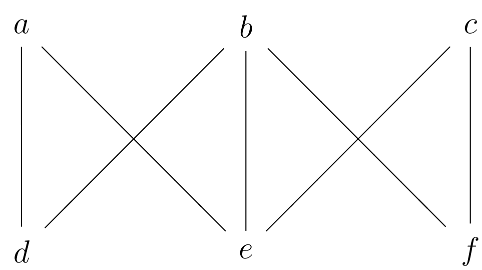
Sea $i = \text{ínf}\{\text{ínf}\{a, b\}, c\}$, entonces $i \leq \text{ínf}\{a, b\}$ e $i \leq c$. Así tenemos que $i \leq a$,

$i \leq b$ e $i \leq c$, es decir i es cota inferior de $\{a, b, c\}$. Sea x cota inferior de $\{a, b, c\}$, entonces $x \leq \text{ínf}\{a, b\}$ y $x \leq c$, de aquí que $x \leq \text{ínf}\{\text{ínf}\{a, b\}, c\}$. Por lo tanto i es la mayor de las cotas inferiores, lo que implica que $i = \text{ínf}\{a, b, c\}$.

■

Observación 6

El recíproco de la proposición anterior es falso ya que si nos fijamos en el COPO con seis elementos dado por el siguiente diagrama:



$\text{ínf}\{a, b, c\} = e$ pero $\text{ínf}\{\text{ínf}\{a, b\}, c\ \}$ no existe.

1.2. Retículas

Definición 1.2.1

Una **retícula** es un conjunto parcialmente ordenado en el cual, cada par de elementos tienen supremo e ínfimo. Es decir, $(\mathscr{L}, \leq)$ es una retícula si para cualesquiera $a, b \in \mathscr{L}$ existe sup $\{a, b\} = a \vee b$ y existe ínf $\{a, b\} = a \wedge b$.

Ejemplo 4

Sea $\mathbb{V}$ un $\mathbb{F}$-espacio vectorial. El conjunto de subespacios vectoriales de $\mathbb{V}$ forman una retícula con el orden dado por la inclusión. Donde, si $\mathbb{V}_1$ y $\mathbb{V}_2$ son subespacios de $\mathbb{V}$ tenemos que:

$$\mathbb{V}_1 \vee \mathbb{V}_2 = \mathbb{V}_1 + \mathbb{V}_2 = \langle \mathbb{V}_1 \cup \mathbb{V}_2 \rangle \qquad \text{y} \qquad \mathbb{V}_1 \wedge \mathbb{V}_2 = \mathbb{V}_1 \cap \mathbb{V}_2.$$

Ejemplo 5

Los números naturales $\mathbb{N}$ junto con la relación de orden $|$, "divide a", es una retícula.

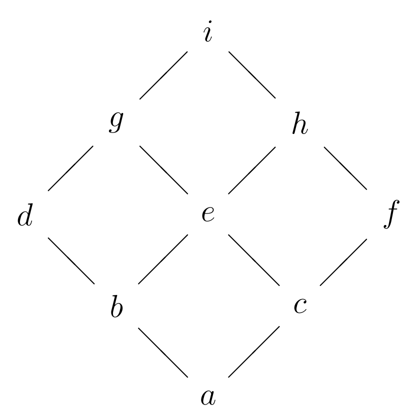
Donde para $n, m \in \mathbb{N} : n \vee m = \text{mcm}(n, m)$ y $n \wedge m = \text{mcd}(n, m)$.

Ejemplo 6

Si X es un conjunto entonces $(\mathcal{P}(X), \subseteq)$ es una retícula donde para cualesquiera $A, B \in \mathcal{P}(X)$:$A \vee B = A \cup B$ y $A \wedge B = A \cap B$.

Ejemplo 7

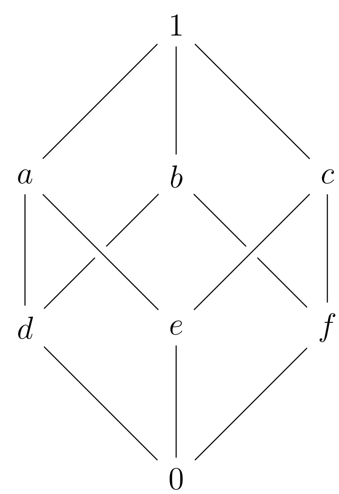
El conjunto $\{a, b, c, d, e, f, g, h, i\}$ con la relación dada por:



es una retícula. Donde, por ejemplo, $b \wedge c = a$, $d \wedge e = b$, $d \wedge f = a$, $b \vee c = e$, $g \vee h = i$ y $d \vee f = i$.

Ejemplo 8

El conjunto $\{1, a, b, c, d, e, f, 0\}$ es una retícula con la relación dada por:



Ejemplo 9

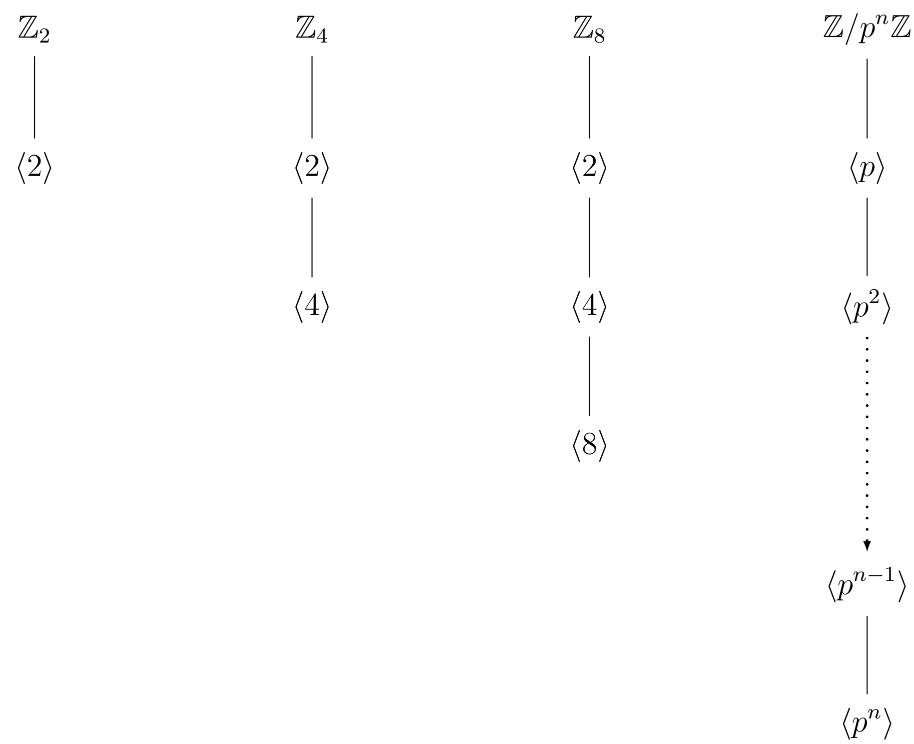
Un conjunto totalmente ordenado $(X, <)$ es una retícula donde, para cualesquiera $x, y \in X$: $x \vee y =$máx$\{x, y\}$ y $x \wedge y =$mín$\{x, y\}$.

Ejemplo 10

Si M es un R-módulo izquierdo entonces la clase de submódulos de M, denotada por $(S_R(M), \subseteq)$, es una retícula donde, para $A, B \in S_R(M)$ se tiene que $A \vee B = A + B$ y $A \wedge B = A \cap B$.

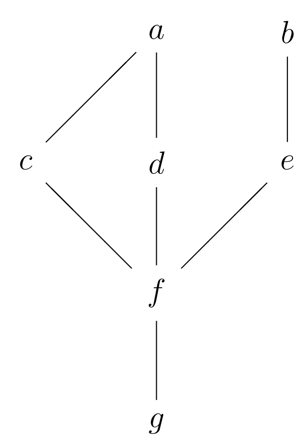
Ejemplo 11

Para $G = \mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$, la retícula de subgrupos de G es la retícula de divisiores de n (es decir, los divisores de n son escritos en una línea con n en la parte inferior, 1 en la parte superior y las aristas hacia arriba desde a a b si $b|a$). Algunos ejemplos de esto para algunos valores de n son:



Ejemplo 12

El conjunto representado por el diagrama



no es una retícula puesto que no existe $a \vee e$.

Definición 1.2.2

Si $\mathscr{L}$ es una retícula e invertimos el orden, es decir, se cambia "$\leq$" por "$\geq$" y "$\vee$" por "$\wedge$", obtenemos una retícula a la que llamamos **retícula dual** y la denotamos por $\mathscr{L}^{OP}$.

Proposición 1.2.1

En cualquier retícula $(\mathscr{L}, \leq)$, las operaciones binarias "$\vee$" y "$\wedge$" son asociativas, conmutativas y satisfacen la propiedad de absorción:

$$\forall a, b \in \mathscr{L} : (a \vee b) \wedge a = (a \wedge b) \vee a = a.$$

Demostración:

La conmutatividad es inmediata, así que demostraremos solamente la asociatividad y la absorción. Sean $a, b, c \in \mathscr{L}$. Para demostrar la asociatividad tenemos que verificar que se cumplen:

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

$$a \wedge (b \wedge c) = (a \wedge b) \wedge c.$$

Es claro que $a \leq a \vee (b \vee c)$ y $b \vee c \leq a \vee (b \vee c)$ y además $b \leq b \vee c$ y $c \leq b \vee c$, así, por transitividad, tenemos que $b \leq a \vee (b \vee c)$ y $c \leq a \vee (b \vee c)$.

Así $a \vee (b \vee c)$ es una cota superior de a y b, de modo que por la definición de supremo tenemos

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

Como $a \vee (b \vee c)$ es cota superior de $a \vee b$ y c entonces tenemos que

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

Análogamente

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

Y por antisimetría tenemos que $a \vee (b \vee c) = (a \vee b) \vee c$ por lo que queda demostrado la asociatividad de la yunta.

De forma dual se demuestra que $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

Para demostrar la propiedad de absorción, *i.e.*, $a \vee (a \wedge b) = a = a \wedge (a \vee b)$ demostremos que $a \vee (a \wedge b) = a$, ya que la otra igualdad se puede demostrar de forma análoga.

Como $a \wedge b \leq a$ y $a \leq a$, entonces a es una cota superior de $\{a, a \wedge b\}$, así tenemos que $a \vee (a \wedge b) \leq a$.
Por otra parte, es claro que $a \leq a \vee (a \wedge b)$. Por lo tanto $a \vee (a \wedge b) = a$. ■

Lema 1.2.1
Sea $(\mathscr{L}, \leq)$ una retícula, entonces para cualesquiera $a, b \in \mathscr{L}$ son equivalentes:

(1) $a \leq b$

(2) $a \wedge b = a$

(3) $a \vee b = b$.

Demostración:
[(1) $\Rightarrow$ (2)] Como $a \leq b$ y $a \leq a$ entonces a es una cota inferior de $\{a, b\}$ y como $a \wedge b$ es la mayor de las cotas inferiores tenemos que $a \leq a \wedge b$ y además $a \wedge b \leq a$. Por lo tanto $a \wedge b = a$.
[(2) $\Leftarrow$ (1)] Si $a \wedge b = a$ entonces $a =$ínf$\{a, b\}$ y por lo tanto $a \leq b$.

[(1) $\Leftrightarrow$ (3)] Similarmente se demuestra que $a \leq b \Leftrightarrow a \vee b = b$. ■

Lema 1.2.2
Sea $(\mathscr{L}, \leq)$ una retícula, entonces se cumplen las siguientes proposiciones para $a, b, c \in \mathscr{L}$:

(i) Si $b \leq c$ entonces $a \wedge b \leq a \wedge c$ y $a \vee b \leq a \vee c$.

(ii) Si $a \leq b$ y $a \leq c$ entonces $a \leq b \vee c$ y $a \leq b \wedge c$.

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

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

(v) Si $a \leq c$ entonces $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.

(vi) Si $c \leq a$ entonces $(a \wedge b) \vee c \leq a \wedge (b \vee c)$.

Demostración:

(i) Supongamos que $b \leq c$. Lo que queremos demostrar es equivalente, por el Lema 1.2.1, a $(a \wedge b) \wedge (a \wedge c) = a \wedge b$. Haciendo uso de las leyes conmutativas y asociativas tenemos que $(a \wedge b) \wedge (a \wedge c) = (a \wedge a) \wedge (b \wedge c) = a \wedge b$.
Similarmente se demuestra que $a \vee b \leq a \vee c$.

(ii) Como $a \leq b$ y $a \leq c$, tenemos que $c \leq b \vee c$, entonces por transitividad $a \leq b \vee c$. También, como $a \leq b$ y $a \leq c$, entonces a es cota inferior de b y c, por definición de ínfimo tenemos que $a \leq b \wedge c$.

(iii) Sabemos que $a \leq a \vee b$ y $a \leq a \vee c$, por (ii) tenemos:

$$a \leq (a \vee b) \wedge (a \vee c) \qquad \textbf{(1)}$$

Además tenemos que $b \wedge c \leq b \leq a \vee b$ y $b \wedge c \leq c \leq a \vee c$, usando una vez más (ii) tenemos:

$$b \wedge c \leq (a \vee b) \wedge (a \vee c) \qquad \textbf{(2)}$$

De **(1)** y **(2)** tenemos que $(a \vee b) \wedge (a \vee c)$ es cota superior de $\{a, b \wedge c\}$, de aquí que $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$.

(iv) La demostración es dual a (iii).

(*v*) De (*iii*) tenemos que $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$. Como $a \leq c$ entonces $a \vee c = c$ y por lo tanto $(a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$, que es equivalente a lo que se quería demostrar.

(*vi*) Como $b \leq b \vee c$ entonces $a \wedge b \leq a \wedge (b \vee c)$ y además, como $c \leq a$, tenemos que $(a \wedge b) \vee c = c \vee (a \wedge b) \leq c \vee a \wedge (b \vee c) = a \wedge (b \vee c)$.

$\blacksquare$

Definición 1.2.3

1.- Si $(\mathscr{L}, \leq)$ y $(\mathscr{L}', \leq)$ son retículas, un **morfismo de retículas**

$$\alpha : \mathscr{L} \longrightarrow \mathscr{L}'$$

es una función que satisface:

$\forall a, b \in \mathscr{L} : \alpha(a \vee b) = \alpha(a) \vee \alpha(b)$ y $\alpha(a \wedge b) = \alpha(a) \wedge \alpha(b)$.

2.- Un **isomorfismo de retículas** es un morfismo de retículas biyectivo, es decir, es inyectivo y suprayectivo o equivalentemente:
Un morfismo de retículas $\alpha : \mathscr{L} \longrightarrow \mathscr{L}'$ es un **isomorfismo de retículas** si existe un morfismo de retículas $\beta : \mathscr{L}' \longrightarrow \mathscr{L}$ tal que $\alpha \circ \beta = 1_{\mathscr{L}'}$ y $\beta \circ \alpha = 1_{\mathscr{L}}$.

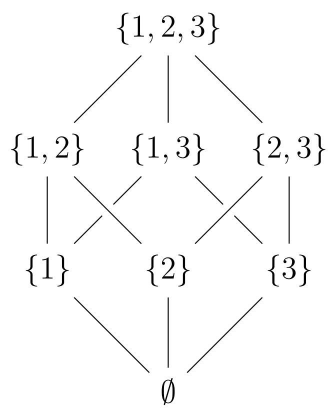
3.- Un morfismo $\mathscr{L}^{OP} \longrightarrow \mathscr{L}'$ es llamado **antimorfismo** de $\mathscr{L}$ a $\mathscr{L}'$.

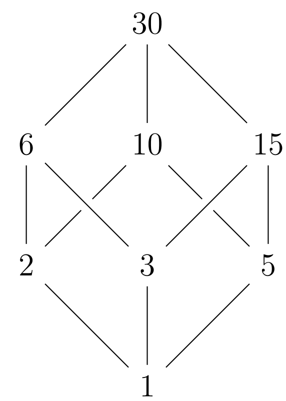
Ejemplo 13

Para cualquier número natural n consideramos el conjunto

$$D(n) = \{m \in \mathbb{N} : m|n\}.$$

Las retícula $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$ y $(D(30), |)$ son isomorfas.





Proposición 1.2.2

La inversa de un isomorfismo de retículas también es un isomorfismo de retículas.

<u>Demostración:</u>

Sean $\alpha : \mathscr{L} \longrightarrow \mathscr{L}'$ un isomorfismo de retículas y $a, b \in \mathscr{L}'$. Como α es suprayectivo, existen $x, y \in \mathscr{L}$ tal que $a = \alpha(x)$ y $b = \alpha(y)$ entonces $\alpha^{-1}(a \wedge b) = \alpha^{-1}(\alpha(x) \wedge \alpha(y)) = \alpha^{-1}(\alpha(x \wedge y)) = x \wedge y = \alpha^{-1}(a) \wedge \alpha^{-1}(b)$. Dualmente se demuestra que $\alpha^{-1}(a \vee b) = \alpha^{-1}(a) \vee \alpha^{-1}(b)$. ■

Proposición 1.2.3

Si $(\mathscr{L}, \leq)$ y $(\mathscr{L}', \leq)$ son retículas entonces cada función entre $\mathscr{L}$ y $\mathscr{L}'$ es isomorfismo de orden si y sólo si es un isomorfismo de retículas.

<u>Demostración:</u>

[⇒] Sea $\alpha : \mathscr{L} \longrightarrow \mathscr{L}'$ un isomorfismo de orden y sean $x, y \in \mathscr{L}$. Tenemos que $x \wedge y \leq x, y$, entonces, como α preserva orden, tenemos que $\alpha(x \wedge y) \leq \alpha(x)$ y $\alpha(x \wedge y) \leq \alpha(y)$. Así $\alpha(x \wedge y)$ es una cota inferior de $\alpha(x)$ y de $\alpha(y)$. Supongamos que b es una cota inferior de $\alpha(x)$ y de $\alpha(y)$, *i.e.* $b \leq \alpha(x)$ y $b \leq \alpha(y)$.

Como α es suprayectivo entonces existe $a \in \mathscr{L} : b = \alpha(a)$ y así lo anterior lo podemos reescribir como $\alpha(a) \leq \alpha(x)$ y $\alpha(a) \leq \alpha(y)$. Por hipótesis α^{-1}

también preserva orden tenemos que $a \leq x$ y $a \leq y$ (a es cota inferior), entonces $a \leq x \wedge y$ y por lo tanto $b = \alpha(a) \leq \alpha(x \wedge y)$.
Por lo tanto $\alpha(x \wedge y)$ es la mayor de las cotas inferiores de $\alpha(x)$ y de $\alpha(y)$, y así hemos demostrado que $\alpha(x \wedge y) = \alpha(x) \wedge \alpha(y)$.
Se demuestra dualmente que $\alpha(x \vee y) = \alpha(x) \vee \alpha(y)$.
[$\Leftarrow$] Si $a \leq b$ y α es isomorfismo de retículas entonces $\alpha(a) = \alpha(a \wedge b) = \alpha(a) \wedge \alpha(b)$ si y sólo si $\alpha(a) \leq \alpha(b)$. Como la inversa de un isomorfismo de retículas también es isomorfismo de retículas, y como ya demostramos, cada morfismo de retículas es un morfismo de orden entonces la inversa también es un isomorfismo de orden. ■

Definición 1.2.4
Sea $\mathscr{L}$ una retícula y $a, b \in \mathscr{L}$ tales que $a \leq b$. Entonces definimos el **intervalo** $[a, b] = \{x \in \mathscr{L} : a \leq x \leq b\}$.

Ejemplo 14
Sea $\alpha : A \longrightarrow L$ un morfismo de módulos.
Entonces $\hat{\alpha} : [\mathrm{Ker}\alpha, A] \longrightarrow [0, \mathrm{Im}\alpha]$, tal que para $U \in [\mathrm{Ker}\alpha, A]$ se tiene que $\hat{\alpha}(U) = \alpha(U)$, es un isomorfismo de retículas.
Demostración:
(i) Veamos que $\hat{\alpha}$ está bien definido. Sean $U_1 = U_2 \in [\mathrm{Ker}\alpha, A]$. Si $x \in \alpha(U_1)$ entonces existe $u \in U_1$ tal que $x = \alpha(u)$, pero $u \in U_2$ entonces $\alpha(u) \in \alpha(U_2)$. Así $\alpha(U_1) \subseteq \alpha(U_2)$. Simétricamente se tiene que $\alpha(U_2) \subseteq \alpha(U_1)$ y por lo tanto $\alpha(U_1) = \alpha(U_2)$.
(ii) Veamos que $\hat{\alpha}$ es inyectivo. Supongamos que $\hat{\alpha}(U_1) = \hat{\alpha}(U_2)$ entonces $\alpha(U_1) = \alpha(U_2)$. Luego $\alpha^{-1}(\alpha(U_1)) = \alpha^{-1}(\alpha(U_2))$ lo que implica que $U_1 + \mathrm{Ker}\alpha = U_2 + \mathrm{Ker}\alpha$ y así tenemos que $U_1 = U_2$ y por lo tanto $\hat{\alpha}$ es inyectivo.
(iii) Veamos que $\hat{\alpha}$ es suprayectivo. Sea $V \in [0, \mathrm{Im}\alpha]$ entonces $0 \leq V \leq \mathrm{Im}\alpha$ lo que implica que $\mathrm{Ker}\alpha = \alpha^{-1}(0) \leq \alpha^{-1}(V) \leq \alpha^{-1}(\mathrm{Im}\alpha) = A$ de aquí que

$\alpha^{-1}(V) \in [\text{Ker}\alpha, A]$ y entonces $\hat{\alpha}(\alpha^{-1}(V)) = \alpha(\alpha^{-1}(V)) = V \cap \text{Im}\alpha = V$. Por lo tanto $\hat{\alpha}$ es suprayectivo.
(iv) Veamos que $\hat{\alpha}$ es morfismo de retículas. Sean $U_1, U_2 \in [\text{Ker}\alpha, A]$ entonces $\hat{\alpha}(U_1 + U_2) = \alpha(U_1 + U_2) = \alpha(U_1) + \alpha(U_2) = \hat{\alpha}(U_1) + \hat{\alpha}(U_2)$.
Además, como $\text{Ker}\alpha \leq U_1, U_2$, $\hat{\alpha}(U_1 \cap U_2) = \alpha(U_1 \cap U_2) = \alpha(U_1) \cap \alpha(U_2) = \hat{\alpha}(U_1) \cap \hat{\alpha}(U_2)$.
Por lo tanto $[\text{Ker}\alpha, A] \cong [0,\text{Im}\alpha]$. ■
Como consecuencia de lo anterior tenemos:

Teorema 1.2.1 (4to Teorema de isomorfismos para módulos)
Sea A un R-módulo y $C \leq A$. Si $\nu : A \longrightarrow A/C$ es el epimorfismo canónico, entonces $\bar{\nu} : [C, A] \longrightarrow [0, A/C]$ es un isomorfismo de retículas.

