# Las retículas de prerradicales sobre los anillos $\mathbb{Z}_{p^n}$

Silvia Claudia Gavito Ticozzi

Director de Tesis: Dr. Rogelio Fernández-Alonso González

# Agradecimientos

Aunque la conclusión del camino que falta por recorrer se vislumbra aún lejana, quisiera aprovechar esta pausa para agradecer y expresar mi más sincero reconocimiento a todas las personas que me han ayudado a completar este trecho.

En primer lugar, y aunque las palabras siempre resultan insuficientes al referirme a ella, quisiera agradecer a mi grandiosa familia: a mis padres, Paola y José Luis, por su apoyo incondicional y a mi incomparable hermana Sandra, por ser mi eterna cómplice y mi pequeña hermana mayor en muchos sentidos. Ringrazio anche alla mia cara nonnina, che è sempre stata un esempio per me, per trasmettermi la sua gioia di vivere.

Sin duda esta meta no habría podido ser alcanzada sin la ayuda y guía de tantos excelentes profesores; en especial, quisiera agradecer al Dr. Rogelio Fernández Alonso, a quien debo prácticamente toda mi formación algebraica, por su generosidad, su inagotable paciencia y por compartir conmigo su gran calidad humana y académica. Excluyendo a los inevitables errores, de los cuales sólo yo soy responsable, éste trabajo es, sin duda, también suyo. Deseo agradecer, asimismo, a mis sinodales: el Dr. José Ríos y el Dr. Mario Pineda, por su gran disposición para revisar este trabajo, por sus oportunas correcciones y por sus invaluables sugerencias y opiniones.

Agradezco al CONACyT y a mi Universidad las becas que me permitieron realizar mis estudios y desarrollar este trabajo de tesis. Quisiera diri-

gir un reconocimiento especial al Departamento de Matemáticas de la UAM-Iztapalapa, encabezado por el Dr. Carlos Signoret, de quien he recibido apoyo permanente, y a la Dra. Shirley Bromberg, Coordinadora del Posgrado, por todas las facilidades que me brindó durante la etapa crucial de mis estudios de maestría. En particular, agradezco de corazón a la Dra. Lourdes Palacios y a la Dra. Laura Hidalgo, por su inconmensurable apoyo, por haberme brindado invaluables oportunidades de crecer y mejorar mi formación matemática, así como por sus valiosísimos consejos y recomendaciones.

Elsa Báez: Para ellas va además toda mi admiración y respeto.

Gracias también a mis compañeros del cubículo de Posgrado, en especial a Rosa María, Leopoldo e Ismael, por su ayuda, interés y consejos, así como a las secretarias: Beatriz, Silvia, Lourdes, Ana y Michel, por su gentileza y apoyo.

Gracias a Gaby, Jessy y Víctor Daniel, por darme el maravilloso regalo de su amistad.

Por último, gracias Manuel, por todo tu cariño, por el interés que siempre muestras hacia todo lo que hago, en particular hacia este trabajo al que también aportaste tu gran talento matemático y técnico, y por soportar con heroica paciencia y amorosa comprensión mis ataques de nervios. Te amo.

# Índice general

# Introducción

Si bien existen referencias aisladas previas del concepto de prerradical como cierto tipo de funtor sobre la categoría de $R-$módulos, son los matemáticos de origen checo L. Bican, P. Jambor, T. Kepka y P. Němec los primeros en manifestar la necesidad de proveer, en sus propias palabras, "un antecedente de la teoría de prerradicales" ([2], pág. 75), así como de investigar más profundamente sus propiedades.

En nuestro país, el grupo de Teoría de Anillos, constituido por los investigadores[1] Rogelio Fernández-Alonso, Francisco Raggi, Hugo Rincón, José Ríos y Carlos Signoret, de tres distintos centros de investigación (el Departamento de Matemáticas de la UAM-Iztapalapa, el Instituto de Matemáticas de la UNAM y la Facultad de Ciencias de la UNAM), ha estudiado la teoría de prerradicales sobre un anillo $R$ (asociativo, con elemento unitario y no necesariamente conmutativo) desde un punto de vista reticular, el cual ha probado ser muy útil no sólo en diversas ramas del Álgebra, sino de la matemática en general. En este contexto aparece el problema de describir la estructura de la retícula de prerradicales sobre $R$. Al respecto, surge la cuestión de saber en qué casos es posible dar respuesta a preguntas como las siguientes:

1) ¿Es la retícula de prerradicales sobre $R$ un conjunto? Y, de serlo, ¿es finito?

2) ¿Es distributiva la retícula de prerradicales sobre $R$?

[1] En riguroso orden alfabético.

3) ¿Es posible describir los elementos irreducibles y primos de la retícula de prerradicales sobre $R$?

El objetivo principal del presente trabajo es ofrecer una descripción de la retícula de prerradicales sobre $R$ y responder a las preguntas $1)-3)$, en el caso especial de $R = \mathbb{Z}_{p^n}$, donde $p$ es un número primo y $n \geq 1$. Para tal propósito se hace uso de diversas teorías de la matemática, tales como: la Teoría de Retículas[2] (que es posible ubicar dentro de la Combinatoria), la Teoría de Anillos y Módulos y, por supuesto, la Teoría de Prerradicales. Esta suerte de "eclecticismo" desde el punto de vista metodológico es quizás la característica primordial de este trabajo, el cual se compone de cinco capítulos. Presentamos a continuación el contenido sintético de cada uno de ellos.

En el primer capítulo se establecen los conceptos y propiedades elementales de la Teoría de Retículas y de la Teoría de Anillos y Módulos. Asimismo, aunque de manera muy concisa, se presentan los elementos básicos de la Teoría de Categorías y Funtores. Lo anterior, con el fin de contar con los prerrequisitos necesarios para introducir la noción de prerradical.

En el segundo capítulo se presenta la teoría básica de prerradicales y sus propiedades.

En el tercer capítulo destaca un resultado de la Teoría de Grupos (abelianos) probado en la década de los 40's por el matemático ruso L. Ya. Kulikov, al que en adelante nos referiremos como el Teorema de Kulikov, el cual ofrece un criterio para determinar bajo qué condiciones un $p-$grupo es suma directa de subgrupos cíclicos.

Por su parte, el cuarto capítulo está destinado a presentar tres retículas que resultan ser isomorfas y que cuentan con propiedades muy importantes.

Finalmente, en el quinto capítulo desemboca, se unifica y cobra sentido el material expuesto en los capítulos anteriores : como consecuencia del Teorema de Kulikov, el comportamiento de los prerradicales sobre $\mathbb{Z}_{p^n}$ depende sólo de

[2]En inglés, 'Lattice Theory'.

su conducta sobre los ideales de éste último, los cuales forman una cadena de longitud $n$. Gracias a este comportamiento, y al hecho de que la retícula de prerradicales sobre $\mathbb{Z}_{p^n}$ resulta ser isomorfa a las retículas estudiadas en el Capítulo 4, es posible llevar a cabo nuestro objetivo inicial de manera bastante sencilla.

Ahora bien, una vez alcanzado este primer peldaño, una pregunta natural es si se puede generalizar a una clase más extensa de anillos la situación anterior. La respuesta es afirmativa si se consideran anillos $R$ del tipo de $\mathbb{Z}_{p^n}$, es decir, anillos locales (con un único ideal máximo) y que cumplan una propiedad análoga a la del Teorema de Kulikov, esto es, que todo $R-$módulo (izquierdo y derecho) pueda escribirse como suma directa de submódulos cíclicos. Tales anillos reciben el nombre de anillos de Köthe ([5]). En particular, todo anillo uniserial (artiniano de ideales principales) es de Köthe. Luego, todo anillo uniserial local cumple con las condiciones deseadas y es posible generalizar el tratamiento expuesto más adelante para dicho tipo de anillos (ver [10]). De esta manera, el presente trabajo abre la puerta a la búsqueda de clases de anillos sobre los que se pueda hacer una descripción similar de la retícula de prerradicales.

# Capítulo 1

# Preliminares

A fin de que el presente trabajo sea lo más autocontenido posible, en este primer capítulo se presentan las definiciones y propiedades básicas relativas a conjuntos parcialmente ordenados y retículas, grupos y módulos, así como el lenguaje categórico necesario y gran parte de la notación y terminología que se usarán en lo subsecuente. Se suponen conocidos algunos conceptos elementales como los de relación y diagrama de Hasse. Además, omitimos la demostración de algunos resultados al considerarlos del dominio común, o bien, al ser ejercicios de alguna fuente citada en la bibliografía. En este último caso, se anexa a la propiedad la referencia correspondiente.