Lema 1.2.3
Sea $C \leq A$, entonces C es máximo si y sólo si A/C es simple.

Proposición 1.2.4
Si $\mathscr{C}$ es una cadena, $\mathscr{L}$ una retícula y $f : \mathscr{C} \longrightarrow \mathscr{L}$ un morfismo de orden, entonces f es un morfismo de retículas.
Demostración:
Para cualesquiera $a, b \in \mathscr{C}$ demostremos que $f(a \wedge b) = f(a) \wedge f(b)$ y $f(a \vee b) = f(a) \vee f(b)$.
Como $\mathscr{C}$ es una cadena, sus elementos son comparables. Sin pérdida de generalidad supongamos que $a \leq b$. Entonces por Lema 1.2.1 y por hipótesis $a = a \wedge b$ y así $f(a) \leq f(b)$, esto implica que $f(a \wedge b) = f(a) = f(a) \wedge f(b)$, ya por por el inciso (i) del Lema 1.2.2, se tiene que $f(a) \leq f(b)$ implica que $f(a) = f(a) \wedge f(a) \leq f(a) \wedge f(b)$.
Dualmente se tiene que $f(a \vee b) = f(a) \vee f(b)$. Por lo tanto f es un morfismo de retículas. ■

Definición 1.2.5

Si $\mathscr{L}$ es una retícula entonces una **subretícula** de $\mathscr{L}$ es un subconjunto $\mathscr{L}' \subseteq \mathscr{L}$ tal que: $a, b \in \mathscr{L}'$ implica que $a \vee b \in \mathscr{L}'$ y $a \wedge b \in \mathscr{L}'$. Y por tanto $\mathscr{L}'$ es una retícula por sí misma.

Proposición 1.2.5

Un COPO es una cadena si y sólo si cada uno de sus subconjuntos es una subretícula.

Demostración:

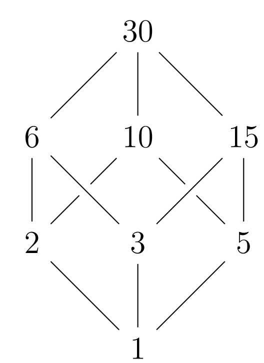
[$\Rightarrow$] Sea X un subconjunto de una cadena $\mathscr{C}$ y $x, y \in X$. Como los elementos de una cadena son comparables entonces $x \wedge y = \min\{x, y\}$ y $x \vee y = \max\{x, y\}$ existen y pertenecen a $\{x, y\} \subseteq X$. Por lo tanto X es una subretícula de $\mathscr{C}$.

[$\Leftarrow$] Supongamos que todo subconjunto de $\mathscr{C}$ es una subretícula. Tomemos un subconjunto cualquiera con dos elementos $\{x, y\}$.

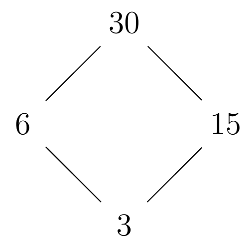
Si $x \wedge y = x$ entonces $x \leq y$, y si $x \wedge y = y$ entonces $y \leq x$. En ambos casos los elementos son comparables. Por lo tanto $\mathscr{C}$ es una cadena. ■

Ejemplo 15

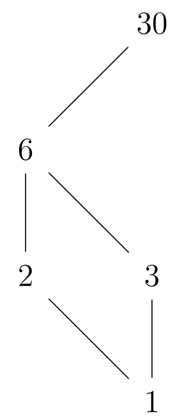
Consideremos la retícula $D(30)$, de divisores de 30:



Son subretículas de $D(30)$:

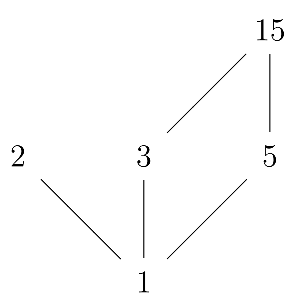


L_1

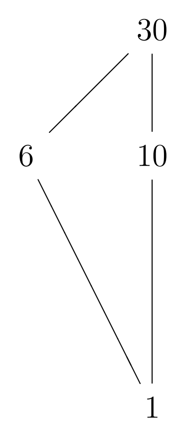


L_2

pero no lo son:



L_3



L_4

Ya que por ejemplo, en L_3 se tiene que $2 \vee 3 = 6 \notin L_3$ y en L_4, $6 \wedge 10 = 2 \notin L_4$.

1.3. Retículas completas

Definición 1.3.1
Una retícula $\mathscr{L}$ es **completa** si cada subconjunto $S \subseteq \mathscr{L}$ tiene supremo e ínfimo en S denotados por $\bigvee S$ y $\bigwedge S$ respectivamente.

Observación 7
Notar que a diferencia de la definición equivalente de retícula, donde un conjunto parcialmente ordenado $\mathscr{L}$ es una retícula si cada subconjunto finito tiene yunta y cuña; en una retícula completa los subconjuntos pueden ser infinitos y no necesariamente finitos.
En una retícula completa $\mathscr{L}$ existe un elemento mayor denotado por $\mathbf{1}$ y un elemento menor denotado por $\mathbf{0}$. Ya que $\mathscr{L}$ es subconjunto de sí mismo y éste tiene supremo e ínfimo.

Ejemplo 16
Si X es un conjunto, entonces la retícula $(\mathcal{P}(X), \subseteq)$, con $\bigvee\{A_i\}_{i\in I} = \bigcup\limits_{i\in I} A_i$ y $\bigwedge\{A_i\}_{i\in I} = \bigcap\limits_{i\in I} A_i$ es completa.

Ejemplo 17
La retícula de subgrupos de un grupo G, $([0, G], \subseteq)$, con $\bigvee\{S_i\}_{i\in I} = \langle\bigcup\limits_{i\in I} S_i\rangle$ y $\bigwedge\{S_i\}_{i\in I} = \bigcap\limits_{i\in I} S_i$ es completa.

Ejemplo 18
La retícula de submódulos de un R-módulo M, $(S_R(M), \subseteq)$, con
$\bigvee\{S_i\}_{i\in I} = \sum\limits_{i\in I} S_i$ y $\bigwedge\{S_i\}_{i\in I} = \bigcap\limits_{i\in I} S_i$ es completa.

Ejemplo 19
$(\mathbb{N}, \leq)$ no es una retícula completa pues $\bigvee \mathbb{N}$ no existe.

Teorema 1.3.1

Un COPO $\mathscr{L}$ es una retícula completa si cada subconjunto de $\mathscr{L}$ tiene yunta.

Demostración:

Para cada subconjunto $S \subseteq \mathscr{L}$ definamos: $B = \{b \in \mathscr{L} | \forall s \in S : b \leq s\}$ el conjunto de las cotas inferiores de S en $\mathscr{L}$. Notar que $B \neq \emptyset$ ya que $\sup\emptyset \in \mathscr{L}$.

Sea x la menor de las cotas superiores de B en $\mathscr{L}$, *i.e.* $x = \sup B \in \mathscr{L}$.

Si $s \in S$ entonces para cada $b \in B$ tenemos que $b \leq s$ entonces $x = \sup B \leq s$.

Si y es cualquier elemento tal que $\forall s \in S : y \leq s$ entonces $y \in B$ y por lo tanto $y \leq \sup B = x$. De aquí tenemos que $x =$ínf S.

Por lo tanto S tiene ínfimo y así $\mathscr{L}$ es una retícula completa. ∎

Observación 8

Dualizando del teorema anterior se tiene que un COPO $\mathscr{L}$ es una retícula completa si cada subconjunto de $\mathscr{L}$ tiene cuña.

Definición 1.3.2

Si $\mathscr{L}$ es una retícula completa entonces una **subretícula completa** $\mathscr{L}'$ de $\mathscr{L}$ es una subretícula tal que $S \subseteq \mathscr{L}'$ implica que $\bigvee S \in \mathscr{L}'$ y $\bigwedge S \in \mathscr{L}'$.

Ejemplo 20

Sean $\mathscr{L}$ una retícula y $a, b \in \mathscr{L}$, el intervalo $[a, b] = \{x \in \mathscr{L} : a \leq x \leq b\}$ es una subretícula completa de $\mathscr{L}$.

Ejemplo 21

Si $\mathscr{L}$ una retícula, un subconjunto $I \subseteq \mathscr{L}$ es llamado **ideal** si éste satisface:

(i) Si $a \in I$ y $x \in \mathscr{L}$ tal que $x \leq a$ entonces $x \in I$.

(ii) Si $a, b \in I$ entonces $a \vee b \in I$.

(iii) Si $\mathscr{L}$ tiene $\mathbf{0}$ entonces $\mathbf{0}\in I$.

Dualmente definimos un **filtro** como un subconjunto $F \subseteq \mathscr{L}$ tal que satisface:

(i) Si $a \in F$ y $x \in \mathscr{L}$ tal que $a \leq x$ entonces $x \in F$.

(ii) Si $a, b \in F$ entonces $a \wedge b \in F$.

(iii) Si $\mathscr{L}$ tiene **1** entonces $\mathbf{1} \in F$.

Los ideales y los filtros son subretículas completas.

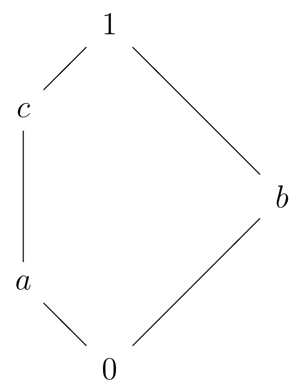
Capítulo 2

Retículas modulares

Dedekind observó que los grupos aditivos de un anillo y los subgrupos normales de un grupo forman retículas de una forma natural y que esas retículas tienen una propiedad especial, a la cual nos referiremos como ley modular. La modularidad es una consecuencia de la distributividad, y la observación de Dedekind dio como resultado ejemplos de retículas que son modulares pero no necesariamente distributivas, por ejemplo la retícula de submódulos de un módulo. La modularidad es la generalización más conocida de distributividad.

En el Lema 1.2.2 inciso (vi) vimos que para cualquier retícula $\mathscr{L}$ se cumple que $a, b \in \mathscr{L}$ y $a \leq c$ entonces $a \vee (b \wedge c) \leq (a \vee b) \wedge c$. Pero no necesariamente se tiene que $a \vee (b \wedge c) \geq (a \vee b) \wedge c$. Para precisar más esto definamos lo siguiente.

Definición 2.0.1
La retícula del **pentágono** (N_5) es una retícula de cinco elementos $0, a, b, c, 1$ tales que $0 < a < c < 1$, $0 < b < 1$ y $a \| b$, $b \| c$. Es decir, la podemos representar con el siguiente diagrama:



Proposición 2.0.1
La retícula del pentágono no cumple la propiedad de que si $a, b \in N_5$ y $a \leq c$ entonces $a \vee (b \wedge c) \geq (a \vee b) \wedge c$.

<u>Demostración:</u>
Supongamos que se cumple la desigualdad. Basados en el diagrama anterior tenemos que $a \leq c$ pero $c = (a \vee b) \wedge c \leq a \vee (b \wedge c) = a$ entonces tenemos que $c \leq a$ y esto implicaría que $a = c$ pero claramente esto no es cierto. ■

La proposición anterior demuestra que existen retículas en las que no se da la propiedad de que para elementos a, b, c en dichas retículas $a \leq c$ implique que $a \vee (b \wedge c) = (a \vee b) \wedge c$. Esto nos hace preguntarnos qué retículas cumplen esta igualdad, para ello definamos lo siguiente.

Definición 2.0.2
Una retícula $\mathscr{L}$ es llamada **modular** si para $a, b, c \in \mathscr{L}$, con $a \leq c$, se cumple que:

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

Observación 9

Una subretícula de una retícula modular también es una retícula modular.

Ejemplo 22

Si G es un grupo, entonces la retícula de subgrupos normales de G, $N(G)$, es una retícula modular.

Ejemplo 23

La retícula de ideales de $\mathbb{Z}$ es una retícula modular.

Ejemplo 24

La retícula $S_R(M)$ de submódulos de un R-módulo es una retícula modular.

Demostración:

Sean $K, L, N \in S_R(M)$ tales que $N \leq L$.

Queremos demostrar que $N + (K \cap L) = (N + K) \cap L$, pero ya hemos demostrado una desigualdad para cualquier retícula, es decir, ya sabemos que se cumple:

$$(K \cap L) + N \leq (K + N) \cap L.$$

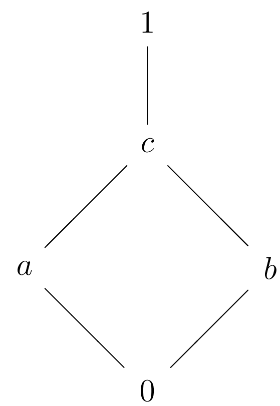
Así que basta demostrar que se cumple la desigualdad recíproca.

Sea $x \in (K+N) \cap L$ entonces $x = y+z$ con $y \in K$, $z \in N$ y $x \in L$. Entonces $y = x - z \in K \cap L \subseteq (K \cap L) + N$. Por lo tanto $(K+N) \cap L = (K \cap L) + N$.

$\blacksquare$

Ejemplo 25

Las siguiente retícula es modular:



A continuación daremos una equivalencia a la propiedad que tienen las retículas modulares.

Teorema 2.0.1

Una retícula $\mathscr{L}$ es modular si y sólo si para $a, b, c \in \mathscr{L}$ tales que $a \leq c$, $a \wedge b = c \wedge b$ y $a \vee b = c \vee b$ implica que $a = c$.

Demostración:

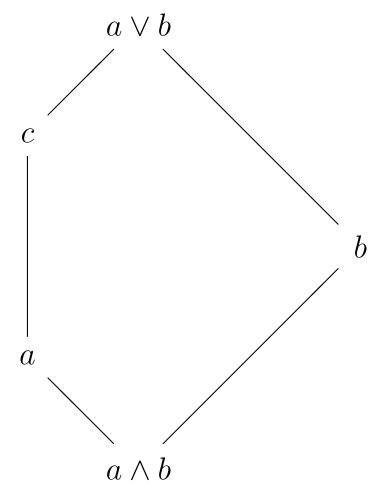
[$\Rightarrow$] Sea $\mathscr{L}$ una retícula modular y $a, b, c \in \mathscr{L}$ tales que $a \leq c$, $a \wedge b = c \wedge b$ y $a \vee b = c \vee b$. Entonces tenemos que $a \vee (b \wedge c) = a \vee (a \wedge b) = a$ por la propiedad de absorción, y por otro lado $(a \vee b) \wedge c = (c \vee b) \wedge c = c$. Como $\mathscr{L}$ es modular entonces tenemos que $a = a \vee (b \wedge c) = (a \vee b) \wedge c$.

[$\Leftarrow$] Supongamos que $a \leq c$ y denotemos por $\alpha = a \vee (b \wedge c)$ y a $\beta = (a \vee b) \wedge c$. Veamos que $\alpha = \beta$.

Sabemos que para toda retícula se cumple la desigualdad $\alpha \leq \beta$, así que tenemos lo siguiente, $a \leq \alpha \leq \beta \leq c$. Demostraremos que $\alpha \wedge b = \beta \wedge b$ y que $\alpha \vee b = \beta \vee b$.

Notemos que $\beta = (a \vee b) \wedge c \leq a \vee b \leq \alpha \vee b \leq \beta \vee b$. Como $b \leq \alpha \vee b$ y $\beta \leq \alpha \vee b$ tenemos que $b \vee \beta \leq \alpha \vee b$ y por lo tanto tenemos que $b \vee \beta = \alpha \vee b$. Dualmente $\alpha \wedge b = \beta \wedge b$.
Así se cumplen las condiciones de la hipótesis y concluimos que $\alpha = \beta$, y por tanto $\mathscr{L}$ es modular. ■

Teorema 2.0.2
Una retícula $\mathscr{L}$ es modular si y sólo si no contiene subretículas isomorfas a N_5.
<u>**Demostración:**</u>
[$\Rightarrow$] Es claro que si $\mathscr{L}$ es una retícula modular no puede tener subretículas no modulares.
[$\Leftarrow$] Supongamos que $\mathscr{L}$ no es modular, usando el teorema anterior, existen tres elementos distintos en $a, b, c \in \mathscr{L}$ tal que $a < c$, $a \wedge b = c \wedge b$ y $a \vee b = c \vee b$ pero entonces el subconjunto $\{a, b, c, a \wedge b, a \vee b\}$ es una retícula isomorfa a N_5.



Lo que es una contradicción, por lo tanto $\mathscr{L}$ es modular. ■

Ejemplo 26
Toda cadena es una retícula modular, ya que todos los elementos de una ca-

dena son comparables y por tanto, ésta no puede tener subretículas isomorfas al pentágono.

Teorema 2.0.3 (2º Teorema de isomorfismos para ret. modulares) Para cualesquiera elementos $a, b \in \mathscr{L}$, de una retícula modular, se tiene que

$$[a \wedge b, a] \cong [b, a \vee b].$$

Demostración:

Sea $\alpha : [b, a \vee b] \longrightarrow [a \wedge b, a]$ donde $\forall x \in [b, a \vee b] : \alpha(x) = a \wedge x$. Para demostrar que α es isomorfismo de retículas demostremos que es morfismo con inversa β.

Sea $\beta : [a \wedge b, a] \longrightarrow [b, a \vee b]$ tal que $\forall y \in [a \wedge b, a] : \beta(y) = y \vee b$.

Sea $x \in [b, a \vee b]$ entonces $a \wedge b \leq \alpha(x) = a \wedge x \leq a$ y por absorción $a = a \wedge (a \vee b)$. Como entre dos retículas una función es isomorfismo de retículas si y sólo si es isomorfismo de orden (por Proposición 1.2.3), demostraremos que α es isomorfismo de orden.

Veamos que $\alpha^{-1} = \beta$.

Como $b \leq x \leq a \vee b$ tenemos que

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

Pero también como $a \wedge b \leq y \leq a$ tenemos que

$$\begin{aligned} \alpha\beta(y) &= a \wedge (y \vee b) \\ &= y \vee (a \wedge b) \\ &= y \end{aligned}$$

ya que $\mathscr{L}$ es modular.

Además α preserva orden ya que si $x, y \in [b, a \vee b]$ y $x \leq y$, entonces $\alpha(x) = x \wedge a \leq y \wedge a = \alpha(y)$. Dualmente β es morfismo de orden. ■

Observación 10

El resultado anterior aplicado a la retículas de submódulos de un módulo M es el **segundo teorema de isomorfismos para módulos**:
Si $A, B \in S_R(M)$ entonces:

$$\frac{A+B}{B} \cong \frac{A}{A \cap B}$$

El 2do teorema de isomorfismos para retículas nos lleva a definir una clase particular de isomorfismos entre intervalos de una retícula modular.

Definición 2.0.3

1.- Dos intervalos de una retícula modular son llamados **similares** si pueden expresarse de la forma $[a \wedge b, a]$, $[b, a \vee b]$ para algunos elementos a, b en la retícula.

2.- Dos intervalos I, J de una retícula modular son **proyectivos** si existe una sucesión de intervalos $I = I_0, I_1, ..., I_{n-1}, I_n = J$ tal que I_{k-1} y I_k sean similares para $1 \leq k \leq n$.

Ejemplo 27

El segundo teorema de isomorfismos para módulos nos asegura que si $[A, B]$ y $[C, D]$ son intervalos proyectivos en $S_R(M)$, entonces $\frac{B}{A} \cong \frac{D}{C}$; pues podemos escribir dos intervalos similares como $[W, X]$ y $[Y, Z]$, donde $W = X \cap Y$ y $Z = X + Y$ de tal manera que $\frac{X}{W} \cong \frac{Z}{Y}$.

Para lo siguiente ya no se supone que todas las retículas sean modulares, pero muchos de los resultados que vienen a continuación están relacionados con las retículas modulares, que es el objetivo principal de este trabajo.

2.1. Retículas complementadas

Definición 2.1.1

1.- Sea $\mathscr{L}$ una retícula con 0 y 1. Si $a \in \mathscr{L}$ entonces un **complemento** de a en $\mathscr{L}$ es un elemento $c \in \mathscr{L}$ tal que:

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

Denotamos este hecho por $a \oplus c = 1$.

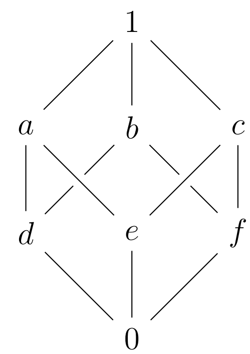
2.- La retícula $\mathscr{L}$ es **complementada** si cada elemento de $\mathscr{L}$ tiene complemento en $\mathscr{L}$.

Ejemplo 28

Sea $S_F(V)$ la retícula de subespacios de un F-espacio vectorial V. Si $W \leq V$ y γ es una base de W, entonces la podemos extender a una base β de V.
Sea $\langle \beta - \gamma \rangle = W'$. Veamos que W' es un complemento de W.
Primero notamos que $V = W + W'$ pues $\beta \subseteq W + W'$. Si $x \in W \cap W'$ tal que $x \neq 0$ entonces $x = a_1\gamma_{i_1} + ... + a_n\gamma_{i_n =} b_1\beta_{j_1} + ... + b_m\beta_{j_m}$ con $a_i, b_j \in F$, $a_1 \neq 0$, $\gamma_{i_k} \in \gamma$ y $\beta_{j_l} \in \beta - \gamma$. Si despejamos γ_{i_1} observamos que se encuentra en $\langle (\beta - \gamma) \cup \{\gamma_{i_2}, ..., \gamma_{i_n}\} \rangle$, lo que contradice que β es linealmente independiente.
Por lo que tenemos que $W \cap W' = 0$ y $W + W' = V$ y por lo tanto $W \oplus W' = V$.