## 1.1. *Copos* y retículas

### 1.1.1. Conjuntos parcialmente ordenados

**Definición 1.1** *Una relación* " $\leq$ " *sobre un conjunto* $P$ *es un orden parcial si es:*

*1) Reflexiva :* $\forall\ a \in P\ (a \leq a)$

*2) Antisimétrica :* $\forall\ a, b \in P\ [(a \leq b\ \ y\ \ b \leq a) \Rightarrow a = b]$

*3) Transitiva :* $\forall\ a, b, c \in P\ [(a \leq b\ \ y\ \ b \leq c) \Rightarrow a \leq c]$.

*En tal caso, se llama a la pareja* $\langle P, \leq \rangle$ *un conjunto parcialmente ordenado o copo.*

**Notación 1.2** *Denotaremos por* $a \geq b$ *a la expresión* $b \leq a$. *Asimismo, se usará la notación* $a < b$ $(b > a)$ *para abreviar la condición* $a \leq b,\ a \neq b$ $(a \geq b,\ a \neq b)$.

**Definición 1.3** *Sean* $\langle P, \leq \rangle$ *y* $\langle P', \preceq \rangle$ *dos copos y sea* $f : P \longrightarrow P'$ *una función.*

*1.a) Se dice que* $f$ *es un homomorfismo de copos que preserva el orden si* $\forall\ a, b \in P\ [a \leq b \Rightarrow f(a) \preceq f(b)]$.

*1.b) Se dice que* $f$ *es un homomorfismo de copos que invierte el orden si* $\forall\ a, b \in P\ [a \leq b \Rightarrow f(a) \succeq f(b)]$.

*2.a) Decimos que* $f$ *es un isomorfismo de copos si* $f$ *es una función biyectiva tal que* $\forall\ a, b \in P\ [a \leq b \Leftrightarrow f(a) \preceq f(b)]$.

*2.b) Decimos que* $f$ *es un anti-isomorfismo de copos si* $f$ *es una función biyectiva tal que* $\forall\ a, b \in P\ [a \leq b \Leftrightarrow f(a) \succeq f(b)]$.

**Observación 1.4** *Sean* $\langle P, \leq \rangle$ *y* $\langle P', \preceq \rangle$ *dos copos y sea* $f : P \longrightarrow P'$ *una función biyectiva con inversa* $f^{-1} : P' \longrightarrow P$. *Entonces* $f$ *es un (anti-) isomorfismo de copos si y sólo si tanto* $f$ *como su inversa* $f^{-1}$ *(invierten) preservan el orden.*

**Definición 1.5** *Sean* $\langle P, \leq \rangle$ *un copo y* $Q \subseteq P$. *Entonces existe un orden parcial natural "* $\leq_Q$ *" sobre* $Q$, *inducido por "* $\leq$ *", tal que para* $a, b \in Q$ *se tiene que* $a \leq_Q b$ *si y sólo si* $a \leq b$. *Llamamos a* $\langle Q, \leq_Q \rangle$ *(o, simplemente,* $\langle Q, \leq \rangle$*) un subcopo de* $\langle P, \leq \rangle$.

En adelante, denotaremos a la cardinalidad de un conjunto $P$ por $|P|$.

Sea $\langle P, \leq \rangle$ un *copo*. Diremos que $\langle P, \leq \rangle$ es finito si $|P| < \infty$.

**Definición 1.6** *Un copo $\langle P, \leq \rangle$ se llama plano si tiene un diagrama de Hasse tal que ningún par de aristas se intersectan en un punto distinto de sus vértices.*

**Definición 1.7** *Dado un copo $\langle P, \leq \rangle$, con $a, b \in P$ tales que $a \leq b$, se define el intervalo determinado por $a$ y $b$ como:*

$$[a, b] := \{c \in P \mid a \leq c \leq b\}.$$

**Definición 1.8** *Dado un copo $\langle P, \leq \rangle$, con $a, b \in P$, se dice que $a$ cubre $a$ $b$ si $b < a$ y no existe $c \in P$ tal que $b < c < a$.*

**Observación 1.9** *Dado un copo $\langle P, \leq \rangle$, con $a, b \in P$, se tiene que $a$ cubre $a$ $b$ si y sólo si $b < a$ y $[b, a] = \{a, b\}$.*

**Definición 1.10** *Sean $\langle P, \leq \rangle$ un copo y $Q \subseteq P$. Decimos que $m \in Q$ es:*

*1.a) el elemento menor de $Q$, si para todo $a \in Q$, $m \leq a$;*

*1.b) el elemento mayor de $Q$, si para todo $b \in Q$, $b \leq m$;*

*2.a) un elemento mínimo de $Q$, si no existe $a \in Q$ tal que $a < m$;*

*2.b) un elemento máximo de $Q$, si no existe $b \in Q$ tal que $m < b$.*

Los elementos menor y mayor de un *copo* suelen denotarse por **0** y **1**, respectivamente.

**Definición 1.11** *Sean $\langle P, \leq \rangle$ un copo y $Q \subseteq P$. Decimos que $c \in P$ es:*

*1.a) una cota inferior de $Q$, si para todo $a \in Q$, $c \leq a$;*

*1.b) una cota superior de $Q$, si para todo $b \in Q$, $b \leq c$;*

*2.a) el ínfimo de $Q$, si es la mayor cota inferior de $Q$ (si existe);*

*2.b) el supremo de $Q$, si es la menor cota superior de $Q$ (si existe).*

**Definición 1.12** *Sea $\langle P, \leq \rangle$ un copo con elemento menor y elemento mayor $\mathbf{0}$ y $\mathbf{1}$, respectivamente.*

1) *Un elemento $a \in P$, $a \neq \mathbf{0}$, se llama átomo si no existe $b \in P$ tal que $\mathbf{0} < b < a$.*

2) *Un elemento $a \in P$, $a \neq \mathbf{1}$, se llama coátomo si no existe $b \in P$ tal que $a < b < \mathbf{1}$.*

**Observación 1.13** *Dado un copo $\langle P, \leq \rangle$ con elemento menor $\mathbf{0}$ y elemento mayor $\mathbf{1}$, las siguientes afirmaciones son equivalentes para un elemento $b \in P$:*

*(a) $b$ cubre a $\mathbf{0}$ ($\mathbf{1}$ cubre a $b$).*

*(b) $b$ es un elemento mínimo (máximo) en el subcopo $\langle P \setminus \{\mathbf{0}\}, \leq \rangle$ ($\langle P \setminus \{\mathbf{1}\}, \leq \rangle$).*

*(c) $b$ es un átomo (coátomo).*

**Definición 1.14** *Sea $\langle C, \leq \rangle$ un copo. Si el orden parcial " $\leq$ " sobre $C$ satisface además la propiedad:*

$$\forall\ a, b \in C\ (a \leq b \ \text{ ó } \ a \geq b),$$

*decimos que es un orden total o lineal. En este último caso, se dice que cualesquiera dos elementos de $C$ son comparables y se llama al copo $\langle C, \leq \rangle$ una cadena.*

**Observación 1.15** *Si $\langle C, \leq \rangle$ es una cadena y $Q \subseteq C$, entonces $m \in Q$ es un elemento menor (mayor) de $Q$ si y sólo si $m$ es un elemento mínimo (máximo) de $Q$. En tal caso, escribiremos:*

$$m := \min Q \quad (m := \max Q).$$

**Definición 1.16** *Un copo $\langle P, \leq \rangle$ se llama inductivo si toda cadena en $\langle P, \leq \rangle$ tiene una cota superior en $P$.*

**Lema 1.17** *(Lema de Zorn)*
*Todo copo inductivo no vacío tiene (al menos) un elemento máximo.*

**Observación 1.18** *Si en el conjunto de cadenas en un copo no vacío $\langle P, \leq \rangle$ consideramos el orden dado por la contención, entonces, como la unión de una cadena de cadenas es también una cadena, se sigue del Lema de Zorn la existencia de (al menos) una cadena máxima en $\langle P, \leq \rangle$.*

**Definición 1.19** *Sea $\langle C, \leq \rangle$ una cadena finita en un copo $\langle P, \leq \rangle$. Se define la longitud de $\langle C, \leq \rangle$ como $|C| - 1$.*

Un *copo* $\langle P, \leq \rangle$ satisface la *Condición de Cadena de Jordan-Dedekind* si todas las cadenas máximas entre dos puntos fijos de $P$ tienen la misma longitud.

**Definición 1.20** *Sea $\langle P, \leq \rangle$ un copo. Si toda cadena máxima en $\langle P, \leq \rangle$ tiene la misma longitud $n$ decimos que $\langle P, \leq \rangle$ es graduado, de rango $n$.*

El siguiente teorema nos ofrece una útil caracterización de *copo* graduado.

**Teorema 1.21** *Para un copo finito $\langle P, \leq \rangle$ con elemento menor $\mathbf{0}$ y elemento mayor $\mathbf{1}$, son equivalentes las siguientes condiciones:*

*(a) $\langle P, \leq \rangle$ satisface la Condición de Cadena de Jordan-Dedekind.*

*(b) Todas las cadenas máximas en $\langle P, \leq \rangle$ tienen la misma longitud.*

*(c) Existe una función $\rho : P \longrightarrow \mathbb{N}$, tal que:*

*(i) $\rho(\mathbf{0}) = 0$.*

*(ii) Para cada $a, b \in P$, si $a$ cubre a $b$, entonces $\rho(a) = \rho(b) + 1$.*

*Demostración.*

$(a) \Rightarrow (b)$. Se sigue de inmediato del hecho de que toda cadena máxima debe incluir a $\mathbf{0}$ y a $\mathbf{1}$.

$(b) \Rightarrow (c)$. Sea $a \in P$ y sea $\mathbf{0} = a_0 < a_1 < \cdots < a_r = a < \cdots < a_n = \mathbf{1}$ una cadena máxima. Definimos $\rho : P \longrightarrow \mathbb{N}$ tal que $\rho(a) := r$. Nótese que esta definición no depende de la cadena ya que si $\mathbf{0} = b_0 < b_1 < \cdots < b_s = a < \cdots < b_m = \mathbf{1}$ es otra cadena máxima, entonces, por hipótesis, debe ocurrir que $n = m$ y, por tanto, también debe suceder que $r = s$, pues de lo contrario podríamos construir una cadena máxima de longitud distinta de $n$. Por lo tanto, $\rho$ es una función bien definida que claramente satisface las propiedades $(i)$ y $(ii)$ de $(c)$.

$(c) \Rightarrow (a)$. Sean $a, b \in P$ y supongamos que las cadenas $a = a_0 < a_1 < \cdots < a_n = b$ y $a = b_0 < b_1 < \cdots < b_m = b$ son máximas. Entonces se tiene que $\rho(a_1) = \rho(a)+1 = \rho(b_1)$, $\rho(a_2) = \rho(a_1)+1 = \rho(b_1)+1 = \rho(b_2), \ldots,$ $\rho(b) = \rho(a_n) = \rho(a_{n-1}) + 1 = \rho(b_{n-1}) + 1 = \rho(b_n)$. Luego, $n = m$, pues si $n < m$, entonces $\rho(b) = \rho(b_m) > \rho(b_n)$, una contradicción. Similarmente, se obtiene una contradicción de suponer que $n > m$. □

La función presentada en el inciso $(c)$ del Teorema 1.21 recibe el nombre de *función de graduación*.

**Definición 1.22** *Para un copo finito $\langle P, \leq \rangle$ con elemento menor $\mathbf{0}$, elemento mayor $\mathbf{1}$ y con función de graduación $\rho : P \longrightarrow \mathbb{N}$, se define el rango de un elemento $a \in P$ como $\rho(a)$. Luego, $\langle P, \leq \rangle$ es de rango $n$ si $\rho(\mathbf{1}) = n$.*

### 1.1.2. Retículas

**Definición 1.23** *Un copo $\langle L, \leq \rangle$ es una retícula si para cada $a, b \in L$ existen el supremo y el ínfimo de $\{a, b\}$ (que denotaremos por $a \vee b$ y $a \wedge b$, respectivamente).*

**Definición 1.24** *Sean* $\langle L, \leq, \vee, \wedge\rangle$ *y* $\langle L', \preceq, \vee, \wedge\rangle$ *dos retículas. Una función* $f : L \longrightarrow L'$ *es un*

1) *homomorfismo de retículas, si:*

$\forall\, a, b \in L\ [f(a \wedge b) = f(a) \wedge f(b)\ \ y\ \ f(a \vee b) = f(a) \vee f(b)]$;

2) *anti-homomorfismo de retículas, si:*

$\forall\, a, b \in L\ [f(a \wedge b) = f(a) \vee f(b)\ \ y\ \ f(a \vee b) = f(a) \wedge f(b)]$;

3) *isomorfismo (anti-isomorfismo) de retículas, si es un homomorfismo (anti-homomorfismo) de retículas biyectivo.*

Sea $\langle L, \leq, \vee, \wedge\rangle$ una retícula. En adelante denotaremos por $Id_L$ al isomorfismo identidad de $L$ en $L$. Además, como es natural, diremos que dos retículas son isomorfas si existe un isomorfismo de retículas entre ellas.

Intuitivamente es plausible que todo (anti-)isomorfismo de retículas es un (anti-)isomorfismo de *copos*. No obstante, como las operaciones reticulares se definen en términos del orden, también resulta que todo (anti-)isomorfismo de *copos* es un (anti-)isomorfismo de retículas, como lo afirma el siguiente:

**Teorema 1.25** *Sean* $\langle L, \leq, \vee, \wedge\rangle$ *y* $\langle L', \preceq, \vee, \wedge\rangle$ *dos retículas. Una función* $h : L \longrightarrow L'$ *es un isomorfismo (anti-isomorfismo) de copos si y sólo si es un isomorfismo (anti-isomorfismo) de retículas.*

*Demostración.* Sea $h : L \longrightarrow L'$ es un isomorfismo de *copos*. Por la Observación 1.4, tanto $h$ como su inversa $h^{-1} : L' \longrightarrow L$ preservan el orden. Luego, $h(a \wedge b) \preceq h(a)$ y $h(a \wedge b) \preceq h(b)$, de donde $h(a \wedge b) \preceq h(a) \wedge h(b)$. Por otro lado, $h(a) \wedge h(b) \preceq h(a)$ y $h(a) \wedge h(b) \preceq h(b)$, de donde $h^{-1}(h(a) \wedge h(b)) \leq a$ y $h^{-1}(h(a) \wedge h(b)) \leq b$. Por tanto, $h^{-1}(h(a) \wedge h(b)) \leq a \wedge b$; es decir, $h(a \wedge b) \succeq h(a) \wedge h(b)$. Se sigue que $h(a \wedge b) = h(a) \wedge h(b)$. Análogamente, $h(a \vee b) = h(a) \vee h(b)$. Concluimos que $h$ es un isomorfismo de retículas.

Supongamos ahora que $h : L \longrightarrow L'$ es un isomorfismo de retículas y sean $a, b \in L$ tales que $a \leq b$. Por un lado, $h(a) = h(a \wedge b) = h(a) \wedge h(b) \preceq h(b)$. Por tanto, $h$ preserva el orden. Por otra parte, si $a', b' \in L'$, entonces existen $a, b \in L$ tales que $h(a) = a'$ y $h(b) = b'$. Luego, si $a' \preceq b'$ se tiene que $h^{-1}(a') = h^{-1}(a' \wedge b') = h^{-1}(h(a) \wedge h(b)) = h^{-1}(h(a \wedge b)) = a \wedge b \leq b = h^{-1}(h(b)) = h^{-1}(b')$. Por tanto, $h^{-1}$ preserva el orden. Se sigue de la Observación 1.4 que $h$ es un isomorfismo de *copos*.
La demostración para el caso en el que $h$ es anti-isomorfismo es similar. □

**Definición 1.26** *Una subretícula $\langle K, \leq, \vee, \wedge \rangle$ de una retícula $\langle L, \leq, \vee, \wedge \rangle$ es un subconjunto $K$ de $L$ tal que para cada $a, b \in K$ se tiene que $a \vee b \in K$ y $a \wedge b \in K$.*

**Definición 1.27** *Decimos que $\langle L, \leq, \vee, \wedge \rangle$ es una retícula completa si para cada subconjunto $\{a_i\}_{i \in I}$ de elementos de $L$ existen el supremo de $\{a_i\}_{i \in I}$ y el ínfimo de $\{a_i\}_{i \in I}$ (denotados por $\bigvee_{i \in I} a_i$ y $\bigwedge_{i \in I} a_i$, respectivamente).*

**Definición 1.28** *Decimos que $\langle L, \leq, \vee, \wedge \rangle$ es una retícula:*

1) *distributiva, si para cada $a, b, c \in L$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$;*

2) *modular, si para cada $a, b, c \in L$, con $b \leq a$, se tiene que $a \wedge (b \vee c) = b \vee (a \wedge c)$;*