Ejemplo 29

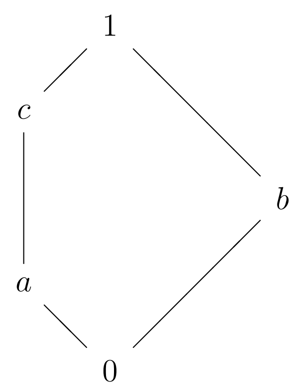
La retícula



es una retícula complementada.

Ejemplo 30

En la retícula N_5, b tiene dos complementos.



Observación 11

Sea $N \leq M$ es un complemento en $S_R(M)$ si y sólo si N es sumando directo de M.

Proposición 2.1.1

Si $\mathscr{L}$ es una retícula modular complementada, entonces cada intervalo de $\mathscr{L}$ es complementado.

Demostración:

Sean $a, b \in \mathscr{L}$ tal que $a \leq b$ y $d \in [a, b]$. Sea $c \in \mathscr{L}$ un complemento de d, *i.e.*, $d \wedge c = 0$ y $d \vee c = 1$, entonces, por modularidad, se tiene que $a \vee (c \wedge b) = (a \vee c) \wedge b$.

Veamos que $a \vee (c \wedge b) = b \wedge (a \vee c)$ es un complemento de d en $[a, b]$. Sabemos que $\mathscr{L}$ es modular, entonces, como $a \leq d$ tenemos que $(a \vee (c \wedge b)) \wedge d = a \vee ((c \wedge b) \wedge d) = a \vee 0 = a$.

Por otra parte, como $d \leq b$ tenemos que $((a \vee c) \wedge b) \vee d = ((a \vee c) \vee d) \wedge b = 1 \wedge b = b$.

Por lo tanto d tiene complemento en $[a, b]$ y así cada intervalo de $\mathscr{L}$ es complementado. ■

Proposición 2.1.2

La retícula $\mathscr{L}$ es modular si y sólo si cada intervalo I de $\mathscr{L}$ tiene la siguiente propiedad:

Si $c \in I$ tiene dos complementos $a, b \in I$ con $a \leq b$ entonces $a = b$.

Demostración:

[$\Rightarrow$] Supongamos que $\mathscr{L}$ es modular. Sean $I = [x, y]$ un intervalo de $\mathscr{L}$ y $a, b \in I$, tales que $a \leq b$, complementos de c en I. Entonces, como $a \leq b$ y por modularidad, tenemos:

$$b = b \wedge y = b \wedge (a \vee c) = a \vee (b \wedge c) = a \vee x = a.$$

[$\Leftarrow$] Si $a, b \in \mathscr{L}$ tales que $a \leq b$ entonces, por Lema 1.2.2, tenemos que

$$\alpha = a \vee (b \wedge c) \leq (a \vee c) \wedge b = \beta$$

Demostremos que α y β son complementos de c en el intervalo $[b \wedge c, a \vee c]$.

Como $b \wedge c \leq c$, tenemos

$$\begin{aligned} \alpha \wedge c &= ((c \wedge b) \vee a) \wedge c \\ &\geq (c \wedge a) \vee (c \wedge b) \\ &= c \wedge b && \text{por Lema 1.2.2, } (i). \end{aligned}$$

Así $\alpha \wedge c \geq c \wedge b$.

Pero también observamos que $\alpha \leq b$ y esto implica que $\alpha \wedge c \leq c \wedge b$ y por lo tanto tenemos que $\alpha \wedge c = c \wedge b$. Y también $\alpha \vee c = ((c \wedge b) \vee a) \wedge c = (c \wedge a) \vee (c \wedge b) = a \vee c$.

Por otra parte tenemos también que $\beta \wedge c = (c \vee a) \wedge b \wedge c = b \wedge c$ y además

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

y como $a \leq \beta$ tenemos que $\beta \vee c = a \vee c$.

En resumen tenemos que:

$\alpha \wedge c = c \wedge b = \beta \wedge c$ y además $\alpha \vee c = a \vee c = \beta \vee c$.

Así α y β son complementos de c en $[b \wedge c, a \vee c]$, y, como $\alpha \leq \beta$, por la hipótesis concluimos que $\alpha = (a \wedge b) \vee a = (c \vee a) \wedge b = \beta$, *i.e.*, se cumple la modularidad. ■

2.2. Retículas con condiciones de cadena

Definición 2.2.1

1.- Sea $\mathscr{L}$ una retícula modular y completa. Dos cadenas

$$a = a_0 \leq a_1 \leq ... \leq a_m = b$$

$$a = b_0 \leq b_1 \leq ... \leq b_n = b$$

entre el mismo par de elementos $a, b \in \mathscr{L}$ son llamadas **equivalentes** si $m = n$ y existe una permutación π de $\{1, ..., n\}$ tal que los intervalos $[a_{i-1}, a_i]$ y $[b_{\pi(i)-1}, b_{\pi(i)}]$ son proyectivos.

2.- Un **refinamiento** de una cadena $a = a_0 \leq a_1 \leq ... \leq a_m = b$ se obtiene por la inserción de nuevos elementos en la cadena.

Teorema 2.2.1 (Del refinamiento de Schreier)
Cualesquiera dos cadenas finitas entre el mismo par de elementos de una retícula modular tienen refinamientos equivalentes.

Demostración:
Sean $\mathscr{L}$ una retícula modular, dos elementos $a, b \in \mathscr{L}$ y dos cadenas finitas

$$a = a_0 \leq a_1 \leq ... \leq a_m = b \qquad \textbf{(1)}$$

$$a = b_0 \leq b_1 \leq ... \leq b_n = b \qquad \textbf{(2)}$$

Para cada $i = 1, ..., m$ y $j = 1, ..., n$ sean:

$$a_{ij} = (a_i \wedge b_j) \vee b_{j-1} = (a_i \vee b_{j-1}) \wedge b_j$$

$$b_{ij} = (b_j \wedge a_i) \vee a_{i-1} = (b_j \vee a_{i-1}) \wedge a_i$$

Observe que $a_{i-1,j} \wedge (a_i \wedge b_j) = (a_{i-1} \vee b_{j-1}) \wedge b_j \wedge a_i \wedge b_j = (a_{i-1} \vee b_{j-1}) \wedge a_i \wedge b_j$.

Mientras que, como $a_{i-1} \wedge b_j \leq a_i$, y por modularidad, tenemos:

$$\begin{aligned} a_{i-1,j} \vee (a_i \wedge b_j) &= (a_{i-1} \wedge b_j) \vee b_{j-1} \vee (a_i \wedge b_j) \\ &= ((a_{i-1} \wedge b_j) \vee (a_i \wedge b_j)) \vee b_{j-1} \\ &= (((a_{i-1} \wedge b_j) \vee b_j) \wedge a_i) \vee b_{j-1} \\ &= (a_i \wedge b_j) \vee b_{j-1} \\ &= a_{ij}. \end{aligned}$$

De lo anterior tenemos que:

$$a_{i-1,j} \wedge (a_i \wedge b_j) = (a_{i-1} \vee b_{j-1}) \wedge a_i \wedge b_j \text{ y también}$$

$$a_{i-1,j} \vee (a_i \wedge b_j) = (((a_{i-1} \wedge b_j) \vee b_j) \wedge a_i) \vee b_{j-1} = (a_i \wedge b_j) \vee b_{j-1} = a_{ij}.$$

Por lo tanto los intervalos

$$[(a_{i-1} \vee b_{j-1}) \wedge a_i \wedge b_j, a_i \wedge b_j] \qquad \textbf{(3)}$$

y

$$[(a_{i-1} \vee b_{j-1}) \wedge b_j, (a_i \wedge b_j) \vee b_{j-1}] = [a_{i-1,j}, a_{ij}]$$

son similares.
Simétricamente el intervalo **(3)** es similar a $[b_{j-1}, b_{ji}]$. Por lo tanto $[b_{j-1,i}, b_{ji}]$ es proyectivo a $[a_{i-1,j}, a_{ij}]$.

Así obtenemos:

$$a = a_{01} \leq a_{11} \leq ... \leq a_{m1} \leq a_{12} \leq ... \leq a_{mn} = b$$

$$a = b_{01} \leq b_{11} \leq ... \leq b_{n1} \leq b_{12} \leq ... \leq b_{nm} = b$$

donde $b_{ni} = a_i = a_{0,i+1}$ y $a_{mj} = b_j = a_{0,j+1}$ son equivalentes y son refinamientos de **(1)** y **(2)** respectivamente. ■

Definición 2.2.2

Una **cadena de composición**, entre dos elementos a y b de una retícula, es una cadena $a = a_0 < a_1 < ... < a_m = b$ que no tiene refinamientos excepto repeticiones de elementos dados a_i. El entero m es la **longitud de la cadena**.

Una implicación inmediata del Teorema del refinamiento de Schreier es la siguiente:

Corolario 2.2.1 (Teorema de Jordan-Hölder para retículas)
Cualesquiera dos cadenas de composición entre el mismo par de elementos de una retícula modular son equivalentes.

La versión del Teorema de Jordan-Hölder para módulos es la siguiente:

Teorema 2.2.2 (de Jordan-Hölder para módulos)
Cualesquiera dos cadenas finitas de un módulo tienen refinamientos isomorfos.

Definición 2.2.3
Una retícula modular y completa $\mathscr{L}$ es de **longitud finita** si existe una cadena de composición entre 0 y 1. La **longitud de** $\mathscr{L}$ es la longitud de la cadena de composición entre 0 y 1.

Definición 2.2.4

1.- Una retícula $\mathscr{L}$ es **noetheriana** (o satisface la CCA) si no existe una cadena estrictamente ascendente $a_0 < a_1 < ...$ en $\mathscr{L}$.

2.- Una retícula $\mathscr{L}$ es **artiniana** (o satisface la CCD) si no existe una cadena estrictamente descendente $a_0 > a_1 > ...$ en $\mathscr{L}$.

Proposición 2.2.1
Una retícula $\mathscr{L}$ es noetheriana (artiniana) si y sólo si cada subconjunto no vacío de $\mathscr{L}$ tiene un elemento máximo (mínimo).

<u>**Demostración:**</u>

Ver Teorema 1.1.1. ■

Proposición 2.2.2

Toda retícula noetheriana tiene elemento mayor. Dualmente, toda retícula artiniana tiene elemento menor.

<u>**Demostración:**</u>

Sea $\mathscr{L}$ una retícula noetheriana y m un elemento máximo en $\mathscr{L}$. Entonces para cada elemento $a \in \mathscr{L}$ se tiene que $m \leq m \vee a$. Como m es máximo en $\mathscr{L}$ tenemos que $m = m \vee a$ por lo que $a \leq m$. Por lo tanto m es elemento mayor en en $\mathscr{L}$. ■

Proposición 2.2.3

Sea $\mathscr{L}$ una retícula modular complementada. Si $a < b$ entonces no existe elemento tal que sea complemento de a y b.

<u>**Demostración:**</u>

Demostremos esta proposición por reducción al absurdo. Supongamos que existe $c \in \mathscr{L}$ tal que c es complemento de a y de b en $\mathscr{L}$ tales que $a < b$, es decir, $a \vee c = 1 = b \vee c$ y $a \wedge c = 0 = b \wedge c$. Por el Lema 1.2.2 obtenemos de lo anterior que $a = b$, lo que contradice que $a < b$. Por lo tanto no hay elemento en $\mathscr{L}$ que sea complemento de a y b en $\mathscr{L}$. ■

Proposición 2.2.4

Sea $(\mathscr{L}, \leq)$ un COPO tal que cada subconjunto no vacío tiene supremo (ínfimo). Las siguientes proposiciones son equivalentes:

(i) $\mathscr{L}$ es una retícula noetheriana (artiniana).

(ii) Para cada subconjunto $\emptyset \neq A \subseteq \mathscr{L}$ existe un subconjunto finito $F \subseteq A$ tal que $\bigvee A = \bigvee F$ $(\bigwedge A = \bigwedge F)$.

<u>**Demostración:**</u>

[$(i) \Rightarrow (ii)$] Sean $\mathscr{L}$ una retícula noetheriana y $\mathscr{F} = \{\bigvee F | F \subseteq A$ y F es finito$\}$. Como $\mathscr{L}$ es noetheriana existe un elemento máximo $\bigvee F_0 \in \mathscr{F}$. Es claro que $\bigvee F_0 \leq \bigvee A$.
Además si $a \in A$, por maximalidad, $\bigvee F_0 = (\bigvee F_0) \vee a$ lo que implica que $a \leq \bigvee F_0$. Entonces $\bigvee A \leq \bigvee F_0$ y por tanto $\bigvee A = \bigvee F_0$.

[$(ii) \Rightarrow (i)$] Sea $a_1 \leq a_2 \leq ... \leq a_n \leq ...$ una sucesión no decreciente en $\mathscr{L}$. Sea $A = \{a_1, a_2, ..., a_n, ...\}$, por la hipótesis existe $F \subseteq A$ finito, tal que $\bigvee A = \bigvee F$, *i.e.* existe un elemento $n_0 \in \mathbb{N}$ tal que $\bigvee\limits_{n \in \mathbb{N}} a_n = \bigvee\limits_{n=1}^{n_0} a_n = a_{n_0}$. Entonces $\forall n \in \mathbb{N}$ tal que $n_0 < n$ se tiene que $\bigvee\limits_{n_0 < n} a_n \leq a_{n_0}$ o $a_n = a_{n_0}$, lo que demuestra que $\mathscr{L}$ es noetheriana. Dualmente para el caso artinitano. ■

Proposición 2.2.5

Una retícula modular y completa es de longitud finita si y sólo si es noetheriana y artiniana.

<u>**Demostración:**</u>

[$\Rightarrow$] Sea $\mathscr{L}$ una retícula modular tal que su longitud es m, entonces cada cadena estrictamente ascendente (o estrictamente descendente) en $\mathscr{L}$ tiene a lo más $m + 1$ elementos, entonces $\mathscr{L}$ es noetheriana y artiniana.
[$\Leftarrow$] Supongamos que $\mathscr{L}$ es noetheriana y artiniana. Entonces para cada $a \neq 0$ en $\mathscr{L}$ existe, por la Proposición 2.2.1, un elemento máximo b tal que $a < b$. Si repetimos este proceso, generamos una cadena descendente $1 > a_1 > a_2 > ...$ Como $\mathscr{L}$ también es artiniana, esta cadena se estaciona después de un número finito de pasos. Es decir, obtenemos una cadena $1 > a_1 > a_2 > ... > 0$, la cual es una cadena de composición. Por tanto $\mathscr{L}$ es de longitud finita. ■

Proposición 2.2.6

Sea a un elemento de una retícula modular y completa $\mathscr{L}$. Entonces $\mathscr{L}$ es noetheriana (artiniana) si y sólo si los intervalos $[0, a]$ y $[a, 1]$ son noetherianos (artinianos).

<u>**Demostración:**</u>

[$\Rightarrow$] Si $\mathscr{L}$ es noetheriana o artiniana, cada intervalo de $\mathscr{L}$ es noetheriano o artiniano.

[$\Leftarrow$] Supongamos que $[0,a]$ y $[a,1]$ son noetherianos y sea $b_1 < b_2 < ...$ una cadena estrictamente ascendente en $\mathscr{L}$.

Entonces existe un entero n tal que

$$b_n \wedge a = b_{n+1} \wedge a = c \in [0,a] \Rightarrow 0 \leq c \leq a$$

$$b_n \vee a = b_{n+1} \vee a = d \in [a,1] \Rightarrow a \leq d \leq 1$$

entonces $c \leq a \leq d$ y por tanto $a \in [c,d]$.

Notar que b_n y b_{n+1} son complementos de a en $[c,d]$. Como $\mathscr{L}$ es modular y $b_n \leq b_{n+1}$ podemos hacer uso de la Proposición 2.1.2 y así $b_n = b_{n+1}$.

Por lo tanto $\mathscr{L}$ debe ser noetheriana. Dualmente para el caso artiniano. ■

Ejemplo 31

Si M es un módulo. Una cadena de composición entre $\{0\}$ y M en $S_R(M)$ es una cadena de submódulos $\{0\} = M_0 \subset M_1 \subset ... \subset M_n = M$ tal que cada módulo cociente M_i/M_{i-1} es simple.

Como caso particular: tomemos la cadena de composición

$0 \leq \mathbb{Z}_2 \leq \mathbb{Z}_4 \leq \mathbb{Z}_8 \leq ... \leq \mathbb{Z}_{2^n}$. Notar que $\mathbb{Z}_{2^n}/\mathbb{Z}_{2^{n-1}} \cong \mathbb{Z}_2$, pero 2 es primo y entonces $\mathbb{Z}_2$ es campo, por lo tanto $\mathbb{Z}_2$ es simple.

Ejemplo 32

Un espacio vectorial V es de longitud finita si y sólo si es de dimensión finita y su longitud es la dimensión de V.

2.3. Retículas distributivas

La Teoría de Retículas evolucionó en el siglo XIX a través de los trabajos de George Boole, Charles Saunders Pierce y Ernst Schröder , y después con los trabajos de Richard Dedekind, Garret Birkhoff, Oystein Ore, John von Neumann, y otros durante la primera mitad del siglo XX. Boole estableció los fundamentos para las álgebras que llevan su nombre.

Recordemos que en cualquier retícula $\mathscr{L}$, si $a, b, c \in \mathscr{L}$ siempre se cumple que

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

Pero la otra desigualdad no siempre se tiene por lo que surge otro concepto que definiremos a continuación.

Definición 2.3.1
Una retícula $\mathscr{L}$ es **distributiva** si para cualesquiera $a, b, c \in \mathscr{L}$ se cumple que

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

Proposición 2.3.1
Toda retícula distributiva es modular.
<u>**Demostración:**</u>
Sea $\mathscr{L}$ es una retícula distributiva y $a, b, c \in \mathscr{L}$ tal que $a \leq c$, entonces $(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c) = a \vee (b \wedge c)$. ■

También se puede definir una retícula distributiva de la siguiente manera.

Lema 2.3.1
Una retícula $\mathscr{L}$ es distributiva si y sólo si para cualesquiera $a, b, c \in \mathscr{L}$ se

cumple que $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$ y por tanto se cumple la igualdad $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

Demostración:

[⇒] Supongamos que $\mathscr{L}$ es una retícula distributiva, entonces

$$\begin{aligned}
(a \vee b) \wedge (a \vee c) &= a \vee ((a \vee b) \wedge c)) && \text{Proposición 2.3.1 y } a \leq a \vee b \\
&= a \vee ((a \wedge c) \vee (b \wedge c) && \text{por distributividad} \\
&= (a \vee (a \wedge c)) \vee (b \wedge c) && \text{por asociatividad} \\
&= a \vee (b \wedge c) && \text{por absorción.}
\end{aligned}$$

[⇐]

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

■

Proposición 2.3.2

Toda cadena es una retícula distributiva.

Demostración:

Sean a, b, c elementos de una cadena, entonces tenenemos seis posibilidades: $a \leq b \leq c$, $a \leq c \leq b$, $b \leq a \leq c$, $b \leq c \leq a$, $c \leq a \leq b$ y $c \leq b \leq a$. En cualquiera de los casos se tiene que $(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$. ■

Observación 12

La clase de retículas distributivas es cerrada bajo subretículas, es decir, una subretícula de una retícula distributiva también es una retícula distributiva.

Veamos una caracterización para las retículas distributivas que nos ayudará para demostrar algunas propiedades.

Teorema 2.3.1
$\mathscr{L}$ es una retícula distributiva si y sólo si para cualesquiera $a, b, c \in \mathscr{L}$: $a \wedge c = b \wedge c$, $a \vee c = b \vee c \Rightarrow a = b$.

Demostración:

[⇒] Supongamos que $\mathscr{L}$ es una retícula distributiva y sean $a, b, c \in \mathscr{L}$ tales que $a \wedge c = b \wedge c$ y $a \vee c = b \vee c$.

Entonces:

$$
\begin{aligned}
a &= a \wedge (a \vee c) && \text{por absorción} \\
&= a \wedge (b \vee c) && \text{por hipótesis} \\
&= (a \wedge b) \vee (a \wedge c) && \text{por distributividad} \\
&= (a \wedge b) \vee (b \wedge c) && \text{por hipótesis} \\
&= b \wedge (a \vee c) && \text{por distributividad} \\
&= b \wedge (b \vee c) && \text{por absorción} \\
&= b
\end{aligned}
$$

[⇐] Supongamos que $\forall a, b, c \in \mathscr{L} : a \wedge c = b \wedge c$, $a \vee c = b \vee c \Rightarrow a = b$. Por el Teorema 2.0.1 tenemos que $\forall a, b, c \in \mathscr{L} : a \leq c$, $a \wedge b = b \wedge c$, $a \vee b = b \vee c \Rightarrow a = c$ es equivalente a que $\mathscr{L}$ sea modular. Por lo tanto $\mathscr{L}$, con la hipótesis, es modular. De aquí que $a \wedge b \leq a \vee b$ implica que $(a \wedge b) \vee (c \wedge (a \vee b)) = ((a \wedge b) \vee c) \wedge (a \vee b)$ y $b \wedge c \leq b \vee c$ implica que $(b \wedge c) \vee (a \wedge (b \vee c)) = ((b \wedge c) \vee a) \wedge (b \vee c)$.

Sean $\alpha = (a \wedge b) \vee (c \wedge (a \vee b))$ y $\beta = (b \wedge c) \vee (a \wedge (b \vee c))$.

Demostremos que $\alpha \wedge b = \beta \wedge b$.