3) *autodual, si existe un anti-isomorfismo $f : L \longrightarrow L$;*

4) *graduada, si $\langle L, \leq \rangle$ como copo es graduado;*

5) *finita, si $\langle L, \leq \rangle$ como copo es finito;*

6) *plana, si $\langle L, \leq \rangle$ como copo es plano.*

**Observación 1.29** *Toda retícula distributiva es modular.*

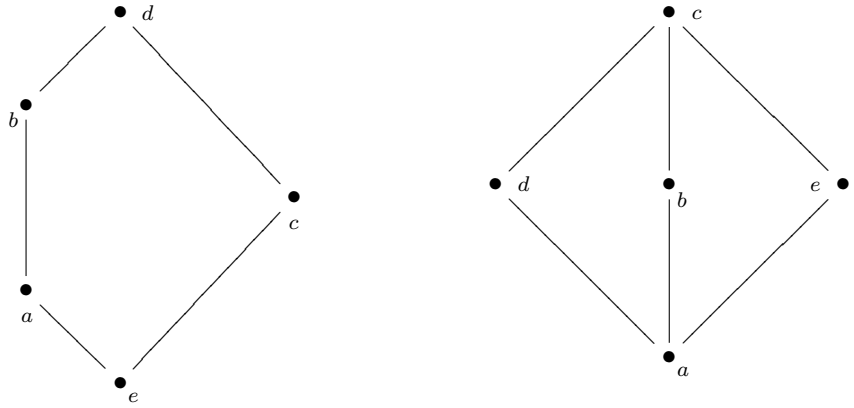



Figura 1.1: Diagramas pentagonal y de diamante.

Presentamos enseguida útiles criterios que caracterizan a las retículas distributivas y a las retículas distributivas finitas planas, mismos que corresponden a los Ejercicios 2.6 de [1] y II.1.45 de [12], respectivamente.

**Teorema 1.30** *Una retícula es distributiva si y sólo si no contiene subretículas cuyos diagramas de Hasse sean pentagonales o de diamante (véase la Figura 1.1).*

**Teorema 1.31** *Una retícula distributiva finita $\langle L, \leq, \vee, \wedge \rangle$ es plana si y sólo si no existe un elemento cubierto por otros tres elementos en $L$.*

**Definición 1.32** *Dada una retícula $\langle L, \leq, \vee, \wedge \rangle$ con elemento menor $\mathbf{0}$ y elemento mayor $\mathbf{1}$, decimos que $L$ es atómica (coatómica), si para cada $b \in L$, $b \neq \mathbf{0}$ ($b \neq \mathbf{1}$), existe un átomo (coátomo) $a \in L$ tal que $a \leq b$ ($a \geq b$).*

**Definición 1.33** *Dada una retícula $\langle L, \leq, \vee, \wedge \rangle$, un elemento $a \in L$ es:*

1) *$\wedge -$ irreducible, o simplemente irreducible, si:*
   $\forall\, c, d \in L\ [a = c \wedge d \Rightarrow (a = c \ \ \acute{o} \ \ a = d)]$.

2) *$\vee -$ irreducible, o coirreducible, si:*
   $\forall\, c, d \in L\ [a = c \vee d \Rightarrow (a = c \ \ \acute{o} \ \ a = d)]$.

Sea $\langle L, \leq, \vee, \wedge \rangle$ una retícula con elemento menor $\mathbf{0}$ y elemento mayor $\mathbf{1}$. En adelante, denotaremos por $[L]_{\wedge}$ al conjunto de todos los elementos irreducibles $a \neq \mathbf{1}$ de $L$; y, por $[L]_{\vee}$, al conjunto de todos los elementos coirreducibles $a \neq \mathbf{0}$ de $L$.

### 1.1.3. Producto de retículas

Muchas retículas importantes pueden ser representadas de manera más conveniente como combinaciones aritméticas de retículas más pequeñas si se usa una generalización de las operaciones aritméticas suma, producto y exponenciación. Nosotros nos restringiremos a hablar de las dos últimas.

**Definición 1.34** *Dadas dos retículas* $\langle L, \leq, \vee_L, \wedge_L \rangle$ *y* $\langle L', \leq', \vee_{L'}, \wedge_{L'} \rangle$,[1] *se define el producto* $LL'$ *como el conjunto:*

$$LL' := \{(a, a') \mid a \in L,\, a' \in L'\}.$$

*Si definimos el orden "* $\preceq$ *" en* $LL'$ *como:*

$$((a, a') \preceq (b, b')) \Leftrightarrow (a \leq b \quad y \quad a' \leq' b'),$$

*resulta que* $\langle LL', \preceq \rangle$ *es un copo.*
*Más aún, se tiene que* $\langle LL', \preceq, \vee, \wedge \rangle$ *es una retícula, con el supremo y el ínfimo dados, de manera natural, por:*

*1)* $(a, a') \vee (b, b') = (a \vee_L b,\, a' \vee_{L'} b')$,

*2)* $(a, a') \wedge (b, b') = (a \wedge_L b,\, a' \wedge_{L'} b')$.

La definición anterior se puede generalizar para el producto de $n$ retículas, $L_1 L_2 \cdots L_n$, con $n \geq 1$. De hecho, se tiene una generalización aún mayor, como lo afirma la siguiente:

[1] Para evitar confusiones, en esta definición distinguimos mediante la notación a los supremos e ínfimos de $L$ y $L'$.

**Definición 1.35** *Dadas dos retículas* $\langle L, \leq, \vee_L, \wedge_L \rangle$ *y* $\langle L', \leq', \vee_{L'}, \wedge_{L'} \rangle$, *se define a* $L^{L'}$ *como el conjunto de todos los homomorfismos de retículas* $f : L' \longrightarrow L$. *Dicho conjunto, con el orden dado por* $f \preceq g \Leftrightarrow f(a') \leq g(a')$ *para cada* $a' \in L'$, *y con el supremo e ínfimo dados por:*

1) $f \vee g := h_1$, *con* $h_1 : L' \longrightarrow L$ *un homomorfismo de retículas tal que para cada* $a' \in L'$, $h_1(a') = f(a') \vee_L g(a')$,

2) $f \wedge g := h_2$, *con* $h_2 : L' \longrightarrow L$ *un homomorfismo de retículas tal que para cada* $a' \in L'$, $h_2(a') = f(a') \wedge_L g(a')$,

*resulta ser una retícula.*

**Ejemplo 1.36** *Presentamos un ejemplo al cual haremos referencia más adelante. Para cada* $n \in \mathbb{N}$ *denotaremos por* $\mathbf{n+1}$ *al conjunto* $\{0, 1, 2, \ldots, n\}$. *Claramente,* $\langle \mathbf{n+1}, \leq \rangle$, *con el orden heredado de* $\langle \mathbb{N}, \leq \rangle$, *es una cadena. Más aún,* $\langle \mathbf{n+1}, \leq, \vee, \wedge \rangle$, *con el supremo e ínfimo dados por:*

1) $\forall\, k, l \in \mathbf{n+1}$, $k \vee l = \text{máx}\{k, l\}$,[2]

2) $\forall\, k, l \in \mathbf{n+1}$, $k \wedge l = \text{mín}\{k, l\}$,

*es una retícula.*

*Luego, para cada* $n \geq 1$ $\langle (\mathbf{n+1})^n, \preceq, \vee, \wedge \rangle$ *es una retícula, con el orden, supremo e ínfimo dados de la siguiente manera.*

*Sean* $(k_1, \ldots, k_n), (l_1, \ldots, l_n) \in (\mathbf{n+1})^n$. *Entonces:*

1) $(k_1, \ldots, k_n) \preceq (l_1, \ldots, l_n) \Leftrightarrow k_i \leq l_i$ *para cada* $i \in \{1, \ldots, n\}$.

2) $(k_1, \ldots, k_n) \vee (l_1, \ldots, l_n) = (m_1, \ldots, m_n)$, *con* $m_i = \text{máx}\{k_i, l_i\}$ *para cada* $i \in \{1, \ldots, n\}$.

3) $(k_1, \ldots, k_n) \wedge (l_1, \ldots, l_n) = (m'_1, \ldots, m'_n)$, *con* $m'_i = \text{mín}\{k_i, l_i\}$ *para cada* $i \in \{1, \ldots, n\}$.

[2] Ver Observación 1.15.

### 1.1.4. Grandes retículas

Gran parte de los conceptos de la Teoría de Conjuntos, tales como los de contención, unión, intersección, producto cartesiano, relación (de orden, de equivalencia) e incluso el de función, pueden extenderse a clases que no necesariamente son conjuntos. Esta afirmación tiene una justificación desde un punto de vista axiomático dentro del Sistema de Gödel-Bernays (o Teoría de Clases) ([6], pág. 9 y [14], pág. 23), en el que el objeto primitivo es la clase. En este contexto más general, podemos hablar de *clase parcialmente ordenada*,[3] llamando a una clase parcialmente ordenada que cumple las propiedades de retícula una *gran retícula*.