Como $a \wedge b \leq b$,

$$\begin{aligned}
\alpha \wedge b &= ((a \wedge b) \vee (c \wedge (a \vee b))) \wedge b \\
&= (a \wedge b) \vee ((c \wedge (a \vee b)) \wedge b) && \text{por modularidad} \\
&= (a \wedge b) \vee (c \wedge ((a \vee b) \wedge b)) && \text{por asociatividad} \\
&= (a \wedge b) \vee (c \wedge b). && \text{por absorción}
\end{aligned}$$

Similarmente, como $b \wedge c \leq b$,

$$\begin{aligned}
\beta \wedge b &= ((b \wedge c) \vee (a \wedge (b \vee c))) \wedge b \\
&= (b \wedge c) \vee ((a \wedge (b \vee c)) \wedge b) && \text{por modularidad} \\
&= (b \wedge c) \vee (a \wedge ((b \vee c) \wedge b)) && \text{por asociatividad} \\
&= (b \wedge c) \vee (a \wedge c). && \text{por absorción}
\end{aligned}$$

Por lo tanto $\alpha \wedge b = \beta \wedge b$. Dualmente se demuestra $\alpha \vee b = \beta \vee b$.

Ahora, por hipótesis concluimos que $\alpha = \beta$ y entonces $\alpha \wedge a = \beta \wedge a$. Además

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

y también

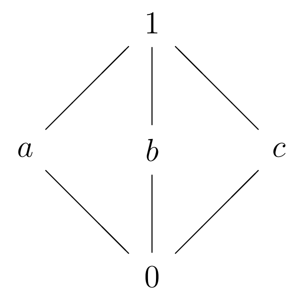
$$\begin{aligned}
\beta \wedge a &= a \wedge ((b \wedge c) \vee a) \wedge (b \vee c) \\
&= a \wedge (b \vee c).
\end{aligned}$$

Finalmente $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ y por lo tanto $\mathscr{L}$ es distributiva.

■

Definición 2.3.2

La retícula del **diamante**, denotada por $\mathbf{M_5}$, donde $M_5 = \{0, a, b, c, 1\}$, es la retícula representada por el siguiente diagrama:



Proposición 2.3.3

M_5 no es una retícula distributiva.

<u>**Demostración:**</u>

Demostremos esto por reducción al absurdo. Supongamos que M_5 es distributiva.

Siguiendo el diagrama observamos que $a \wedge c = 0 = b \wedge c$ y que $a \vee c = 1 = b \vee c$, como estamos suponiendo que M_5 es distributiva y por el Teorema 2.3.1, tenemos que $a = b$. Lo que claramente no ocurre y por tanto genera una contradicción. Por lo tanto M_5 no es distributiva. ∎

Veamos otra equivalencia de retículas distributivas.

Teorema 2.3.2

$\mathscr{L}$ es una retícula distributiva si y sólo si es modular y no contiene subretículas isomorfas a M_5.

<u>**Demostración:**</u>

[$\Rightarrow$] Por la proposición anterior $\mathscr{L}$ no puede contener subretículas isomorfas al diamante. Además,por la Proposición 2.3.1, toda retícula distributiva es modular.

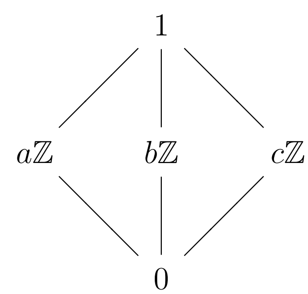
[$\Leftarrow$] Demostremos esta parte por contrapositiva, es decir, vamos a demostrar que si $\mathscr{L}$ no es distributiva, entonces $\mathscr{L}$ no es modular o $\mathscr{L}$ contiene una subretícula isomomorfa a M_5.
Supongamos que que $\mathscr{L}$ es modular y que no es distributiva y veamos que así $\mathscr{L}$ tiene una subretícula isomorfa al diamante.
Como $\mathscr{L}$ no es distributiva, existen $a, b, c \in \mathscr{L}$ tales que $a \neq b$, $b \wedge c = a \wedge c$, $a \vee c = b \vee c$, entonces $a \| b$, ya que si $a \leq b$, por Teorema 2.0.1, se tendría que $a = b$, lo cual es una contradicción.
Veamos que $a \| c$. Supongamos que $a \leq c$, entonces $c = a \vee c = b \vee c$, por lo tanto $b \leq c$, con lo que $a = a \wedge c = b \wedge c = b$, entonces $a = b$, lo que contradice la hipótesis. Si $c \leq a$ entonces $c = a \wedge c = b \wedge c$, también $c \leq b$ y $a = a \vee c = b \vee c = b$, que también es una contradicción. Por lo tanto $a \| c$.
Si intercambiamos a "a" por "b" en las desigualdades anteriores, también se cumplen, y por lo tanto tenemos que se cumple $b \| c$.
En resumen tenemos: $a \| c$, $b \| c$ y $a \| b$, entonces podemos construir la retícula $D = \{a \wedge c = b \wedge c, a, b, c, a \vee c = b \vee c\}$ tal que

$$\begin{tikzcd}[arrows=dash]
 & a \vee c = b \vee c \arrow[dl] \arrow[d] \arrow[dr] & \\
a \arrow[dr] & b \arrow[d] & c \arrow[dl] \\
 & a \wedge c = b \wedge c &
\end{tikzcd}$$

que claramente es una subretícua isomorfa al diamante. ∎

Ejemplo 33
La retícula de ideales de $\mathbb{Z}$ es distributiva.
<u>**Demostración:**</u>
Sabemos que los ideales de $\mathbb{Z}$ son de la forma $a\mathbb{Z}$ con $a \in \mathbb{N}$ donde $a\mathbb{Z} \subseteq b\mathbb{Z}$

si y sólo si $b|a$.
La cuña y la yunta están dados por:
$a\mathbb{Z} \wedge b\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} = [a,b]\mathbb{Z}$, donde $[a,b]$ es el mínimo común múltiplo y
$a\mathbb{Z} \vee b\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} = (a,b)\mathbb{Z}$, donde (a,b) es el máximo común divisor.
Notemos que $([0,\mathbb{Z}],\subseteq)$ es una retícula modular pues la retícula de submódulos de un módulo es modular. Supongamos que $([0,\mathbb{Z}],\subseteq)$ no es distributiva, entonces contendría una retícula isomorfa al diamante, es decir, una retícula con diagrama:



Donde $1 = (a,b)\mathbb{Z} = (a,c)\mathbb{Z} = (b,c)\mathbb{Z}$ y $0 = [a,b]\mathbb{Z} = [a,c]\mathbb{Z} = [b,c]\mathbb{Z}$. Entonces $(a,b) = (a,c) = (b,c)$ y $[a,b] = [b,c] = [a,c]$. Como $(a,b)[a,b] = ab$ y $(a,c)[a,c] = ac$, se tiene que $ab = ac$, lo que implica que $b = c$ y por lo tanto $b\mathbb{Z} = c\mathbb{Z}$, lo que es una contradicción. Por lo tanto $([0,\mathbb{Z}],\subseteq)$ es una retícula distributiva. ■

Proposición 2.3.4
Un elemento de una retícula distributiva $\mathscr{L}$ con 0 y 1 puede tener a lo sumo un complemento.
Demostración:
Sean $\mathscr{L}$ una retícula distributiva con 0 y 1 y $a \in \mathscr{L}$. Si a no tiene complemento la proposición que deseamos demostrar es verdadera.
Supongamos entonces que a tiene complementos b y c entonces:

$$c = c \wedge 1 = c \wedge (a \vee b) = (c \wedge a) \vee (c \wedge b) = 0 \vee (c \wedge b) = c \wedge b.$$

Entonces tenemos $c = c \wedge b$ lo que implica que $c \leq b$. Pero también se tiene que:

$$b = b \wedge 1 = b \wedge (a \vee c) = (b \wedge a) \vee (b \wedge c) = 0 \vee (b \wedge c) = b \wedge c.$$

Lo que implica que $b \leq c$ y por tanto $b = c$. ■

Proposición 2.3.5
En una retícula distributiva $\mathscr{L}$, con 0 y 1, los elementos que tienen complemento forman una subretícula.
Demostración:
Sea C el subconjunto de $\mathscr{L}$ de elementos que tienen complemento. Si $a, b \in C$ y $a \oplus a^* = 1 = b \oplus b^*$ entonces, usando la distributividad, $(a \wedge b) \wedge (a^* \vee b^*) = (a \wedge b \wedge a^*) \vee (a \wedge b \wedge b^*) = 0 \vee 0 = 0$. Por otro lado, $(a \wedge b) \vee (a^* \vee b^*) = (a \vee a^* \vee b^*) \wedge (b \vee a^* \vee b^*) = 1 \wedge 1 = 1$. Por lo tanto $(a^* \vee b^*)$ es complemento de $(a \wedge b)$.
Dualmente el complemento de $a \vee b$ es $a^* \wedge b^*$. Por lo tanto, hemos demostrado que $a \wedge b$ y $a \vee b$ pertenecen a C. Por lo tanto C es una subretícula de $\mathscr{L}$.

■

2.3.1. Álgebras booleanas

Definición 2.3.3
Un **álgebra booleana** es una retícula con 0 y 1, distributiva y complementada.

Como toda álgebra booleana es distributiva cada elemento tiene complemento y es único.

Notación 2
Para cada elemento a de un álgebra booleana $\mathscr{L}$ denotamos como a^* al único complemento de a en $\mathscr{L}$.

Observación 13
Una definición equivalente de álgebra booleana es la siguiente:

Sea $\mathscr{L}$ un conjunto, definimos en él dos operaciones binarias "$\vee$" y "$\wedge$" tales que para $a, b, c \in \mathscr{L}$ se cumplen:

1.- $a \vee (b \vee c) = (a \vee b) \vee c$ y $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

2.- $a \vee b = b \vee a$ y $a \wedge b = b \wedge a$.

3.- $a \vee (a \wedge b) = a$ y $a \wedge (a \vee b) = a$.

4.- $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ y $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

5.- Existen $0, 1 \in \mathscr{L}$ tales que para todo $a \in \mathscr{L}$ se cumplen $a \vee 0 = a$, $a \wedge 0 = 0$, $a \vee 1 = 1$ y $a \wedge 1 = a$.

6.- Para cada $a \in \mathscr{L}$ existe $a^* \in \mathscr{L}$ tal que $a \vee a^* = 1$ y $a \wedge a^* = 0$.

Ejemplo 34
El álgebra booleana más simple, a excepción de un álgebra de boole con un elemento, es $\mathbb{Z}_2$. Es fácil observar que $\mathbb{Z}_2$ con $a \wedge b = ab$ y $a \vee b = a + b + ab$ y $a* = 1 - a$ es un álgebra booleana.

Proposición 2.3.6
Sean $\mathscr{L}$ un álgebra booleana y $a, b \in \mathscr{L}$, entonces se cumple que:

(i) $(a^*)^* = a$.

(ii) (**Leyes de De Morgan**) $(a \wedge b)^* = a^* \vee b^*$ y $(a \vee b)^* = a^* \wedge b^*$.

(iii) $b \wedge a = 0$ si y sólo si $b \leq a^*$.

<u>**Demostración:**</u>

(i) Observemos que $(a^*)^*$ y a son complementos de a^*. Como $\mathscr{L}$ es distributiva, entonces los complementos son únicos. Por lo tanto $a = (a^*)^*$.

(ii) Sabemos que $(a \wedge b)^*$ es complemento de $a \wedge b$, así que basta demostrar que $a^* \vee b^*$ es complemento de $a \wedge b$.

Primero tenemos que $(a \wedge b) \wedge (a^* \vee b^*) = (a \wedge b \wedge a^*) \vee (a \wedge b \wedge b^*) = (b \wedge 0) \vee (a \wedge 0) = 0 \vee 0 = 0$.

También se tiene que $(a \wedge b) \vee (a^* \vee b^*) = (a^* \vee b^* \vee a) \wedge (a^* \vee b^* \vee b) = (b^* \vee 1) \wedge (a^* \vee 1) = 1 \wedge 1 = 1$. Por lo tanto $a^* \vee b^*$ es complemento de $a \wedge b$ y por unicidad se obtiene que $(a \wedge b)^* = a^* \vee b^*$.

El otro caso se demuestra de forma dual.

(iii) $[\Rightarrow]$ Tenemos que $b = b \wedge 1 = b \wedge (a^* \vee a) = (b \wedge a^*) \vee (b \wedge a) = (b \wedge a^*) \vee 0 = b \wedge a^*$, lo que implica que $b \leq a^*$.

$[\Leftarrow]$ Si $b \leq a^*$ entonces $b \wedge a \leq a^* \wedge a$ y esto implica que $b \wedge a \leq 0$. Por lo tanto $b \wedge a = 0$ ■

Proposición 2.3.7

Si $\mathscr{L}$ es un álgebra booleana completa, entonces

$$(\bigvee_I a_i) \wedge c = \bigvee_I (a_i \wedge c)$$

y, dualmente,

$$(\bigwedge_I a_i) \vee c = \bigwedge_I (a_i \vee c)$$

se cumplen para cualquier conjunto de índices I y $c \in \mathscr{L}$.

<u>**Demostración:**</u>

Primero observemos que $\forall i \in I : (\bigwedge_I a_i) \vee c$ es una cota superior de $a_i \wedge c$. De aquí que $\bigvee_I (a_i \wedge c) \leq (\bigvee_I a_i) \wedge c$.

Para probar la desigualdad recíproca es suficiente demostrar que para toda cota superior u de $c \wedge a_i$ se cumple que $(\bigvee_I a_i) \wedge c \leq u$.

Sea u una cota superior de $c \wedge a_i$, para toda $i \in I$, es decir se tiene que $\forall i \in I : c \wedge a_i \leq u$ y esto implica que para todo $i \in I$ se cumple que $a_i = a_i \wedge 1 = a_i \wedge (c \vee c^*) = (c \wedge a_i) \vee (c^* \wedge a_i) \leq u \vee c^*$.
Entonces $c \wedge \bigvee\limits_I a_i \leq c \wedge (u \vee c^*) = (c \wedge u) \vee (c \wedge c^*) = c \wedge u \leq u$.
Como $\bigvee\limits_I (c \wedge a_i)$ es cota superior de $c \wedge a_i$ entonces $c \wedge (\bigvee\limits_I a_i) \leq \bigvee\limits_I (c \wedge a_i)$.
Por lo tanto $c \wedge (\bigvee\limits_I a_i) = \bigvee\limits_I (c \wedge a_i)$. ■

Definición 2.3.4

1.- Una **subálgebra** de un álgebra booleana $\mathscr{L}$ es una subretícula $\mathscr{L}'$ de $\mathscr{L}$ tal que $0 \in \mathscr{L}'$ y $a \in \mathscr{L}'$ implica que $a^* \in \mathscr{L}'$.

2.- Un **morfismo entre dos álgebras booleanas** A y B es un morfismo de retículas $\alpha : A \longrightarrow B$, tal que $\alpha(a^*) = \alpha(a)^*$ para toda $a \in A$.

Ejemplo 35
Si S es un conjunto, entonces el conjunto $\mathcal{P}(S)$ de todos los subconjuntos de S es un álgebra booleana. Cada subconjunto de $\mathcal{P}(S)$ que contenga a $\emptyset$ y sea cerrado bajo complementos y uniones finitas es una subálgebra de $\mathcal{P}(S)$.

Las definiciones básicas para tratar el siguiente ejemplo pueden ser consultadas en el Apéndice A.

Ejemplo de Equivalencia de Categorías: SET^{OP} y CABool

En teoría de categorías, una equivalencia de categorías es una relación entre dos categorías que establece que estas categorías son "esencialmente la misma". Hay numerosos ejemplos de equivalencias entre categorías de muchas áreas de las matemáticas. El establecimiento de una equivalencia implica demostrar fuertes similitudes entre las estructuras matemáticas en cuestión. La

equivalencia entre dos categorías preserva objetos terminales, objetos iniciales, epimorfismos, monomorfismos, entre otras propiedades categóricas muy importantes. En algunos casos, estas estructuras pueden parecer no estar relacionadas a un nivel superficial o intuitivo, por lo que la noción es bastante útil y poderosa, se "traducen" teoremas entre diferentes tipos de estructuras matemáticas, sabiendo que el significado esencial de estos teoremas se conserva bajo la traducción.
Si una categoría es equivalente a la opuesta (o dual) de otra categoría, entonces se habla de una dualidad de categorías, y se dice que las dos categorías son dualmente equivalentes.

La categoría **CABool** está definida como sigue:

* Los objetos son álgebras booleanas atómicas completas.

* Los morfismos son morfimos completos, esto es:
  $f : B \longrightarrow C$ es un **morfismo completo** si para cada $A \subseteq B$ se tiene que

  $$f(\bigvee A) = \bigvee\{f(a) : a \in A\} \qquad \text{y} \qquad f(\bigwedge A) = \bigwedge\{f(a) : a \in A\}$$

  Observe que $1 = \bigwedge \emptyset$ y $0 = \bigvee \emptyset$, entonces

  $$f(1) = f(\bigwedge \emptyset) = \bigwedge\{f(a) : a \in \emptyset\} = 1$$
  $$\text{y}$$
  $$f(0) = f(\bigvee \emptyset) = \bigvee\{f(a) : a \in \emptyset\} = 0$$

  por lo que un morfismo completo preserva 0 y 1.

* La composición de morfismos en **CABool** es como en $\mathbb{L}\Game\approx$.

Teorema 2.3.3
La categoría **CABool** es equivalente a $\mathbf{Set}^{\mathbf{OP}}$.

<u>**Demostración:**</u>

Para cada conjunto X, $\mathcal{P}(X)$ es un álgebra booleana atómica y completa. Si $f : Y \longrightarrow X$ es una función, entonces $f^{-1} : \mathcal{P}(X) \longrightarrow \mathcal{P}(Y)$, la cual toma, para cada subconjunto de X, su preimagen bajo f, es un morfismo completo, ya que:

$$f^{-1}(\bigcup A) = \bigcup\{f^{-1}(a) : a \in A\}$$
$$\text{y}$$
$$f^{-1}(\bigcap A) = \bigcap\{f^{-1}(a) : a \in A\}$$

se cumplen. Esto define un funtor $F : \mathbf{Set}^{\mathbf{OP}} \longrightarrow \mathbf{CABool}$, pues si $f : Y \longrightarrow X$ es un morfismo en $\mathbf{Set}^{\mathbf{OP}}$ entonces $F_1(f) : F_0(Y) \longrightarrow F_0(X)$ nos da un morfismo $f^{-1} : \mathcal{P}(X) \longrightarrow \mathcal{P}(Y)$ en $\mathbf{CABool}$ tal que $A \mapsto f^{-1}(A)$ ya que f^{-1} es un morfismo de álgebras booleanas completo.

Ahora bien, dada un álgebra booleana atómica y completa B. Definimos $G(B)$ el conjunto de átomos de B. Dado un morfismo $g : B \longrightarrow C$ tenemos una función $G(g) : G(C) \longrightarrow G(B)$ definida por $G(g)(c)$ es el único $b \in G(B)$ tal que $c \leq g(b)$.

Veamos que esto está bien definido:

(i) Existe un átomo b con $c \leq g(b)$ porque $1_B = \bigvee G(B)$, ya que B es atómica, entonces $1_C = g(1_B) = \bigvee\{g(b) : b \text{ es un átomo}\}$. Para justificar esta parte demostremos lo siguiente:

Si c es un átomo y $c \leq \bigvee A$, donde A es un álgebra booleana completa, entonces existe $a \in A$ con $c \leq a$.

En efecto, por la Proposición 2.3.7 sabemos que en un álgebra booleana completa A se tiene que $(\bigvee_I a_i) \wedge c = \bigvee_I (a_i \wedge c)$, para cualquier conjunto de índices I y $c \in A$. Supongamos que $c \leq \bigvee A$ y que para todo $c \not\leq a$. Como c es un átomo se tiene que $\forall a \in A : c \wedge a = c$ ó $c \wedge c = 0$, pero $c \not\leq a$, entonces $c \wedge a = 0$. Por lo que tenemos que $c = c \wedge (\bigvee A) =$

$c \wedge (\bigvee_{a \in A} a) = \bigvee_{a \in A} (c \wedge a) = 0$. Lo que contradice el hecho de que c es un átomo. Por lo tanto concluimos que existe $a \in A$ tal que $c \leq a$.

(ii) Ahora veamos que $G(g)(c)$ es el único $b \in G(B)$ tal que $c \leq g(b)$.

Supongamos que $c \leq g(b)$ y $c \leq g(b')$, esto implica que:

$$c \leq g(b) \wedge g(b') = g(b \wedge b') = g(0) = 0$$

que claramente es una contradicción, por lo tanto b es único.

Así, hemos definido un funtor $G : \mathbf{CABool} \longrightarrow \mathbf{Set^{OP}}$.

Observemos ahora que los átomos del álgebra booleana $\mathcal{P}(X)$ son precisamente los conjuntos unitarios de X.
Notemos que $GF(X) = \{\{x\} : x \in X\}$ que claramente es isomorfo a X. Por otro lado tenemos que $FG(B) = \mathcal{P}(\{b \in B : b \text{ es átomo}\})$.
Resta demostrar que existe un isomorfismo de álgebras booleanas completo entre $FG(B)$ y B.

Sean X el conjunto de átomos de B y $\alpha : B \longrightarrow FG(B) = \mathcal{P}(X)$ definida por $\alpha(x) = \{a : a \leq x\}$.
Notemos que $\alpha(x) = \{x\}$ si y sólo si x es átomo de B y $\alpha(x)$ y $\alpha(x^*)$ son complementos uno del otro, pues $a \leq 1 = x \vee x^*$, entonces$a \leq x$ ó $a \leq x^*$ lo que implica que $a \in \alpha(x)$ ó $\alpha(x^*)$. Entonces $a \in \alpha(x) \cup \alpha(x^*)$. Por lo tanto $X = \alpha(x) \cup \alpha(x^*)$.
Por otro lado si $a \in \alpha(x) \cap \alpha(x^*)$ entonces $a \leq x$ y $a \leq x^*$, lo que implica que $a \leq x \wedge x^* = 0$. Por lo tanto $\alpha(x) \cap \alpha(x^*) = \emptyset$.

Ahora veamos que α es morfismo de álgebras booleanas.

(i) $\alpha(x^*) = X \setminus \alpha(x)$ por la observación anterior.