## 1.2. Grupos

En lo sucesivo, por "grupo" entenderemos un grupo abeliano bajo la notación aditiva, con elemento neutro 0. Asimismo, denotaremos por $\mathbb{P}$ al conjunto de los números primos y, por $p$, a un número primo fijo.

Sea $A$ un grupo. Recordemos que el orden de un elemento $a \in A$, que en adelante denotaremos por $o(a)$, es el menor entero positivo $n$ tal que $na = 0$, cuando éste existe. En tal caso, decimos que $a$ es de orden finito; de lo contrario, decimos que $a$ es de orden infinito y escribimos $o(a) = \infty$.

Por su parte, si $B$ es un subgrupo de $A$, escribiremos $B \leq A$. También, como es usual, el subgrupo trivial $\{0\}$ será denotado simplemente por $0$.

**Definición 1.37** *Dado un grupo $A$, decimos que:*

[3] También es posible definir una clase parcialmente ordenada como una categoría $C$ (véase la sección 1.4) tal que para cada $A, A' \in C$ existe un único morfismo $f : A \longrightarrow A'$, en cuyo caso se escribe $A \leq A'$, y que cumple las siguientes propiedades:

1) Para toda $A \in C$, $A \leq A$.

2) Para cada $A, A', A'' \in C$, si $A \leq A'$ y $A' \leq A''$, entonces $A \leq A''$.

(Ver [6], pág. 239).

1) *A es un grupo de torsión, si todo elemento de A es de orden finito.*

2) *A es libre de torsión, si ninguno de sus elementos, a excepción del* 0*, es de orden finito.*

**Definición 1.38** *Un grupo A se llama p−primario o p−grupo si para todo* $a \in A$ *existe* $k \in \mathbb{N}$ *tal que* $o(a) = p^k$.

**Definición 1.39** *Un grupo A se llama elemental si para todo* $0 \neq a \in A$, $o(a) = p_1 p_2 \dots p_n$, *con* $p_1, p_2, \dots, p_n$ *primos distintos; es decir, si todos los elementos de A tienen órdenes finitos y libres de cuadrados.*

**Definición 1.40** *Sean A un grupo. Para* $n > 0$ *se definen los siguientes subgrupos de A:*

$$nA := \{\, na \mid a \in A \,\}$$

*y*

$$A\,[n] := \{\, a \mid a \in A,\, na = 0 \,\}\,.$$

Luego, $a \in nA$ si y sólo si la ecuación $nx = a$ tiene una solución $x \in A$, y $a \in A\,[n]$ si y sólo si $o(a)$ es finito y $o(a) \big| n$.

**Definición 1.41** *Un grupo A es acotado si existe* $n > 0$ *tal que* $nA = 0$. *En tal caso también se dice que A es n−acotado.*

**Observación 1.42** *Los p−grupos, grupos elementales y grupos acotados son de torsión.*

**Definición 1.43** *Sea A un grupo y* $a \in A$.

1) *Si* $p^r x = a$ *no es soluble para algún* $r \in \mathbb{N}$,[4] *entonces existe el mayor entero no negativo* $r_0$ *para el cual* $p^{r_0} x = a$ *es soluble para algún* $x \in A$. *En este caso, se llama a* $r_0$ *la p−altura de a.*

[4] Y, por tanto, en tal caso, $p^k x = a$ no es soluble $\forall\, k \geq r$.

*2) Si $p^r x = a$ es soluble para cada $r$, se dice que $a$ es de p−altura infinita.*

**Observación 1.44** *De hecho, 0 es de altura infinita en cada primo.*

Denotamos a la $p-$altura de un elemento $a \in A$ como $h_p(a)$. Si $a$ es de $p-$altura infinita, escribimos $h_p(a) = \infty$.

**Definición 1.45** *Sea $A$ un grupo. Se define la p-componente de $A$ como:*

$$A_p := \{\, a \in A \mid \exists\, n \in \mathbb{N},\ o(a) = p^n \,\} \leq A.$$

**Definición 1.46** *Sea $A$ un grupo. Un conjunto $\{\, a_1, a_2, \ldots, a_k \,\}$ de elementos de $A$ distintos de cero es llamado independiente si*

$$n_1 a_1 + n_2 a_2 + \cdots + n_k a_k = 0 \quad (n_i \in \mathbb{Z})$$

*implica que:*

$$n_1 a_1 = n_2 a_2 = \cdots = n_k a_k = 0.$$

*Más explícitamente, lo anterior significa que, para cada $i = 1, 2, \ldots, k$, se tiene que:*

$$o(a_i) = \infty \quad y \quad n_i = 0,$$

*o bien,*

$$o(a_i) < \infty \quad y \quad o(a_i) \big| n_i.$$

*Un conjunto de elementos no cero de $A$ es dependiente si no es independiente.*

**Observación 1.47** *La definición anterior puede ampliarse al caso de un subconjunto infinito de $A$: si $L = \{\, a_\alpha \,\}_{\alpha \in I}$ (con $I$ un conjunto de índices arbitrario) es un conjunto de elementos distintos de cero de $A$, entonces $L$ se dice independiente si todo subconjunto finito de $L$ lo es. De este modo, la independencia es, por definición, una propiedad de carácter finito.*

**Definición 1.48** *Un conjunto independiente $M$ de un grupo $A$ es máximo si ningún conjunto independiente en $A$ contiene a $M$ propiamente; así, si $0 \neq a \in A \setminus M$, entonces $M \cup \{ a \}$ ya no es un conjunto independiente.*

**Observación 1.49** *Por el Lema de Zorn, todo conjunto independiente en un grupo $A$ puede ser extendido a uno máximo.*

## 1.3. Anillos y Módulos

### 1.3.1. Notación y definiciones

En adelante, denotaremos por $R$ a un anillo asociativo con $1 \neq 0$.

Asimismo, asumiremos las definiciones de anillo, ideal izquierdo, ideal (bilateral), anillo cociente, así como los tres Teoremas de Isomorfismo de Nöether. A continuación expondremos la notación, definiciones y propiedades básicas de la Teoría de Módulos.

**Definición 1.50** *Un $R-$módulo (izquierdo)*[5] *es una pareja $(M, \lambda)$ donde $M$ es un grupo y $\lambda : R \times M \longrightarrow M$ es una función dada por $\lambda(r, x) = r \cdot x$ para cada $r \in R$, $x \in M$, tal que:*

*1)* $\forall\, r \in R,\ \forall\, x, y \in M,\ \ r \cdot (x + y) = r \cdot x + r \cdot y;$

*2)* $\forall\, r, s \in R,\ \forall\, x \in M,\ \ (r + s) \cdot x = r \cdot x + s \cdot x;$

*3)* $\forall\, r, s \in R,\ \forall\, x \in M,\ \ (rs) \cdot x = r \cdot (s \cdot x);$

*4)* $\forall\, x \in M,\ \ 1 \cdot x = x.$

Suele llamarse *multiplicación escalar* a la función $\lambda$ antes definida.

**Ejemplo 1.51** *Si bien la lista de ejemplos de $R-$módulos es grande y bastante bien conocida, hacemos énfasis en un par de ellos por ser relevantes para la teoría que presentaremos posteriormente:*

[5] Una definición análoga se tiene para $R-$módulo derecho.

1) *Sea* $R = \mathbb{Z}$. *Para cualquier grupo* $A$ *la función* $\lambda : R \times A \longrightarrow A$ *dada por* $\lambda(n, a) = na$ *para toda* $n \in \mathbb{Z}$ *y para toda* $a \in A$ *claramente satisface las propiedades de la Definición 1.50. Luego, todo grupo abeliano es un* $\mathbb{Z}-$*módulo.*

2) $R$ *es* $R-$*módulo, es decir, todo anillo resulta ser módulo sobre sí mismo.*

En lo subsecuente denotaremos simplemente por $M$ a un $R-$módulo $(M, \lambda)$.

**Definición 1.52** *Sean* $M$ *y* $N$ *dos* $R-$*módulos. Una función* $f : M \longrightarrow N$ *se llama:*

1) *Homomorfismo de* $R-$*módulos o* $R-$*homomorfismo, si para cada* $r, s \in R$ *y para cada* $x, y \in M$ *se tiene que:*

$$f(r \cdot x + s \cdot y) = r \cdot f(x) + s \cdot f(y).$$

2) *Monomorfismo, si* $f$ *es un* $R-$*homomorfismo inyectivo.*

3) *Epimorfismo, si* $f$ *es un* $R-$*homomorfismo suprayectivo.*

4) *Isomorfismo, si* $f$ *es un* $R-$*homomorfismo biyectivo.*

Se dice que dos $R-$módulos $M$ y $N$ son isomorfos si existe un isomorfismo entre ellos. En tal caso, se escribe $M \cong N$. Usaremos esta notación más adelante.