(ii) $\alpha(x \vee y) = \{a : a \leq x \vee y\} = \{a : a \leq x \text{ ó } a \leq y\}$, pues a es átomo, y éste último conjunto es igual a $\{a : a \leq x\} \cup \{a : a \leq y\} = \alpha(x) \cup \alpha(y)$.

(*iii*) $\alpha(x \wedge y) = \{a : a \leq x \wedge y\} = \{a : a \leq x \text{ y } a \leq y\} = \alpha(x) \cap \alpha(y)$.

(*iv*) $\alpha(0) = \{a : a \leq 0\} = \emptyset$.

(*v*) $\alpha(1) = \{a : a \leq 1\} = X$.

Por lo tanto α es un morfismo de álgebras booleanas.

Veamos que α es inyectivo.
Supongamos que $\alpha(x) = \emptyset$. Si $x \neq 0$ entonces debe existir un átomo a tal que $a \leq x$, pero esto implica que $\alpha(x) \neq \emptyset$. Por lo tanto $x = 0$ y α es inyectivo.

Por último veamos que α es suprayectivo.
Sean $Y \in \mathcal{P}(X)$ y $y = \bigvee Y$, esto se puede hacer porque B es completa. Entonces $\alpha(y) = \alpha(\bigvee Y) = \bigcup\{\alpha(x) : x \in Y\} = \bigcup\{\{x\} : x \in Y\} = Y$, ya que cada $x \in Y$ es un átomo.
Por lo tanto α es un isomorfismo de álgebras booleanas y por tanto $FG(B)$ y B son isomorfos.

Finalmente $\mathbf{Set}^{\mathbf{OP}}$ y **CABool** son equivalentes. ■

2.4. Retículas continuas

Para esta sección las retículas a las que nos referiremos serán completas.

Definición 2.4.1

1.- Un subconjunto D de una retícula $\mathscr{L}$ es llamado **dirigido superiormente (inferiormente)** si cada subconjunto finito de D tiene una cota superior (inferior) en D.

2.- Una retícula completa $\mathscr{L}$ es llamada **superiormente continua** si para cada $a \in \mathscr{L}$ y cada subconjunto dirigido superiormente $D \subseteq \mathscr{L}$ se tiene que

$$(\bigvee D) \wedge a = \bigvee_D (d \wedge a)$$

3.- Si la retícula dual $\mathscr{L}^{OP}$ es superiormente continua entonces decimos que $\mathscr{L}$ es **inferiormente continua**.

4.- $\mathscr{L}$ es continua si es superior e inferiormente continua.

Teorema 2.4.1
Si $\mathscr{L}$ es una retícula modular y complementada, entonces $\mathscr{L}$ es superiormente continua si y sólo si $D \subseteq \mathscr{L}$ es un subconjunto dirigido superiormente y existe $c \in \mathscr{L} \setminus \{0\}$ tal que

$$\forall d \in D : c \wedge d = 0 \Longrightarrow \bigvee D < 1$$

Demostración:
[⇒] Supongamos que $\mathscr{L}$ es retícula superiormente continua y $c \in \mathscr{L} \setminus \{0\}$ tal que $\forall d \in D : c \wedge d = 0$, entonces:

$$(\bigvee D) \wedge c = \bigvee_D (d \wedge c) = 0$$

Si $\bigvee D = 1$ entonces $(\bigvee_D d) \wedge c = 1 \wedge c = c = 0$ pero por hipótesis $c \neq 0$. Por lo tanto $\bigvee D \neq 1$.
[⇐] Sean $a \in \mathscr{L}$ y $D \subseteq \mathscr{L}$ un subconjunto dirigido superiormente.
Como para cada $d \in D$ tenemos que $d \wedge a \leq \bigvee D \wedge a$ tenemos que:

$$\bigvee_D (d \wedge a) \leq (\bigvee D) \wedge a$$

Por la proposición 2.1.1 sabemos que en toda retícula modular y complementada todo intervalo es complementado por tanto existe $c \in [0, (\bigvee D) \wedge a]$ tal que c es complemento de $\bigvee_D (d \wedge a)$ en dicho intervalo. Es decir:

$$\bigvee_D (d \wedge a) \vee c = (\bigvee D) \wedge a \qquad \textbf{(1)}$$

$$\text{y también } (\bigvee_D (d \wedge a)) \wedge c = 0.$$

Por otro lado, sea $b \in \mathscr{L}$ un complemento de $\bigvee D$ en $\mathscr{L}$, entonces:

$$(\bigvee D) \vee b = 1 \text{ y } (\bigvee D) \wedge b = 0.$$

Así, para cada $d \in D$ tenemos, por modularidad y por el hecho de que $d \leq \bigvee D$, que:

$(d \vee b) \wedge \bigvee D = d \vee (b \wedge (\bigvee D)) = d \vee 0 = d$, pues b es complemento de $\bigvee D$.

Entonces $(d \vee b) \wedge \bigvee D \wedge c = d \wedge c$. Como $c \in [0, (\bigvee D) \wedge a]$ entonces $c \leq (\bigvee D) \wedge a \leq a$.
Por lo tanto $d \wedge c = d \wedge c \wedge a = (d \wedge a) \wedge c \leq \bigvee_D (d \wedge a) \wedge c = 0$, entonces $(d \vee b) \wedge c = 0$, pues c es complemento de $\bigvee_D (d \wedge a)$.

Hemos llegado a que $(d \vee b) \wedge \bigvee D \wedge c = d \wedge c = 0$. Usando la hipótesis, si $c \neq 0$ entonces $1 = (\bigvee D) \vee b = \bigvee_D (d \vee b) < 1$ lo que es una contradicción.
Por lo tanto $c = 0$ y de **(1)** tenemos que $\bigvee_D (d \wedge a) = (\bigvee D) \wedge a$. ■

Definición 2.4.2

1.- Un elemento c de una retícula completa $\mathscr{L}$ es llamado **compacto** si para cada subconjunto $D \subseteq \mathscr{L}$ tal que $c \leq \bigvee D$ existe un subconjunto finito $F \subseteq D$ tal que $c \leq \bigvee F$.

2.- Un elemento $c \in \mathscr{L}$ es **fuertemente compacto** si para cada subconjunto dirigido superiormente $D \subseteq \mathscr{L}$ y $c < \bigvee D$ existe un elemento $d_0 \in D$ tal que $c \leq d_0$.

Observación 14

Un elemento en una retícula completa es compacto si y sólo si es fuertemente compacto.

<u>Demostración:</u>

[$\Rightarrow$] Sea $c \in \mathscr{L}$ un elemento compacto. Entonces para cada subconjunto dirigido superiormente $D \subseteq \mathscr{L}$ tal que $c < \bigvee D$ existe un subconjunto finito $F \subseteq D$ tal que $c \leq \bigvee F$. Ya que en un conjunto dirigido superiormente cada subconjunto finito tiene cota superior tenemos que existe un elemento $d_0 \in D$ tal que $\bigvee F = d_0$ y $c \leq d_0$.

[$\Leftarrow$] Si c es un elemento fuertemente compacto y $X \subseteq \mathscr{L}$ tal que $c \leq \bigvee X$, consideremos

$$\mathscr{F} = \{\bigvee F | F \subseteq X \text{ tal que } F \text{ es finito}\}$$

Podemos observar que $(\mathscr{F}, \subseteq)$ es superiormente dirigido y $\bigvee \mathscr{F} = \bigvee X$ lo que implica que $c \leq \bigvee \mathscr{F}$. El hecho de que c es fuertemente compacto implica que existe un elemento $\bigvee F \in \mathscr{F}$ tal que $c \leq \bigvee F$. ■

Ejemplo 36

Para un conjunto M y $(\mathcal{P}(M), \subseteq)$, la retícula completa de los subconjuntos de M. Un subconjunto finito $X \subseteq M$ es compacto en $(\mathcal{P}(M), \subseteq)$.

<u>Demostración:</u>

Sean $X = \{x_1, x_2, ..., x_n\} \subseteq M$ y $\mathscr{D} \subseteq \mathcal{P}(M)$ tal que $X \subseteq \bigcup \mathfrak{D}$, esto implica que $\forall x_i \in X : \exists D_i \in \mathscr{D}$ tal que $x_i \in D_i$. Entonces sea $F = \{D_i | i \in \{1, ..., n\}\}$ y es claro que $X \subseteq \bigcup F$ y que F es finito. Por tanto X es compacto en $(\mathcal{P}(M), \subseteq)$. ■

Ejemplo 37

Recordemos que un R-módulo M es **finitamente generado** si $M = RX = \bigcap\{N \leq M | X \subseteq N\} = \{\sum_{i=1}^{n} r_i x_i | r_i \in R \text{ y } x_i \in X\}$ tal que X es finito. Sea M un R-módulo. Entonces $N \leq M$ es compacto si y sólo si N es finitamente generado.

<u>**Demostración:**</u>

[$\Rightarrow$] Sea $N \leq M$, como $N = \sum\limits_{x \in N} Rx$ y N es compacto entonces existe $F \subseteq N$ finito tal que $N \leq \sum\limits_{x \in F} Rx$ y por lo tanto $N = \sum\limits_{x \in F} Rx$, así N es finitamente generado.

[$\Leftarrow$] Supongamos que N es finitamente generado, es decir, existe un conjunto $X = \{x_1, x_2, ..., x_n\}$ tal que $N = RX$ y como $N \leq \sum\limits_{i \in I} N_i$ tal que para todo $i \in I$ se tiene que $N_i \leq M$, existe una familia de submódulos N_{i_k} con $k = 1, ..., n$ tal que $x_k \in N_{i_k}$. Entonces $N = Rx_1 + ... + Rx_n = \sum\limits_{k=1}^{n} Rx_k \leq \sum\limits_{k=1}^{n} N_{i_k}$. Por lo tanto N es compacto. ■

Definición 2.4.3

1.- Una retícula $\mathscr{L}$ es **compacta** si 1 es compacto.

2.- $\mathscr{L}$ es **compactamente generada** si cada elemento de la retícula es una yunta de elementos compactos.

Ejemplo 38

La retícula de submódulos $S_R(M)$ de un $R-$módulo M, es compactamente generada.

<u>**Demostración:**</u>

Sea $N \in S_R(M)$. Notemos que se puede escribir a $N = \sum\limits_{x \in N} Rx$ y por el Ejemplo 37 sabemos que $\forall x \in X : Rx$ es compacto, puesto que es finitamente generado. ■

En la Definición 2.4.3 hay que observar que la yunta de dos elementos compactos se puede tomar en un conjunto dirigido por el siguiente lema.

Lema 2.4.1

Si a y b son compactos en una retícula $\mathscr{L}$ entonces $a \vee b$ es compacto.

<u>**Demostración:**</u>

Si D es dirigido superiormente y $a \vee b \leq \bigvee_D d$ entonces, como a y b son compactos, existen $d_0, d_1 \in D$ tales que $a \leq d_0$ y $b \leq d_1$. Así tenemos que $a \vee b \leq d_0 \vee d_1$. Además D es dirigido y por esto existe $d_2 \in D$ tal que

$$a \vee b \leq d_0 \vee d_1 \leq d_2.$$

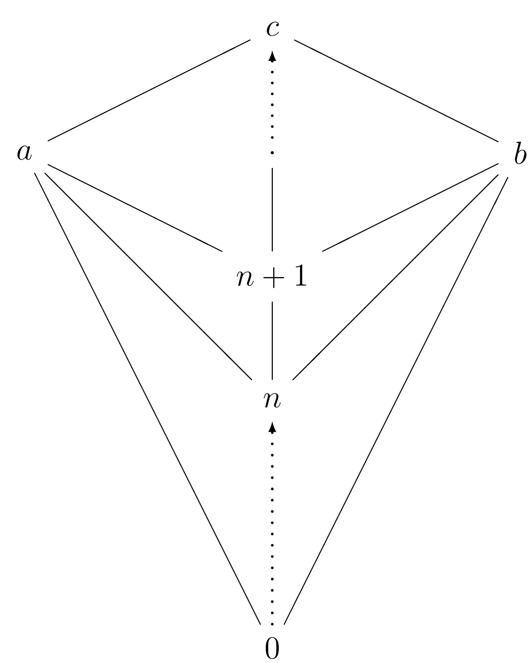
Por tanto $a \vee b$ también es compacto. ■

Observación 15

La cuña de dos elementos compactos no necesariamente es un elemento compacto.

<u>**Demostración:**</u>

Sea $\mathscr{L}$ la semiretícula superior (un COPO en el que cualquier subconjunto no vacío tiene supremo) que consiste de todos los números naturales $\mathbb{N}$ con la adjunción de la cotas superiores a, b, c de tal modo que $a \vee b = c$ y $a \| b$, como se muestra en el siguiente diagrama de Hasse.



Todas las cotas inferiores de a y las cotas inferiores de b, denotadas por $[0, a]$ y $[0, b]$ respectivamente, son ideales en $\mathscr{L} = \mathbb{N} \cup \{a, b, c\}$. Es más, $[0, a]$ y $[0, b]$ son ideales principales.
Es claro que a y b son elementos compactos, entonces $[0, a]$ y $[0, b]$ son compactos. Ahora bien, fijémonos en la cuña de $[0, a]$ y $[0, b]$, es decir, $[0, a] \cap [0, b] = \mathbb{N}$, y es claro que $\mathbb{N}$ no es compacto. ■

Observación 16
Las desigualdades en una retícula compactamente generada pueden ser verificadas de una forma especial. Para demostrar que $x \leq y$ sólo es necesario demostrar que para cada elemento compacto c en $\mathscr{L}$, $c \leq x$ implica que $c \leq y$.

Proposición 2.4.1
Toda retícula compactamente generada es superiormente continua.
<u>**Demostración:**</u>
Supongamos que $\mathscr{L}$ es una retícula compactamente generada. Sea $D \subseteq \mathscr{L}$ un subconjunto dirigido. La siguiente desigualdad se cumple para cualquier retícula $\mathscr{L}$ y cada $a \in \mathscr{L}$:

$$\bigvee_D (a \wedge d) \leq a \wedge (\bigvee_D d).$$

En cuanto a la desigualdad recírpoca, por la Observación 16, sea c un elemento compacto en $\mathscr{L}$ tal que $c \leq a \wedge (\bigvee D)$. Entonces $c \leq \bigvee D$ y por tanto $c \leq d_0$, para algún $d_0 \in D$. Pero claramente $c \leq a$ y de aquí $c \leq a \wedge d_0 \leq \bigvee_D (a \wedge d)$. ■

Lema 2.4.2 (Krull)
Sea $\mathscr{L}$ una retícula compacta, entonces la subretícula $[a, 1]$ tiene al menos un elemento máximo distinto de 1.
<u>**Demostración:**</u>

Sea $S = [a, 1] \setminus \{1\}$, notar que $S \neq \emptyset$ ya que $a \in S$. Veamos que se cumplen las condiciones para poder aplicar el lema de Zorn al conjunto S.
Sea C una cadena en S, como $\mathscr{L}$ es compacta entonces 1 es compacto por lo que si $\bigvee C = 1$ tenemos que existe $c_0 \in C$ tal que $1 \leq c_0$ lo que implica que $1 = c_0$ pero esto es una contradicción pues estábamos suponiendo que $c_0 \in C \subseteq S$ y $1 \notin S$. Por lo tanto $\bigvee C \neq 1$ y también $a \leq \bigvee C$, $i, e.$ $\bigvee C \in S$, por lo tanto podemos aplicar el Lema de Zorn y asegurar la existencia de un máximo en el conjunto S. ■

Definición 2.4.4

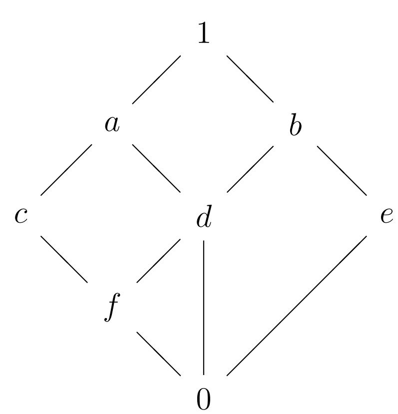
1.- Un elemento a en una retícula $\mathscr{L}$ con 0 tal que $a \neq 0$ es llamado **átomo** si $b < a$ implica que $b = 0$.

2.- $\mathscr{L}$ es llamada **localmente atómica** si cada elemento de $\mathscr{L}$ es una yunta de átomos.

3.- Una retícula con cero es llamada **atómica** si cada intervalo $[0, a]$ contiene al menos un átomo para cada $a > 0$.

Ejemplo 39

Si consideramos la retícula



observamos que f, d y e son átomos.

Proposición 2.4.2

En una retícula continua superiormente $\mathscr{L}$, cada átomo es un elemento compacto.

Demostración:

Sea $a \in \mathscr{L}$ un átomo en una retícula continua superiormente tal que $a \leq \bigvee D$. Por reducción al absurdo supongamos que ocurre que $\forall d \in D : a \nleq d$. Como a es un átomo tenemos que $\forall d \in D : a \wedge d = a$ o $a \wedge d = 0$, pero como $a \nleq d$ entonces $a \wedge d = 0$. Como $\mathscr{L}$ es continua superiormente tenemos que $a = a \wedge (\bigvee D) = \bigvee\limits_{D} (a \wedge d) = 0$ lo que es una contradicción pues a es un átomo y por definición $0 \prec a$. Por lo tanto $\exists d_0 \in D : a \leq d_0$. ■

Ejemplo 40

Si M es un módulo, la retícula $S_R(M)$ de submódulos de M es superiormente continua, pero no necesariamente continua. Los átomos en $S_R(M)$ son los submódulos simples. $S_R(M)$ es localmente atómica si y sólo si M es un módulo semisimple.

Proposición 2.4.3

Todo elemento en una retícula completa es compacto si y sólo si la retícula es noetheriana.

Demostración:

[$\Rightarrow$] Supongamos que en una retícula $\mathscr{L}$ todo elemento es compacto. Sea $a_1 \leq a_2 \leq ... \leq a_n \leq ...$ una sucesión no decreciente en $\mathscr{L}$.

El elemento $c = \bigvee\limits_{n \in \mathbb{N}} a_n \in \mathscr{L}$ es compacto por hipótesis. Además se tiene que $c \leq \bigvee\limits_{n \in \mathbb{N}} a_n$ y por compacidad podemos obtener un subconjunto finito $F \subseteq \mathbb{N}$ y $n_0 \in \mathbb{N}$ tal que $\bigvee\limits_{n \in \mathbb{N}} a_n \leq \bigvee\limits_{n \leq n_0} a_n$. Lo que implica que $a_{n_0} = a_{n_0+1} = a_{n_0+2} = ...$ Por tanto $\mathscr{L}$ es noetheriana.

[$\Leftarrow$] Ver Proposición 2.2.4. ■

Proposición 2.4.4

Toda rertícula artiniana es atómica.

Demostración:

Sean $\mathscr{L}$ una retícula artiniana, $a \in \mathscr{L}$ tal que $0 < a$ y $c \in [0, a]$, con $c \neq 0$. Supongamos que c no es un átomo en $[0, a]$. Entonces existe un elemento $c_1 \in [0, a]$ tal que $0 < c_1 < c$. Si tampoco c_1 es un átomo en $[0, a]$, continuamos con este proceso, es decir, tendíamos $0 < c_n < c_{n-1} < ... < c_3 < c_2 < c_1 < c$. Como la retícula es artiniana, después de un número finito de pasos, se tiene que existe un átomo en $[0, a]$. Por tanto $\mathscr{L}$ es atómica. ■

2.5. Pseudocomplementos y suplementos

Para esta sección nos referiremos a $\mathscr{L}$ como una retícula modular con 0 y 1.

Definición 2.5.1

1.- Sea $a \in \mathscr{L}$, definimos el **pseudocomplemento** de a en $\mathscr{L}$ como un elemento c tal que $a \wedge c = 0$ y c es máximo con esta propiedad.

2.- Sea $a \in \mathscr{L}$, definimos el **suplemento** de a en $\mathscr{L}$ como un elemento c tal que $a \vee c = 1$ y c es mínimo con esta propiedad.

3.- Sea $a \in \mathscr{L}$, el **pseudocomplemento fuerte** de a en $\mathscr{L}$ como un elemento c tal que $a \wedge c = 0$ y c es el elemento mayor con esta propiedad.

4.- Sea $a \in \mathscr{L}$, el **suplemento fuerte** de a en $\mathscr{L}$ como un elemento c tal que $a \vee c = 1$ y c es el elemento menor con esta propiedad.

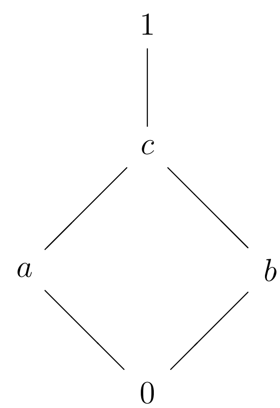
5.- La retícula $\mathscr{L}$ es **pseudocomplementada** si para cada intervalo $I \subseteq \mathscr{L}$ y cada $a \in I$ existe un pseudocomplemento de a en I.

Observación 17

Claramente c es un suplemento de b en $\mathscr{L}$ si y sólo si c es un pseudocomplemento de b en $\mathscr{L}^{OP}$.

Ejemplo 41

En la siguiente retícula modular, b es pseudocomplemento de a pero no un complemento.



Ejemplo 42

Sea M un módulo y $N \leq M$, N es un complemento en $S_R(M)$ si y sólo si N es un sumando directo de M.

Ejemplo 43

Sea $\mathscr{C}$ una clase de módulos. Decimos que $\mathscr{C}$ cumple $\leq$ si es cerrada bajo submódulos.

A las clases que cumplen tal condición se les llama **clases hereditarias**, y a la clase de éstas se le denota por $\mathscr{L}_{\leq}$. Es decir, si $\mathscr{C} \in \mathscr{L}_{\leq}$ entonces $M \in \mathscr{C}$ y $N \leq M \Rightarrow N \in \mathscr{C}$. Definimos para $\mathscr{C} \in \mathscr{L}_{\leq}$ la clase
$\mathscr{C}^{\perp_{\leq}} = \{M \in R-Mod | N \leq M \text{ y } N \in \mathscr{C} \Rightarrow N = 0\}$.
Demostremos que $\mathscr{C}^{\perp_{\leq}}$ es un pseudocomplemento fuerte para $\mathscr{C}$ en $\mathscr{L}_{\leq}$.