Como es usual, para cada pareja de $R-$módulos $M$ y $N$ denotaremos por $Hom_R(M, N)$ al conjunto de todos los $R-$homomorfismos $f : M \longrightarrow N$. Presentamos a continuación un resultado auxiliar bien conocido.

**Lema 1.53** *Sea* $M$ *un* $R-$*módulo. Para cada* $x \in M$ *consideremos a los* $R-$*homomorfismos* $d_x : R \longrightarrow M$ *tales que para cada* $r \in R$, $d_x(r) := r \cdot x$. *Entonces:*

$$Hom_R(R, M) = \{d_x \mid x \in M\}.$$

**Definición 1.54** *Sean $M$ un $R-$módulo y $N \subseteq M$. Decimos que $N$ es un $\underline{R-\text{submódulo}}$ (o, simplemente, un submódulo) de $M$ (denotado también como $N \leq M$) si $N$ es un subgrupo del grupo $M$ tal que es cerrado bajo la multiplicación escalar.*

**Ejemplo 1.55** *Presentamos enseguida algunos ejemplos de submódulos:*

1) *Si $M$ es un $R-$módulo, entonces el módulo cero $\{0\}$ (que suele denotarse simplemente por $0$) y $M$ son claramente submódulos de $M$. Se llama a $\{0\}$ el submódulo $\underline{\text{trivial}}$ de $M$.*

2) *Si consideramos a $R$ como $R-$módulo, se tiene que sus submódulos son sus ideales izquierdos.*

3) *Sea $f \in Hom_R(M, N)$. Entonces:*

   (a) *La imagen de $f$, $f(M)$, dada por:*

   $$f(M) = \{f(x) \mid x \in M\}$$

   *es un submódulo de $N$.*

   (b) *El núcleo de $f$, $kerf$, definido como:*

   $$kerf = \{x \in M \mid f(x) = 0\}$$

   *es un submódulo de $M$.*

   (c) *La imagen inversa de $N' \leq N$ bajo $f$, $f^{-1}(N')$, dada por:*

   $$f^{-1}(N') = \{x \in M \mid f(x) \in N'\}$$

   *es un submódulo de $M$.*

Dado un $R-$módulo $M$, la clase de todos los submódulos de $M$ forma el conjunto:

$$\mathcal{S}(M) := \{N \subseteq M \mid N \leq M\}.$$

**Definición 1.56** *Dados un $R-$módulo $M$ y $N, K \in \mathcal{S}(M)$, se definen a continuación operaciones en $\mathcal{S}(M)$:*

*1) La intersección $N \cap K$, dada por:*

$$N \cap K = \{x \in M \mid x \in N \ y \ x \in K\}.$$

*2) La suma $N + K$, dada por:*

$$N + K = \{x + y \mid x \in N, \ y \in K\}.$$

La definición anterior puede generalizarse para una familia arbitraria de submódulos de $M$ como sigue:

**Definición 1.57** *Dados un $R-$módulo $M$ y $\{N_\alpha\}_{\alpha \in I} \subseteq \mathcal{S}(M)$, se definen:*

*1) La intersección arbitraria $\bigcap_{\alpha \in I} N_\alpha$, dada por:*

$$\bigcap_{\alpha \in I} N_\alpha = \{x \in M \mid \forall\, \alpha \in I, \ x \in N_\alpha\} \leq M.$$

*2) La suma arbitraria $\sum_{\alpha \in I} N_\alpha$, dada por:*

$$\sum_{\alpha \in I} N_\alpha = \{x_1 + x_2 + \ \cdots \ + x_n \mid \forall\, i \in \{1, \ldots, n\}, \ x_i \in N_{\alpha_i}\} \leq M.$$

Es bien sabido que, para un $R-$módulo $M$, $\langle \mathcal{S}(M), \leq, \sum, \bigcap \rangle$ es una retícula completa (con elemento mayor $M$ y elemento menor el submódulo 0), que es modular y no necesariamente distributiva.

**Definición 1.58** *Sea $N$ un submódulo de un $R-$módulo $M$, entonces el módulo cociente $M/N$ es el grupo cociente abeliano $M/N$, dotado de una multiplicación escalar $\lambda : R \times M/N \longrightarrow M/N$, tal que $\lambda(r, x+N) = r \cdot x + N$ para cada $r \in R$, $x + N \in M/N$.*

Sea $M$ un $R-$módulo. Para cada $N \in \mathcal{S}(M)$ existen un monomorfismo y un epimorfismo distinguidos : la inclusión canónica, que denotaremos por $N \hookrightarrow M$, y la proyección canónica, denotada como $\pi : M \longrightarrow M/N$.

**Definición 1.59** *Dada una sucesión (finita o infinita) de homomorfismos de $R-$módulos:*

$$\cdots \longrightarrow M_{n-1} \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} M_{n+1} \xrightarrow{f_{n+1}} \cdots ,$$

*se dice que es <u>exacta</u> en $M_n$ si $f_{n-1}(M_{n-1}) = ker\, f_n$. Si es exacta en cada $R-$módulo, la llamamos una <u>sucesión exacta</u> . En particular, una sucesión exacta de la forma:*

$$0 \longrightarrow K \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

*se denomina <u>sucesión exacta corta</u>.*

**Ejemplo 1.60** *Sean $M$ un $R-$módulo y $N \in \mathcal{S}(M)$. Entonces:*

$$0 \longrightarrow N \hookrightarrow M \xrightarrow{\pi} M/N \longrightarrow 0$$

*es una sucesión exacta corta.*

**Observación 1.61** *Sean $M, N$ dos $R-$módulos y $f \in Hom_R(M, N)$. Se tiene que:*

1) *$f$ es monomorfismo $\Leftrightarrow 0 \longrightarrow M \xrightarrow{f} N$ es una sucesión exacta.*

2) *$f$ es epimorfismo $\Leftrightarrow M \xrightarrow{f} N \longrightarrow 0$ es una sucesión exacta.*

3) *$f$ es isomorfismo $\Leftrightarrow 0 \longrightarrow M \xrightarrow{f} N \longrightarrow 0$ es una sucesión exacta.*

**Definición 1.62** *Sea $M$ un $R-$módulo y $\emptyset \neq X \subseteq M$. Se define el conjunto:*

$$RX := \left\{ \sum_{i=1}^{n} r_i \cdot x_i \;\middle|\; n \geq 1,\ r_i \in R,\ x_i \in X \right\}.$$

**Observación 1.63** *Sea $M$ un $R-$módulo. Por convención, se suele escribir $R\emptyset = 0$.*

**Observación 1.64** *Sea $M$ un $R-$módulo y $X \subseteq M$. Entonces $RX \in \mathcal{S}(M)$.*

**Observación 1.65** *$N \in \mathcal{S}(M)$ si y sólo si $RN = N$.*

**Definición 1.66** *Sea $M$ un $R-$módulo y $X \subseteq M$. Se define el submódulo de $M$ generado por $X$ como la intersección de todos los submódulos que contienen a $X$, es decir, el menor submódulo de $M$ que contiene a $X$.*

Denotaremos por $\langle X \rangle$ al submódulo generado por $X$.

**Proposición 1.67** *Sea $M$ un $R-$módulo y $X \subseteq M$. Entonces $\langle X \rangle = RX$.*

*Demostración.* Por la Observación 1.64, $RX$ es un submódulo de $M$. Luego, puesto que $x = 1 \cdot x$ para toda $x \in M$, se tiene que $\langle X \rangle \subseteq RX$. Para la otra contención, basta observar que todo submódulo que contenga a $X$ debe contener a las combinaciones lineales de $RX$. □

**Definición 1.68** *Sean $M$ un $R-$módulo y $X \subseteq M$. Se dice que $M$ es finitamente generado si $M = \langle X \rangle$, con $X = \{x_1, \ldots, x_n\}$ (en tal caso, escribimos $M = \langle \{x_1, \ldots, x_n\} \rangle = \langle x_1, \ldots, x_n \rangle$ y llamamos a $x_1, \ldots, x_n$ los generadores de $M$). En particular, si $X = \{x\}$ y $M = \langle X \rangle$, decimos que $M$ es cíclico.*

Sea $M$ un $R-$módulo; $S$, un anillo, y supongamos que existe un homomorfismo de anillos $f : S \longrightarrow R$. Entonces, se induce en $M$ una estructura de $S-$módulo con la multiplicación escalar dada por:

$$s \cdot x := f(s) \cdot x$$

para cada $s \in S$ y para cada $x \in M$.