(i) Sean $M \in \mathscr{C}^{\perp_{\leq}}$, $N \leq M$ y $K \leq N$ tal que $K \in \mathscr{C}$.
Como $K \leq N \leq M$ y $M \in \mathscr{C}^{\perp_{\leq}}$ entonces $K = 0$. Así $N \in \mathscr{C}^{\perp_{\leq}}$. Por lo tanto $\mathscr{C}^{\perp_{\leq}} \in \mathscr{L}_{\leq}$.

(ii) Sea $M \in \mathscr{C} \cap \mathscr{C}^{\perp_{\leq}}$. Dado que $M \leq M$ y $M \in \mathscr{C}^{\perp_{\leq}}$, entonces $M = 0$ y por lo tanto $\mathscr{C} \cap \mathscr{C}^{\perp_{\leq}} = \{0\}$.

(iii) Sea $\mathscr{D}$ una clase en $\mathscr{L}_{\leq}$ tal que $\mathscr{C} \cap \mathscr{D} = \{0\}$ y $M \in \mathscr{D}$. Si $N \leq M$ tal que $N \in \mathscr{C}$, entonces $N = 0$ pues $N \in \mathscr{D}$, lo que implica que $M \in \mathscr{C}^{\perp_{\leq}}$. Así $\mathscr{D} \subseteq \mathscr{C}^{\perp_{\leq}}$.

Por lo tanto $\mathscr{C}^{\perp_{\leq}}$ es la clase mayor en $\mathscr{L}_{\leq}$ tal que $\mathscr{C} \cap \mathscr{C}^{\perp_{\leq}} = \{0\}$. Es decir $\mathscr{C}^{\perp_{\leq}}$ es un pseudocomplemento fuerte de $\mathscr{C}$.

Ejemplo 44

Sea $\mathbb{V} = \mathbb{R}^2$ visto como un $\mathbb{R}$-espacio vectorial. Notar que para $x \in \mathbb{V}$, $\langle x \rangle = \{ax : a \in \mathbb{R}\}$. Sea $y \in \mathbb{V}$ tal que $y \notin \langle x \rangle$. Observemos que $\langle x \rangle$ y $\langle y \rangle$ representan dos rectas en $\mathbb{R}^2$ que pasan por el origen y $\langle x \rangle \cap \langle y \rangle = \{0\}$.
Supongamos que existe $\langle z \rangle$ tal que $\langle x \rangle \cap \langle z \rangle = \{0\}$ y $\langle y \rangle \leq \langle z \rangle$. Es claro que esto implica que $\langle y \rangle = \langle z \rangle$. Por lo tanto $\langle y \rangle$ es máximo con la propiedad de que $\langle x \rangle \cap \langle y \rangle = \{0\}$, es decir $\langle y \rangle$ es un pseudocomplemento de $\langle x \rangle$ en $\mathbb{R}^2$.
Notar que si $x \notin \langle y \rangle$ o $y \notin \langle x \rangle$ entonces $\langle x \rangle$ y $\langle y \rangle$ son incomparables y por lo tanto $\langle y \rangle$ no es pseudocomplemento fuerte.

Lema 2.5.1

En una retícula modular con 0 y 1, todo complemento es un pseudocomplemento.

Demostración:

Sea c un complemento de a en $\mathscr{L}$, basta demostrar que c es máximo con la propiedad de que $a \wedge c = 0$. Supongamos que existe $c' \in \mathscr{L}$ tal que $a \wedge c' = 0$ y $c \leq c'$.

Entonces, por modularidad, tenemos que:

$$c = (a \wedge c') \vee c = (a \vee c) \wedge c' = 1 \wedge c' = c'.$$

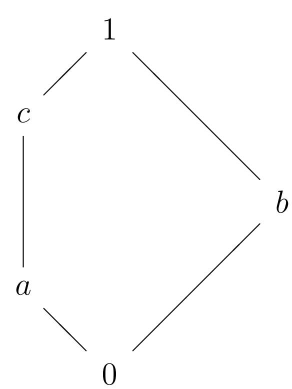
Por lo tanto c es máximo con tal propiedad y así hemos demostrado que c también es pseudocomplemnto de a en $\mathscr{L}$. ■

Como una consecuencia inmediata tenemos el siguiente:

Corolario 2.5.1
Toda retícula modular complementada es pseudocomplementada.

Ejemplo 45
La retícula de submódulos $S_R(M)$ es pseudocomplementada.

Observación 18
Notar que las proposiciones anteriores ya no se cumplen sin la condición de modularidad, pues si usamos la retícula del pentágono:



Observamos que a es un complemento de b en $\mathscr{L}$, pues $a \vee b = 1$ y $a \wedge b = 0$; pero a pesar de que $a \wedge b = 0$, también se cumple que $b \wedge c = 0$ y $a \leq c$. Por lo que a ya no es máximo con tal propiedad y por tanto no es un pseudocomplemento de b en $\mathscr{L}$.

Proposición 2.5.1

Toda retícula superiormente continua es pseudocomplementada.

Demostración:

Sea $\mathscr{L}$ una retícula superiormente continua. Para cada $a \in \mathscr{L}$ definamos $A := \{x \in \mathscr{L} | a \wedge x = 0\}$. Sea $\{x_i\}_{i \in I}$ una cadena en A, entonces, como $\mathscr{L}$ es superiormente continua y toda cadena es un conjunto dirigido superiormente, tenemos que $a \wedge (\bigvee\limits_I x_i) = \bigvee\limits_I (a \wedge x_i) = \bigvee\{0\} = 0$. Observemos además que $\bigvee\limits_I x_i \in A$ es una cota superior de $\{x_i\}_{i \in I}$. Aplicando el Lema de Zorn podemos asegurar la existencia de un elemento máximo c en A, es decir, $a \wedge c = 0$ y c es máximo con tal propiedad. Por lo tanto c es un pseudocomplemento de a en $\mathscr{L}$ y así hemos demostrado que $\mathscr{L}$ es pseudocomplementada. ■

Corolario 2.5.2

Toda retícula compactamente generada es pseudocomplementada.

Demostración:

Aplicando la Proposición 2.4.1 y la Proposición 2.5.1 se obtiene lo deseado.

■

Ejemplo 46

La retícula de submódulos $S_R(M)$ es superiormente continua por tanto también es una retícula pseudocomplementada.

Definición 2.5.2

1.- Un elemento a es **esencial** en $\mathscr{L}$ si para todo $c \in \mathscr{L}$ tal que $c \neq 0$ se cumple que $a \wedge c \neq 0$. Equivalentemente a es esencial en $\mathscr{L}$ si $a \wedge c = 0$ implica que $c = 0$.

2.- En una retícula con 1, un elemento $a \in \mathscr{L}$ es **superfluo** si para todo $b \in \mathscr{L}$ tal que $b \neq 1$ se cumple que $a \vee b \neq 1$. Equivalentemente a es superfluo en $\mathscr{L}$ si $a \vee c = 1$ implica que $c = 1$.

Observación 19

Elemento esencial y elemento superfluo son conceptos duales y por tanto en algunas proposiciones para elementos esenciales se puede dualizar para elementos superfluos y viceversa.

Ejemplo 47

Sean M un R-módulo y $A \in S_R(M)$:

1.- Decimos que A es esencial en M si y sólo si $\forall\ U \leq M : A \cap U = 0$, entonces $U = O$.

2.- Decimos que A es superfluo en M si y sólo si $\forall\ U \leq M : A + U = M$, entonces $U = M$.

Proposición 2.5.2

Los elementos esenciales de $\mathscr{L}$ forman un filtro en $\mathscr{L}$, es decir:

(a) Si a y b son elemento esenciales, entonces $a \wedge b$ es esencial.

(b) Todo $c \in \mathscr{L}$ tal que $a \leq c$, es esencial.

(c) En caso de que $\mathscr{L}$ tenga 1, éste es esencial.

Demostración:

(a) Sean $a, b \in \mathscr{L}$ elementos esenciales, entonces para cualquier $c \in \mathscr{L}$ tal que $c \neq 0$ se tiene que $a \wedge c \neq 0$ y $b \wedge c \neq 0$. Entonces $a \wedge (b \wedge c)$ implica que $(a \wedge b) \wedge c \neq 0$.

(b) Si $a \neq c$ entonces para todo $d \neq 0$ se tiene que $0 \neq a \wedge d \leq c \wedge d$ y por lo tanto $c \wedge d \neq 0$ y por lo tanto c es esenciales.

(c) Es claro que si $c \wedge 1 = 0$, entonces $c = 0$. $\blacksquare$

Proposición 2.5.3

Si a es esencial en $\mathscr{L}$, entonces para cada $b \in \mathscr{L}$, $a \wedge b$ es esencial en $[o, b]$.

Demostración:

Sea $x \in [0, b]$ tal que $x \neq 0$; es decir, $0 \neq x \leq b$, entonces $(a \wedge b) \wedge x = a \wedge (b \wedge x) = a \wedge x \neq 0$, pues a es esencial en $\mathscr{L}$. Por lo tanto $a \wedge b$ es esencial en $[0, b]$. ■

Observación 20

La cuña arbitraria de elementos esenciales no necesariamente es esencial.

Demostración:

Consideremos la retícula de todos los submódulos de $\mathbb{Z}$ visto como $\mathbb{Z}$-módulo, es decir, todos los subgrupos de $\mathbb{Z}$.

Para cada $n \in \mathbb{N}$, el subgrupo $n\mathbb{Z}$ es esencial en $\mathbb{Z}$, ya que, $n\mathbb{Z} \cap m\mathbb{Z} = 0$ entonces $m\mathbb{Z} = 0$. Pero $0 = \bigcap_{n \in \mathbb{N}} n\mathbb{Z}$ no es esencial en $\mathbb{Z}$. ■

Observación 21

El conjunto de elementos superfluos es un ideal de la retícula $\mathscr{L}$.

Proposición 2.5.4

En una retícula $\mathscr{L}$ la relación "ser esencial en" es transitiva.

Demostración:

Lo que queremos demostrar es que para $a, b, c \in \mathscr{L}$ tales que $a \leq b \leq c$, si a es esencial en $[0, b]$ y b es esencial en $[0, c]$, entonces a es esencial en $[0, c]$.

Sea $x \in [0, c]$ tal que $x \neq 0$. Entonces $b \wedge x \neq 0$, puesto que b es esencial en $[0, c]$. De aquí tenemos que $a \wedge x = (a \wedge b) \wedge x = a \wedge (b \wedge x) \neq 0$, pues $(b \wedge x) \in [0, b]$ y a es esencial en $[0, b]$. Por lo tanto a es esencial en $[0, c]$. ■

Proposición 2.5.5

Sean $\mathscr{L}$ una retícula y $a, b, c, d \in L$ tales que $a \leq b \leq c \leq d$ y a es esencial en $[0, d]$, entonces b es esencial en $[0, c]$.

Demostración:

Sea $x \in [0, c]$ tal que $b \wedge x = 0$. Pero $a \leq b$,entonces $a \wedge x = 0$. Como $x \leq c \leq d$, entonces $x = 0$, pues a es esencial en $[0, d]$. Por lo tanto b es esencial en $[0, c]$. ■

Proposición 2.5.6

Sean a y b elementos de una retícula modular $\mathscr{L}$ tales que $a < b$. Si b es esencial en $[a, 1]$ entonces b es esencial en $\mathscr{L}$.

Demostración:

Sea $x \in \mathscr{L} \setminus \{0\}$, entonces tenemos los siguientes casos:

(i) Si $x \vee a = a$ entonces $x \leq a < b$ y $x \wedge b = x \neq 0$.

(ii) Si $a < x \vee a$ entonces, como b es esencial en $[a, 1]$, obtenemos que $a < b \wedge (x \vee a)$ y, por modularidad, $a < a \vee (x \wedge b)$.
De aquí se tiene que $x \wedge b \neq 0$ y por lo tanto b es esencial en $\mathscr{L}$.

■

Proposición 2.5.7

Si c es un pseudocomplemento de a en la retícula modular $\mathscr{L}$, entonces $a \vee c$ es esencial en $\mathscr{L}$.

Demostración:

Sea c un pseudocomplemento de a en $\mathscr{L}$, es decir, $a \wedge c = 0$ y c es máximo con tal propiedad.
Supongamos que existe $d \in \mathscr{L}$ tal que $d \neq 0$ y $(a \vee c) \wedge d = 0$. Queremos demostrar que $d = 0$.
Es claro que $a \wedge (c \vee d) \leq (a \vee c) \wedge (c \vee d)$. Como $c \leq a \vee c$ y $\mathscr{L}$ es modular tenemos:

$$(a \vee c) \wedge (c \vee d) = ((a \vee c) \wedge d) \vee c = 0 \vee c = c.$$

Además, c es pseudocomplmento de a entonces $a \wedge c = 0$ lo que implica que

$$a \wedge (c \vee d) \leq a \wedge (a \wedge (c \vee d)) \leq a \wedge c = 0 \Rightarrow a \wedge (c \vee d) = 0.$$

Como c es máximo con la propiedad de que $a \wedge c = 0$, entonces $c \vee d = c$ lo que implica que $d \leq c$, entonces $d \leq a \vee c$ y por tanto $d = (a \vee c) \wedge d = 0$, por hipótesis. Por lo tanto $a \vee c$ es esencial en $\mathscr{L}$. ■

Definición 2.5.3

Decimos que b es una **extensión esencial** de a si $a \leq b$ y a es esencial en $[0, b]$.

Proposición 2.5.8

Si $\mathscr{L}$ es pseudocomplementada y b es un pseudocomplemento de a, entonces existe un pseudocomplemento c de b en $\mathscr{L}$ tal que $a \leq c$.

Demostración:

Sea c un pseudocomplemento de $a \vee b$ en la retícula $[a, 1]$, entonces $a \leq c$ y $(a \vee b) \wedge c = a$. Por modularidad tenemos que $(a \vee b) \wedge c = a \vee (b \wedge c) = a$. Además c es un pseudocomplemento de b en $\mathscr{L}$ ya que

$$0 = a \wedge b = ((a \vee b) \wedge c) \wedge b = (a \vee b) \wedge c \wedge b = (a \vee b) \wedge b \wedge c = b \wedge c.$$

Para demostrar que a es esencial en $[0, c]$ supongamos que existe $d \in \mathscr{L}$ tal que $d \leq c$ y $a \wedge d = 0$, entonces:

$$a \wedge (b \vee d) = a \wedge c \wedge (b \vee d) = a \wedge (d \vee (b \wedge c)) = a \wedge d = 0.$$

Pero b es máximo con tal propiedad, por lo tanto $d = 0$.

Finalmente, demostremos que c es máximo visto como extensión esencial de a en $\mathscr{L}$.

Supongamos que $c' \in \mathscr{L}$ y $c < c'$, entonces $c' \wedge b \neq 0$ pues c es máximo con la propiedad de que $b \wedge c = 0$, pero $c' \wedge b \wedge a \leq b \wedge a = 0$ lo que implica que a no es esencial en $[0, c']$ lo que es una contradicción, entonces $c' = c$. Por lo tanto c es una extensión esencial máxima de a en $\mathscr{L}$. ■

Proposición 2.5.9
Sea $\mathscr{L}$ una retícula pseudocomplementada. Un elemento $a \in \mathscr{L}$ es pseudocomplemento de algún elemento de $\mathscr{L}$ si y sólo si a es esencialmente cerrado en $\mathscr{L}$.

Demostración:
[$\Rightarrow$] Supongamos que a es pseudocomplemento de un elemento b en $\mathscr{L}$. Tomemos un pseudocomplemento b' de a tal que $b \leq b'$. es claro que a es un pseudocomplemento de b'. Por la Proposición 2.5.8 tenemos que a es una extensión máxima esencialmente cerrada en $\mathscr{L}$.
[$\Leftarrow$] Supongamos que a no tiene una extensión esencial distinta de sí misma, por la Proposición 2.5.8, si b es un pseudocomplemento de a en $\mathscr{L}$, entonces existe un pseudocomplemento c de b en $\mathscr{L}$ tal que $a \leq c$, pero por hipótesis tenemos que $a = c$. Entonces a es un pseudocomplemento de b en $\mathscr{L}$. ■

Ejemplo 48
Si M es un módulo entonces $S_R(M)$ es pseudocomplementada. Un submódulo $L \leq M$ es esencial en M si es elemento esencial en $S_R(M)$ y esto pasa si y sólo si para cada $x \neq 0$ en M existe $a \in A$ tal que $xa \in L$

Definición 2.5.4
La yunta de todos los átomos de una retícula $\mathscr{L}$ es llamada **zoclo** de $\mathscr{L}$ y es denotada por $z(\mathscr{L})$.

Lema 2.5.2
En una retícula $\mathscr{L}$ con 0, $z(\mathscr{L})$ es una cota inferior para la cuña de todos los elementos esenciales de $\mathscr{L}$.

Demostración:
Sean $0 \neq a$ un átomo, $E = \{e \in \mathscr{L} \mid e \text{ es un elemento esencial}\}$ y $0 \neq e \in E$. Observemos que $a \wedge e = 0$ o bien $a \wedge e = a$, como e es esencial entonces $a \wedge e \neq 0$ y por lo tanto se tiene que $a \wedge e = a$, lo que implica que $a \leq e$.

Entonces tenemos que $z(\mathscr{L}) \leq e$ y así $z(\mathscr{L}) \leq \bigwedge E$. ■

Lema 2.5.3

Si en una retícula $\mathscr{L}$ con 1 existe un elemento mayor $m \neq 1$, entonces m es superfluo.

Demostración:

Sea $b \in \mathscr{L}$ tal que $b \neq 1$ entonces $m \vee b = m \neq 1$. Así m es superfluo. ■

Lema 2.5.4

Si $b < c$ y b es superfluo en $[0, c]$, en una retícula modular $\mathscr{L}$ entonces para cada $a \in \mathscr{L}$, $a \vee b$ es superfluo en $[a, a \vee c]$.

Demostración:

Supongamos que para un $x \in [a, a \vee c]$ tenemos que $(a \vee b) \vee x = a \vee c$, entonces, tomando la cuña con c, tenemos que $((a \vee b) \vee x) \wedge c = (a \vee c) \wedge c$ implica $(b \vee (a \vee x)) \wedge c = c$, y, por modularidad, $(b \vee (a \vee x)) \wedge c = c$. Como b es superfluo en $[0, c]$, entonces $(a \vee x) \wedge = 0$ ó $c \leq a \vee x = x$. De aquí tenemos $a \vee c \leq x$ y por lo tanto $a \vee c = x$.

Esto demuestra que $a \vee b$ es superfluo en $[a, a \vee c]$. ■

Lema 2.5.5

Sean $a, b \in \mathscr{L}$ tales que $a < b$, entonces b es superfluo en $\mathscr{L}$ si y solo si a es superfluo en $\mathscr{L}$ y b es superfluo en $[a, 1]$.

Demostración:

$[\Rightarrow]$ Sean $a < b$ elementos de $\mathscr{L}$ tal que b es superfluo en $\mathscr{L}$.

Supongamos que para $d \in \mathscr{L}$ se tiene que $a \vee d = 1$; pero $a \vee d \leq b \vee d = 1$, como b es superfluo en $\mathscr{L}$ entonces $d = 1$. Por lo tanto a es superfluo en $\mathscr{L}$.

Sea $c \in [a, 1]$ tal que $b \vee c = 1$, pero b es superfluo en $\mathscr{L}$, por lo tanto $c = 1$.

$[\Leftarrow]$ Si $b \vee c = 1$ entonces $b \vee (a \vee c) = 1$ y, como b es superfluo en $[a, 1]$, entonces $a \vee c = 1$. Además a es superfluo en $\mathscr{L}$, entonces $c = 1$. Por lo tanto b es superfluo en $\mathscr{L}$. ■

2.6. Operadores de cerradura

Definición 2.6.1

1.- Sea $\mathscr{L}$ una retícula completa. Un **operador de cerradura** en $\mathfrak{L}$ es una función

$$\Phi : \mathscr{L} \longrightarrow \mathscr{L}, \text{ donde } \Phi(a) = a^c \text{ tal que:}$$

(Cl1) $a \leq b \Rightarrow a^c \leq b^c$

(Cl2) $a \leq a^c$

(Cl3) $(a^c)^c = a^c$

2.- Un elemento a es **cerrado bajo** Φ si $a = a^c$.

3.- Sea $\mathscr{L}$ una retícula completa. Si $C \subseteq \mathscr{L}$ y C es cerrado bajo cuñas arbitrarias (*i.e.* $S \subseteq C$ implica que ínf $S \in C$) entonces C es llamado **sistema de cerradura** en $\mathscr{L}$.

Observación 22

De 3 de la definición anterior podemos notar que C es una retícula completa (Teorema 1.3.1 y Observación 8). Además hay que observar que la cuña en C es la misma que en $\mathscr{L}$, pero la yunta en C está dada por

$$\sup_C S = \text{ínf}\,\{\text{cotas superiores de } S \text{ en } C\}.$$

Proposición 2.6.1

Los elementos cerrados bajo Φ forman una retícula completa $\mathscr{L}^c$.

<u>**Demostración:**</u>

Sea $\{a_i\}_{i\in I}$ una familia de elementos cerrados, entonces $\bigwedge\limits_{i\in I} a_i \leq a_i$ lo que implica para toda $i \in I$ se tiene $(\bigwedge a_i)^c \leq a_i^c = a_i$ y de aquí $(\bigwedge a_i)^c \leq \bigwedge a_i$. Como ya sabíamos que $\bigwedge a_i \leq (\bigwedge a_i)^c$ concluimos que $\bigwedge a_i = (\bigwedge a_i)^c$. Es decir, la cuña de $\mathscr{L}^c$ es la misma que $\mathscr{L}$ y por el Teorema 1.3.1 y la

Observación 8, $\mathscr{L}^c$ es una retícula completa. ■

Observación 23

En general $\mathscr{L}^c$ no es una subretícula de $\mathscr{L}$. La cuña en $\mathscr{L}^c$ es la misma que en $\mathscr{L}$, pero la yunta $\overline{\bigvee} a_i = (\bigvee a_i)^c$ para una familia $\{a_i\}_{i\in I}$ de elementos cerrados. Es decir, $\mathscr{L}$ forma un sistema de cerradura en $\mathscr{L}^c$. Recíprocamente si S es un sistema de cerradura en $\mathscr{L}$ podemos definir un operador de cerradura como

$$a^c = \text{ínf}\{s \in S | a \leq s\}.$$

Es claro que cumple con **(Cl1)**, **(Cl2)** y **(Cl3)**. En este sentido se establece una correspondecia biunívoca entre los operadores de cerradura y los sistemas de cerradura.

Un operador de cerradura también puede satisfacer las siguientes propiedades:

(Cl4) $(a \vee b)^c = a^c \vee b^c$

(Cl5) $(a \wedge b)^c = a^c \wedge b^c$

Observación 24

Cuando se satisface **(Cl4)**, $\mathscr{L}^c$ es una subretícula de $\mathscr{L}$. Esto ocurre porque entonces la yunta en $\mathscr{L}^c$ es la misma que la yunta en $\mathscr{L}$.

Proposición 2.6.2

Si $\mathscr{L}$ es una retícula modular completa con un operador de cerradura que satisface **(Cl5)**, entonces $\mathscr{L}^c$ también es una retícula modular.

Demostración:

Supongamos que $a, b, c \in \mathscr{L}^c$ tales que $a \leq c$ y sea $\overline{\vee}$ la yunta en $\mathscr{L}^c$. Entonces tenemos que

$(a \overline{\vee} b) \wedge c = (a \vee b)^c \wedge c^c = ((a \vee b) \wedge c)^c = (a \vee (b \wedge c))^c = a^c \overline{\vee} (b \wedge c)^c = a \overline{\vee} (b \wedge c).$

Lo que demuestra la modularidad en $\mathscr{L}^c$. ■

Un resultado similar se tiene para el caso de la distributividad, es decir, se cumple la siguiente proposición.

Proposición 2.6.3
Si $\mathscr{L}$ es una retícula distributiva completa con un operador de cerradura que satisface **(Cl5)**, entonces $\mathscr{L}^c$ también es una retícula distributiva.
Demostración:
Supongamos que $a, b, c \in \mathscr{L}^c$ y sea $\overline{\vee}$ la yunta en $\mathscr{L}^c$. Entonces tenemos que

$a \wedge (b \overline{\vee} c) = a^c \wedge (b \vee c)^c = (a \wedge (b \vee c))^c = ((a \wedge b) \vee (a \wedge c))^c = (a \wedge b) \overline{\vee} (a \wedge c).$

Por tanto se cumple la distributividad en $\mathscr{L}^c$. ■

Definición 2.6.2
Un operador de cerradura cumple la **condición de finitud (CF)** si para cada subconjunto dirigido $D \subseteq \mathscr{L}$ se tiene

$$\bigvee_D d^c = (\bigvee_D d)^c,$$

es decir, si cada yunta en D (yunta dirigida) de elementos cerrados, es un elemento cerrado.

Proposición 2.6.4
Si $\mathscr{L}$ es una retícula superiormente continua con un operador de cerradura que cumple la CF, entonces $\mathscr{L}^c$ es superiormente continua.
Demostración:
Sea D un subconjunto dirigido de $\mathscr{L}^c$ y $a \in D$. Entonces:

$(\bigvee_D d) \wedge a = (\bigvee_D d^c) \wedge a^c = (\bigvee_D d)^c \wedge a^c = ((\bigvee_D d) \wedge a)^c = (\bigvee_D (d \wedge a))^c$

$= \bigvee\limits_{D}(d \wedge a)^c = \bigvee\limits_{D}(d \wedge a)$.

Por lo tanto $\mathscr{L}^c$ también es superiormente continua. ■

Proposición 2.6.5

Sea Φ un operador de cerradura que cumple la CF en una retícula compactamente generada $\mathscr{L}$. Entonces un elemento cerrado a es compacto en $\mathscr{L}^c$ si y sólo si existe $b \in \mathscr{L}$ tal que $a = b^c$.

<u>**Demostración:**</u>

[$\Rightarrow$] Supongamos que a es compacto en $\mathscr{L}^c$, entonces podemos escribir $a = \bigvee\limits_{D} d$, donde D es un subconjunto dirigido de elementos compactos en $\mathscr{L}$, ya que $\mathscr{L}$ es compactamente generada.

Entonces $a = a^c = \bigvee\limits_{D} d^c$ y como a es compacto en $\mathscr{L}^c$ se tiene que existe $d_0 \in D$ tal que $a = d_0^c$.

[$\Leftarrow$] Si b es un elemento compacto en $\mathscr{L}$ y $D \subseteq \mathscr{L}$ es un conjunto dirigido de elementos compactos tal que $b^c \leq \bigvee\limits_{D} d$ entonces existe $d \in D$ tal que $b \leq d$ y también $b^c \leq d$. Por lo tanto $b^c = b$ también es compacto en $\mathscr{L}^c$. ■

Corolario 2.6.1

Si Φ es un operador de cerradura que cumple la CF en una retícula compactamente generada $\mathscr{L}$, entonces también $\mathscr{L}^c$ es compactamente generada.

<u>**Demostración:**</u>

Sea $a \in \mathscr{L}^c$ entonces $a^c = a$, como $a \in \mathscr{L}$ entonces podemos escribir $a = \bigvee\limits_{D} d$ donde D es un subconjunto dirigido de elementos compactos de $\mathscr{L}$. Además

$$a = a^c = \bigvee_{D} d = (\bigvee_{D} d)^c = \bigvee_{D} d^c$$

por la Proposición 2.6.5, como $\bigvee\limits_{D} d = \bigvee\limits_{D} d^c$, entonces cada $d \in D$ se puede ver como $d = b^c$ tal que $b \in D$ y por tanto todo $d \in D$ es compacto en $\mathscr{L}^c$. Así, henos demostrado que a es una yunta de elementos compactos en $\mathscr{L}^c$ y por tanto $\mathscr{L}^c$ es compactamente generada. ■

Ejemplo 49
Sea X es un espacio topológico, entonces los subconjuntos cerrados forman un sistema de cerradura en la retícula $\mathcal{P}(X)$ de subconjuntos de X. El correspondiente operador de cerradura satisface **(Cl5)**.

2.6.1. Conexiones de Galois

Definición 2.6.3
Sean $\mathscr{L}$ y $\mathscr{L}'$ dos COPO's. Una **conexión de Galois** entre $\mathscr{L}$ y $\mathscr{L}'$ es una pareja (α, β) de funciones tales que

$$\alpha : \mathscr{L} \longrightarrow \mathscr{L}' \qquad\qquad \beta : \mathscr{L}' \longrightarrow \mathscr{L}$$

y que satisfacen:

(i) Para $a_1, a_2 \in \mathscr{L} : a_1 \leq a_2 \Longrightarrow \alpha(a_2) \leq \alpha(a_1)$.

(ii) Para $b_1, b_2 \in \mathscr{L}' : b_1 \leq b_2 \Longrightarrow \beta(b_2) \leq \beta(b_1)$.

(iii) Para $a \in \mathscr{L}$ y $b \in \mathscr{L}' : a \leq \beta\alpha(a)$ y $b \leq \alpha\beta(b)$.

Proposición 2.6.6
Las funciones $\beta\alpha : \mathscr{L} \longrightarrow \mathscr{L}$ y $\alpha\beta : \mathscr{L}' \longrightarrow \mathscr{L}'$ son operadores de cerradura en $\mathscr{L}$ y $\mathscr{L}'$ respectivamente.
Demostración:
Demostremos que se cumplen, para $\beta\alpha$, **(CL1)**, **(CL2)** y **(CL3)**.

(Cl1) Sean $a_1, a_2 \in \mathscr{L}$ tales que $a_1 \leq a_2$, por (i) de la definición de conexión de Galois, tenemos que $\alpha(a_2) \leq \alpha(a_1)$, y además $\alpha(a_1), \alpha(a_2) \in \mathscr{L}'$. Por (ii), tenemos que $\beta(\alpha(a_1)) \leq \beta(\alpha(a_2))$.

(Cl2) Consecuencia directa de (iii).

(Cl3) Si $a \in \mathscr{L}$ entonces $\alpha(a) \in \mathscr{L}'$. Por (iii) tenemos que $\alpha(a) \leq \alpha(\beta(\alpha(a)))$. ∎

Aplicando (i) a $a \leq \beta(\alpha(a))$ tenemos que $\alpha(\beta(\alpha(a))) \leq \alpha(a)$. Así tenemos que $\alpha(\beta(\alpha(a))) = \alpha(a)$ y por lo tanto $\beta\alpha(\beta\alpha(a)) = \beta\alpha(a)$.

■

Definición 2.6.4
Sea R un anillo y $X \subseteq R$ entonces:

1.- El conjunto $\mathfrak{i}(X) = \{r \in R | \forall x \in X : rx = 0\} = \{r \in R : rX = 0\}$ es llamado **anulador izquierdo** de X en R.

2.- El conjunto $\mathfrak{d}(X) = \{r \in R | \forall x \in X : xr = 0\} = \{r \in R : Xr = 0\}$ es llamado **anulador derecho** de X en R.

Proposición 2.6.7
Sean R un anillo y $X \subseteq R$, entonces $\mathfrak{i}(X)$ es un ideal izquierdo y $\mathfrak{d}(X)$ un ideal derecho de R.
Demostración:
Demostremos que $\mathfrak{i}(X) = \{r \in R : rX = 0\}$ es un ideal izquierdo.

(i) Es claro que $0 \in \mathfrak{i}(X)$.

(ii) Si $a, b \in \mathfrak{i}(X)$ entonces $\forall x \in X : ax = 0 = bx$, entonces $ax - bx = 0$ lo que implica que $(a - b)x = 0$. Por lo tanto $a - b \in \mathfrak{i}(X)$.

(iii) Sean $r \in R$ y $a \in$, entonces $\forall x \in X : ax = 0$, por lo que, $rax = 0$. Por lo tanto $\forall a \in$: $ra \in \mathfrak{i}(X)$.
Dualmente $\mathfrak{d}(X)$ es un ideal derecho de R. ■

Proposición 2.6.8
Si I es un ideal izquierdo (derecho) en R, entonces $\mathfrak{i}(I)$ (respectivamente $\mathfrak{d}(I)$) es un ideal bilateral en R.
Demostración:
Por la proposición anterior $\mathfrak{i}(I)$ es un ideal izquierdo en R. Sean $r \in R$ y

$a \in \mathfrak{i}(I)$, entonces $\forall x \in I : (ar)x = a(rx) = 0$, ya que $rx \in I$. Así tenemos que $\forall r \in R : ar \in \mathfrak{i}(I)$. Por lo tanto $\mathfrak{i}(I)$ es un ideal derecho.
Dualmente $\mathfrak{d}(I)$ es un ideal bilateral. ■

Proposición 2.6.9
Para los ideales I de un anillo R, los anuladores derechos $\mathfrak{d}(I)$ forman una retícula. Dualmente los anuladores izquierdos $\mathfrak{i}(I)$ forman una retícula.
Demostración:
Demostremos este hecho para los anuladores derechos, la demostración para los anuladores izquierdos será de forma dual.
Primero proponemos la cuña y la yunta para los ideales derechos como:

$$\mathfrak{d}(I) \wedge \mathfrak{d}(J) = \mathfrak{d}(I) \cap \mathfrak{d}(J)$$
$$\mathfrak{d}(I) \vee \mathfrak{d}(J) = \mathfrak{d}(\mathfrak{i}(\mathfrak{d}(I) + \mathfrak{d}(J))).$$

(i) Es claro que $\mathfrak{d}(I) \cap \mathfrak{d}(J) \leq \mathfrak{d}(I), \mathfrak{d}(J)$. Ahora notemos que $\mathfrak{d}(I) \cap \mathfrak{d}(J) = \{a \in R : Ia = 0 = Ja\} = \{a \in R : (I + J)a = 0\} = \mathfrak{d}(I + J)$.

(ii) También es claro que $\mathfrak{d}(I), \mathfrak{d}(J) \leq \mathfrak{d}(\mathfrak{i}(\mathfrak{d}(I) + \mathfrak{d}(J)))$. Resta probar que $\mathfrak{d}(\mathfrak{i}(\mathfrak{d}(I) + \mathfrak{d}(J)))$ es la menor de las cotas superiores.
Supongamos que existe $\mathfrak{d}(K)$ tal que $\mathfrak{d}(I), \mathfrak{d}(J) \leq \mathfrak{d}(K)$.
Demostremos que $\mathfrak{d}(\mathfrak{i}(\mathfrak{d}(I) + \mathfrak{d}(J))) \leq \mathfrak{d}(K)$. Como $\mathfrak{d}(I), \mathfrak{d}(J) \leq \mathfrak{d}(K)$ entonces $\mathfrak{d}(I) + \mathfrak{d}(J) \leq \mathfrak{d}(K)$, lo que implica que $\mathfrak{i}(\mathfrak{d}(K)) \leq \mathfrak{i}(\mathfrak{d}(I) + \mathfrak{d}(J))$, pero $K \leq \mathfrak{i}(\mathfrak{d}(K))$, entonces $K \leq \mathfrak{i}(\mathfrak{d}(I) + \mathfrak{d}(J))$ y por lo tanto $\mathfrak{d}(\mathfrak{i}(\mathfrak{d}(I) + \mathfrak{d}(J))) \leq \mathfrak{d}(K)$.
Así $\mathfrak{d}(I) \vee \mathfrak{d}(J) = \mathfrak{d}(\mathfrak{i}(\mathfrak{d}(I) + \mathfrak{d}(J)))$. ■

Notación 3
Para un anillo R denotamos por $\mathscr{L}(.R)$ a la retícula de ideales izquierdos de R y dualmente a $\mathscr{L}(R.)$ a la de ideales derechos.

Proposición 2.6.10

Sean $\mathfrak{i} : \mathscr{L}(.R) \longrightarrow \mathscr{L}(R.)$ y $\mathfrak{d} : \mathscr{L}(R.) \longrightarrow \mathscr{L}(.R)$ tales que $\mathfrak{i}(I) = \{a \in R : aI = 0\}$ y $\mathfrak{d}(J) = \{a \in R : Ja = 0\}$, entonces $(\mathfrak{i}, \mathfrak{d})$ es una conexión de Galois entre $\mathscr{L}(.R)$ y $\mathscr{L}(R.)$.

<u>**Demostración:**</u>

(i) Si $I \subseteq J$. Veamos que $\mathfrak{i}(J) \subseteq \mathfrak{i}(I)$. Sea $a \in \mathfrak{i}(J) = \{a \in R | \forall j \in J : aj = 0\}$, entonces $aJ = 0$, pero como $I \subseteq J$, entonces $aI = 0$ y por lo tanto $a \in \mathfrak{i}(I)$. Es decir, $\mathfrak{i}(J) \subseteq \mathfrak{i}(I)$.

(ii) Si $I \subseteq J$ implica que $\mathfrak{d}(J) \subseteq \mathfrak{I}$ es dual al caso anterior.

(iii) Demostremos que $I \subseteq \mathfrak{d}(\mathfrak{i}(I))$. Sea $x \in I$, como para todo $a \in \mathfrak{i}(I)$ se cumple que $ax = 0$, entonces $x \in \mathfrak{d}(\mathfrak{i}(I))$. ■

Proposición 2.6.11

Si I es ideal izquierdo generado por un elemento idempotente e, entonces I es un ideal anulador izquierdo. De hecho $I = \mathfrak{i}((1-e)R)$.

<u>**Demostración:**</u>

Supongamos que I es un ideal izquierdo generado por un elemento idempotente, es decir, $I = Re$. Basta demostrar que se cumple la igualdad $Re = \mathfrak{i}((1-e)R)$.

[$\subseteq$] Sea $a \in Re$, entonces existe $s \in R$ tal que $a = se$. Así, tenemos que $a(1-e)r = se(1-e)r = (se - se^2)r = (se - se)r = 0$. Por lo tanto $a \in \mathfrak{i}((1-e)R)$.

[$\supseteq$] Sea $a \in \mathfrak{i}((1-e)R)$, entonces $\forall r \in R : a(1-e)r = 0 \Rightarrow (a - ae)r = 0$. Para $r = 1$ entonces $(a-ae)r = (a-ae)1 = 0$, entonces $a - ae = 0$ y por lo tanto $a = ae \in Re$. ■

Lema 2.6.1

Las siguientes proposiciones son equivalentes para un anillo A:

(a) Todo ideal anulador derecho es generado por un elemento idempotente.

(b) Todo ideal anulador izquierdo es generado por un elemento idempotente.

<u>**Demostración:**</u>
$[(a) \Rightarrow (b)]$ Supongamos que todo ideal anulador derecho es generado por un elemento idempotente, como para todo $S \subseteq A$ se tiene que $\mathfrak{d}(\mathfrak{i}(S))$ es un anulador derecho, entonces $\mathfrak{d}(\mathfrak{i}(S)) = eA$ para algún idempotente e, ya que, por hipótesis, todo ideal anulador derecho es generado por un idempotente. Entonces tenemos que $\mathfrak{i}(S) = \mathfrak{i}(\mathfrak{d}(\mathfrak{i}(S))) = \mathfrak{i}(eA)$. Ahora demostremos que $\mathfrak{i}(eA) = A(1-e)$. Para ello observemos que $a \in A(1-e) \Leftrightarrow \exists b \in A : a = b(1-e) \Leftrightarrow a(eA) = b(1-e)(eA) = (b-be)(eA) = beA - be^2A = 0 \Leftrightarrow a \in \mathfrak{i}(eA)$.
$[(b) \Rightarrow (a)]$ Es simétrico al caso anterior.

■

Ejemplo 50 (Completamiento de Dedekind-MacNeille)
Sea $\mathscr{L}$ una retícula. Para cada $T \subseteq \mathscr{L}$ sean:

$$\mathbf{CS}(T) = \{a \in \mathscr{L} : a \text{ es cota superior de } T\}$$
$$\text{y}$$
$$\mathbf{CI}(T) = \{a \in \mathscr{L} : a \text{ es cota inferior de } T\}$$

CS y **CI** definen una conexion de Galois del conjunto $\mathcal{P}(\mathscr{L})$ consigo mismo.

(i) Queremos demostrar que $S, T \in \mathcal{P}(\mathscr{L}) : S \subseteq T \Rightarrow \mathbf{CS}(T) \subseteq \mathbf{CS}(S)$. Sea $x \in \mathbf{CS}(T)$ entonces $\forall s \in S : t \leq x$. Como $S \subseteq T$ entonces $\forall s \in S : s \leq x$, por lo tanto $x \in \mathbf{CS}(S)$. De aquí que $\mathbf{CS}(T) \subseteq \mathbf{CS}(S)$.

(ii) Para $S, T \in \mathcal{P}(\mathscr{L}) : S \subseteq T \Rightarrow \mathbf{CI}(T) \subseteq \mathbf{CI}(S)$ la demostración es dual al caso anterior.

(iii) Demostremos que si $T \in \mathcal{P}(\mathscr{L})$ entonces $T \subseteq \mathbf{CS}(\mathbf{CI}(T))$. Por contradicción, supongamos que existe $t_0 \in T$ tal que $t_0 \notin \mathbf{CS}(\mathbf{CI}(T))$, es decir, t_0 no es cota superior de $\mathbf{CI}(T)$. Entonces existe $c \in \mathbf{CI}(T)$ tal que $t_0 < c$. Pero c es cota inferior de T en $\mathscr{L}$ y $t_0 \in T$. Lo que es una contradiccion y por lo tanto $T \subseteq \mathbf{CS}(\mathbf{CI}(T))$.

(iv) Dualmente si $T \in \mathcal{P}(\mathscr{L})$ entonces $T \subseteq \mathbf{CI}(\mathbf{CS}(T))$.

Además $\mathbf{CS}(T)$ es un filtro en $\mathscr{L}$ y $\mathbf{CI}(T)$ es un ideal en $\mathscr{L}$.

(i) Sean $c \in \mathbf{CS}(T)$ y $l \in L$ tales que $c \leq l$. Como $c \in \mathbf{CS}(T)$ entonces $\forall t \in T : t \leq c \leq l$ y por lo tanto l es cota superior de T en $\mathscr{L}$, es decir $l \in \mathbf{CS}(T)$.

(ii) Sean $a, b \in \mathbf{CS}(T)$, entonces $\forall t \in T : t \leq a$ y $t \leq b$, lo que implica que $\forall t \in T : t \leq a \wedge b$. Por lo tanto $a \wedge b \in \mathbf{CS}(T)$.

(iii) Si $\mathscr{L}$ tiene 1 es claro que $1 \in \mathbf{CS}(T)$.
Dualmente $\mathbf{CI}(T)$ es un ideal en $\mathscr{L}$.

Para cada $T \subseteq \mathscr{L}$ escribimos $\overline{T} = \mathbf{CI}(\mathbf{CS}(T))$. Los ideales T que son cerrados en el sentido de que $T = \overline{T}$ forman una retícula completa $\overline{\mathscr{L}}$. Donde

$$\bigwedge I_\alpha = \bigcap I_\alpha \qquad \text{y} \qquad \bigvee I_\alpha = \overline{\bigcup I_\alpha}.$$

Una Aplicación de las conexiones de Galois

El teorema fundamental de la teoría de Galois establece, bajo ciertas condiciones de una extensión de campos, una correspondencia biunívoca entre extensiones intermedias y subgrupos del grupo de Galois de dicha extensión. Esta correspondencia biunívoca invierte el orden entre ambas estructuras dado por la contención. En buena medida este resultado es impactante por la estrecha conexión que establece entre estructuras diferentes. La abstracción de esta situación lleva a una definición simple que genera una gama muy amplia de ejemplos de este tipo de conexiones (conexiones de Galois).

Definición 2.6.5

Si F es un subcampo de un campo E, decimos que E es una **extensión de campo** de F y se denota por E/F. La dimensión de E vista como F-espacio vectorial es llamada **grado** de F y se denota por $[E : F]$.