Luego, para cada $R-$módulo $M$ y para cada homomorfismo de anillos $f : S \longrightarrow R$ existen cuatro módulos: el $R-$módulo $M$, ${}_RM$; el $S-$módulo $M$, ${}_SM$; el $f(S)-$módulo $M$, ${}_{f(S)}M$; y el $\mathbb{Z}-$módulo $M$, ${}_{\mathbb{Z}}M$.[6] De lo anterior se sigue la:

[6] Es bien sabido que, si $R$ es un anillo, existe un único homomorfismo $\chi : \mathbb{Z} \longrightarrow R$.

**Proposición 1.69** *Sea $M$ un $R-$módulo; $S$, un anillo, y supongamos que existe un homomorfismo de anillos $f : S \longrightarrow R$. Se tienen las siguientes inclusiones de retículas:*

$$\mathcal{S}({}_RM) \leq \mathcal{S}({}_SM) = \mathcal{S}({}_{f(S)}M) \leq \mathcal{S}({}_{\mathbb{Z}}M).$$

□

**Definición 1.70** *Sea $M$ un $R-$módulo. Se define el anulador de $M$, $ann(M)$, como el conjunto:*

$$ann(M) := \{r \in R \mid \forall\, x \in M,\ r \cdot x = 0\}.$$

*En particular, si $x \in M$, definimos:*

$$ann(x) := \{r \in R \ \mid \ r \cdot x = 0\}.$$

**Observación 1.71** *Sea $M$ un $R-$módulo. Entonces $ann(M)$ es un ideal (bilateral) de $R$, mientras que $ann(x)$ es un ideal izquierdo de $R$.*

Como consecuencia de la Proposición 1.69 y de la Definición 1.70 se tiene el siguiente corolario.

**Corolario 1.72** *Sea $M$ un $R-$módulo e $I$, un ideal de $R$ tal que $I \subseteq ann(M)$. Entonces un submódulo $N$ de $M$ es un $R-$submódulo si y sólo si $N$ es un $R/I-$submódulo. Es decir,*

$$\mathcal{S}({}_RM) = \mathcal{S}({}_{R/I}M).$$

□

Además, en lo que concierne a $R-$homomorfismos, si tenemos dos $R-$módulos $M$ y $N$, y un homomorfismo de anillos $f : S \longrightarrow R$, entonces se sigue que todo $R-$homomorfismo es también un $S-$homomorfismo. Por tanto, se tiene el siguiente:

**Corolario 1.73** *Sean $M$ y $N$ dos $R-$módulos y sea $f : S \longrightarrow R$ un homomorfismo de anillos. Se tiene que:*

$$Hom_R(M,N) \leq Hom_S(M,N) = Hom_{f(S)}(M,N) \leq Hom_{\mathbb{Z}}(M,N).$$

*En particular, si $M, N$ son $R-$módulos e $I$ es un ideal de $R$ tal que $I \subseteq ann(M)$ e $I \subseteq ann(N)$, entonces:*

$$Hom_R(M,N) = Hom_{R/I}(M,N).$$

□

Dados un $R-$módulo $M$ y $N \in \mathcal{S}(M)$, denotaremos por $\mathcal{S}_N(M)$ al subconjunto de $\mathcal{S}(M)$ dado por:

$$\mathcal{S}_N(M) := \{K \leq M \mid N \leq K\}.$$

**Teorema 1.74** *(Teorema de la Correspondencia)*
*Dados un $R-$módulo $M$ y $N \in \mathcal{S}(M)$, las retículas $\mathcal{S}_N(M)$ y $\mathcal{S}(M/N)$ son isomorfas.*

**Definición 1.75** *Un $R-$módulo $M \neq 0$ se llama <u>simple</u> si $\mathcal{S}(M) = \{0, M\}$.*

Denotaremos por **S** a la clase de todos los $R-$módulos simples. Presentamos a continuación un resultado que caracteriza a los elementos de **S**.

**Proposición 1.76** *$S \in \mathbf{S}$ si y sólo si $S \cong R/K$, con $K$ un ideal izquierdo máximo de $R$.*

*Demostración.* Si $S \in \mathbf{S}$, entonces $S$ es cíclico. Se sigue que $S \cong R/K$, donde $K$ es un ideal izquierdo de $R$. En efecto, sea $S = \langle x \rangle$, con $x \in S$, y definamos $K := ann(x)$. Si consideramos el $R-$homomorfismo $d_x : R \longrightarrow S$ definido en el Lema 1.53, se tiene que $d_x(R) = Rx = \langle x \rangle$ y $ker\, d_x = K$. Luego, la última afirmación se sigue del Primer Teorema de Isomorfismo de Nöether.

Ahora, por el Teorema de la Correspondencia las retículas $\mathcal{S}_K(R)$ y $\mathcal{S}(R/K)$ son isomorfas. Siendo $\mathcal{S}(R/K)$ isomorfa a $\mathcal{S}(S) = \{0, S\}$, debe ocurrir que $K$ sea ideal izquierdo máximo de $R$. La suficiencia también es consecuencia inmediata del Teorema de la Correspondencia. □

**Observación 1.77** *Dado $S \in \mathbf{S}$, se puede hablar de su clase de isomorfismo:*

$$[S] = \{M \mid M \text{ es } R-\text{módulo y } M \cong S\}.$$

*Luego, por la Proposición 1.76, existe una correspondencia biunívoca entre las clases de isomorfismo de $R-$módulos simples y la clase de ideales izquierdos máximos de $R$, la cual es un conjunto.*

En virtud de la observación anterior se tiene el siguiente:

**Corolario 1.78** *Las clases de isomorfismo de $R-$módulos simples forman un conjunto.* □

Podemos elegir un representante de cada clase de isomorfismo de $R-$módulos simples y obtenemos un conjunto completo e irredundante. Denotaremos por $R - simp$ a dicho conjunto.

### 1.3.2. Suma y Producto Directos

**Definición 1.79** *Sean $N, K$ submódulos de un $R-$módulo $M$. Se dice que $M$ es la <u>suma directa</u> (interna) de $N$ y $K$ si:*

*1) $N + K = M$;*

*2) $N \cap K = 0$.*

*En este caso, se escribe $M = N \oplus K$.*

**Observación 1.80** *Sean $N, K$ submódulos de un $R-$módulo $M$. Una consecuencia inmediata de la Definición 1.79 es que todo elemento $x \in M = N \oplus K$ se escribe de manera única como $x = n + k$, con $n \in N$, $k \in K$.*

**Definición 1.81** *Sean $M$ un $R-$módulo y $\{M_\alpha\}_{\alpha\in I} \subseteq \mathcal{S}(M)$. Decimos que la familia $\{M_\alpha\}_{\alpha\in I}$ es independiente si para cada $\alpha \in I$ se tiene que* $M_\alpha \bigcap \left( \sum_{\beta\neq\alpha} M_\beta \right) = 0$.

La Definición 1.79 puede generalizarse para una familia arbitraria de submódulos de un $R-$módulo $M$ como sigue:

**Definición 1.82** *Sean $M$ un $R-$módulo y $\{M_\alpha\}_{\alpha\in I} \subseteq \mathcal{S}(M)$, tales que:*

*1)* $M = \sum_{\alpha\in I} M_\alpha$ ;

*2) $\{M_\alpha\}_{\alpha\in I}$ es una familia independiente.*

*Entonces decimos que $M$ es la suma directa (interna) de $\{M_\alpha\}_{\alpha\in I}$ y escribimos* $M = \bigoplus_{\alpha\in I} M_\alpha$.

**Observación 1.83** *Como consecuencia de la Definición 1.81, la Observación 1.80 puede generalizarse como sigue: cada $x \in M = \bigoplus_{\alpha\in I} M_\alpha$ tiene una representación única como $x = m_1 + \cdots + m_r$, con $m_i \in M_{\alpha_i}$ y $\alpha_i \in I$ para cada $i \in \{1, \ldots, r\}$.*

**Definición 1.84** *Sea $\{M_\alpha\}_{\alpha\in I}$ una familia de $R-$módulos y consideremos su producto cartesiano:*

$$\prod_{\alpha\in I} M_\alpha = \left\{ f : I \longrightarrow \bigcup_{\alpha\in I} M_\alpha \;\middle|\; f(\alpha) \in M_\alpha \;\forall\, \alpha \in I \right\}.$$

*Entonces, tenemos en $\prod_{\alpha\in I} M_\alpha$ una estructura de $R-$módulo, con:*

*1) La suma:*

$$+ : \prod_{\alpha\in I} M_\alpha \times \prod_{\alpha\in I} M_\alpha \longrightarrow \prod_{\alpha\in I} M_\alpha$$

*tal que, para toda $f, g \in \prod_{\alpha\in I} M_\alpha$,*

$$f + g : I \longrightarrow \bigcup_{\alpha\in I} M_\alpha,$$

*donde, para cada* $\alpha \in I$,

$$(f+g)(\alpha) = f(\alpha) + g(\alpha).$$

*2) La multiplicación escalar:*

$$\lambda : R \times \prod_{\alpha\in I} M_\alpha \longrightarrow \prod_{\alpha\in I} M_\alpha$$

*tal que, para cada* $r \in R$ *y para toda* $f \in \prod_{\alpha\in I} M_\alpha$,

$$\lambda(r,f) = r \cdot f : I \longrightarrow \bigcup_{\alpha\in I} M_\alpha,$$

*donde, para cada* $\alpha \in I$,

$$(r \cdot f)(\alpha) = r \cdot (f(\alpha)).$$

*Se llama producto directo de la familia* $\{M_\alpha\}_{\alpha\in I}$ *a la terna* $(\prod_{\alpha\in I} M_\alpha, +, \lambda)$.