Definición 2.6.6

Sea E/F una extensión de campo. Su **grupo de Galois**, denotado por $\mathrm{Gal}(E/F)$, es el conjunto de automorfismos de E tales que fijan a F, es decir, que si $\sigma \in \mathrm{Gal}(E/F)$, entonces para todo $a \in F$ se tiene que $\sigma(a) = a$.

Definición 2.6.7

Sea $\mathrm{Aut}(E)$ el grupo de automorfismos de un campo E. Si G es un subconjunto de $\mathrm{Aut}(E)$, entonces $E^G = \{a \in E : \sigma(a) = a \text{ para todo } \sigma \in G\}$ es llamado el **campo fijo**.

Proposición 2.6.12

Si E es un campo, entonces la función $H \mapsto E^H$, de subconjuntos H de $\mathrm{Aut}(E)$ a subcampos de E, invierte el orden, es decir, si $H \leq G \leq \mathrm{Aut}(E)$, entonces $E^G \subseteq E^H$.

Demostración:

Sea $a \in E^G$, entonces para todo $\sigma \in G$ se tiene $\sigma(a) = a$. En particular, como $H \subseteq G$, es claro que para los $\alpha \in H$ se cumple $\alpha(a) = a$. Por lo tanto $a \in E^H$. ■

Definición 2.6.8

Una extensión de campo finita E/F es una **extensión de Galois** si $F = E^G$.

Definición 2.6.9
Dada una extensión de campo E/F, un **campo intermedio** es un campo I tal que $F \subset I \subset E$.

Lema 2.6.2
Si G es un conjunto de n automorfismos distintos de E, entonces:

$$[E : E^G] \geq n.$$

La demostración puede verse en [10, pág. 77].

Teorema 2.6.1
Si G es un subgrupo de n elementos de $\mathrm{Aut}(E)$, entonces:

$$[E : E^G] = |G|.$$

La demostración puede verse en [10, pág. 78].

Observación 25
Sean E/F una extensión de campo, $\mathscr{L}(E/F)$ la familia de campos intermedios y definamos $B \leq C$ como $B \subset C$. Entonces $\mathscr{L}(E/F)$ es una retícula con $B \vee C$ igual al campo generado por B y C y $B \wedge C = B \cap C$.

Lema 2.6.3
Sean $\mathscr{L}$ y $\mathscr{L}'$ retículas y $\varphi : \mathscr{L} \longrightarrow \mathscr{L}'$ una biyección tal que φ y φ^{-1} son morfismos que invierten orden. Entonces:

$$\varphi(a \wedge b) = \varphi(a) \vee \varphi(b) \text{ y } \varphi(a \vee b) = \varphi(a) \wedge \varphi(b).$$

Demostración:
Como $a, b \leq a \vee b$ tenemos que $\varphi(a \vee b) \leq \varphi(a), \varphi(b)$, entonces $\varphi(a \vee b)$ es una cota inferior de $\varphi(a), \varphi(b)$ y así se tiene que $\varphi(a \vee b) \leq \varphi(a) \wedge \varphi(b)$. Como φ es suprayectivo entonces existe $c \in \mathscr{L}$ tal que $\varphi(c) = \varphi(a) \wedge \varphi(b)$. Entonces $\varphi(c) = \varphi(a) \wedge \varphi(b) \leq \varphi(a), \varphi(b)$ y aplicando φ^{-1} se obtiene que

$a, b \leq c$. De aquí obtenemos que c es una cota superior de a y b, entonces $a \vee b \leq c$. Por lo tanto $\varphi(a) \wedge \varphi(b) = \varphi(c) \leq \varphi(a \vee b)$, lo que implica que $\varphi(a \vee b) = \varphi(a) \wedge \varphi(b)$. Dualmente se demuestra $\varphi(a \wedge b) = \varphi(a) \vee \varphi(b)$. ■

Teorema 2.6.2 (Teorema fundamental de la teoría de Galois)
Sea E/F una extensión de Galois finita con grupo de Galois $G = \mathrm{Gal}(E/F)$.

(i) La función

$$\gamma : \mathrm{Sub}(G) \longrightarrow \mathrm{Int}(E/F)$$

$$\gamma : H \mapsto E^H,$$

es una biyección que invierte orden cuya inversa

$$\delta : \mathrm{Int}(E/F) \longrightarrow \mathrm{Sub}(G)$$

$$\delta : B \mapsto \mathrm{Gal}(E/B),$$

también es una biyección que invierte orden.

(ii) Para cada $B \in \mathrm{Int}(E/F)$ y $H \in \mathrm{Sub}(G)$:

$$\gamma(\delta(B)) = E^{Gal(E/B)} = B \qquad \text{y} \qquad \delta(\gamma(H)) = \mathrm{Gal}(E/E^H) = H.$$

(iii) Para cualesquiera $H, K \in \mathrm{Sub}(G)$ y cualesquiera $B, C \in \mathrm{Int}(E/K)$:

$$E^{H \vee K} = E^H \cap E^K;$$

$$E^{H \cap K} = E^H \wedge E^K;$$

$$\mathrm{Gal}(E/B \vee C) = \mathrm{Gal}(E/B) \cap \mathrm{Gal}(E/C);$$

$$\mathrm{Gal}(E/B \cap C) = \mathrm{Gal}(E/B) \vee \mathrm{Gal}(E/C).$$

<u>Demostración:</u>

(i) Por la Proposición 2.6.3, γ es una función que invierte el orden.
Para demostrar que δ invierte el orden, sean $B, C \in \mathrm{Int}(E/F)$ tales que

$B \subseteq C$ y $\sigma \in \mathrm{Gal}(E/C)$, entonces $\sigma \in \mathrm{Aut}(E)$ y para todo $c \in C$ se cumple $\sigma(c) = c$, pero como $B \subseteq C$, en particular σ fija a los elementos de B, es decir, para todo $b \in B : \sigma(b) = b$.
Hemos demostrado que $\sigma \in \mathrm{Gal}(E/B)$ y por lo tanto

$$\mathrm{Gal}(E/C) = \delta(C) \leq \delta(B) = \mathrm{Gal}(E/B).$$

Por lo tanto δ invierte el orden.

Para ver que γ es inyectiva tenemos que demostrar que si G, H son subgrupos finitos de $\mathrm{Aut}(E)$ con $E^G = E^H$, entonces $G = H$.
Sea $\sigma \in G$, entonces es claro que σ fija a E^G. Para demostrar el recíproco, supongamos que σ fija a E^G y que $\sigma \notin G$. Entonces E^G es fijado por el grupo $G \cup \{\sigma\}$ de $n+1$ elementos, por el Lema 2.6.2 y el Teorema 2.6.1 tenemos la siguiente contradicción:

$$n = |G| = [E : E^G] \geq [E : E^{E \cup \{\sigma\}}] \geq n + 1.$$

Por lo tanto, si σ fija a E^G, entonces $\sigma \in G$.
Si $\sigma \in G$, entonces σ fija a $E^G = E^H$, y de aquí que $\sigma \in H$ y si $\sigma \in H$, entonces σ fija a $E^H = E^G$ y por tanto $\sigma \in G$. Concluimos que $G = H$.
Por lo tanto γ es inyectiva.
Que γ sea suprayectiva puede verse en [9, pág. 228] y [10, pág. 84], donde se demuestra que $\gamma\delta$ es la identidad en $\mathrm{Int}(E/G)$ y por lo tanto $B = E^{Gal(E/B)}$.
Por lo tanto γ es una biyección con inversa δ.

(ii) Esto se tiene por la parte *(i)*, pues $\delta\gamma$ y $\gamma\delta$ son funciones identidad.

(iii) Las primeras dos ecuaciones se tienen por el Lema 2.6.3, pues γ es una biyección que invierte el orden. La segunda pareja de ecuaciones se cumple porque $\delta = \gamma^{-1}$ también es una biyección que invierte el orden.

■

Observación 26

Notar que las funciones γ y δ del Teorema Fundamental de la Teoría de Galois cumplen lo siguiente:

(*i*) Para $G, H \in \mathrm{Sub}G : G \leq H \Longrightarrow \gamma(H) \leq \gamma(G)$.

(*ii*) Para $B, C \in \mathrm{Int}(E/F) : B \leq C \Longrightarrow \delta(C) \leq \delta(B)$.

(*iii*) Para $H \in \mathrm{Sub}(G)$ y para $B \in \mathrm{Int}(E/F)$ se tiene que $H \leq \delta(\gamma(H))$ y $B \leq \gamma(\delta(B))$. De hecho en el Teorema se demuestra la igualdad en ambos casos.

Por lo tanto la pareja de funciones (γ, δ) del Teorema Fundamental de la Teoría de Galois forman una conexión de Galois entre las retículas $\mathrm{Sub}(\mathrm{Gal}(E/F))$ e $\mathrm{Int}(E/F)$.

Conclusiones

El estudio de las retículas constituye por sí sólo un vasto campo de investigación que tiene muchas líneas de aplicación en el álgebra, y en otras ramas de las matemáticas, inclusive en lógica.
Las retículas son fundamentales en el estudio de las estructuras algebraicas, la retícula de un objeto algebraico describe su estructura y proporciona información importante, ya que la estructura puede verse a partir de partes más pequeñas y también el orden de éstas.
Por otro lado, al abstraer las propiedades esenciales del orden en las estructuras, las retículas son ideales para hablar de subestructuras comunes a los objetos algebraicos de hecho una estructura algebraica puede ser caracterizada de acuerdo a las propiedades de sus retículas subyacentes.
Se ha hecho más habitual, desde los 70's, para cada libro de Teoría de Módulos, señalar y demostrar algunas generalizaciones para retículas, casi siempre modulares. Esto ha sido justificado porque la estructura de un módulo sobre un anillo es mejor entendida en términos de la estructura reticular de la retícula de sus submódulos. Citando a Louis H. Rowen "este importante ejemplo (la retícula de todos los submódulos de un módulo) es la razón de ser para el estudio de la teoría de retículas por los estudiosos de la teoría de anillos". De hecho, muchos resultados de la Teoría de Módulos pueden ser demostrados usando solamente Teoría de Retículas.

Es un hecho indiscutible que el teorema fundamental de la teoría de Galois, en el que se sintetiza gran parte de la teoría de Galois, una de las más bellas áreas de la matemática, es un teorema de retículas, por lo que parece ocisoso hablar sobre la utilidad, generalidad y belleza de la teoría de retículas.

Apéndice A

Categorías

Definición A.0.1
Una **categoría** $\mathcal{C}$ está dada por una clase $\mathcal{C}_0$ de **objetos** y una clase $\mathcal{C}_1$ de **morfismos** que tienen la siguiente estructura:

(a) Cada morfismo tiene **dominio** y **codominio**, los cuales son objetos. Se escribe $f : X \to Y$ o $X \xrightarrow{f} Y$ si X es el dominio del morfismo ($X = dom(f)$) y Y es su codominio ($Y = cod(f)$).

(b) Dados dos morfismos f y g tales que $cod(f) = dom(g)$, es decir, se tiene que $X \xrightarrow{f} Y \xrightarrow{g} Z$; la composición de f y g, escrita como $X \xrightarrow{gf} Z$, tiene dominio $dom(f)$ y codominio $cod(g)$.

(c) La composición es **asociativa**, es decir, dados $X \xrightarrow{f} Y$, $Y \xrightarrow{g} Z$ y $Z \xrightarrow{h} W$, se cumple $h(gf) = (hg)f$.

(d) Para cada objeto X existe un **morfismo identidad** Id_X que satisface que para todo $Y \xrightarrow{g} X$ se cumple $Id_X g = g$ y para todo $X \xrightarrow{f} Y$ se cumple $f Id_X = f$.

Observación 27

Podemos denotar a $h = gf$ diciendo que el diagrama

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "h=gf"'] & Y \arrow[d, "g"] \\ & Z \end{tikzcd}$$

conmuta.

Ejemplo 51

1.- La categoría 1 tiene un objeto $*$ y un morfismo Id_*.

2.- 0 es la categroría vacía.

3.- **Set** es la categoría la cual tiene por clase de objetos a la clase de todos los conjuntos, sus morfismos son las funciones entre conjuntos y la composición es la usual.

4- **Grp** es la categoría de grupos y morfismos de grupos con la composición usual de funciones. Similarmente **Rng** es la categoría de anillos, **Mod** es la categoría de módulos donde sus morfismos son los de anillos y módulos, respectivamente y la composición es la usual.

5.- Un preorden es un conjunto X junto con una relación binaria $\leq$, la cual es reflexiva y transitiva. Este puede ser visto como una categoría, con la clase de objetos X y exactamente un morfismo: $x \to y$ si y sólo si $x \leq y$, donde la composición está dada por la transitividad.

6.- **Pos** es la categoría de COPOs y funciones preservadoras de orden donde la composición está dada por la composición usual de funciones.

7.- **Lat** es la categoría donde la clase de obejtos son retículas y los morfismos son los morfismos de retículas y su composición usual de funciones.

Definición A.0.2

Dadas dos categorías $\mathcal{C}$ y $\mathcal{D}$, un **funtor covariante** $F : \mathcal{C} \to \mathcal{D}$ consiste en dos operaciones $F_0 : \mathcal{C}_0 \to \mathcal{D}_0$ y $F_1 : \mathcal{C}_1 \to \mathcal{D}_1$ tal que para cada $X \xrightarrow{f} Y$ se tiene que $F_1(f) : F_0(X) \to F_0(Y)$ y

(a) Si $X \xrightarrow{f} Y \xrightarrow{g} Z$ entonces $F_1(gf) = F_1(g)F_1(f)$.

(b) Para todo $X \in \mathcal{C}$ se cumple $F_1(Id_X) = Id_{F_0(X)}$.

Ejemplo 52

Existe un funtor U : **Top** $\to$ **Set** el cual asigna a cualquier espacio topológico X su conjunto subyacente. Llamamos a este funtor **el funtor que olvida**, es decir. éste olvida la estructura matemática. Similarmente hay funtores que olvidan **Grp** $\to$ **Set**, **Rng** $\to$ **Set**, **Pos** $\to$ **Set**, **Lat** $\to$ **Set**, etc.

Ejemplo 53

Para cada pareja de categorías $\mathcal{C}$ y $\mathcal{D}$ podemos definir el **producto de categorías** $\mathcal{C} \times \mathcal{D}$, con objetos las parejas $(C, D) \in \mathcal{C}_0 \times \mathcal{D}_0$, y como morfismos $(C, D) \to (C', D')$, las parejas (f, g) tales que $C \xrightarrow{f} C'$ en $\mathcal{C}$ y $D \xrightarrow{g} D'$ en $\mathcal{D}$. Existen los funtores proyección $\pi_0 : \mathcal{C} \times \mathcal{D} \to \mathcal{C}$ y $\pi_1 : \mathcal{C} \times \mathcal{D} \to \mathcal{D}$.

Ejemplo 54

Para cada categoría $\mathcal{C}$ existe un único funtor $\mathcal{C} \to 1$ y un único funtor $0 \to \mathcal{C}$.

Ejemplo 55

Dados dos funtores $F : \mathcal{C} \to \mathcal{D}$ y $G : \mathcal{D} \to \mathcal{E}$ se puede definir la composición de funtores $GF : \mathcal{C} \to \mathcal{E}$.

Definición A.0.3

Dada una categoría $\mathcal{C}$ definimos la categoría $\mathcal{C}^{OP}$ la cual tiene los mismos objetos y morfismos que $\mathcal{C}$ pero con la dirección opuesta, es decir, si $X \xrightarrow{f} Y$ en $\mathcal{C}$ entonces $Y \xrightarrow{f} X$ en $\mathcal{C}^{OP}$. Para denotar esto escribimos $\overline{f}$ para el

morfismo $Y \longrightarrow X$ correspondiente a $X \xrightarrow{f} Y$ en $\mathcal{C}$.
La composición en $\mathcal{C}^{OP}$ se define como: $\overline{f}\,\overline{g} = \overline{gf}$.

Definición A.0.4

1.- Un morfismo $A \xrightarrow{f} B$ es **monomorfismo** en una categoría $\mathcal{C}$ si para cualquier otro objeto C y para cualquier pareja de morfismos
$g, h : C \longrightarrow A$, $fg = fh$ implica que $g = h$.

2.- Un morfismo $A \xrightarrow{f} B$ es **epimorfismo** en una categoría $\mathcal{C}$ si para cualquier otro objeto C y para cualquier pareja de morfismos
$g, h : B \longrightarrow C$, $gf = hf$ implica que $g = h$.

El Principio de Dualidad

Dada una propiedad P de un objeto, morfismo, diagrama, etc., podemos asociar con P la propiedad P^{OP}. El objeto, morfismo, etc. tiene la propiedad P^{OP} en $\mathcal{C}$ si y sólo si tiene la propiedad P en $\mathcal{C}^{OP}$.

Definición A.0.5

1.- Si para un morfismo $A \xrightarrow{f} B$ existe $B \xrightarrow{g} A$ tal que $fg = Id_B$ entonces g es llamado **sección** de f, y f es llamado **retracción** de g.

2.- $A \xrightarrow{f} B$ es un **isomorfismo** si existe $B \xrightarrow{g} A$ tal que $fg = Id_B$ y $gf = Id_A$. Decimos que f es el morfismo inverso de g y viceversa.

Observación 28

Toda sección es monomorfismo y toda retracción es epimorfismo.

Definición A.0.6

Definimos $\mathcal{C}(A, B)$ como la clase de morfismos entre dos objetos $A, B \in \mathcal{C}_0$.

Definición A.0.7
Un objeto X es un **objeto terminal** si para cualquier otro objeto Y existe un único morfismo $Y \to X$ en la categoría. Dualmente, X es un **objeto inicial** si para todo Y existe un único morfismo $X \to Y$. Es fácil ver que los objetos iniciales y terminales son únicos salvo isomorfismos.

Ejemplo 56
En la categoría **Set** el conjunto vacío es el objeto inicial y el conjunto unitario es el objeto terminal.

Definición A.0.8
Una **transformación natural** entre dos funtores $F, G : \mathcal{C} \longrightarrow \mathcal{D}$ consiste en una familia de morfismos $(\mu_C : FC \longrightarrow GC)_{C \in \mathcal{C}}$ que satisface que para cada morfismo $f : C \longrightarrow C'$, el diagrama

$$\begin{tikzcd} FC \arrow[r, "\mu_C"] \arrow[d, "Ff"'] & GC \arrow[d, "Gf"] \\ FC' \arrow[r, "\mu_{C'}"'] & GC' \end{tikzcd}$$

conmuta en $\mathcal{D}$.
Denotaremos a una transformación natural μ por $\mu = (\mu_C)_{C \in \mathcal{C}_0} : F \Rightarrow G$. Llamamos a μ_C la **componente** en C de la tranformación natural μ.

Ejemplo 57
Sean P y Q dos preórdenes vistos como categorías. Un funtor $P \longrightarrow Q$ es una función preservadora de orden y existe una única transformación natural entre dos funtores tal que $F \Rightarrow G$ si para todo $x \in P$ se cumple $F(x) \leq G(x)$.

Dos categorías isomorfas se consideran esencialmente la misma categoría. Un **isomorfismo de categorías** $\mathcal{C}$ y $\mathcal{D}$ requiere la existencia de funtores $F : \mathcal{C} \longrightarrow \mathcal{D}$ y $G : \mathcal{D} \longrightarrow \mathcal{C}$ tales que $FG = Id_{\mathcal{D}}$ y $GF = Id_{\mathcal{C}}$. Este concepto

de "igualdad" es muy restrictivo. Un concepto un poco más débil y más flexible es la noción de equivalencia de categorías, que se satisface mucho más frecuentemente.
Las categorías equivalentes tienen el mismo comportamiento con respecto a todas las propiedades categóricas interesantes.

Definición A.0.9

1.- Dos categorías $\mathcal{C}$ y $\mathcal{D}$ son **equivalentes** si existen funtores $F : \mathcal{C} \longrightarrow \mathcal{D}$ y $G : \mathcal{D} \longrightarrow \mathcal{C}$ y transformaciones naturales $\mu : Id_{\mathcal{C}} \Rightarrow GF$ y $\nu : Id_{\mathcal{D}} \Rightarrow FG$ tal que sus componentes son isomorfismos.

2.- F y G son llamados **pseudoinversos** uno del otro.

3.- Un funtor que tiene pseudoinverso es llamado **equivalencia** de categorías.

Un ejemplo importante de una equivalencia de categorías es la llamada "dualidad de Lindenbaum-Tarski" entre **Set** y las álgebras booleanas atómicas completas.

Definición A.0.10
Una **dualidad** entre dos categorías $\mathcal{C}$ y $\mathcal{D}$ es una equivalencia entre $\mathcal{C}^{OP}$ y $\mathcal{D}$ (equivalentemente, entre $\mathcal{D}^{OP}$ y $\mathcal{C}$).

Bibliografía

[1] Anderson, F. W., Fuller, R. K. *Rings and Categories of Modules*, segunda edición, Springer Verlag, New York, 1992.

[2] Dummit, D. S.,Foote, R. M., *Abstract Algebra*, John Wiley & Sons, Inc., Tercera Edición, 2004.

[3] Birkhoff, G., *Lattice Theory*, AMS Colloquium Publications, vol. XXV, Tercera Edición, 1967.

[4] Călugăreanu, G.,*Lattice Concepts of Module Theory*, Kluwer Academic Publishers, The Netherlands, 2000.

[5] Grätzer, G., *General Lattice Theory*, Segunda Edición, Birkhäuser Verlag, Berlín, 1998.

[6] Grätzer, G., *Lattice Theory* First Concepts and Distributive Lattices, Dover Publications, 2008.

[7] Grätzer, G., *Lattice Theory: Foundation*, Birkhäuser Verlag, Basel, 2010.

[8] Kasch, F., *Modules and Rings*, Academic Press, London, 1982.

[9] Rotman, J., *A First Course in Abstract Algebra*, Prentice Hall, 1996.

[10] Rotman, J., *Galois Theory*, Segunda Edición, Springer-Verlag, 1998.

[11] STERN, M., *Semimodular Lattices: Theory and Applications*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1999.

[12] STENTRÖM, BO, *Ring of Quotients* Springer-Verlag, New York, 1975.

[13] VAN OOSTEN, J., *Basic Category Theory*, Lecture Notes (83 pp). BRICS Lecture Series LS-95-01, 1995.