En particular, si $M_\alpha = K \ \forall\, \alpha \in I$, entonces se escribe $\prod_{\alpha\in I} K = K^I$ y, si $I = \emptyset$, $\prod_{\emptyset} M_\alpha = 0 = K^\emptyset$.

**Definición 1.85** *Dados* $\{M_\alpha\}_{\alpha\in I}$ *una familia de* $R-$*módulos y* $f \in \prod_{\alpha\in I} M_\alpha$, *se define el soporte de* $f$ *(que denotaremos por* $sop\,(f)$*), como:*

$$sop\,(f) := \{\alpha \in I \mid f(\alpha) \neq 0\}.$$

**Definición 1.86** *Sea* $\{M_\alpha\}_{\alpha\in I}$ *una familia de* $R-$*módulos. El conjunto:*

$$\bigoplus_{\alpha\in I} M_\alpha := \left\{ f \in \prod_{\alpha\in I} M_\alpha \;\middle|\; sop\,(f) \text{ es finito} \right\} \leq \prod_{\alpha\in I} M_\alpha$$

*se llama la suma directa (externa).*[7]

[7] En algunas ocasiones se denota por $\dot{\bigoplus}_{\alpha\in I} M_\alpha$ a la suma directa externa para distinguirla de la suma directa interna.

En particular, si $M_\alpha = K \ \forall\, \alpha \in I$, entonces se escribe $\bigoplus_{\alpha\in I} K = K^{(I)}$.

**Observación 1.87** *Claramente, si el conjunto de índices $I$ es finito se tiene que* $\prod_{\alpha\in I} M_\alpha = \bigoplus_{\alpha\in I} M_\alpha$.

**Definición 1.88** *Sea $\{M_\alpha\}_{\alpha\in I}$ una familia de $R-$módulos.*

1) *Para cada $\beta \in I$ se tiene un epimorfismo de $R-$módulos:*

$$\prod_{\alpha\in I} M_\alpha \xrightarrow{\pi_\beta} M_\beta$$

*tal que, para cada $f \in \prod_{\alpha\in I} M_\alpha$,*

$$\pi_\beta(f) = f(\beta),$$

*al que llamamos <u>proyección natural</u> del producto directo $\prod_{\alpha\in I} M_\alpha$ en $M_\beta$.*

*En particular, se llama a la restricción $p_\beta := \pi_\beta\big|_{\bigoplus_{\alpha\in I} M_\alpha}$ la proyección natural de la suma directa $\bigoplus_{\alpha\in I} M_\alpha$ en $M_\beta$.*

2) *Para cada $\beta \in I$ se tiene un monomorfismo de $R-$módulos:*

$$M_\beta \xrightarrow{i_\beta} \bigoplus_{\alpha\in I} M_\alpha$$

*tal que, para cada $x \in M_\beta$,*

$$i_\beta(x)(\alpha) = \begin{cases} x, & si\ \alpha = \beta \\ 0, & si\ \alpha \neq \beta, \end{cases}$$

*que recibe el nombre de <u>inclusión natural</u> de $M_\beta$ en la suma directa $\bigoplus_{\alpha\in I} M_\alpha$.*

Dados una familia de $R-$módulos $\{M_\alpha\}_{\alpha\in I}$ y $f \in \prod_{\alpha\in I} M_\alpha$, suele denotarse a $f(\alpha)$ como $f_\alpha$ y a los elementos de $\prod_{\alpha\in I} M_\alpha$ por $(f_\alpha)_{\alpha\in I}$. Por comodidad, en adelante adoptaremos dicha notación.

### 1.3.3. Módulos proyectivos e inyectivos

**Definición 1.89** *Sean $M$ un $R-$módulo y $N \in \mathcal{S}(M)$. Se dice que:*

1) *$N$ es <u>esencial</u> en $M$ (denotado por $N \trianglelefteq M$), si para cada $L \leq M$ se tiene que $N \cap L = 0$ implica que $L = 0$.*

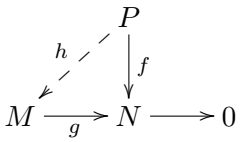
2) *$N$ es <u>superfluo</u> en $M$ (denotado por $N \ll M$), si para cada $L \leq M$ se tiene que $N + L = M$ implica que $L = M$.*

**Definición 1.90** *Sean $M, N, L$ tres $R-$módulos. Entonces:*

1) *Un <u>monomorfismo</u> $f : N \longrightarrow M$ se llama <u>esencial</u> si $f(N) \trianglelefteq M$.*

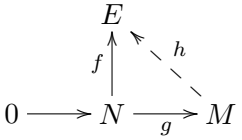
2) *Un <u>epimorfismo</u> $g : M \longrightarrow L$ se llama <u>superfluo</u> si $ker(g) \ll M$.*

**Definición 1.91** *Sea $P$ un $R-$módulo. Se dice que $P$ es <u>proyectivo</u> si para todo $f \in Hom_R(P, N)$ y para todo epimorfismo $g \in Hom_R(M, N)$ existe $h \in Hom_R(P, M)$ tal que el siguiente diagrama conmuta:*




*es decir, $g \circ h = f$.*

**Definición 1.92** *Sea $E$ un $R-$módulo. Se dice que $E$ es <u>inyectivo</u> si para todo $f \in Hom_R(N, E)$ y para todo monomorfismo $g \in Hom_R(N, M)$ existe $h \in Hom_R(M, E)$ tal que el siguiente diagrama conmuta:*




*es decir, $h \circ g = f$.*

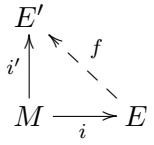
Denotaremos por $\mathcal{E}$ a la clase de todos los $R-$módulos (izquierdos) inyectivos.

Es bien sabido que todo $R-$módulo $M$ puede incluirse en un $R-$módulo inyectivo. Luego, es natural pensar en la "mínima" inclusión de $M$ en un $R-$módulo inyectivo.

**Definición 1.93** *Sea $M$ un $R-$módulo. Una pareja $(E, i)$ es una cápsula inyectiva de $M$ si $E$ es un $R-$módulo inyectivo e $i \in Hom_R(M, E)$ es un monomorfismo esencial.*

Presentamos enseguida un par de resultados bien conocidos:

**Teorema 1.94** *Sea $M$ un $R-$módulo y sean $(E, i)$, $(E', i')$ cápsulas inyectivas de $M$. Entonces existe un isomorfismo $f : E \longrightarrow E'$ tal que el siguiente diagrama conmuta:*




Al ser cualesquiera dos cápsulas inyectivas de un $R-$módulo $M$ isomorfas, se suele hablar de la cápsula inyectiva de $M$. Bajo esta convención, denotaremos por $EM$ a la cápsula inyectiva de un $R-$módulo $M$.

**Teorema 1.95** *(Criterio de Baer)*
*Un $R-$módulo $E$ es inyectivo si y sólo si todo $R-$homomorfismo $f : I \longrightarrow E$, donde $I$ es un ideal izquierdo de $E$, puede extenderse a $R$.*

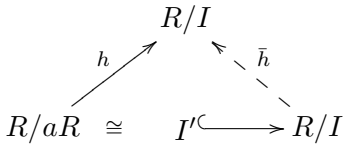
**Definición 1.96** *Un anillo $R$ se llama autoinyectivo izquierdo (derecho), si como $R-$módulo izquierdo (derecho) es inyectivo.*

**Proposición 1.97** *Si $R$ es un DIP[8] e $I \neq 0$ es un ideal de $R$, entonces $R/I$ es autoinyectivo.*

[8]Dominio de ideales principales.

*Demostración.* Sea $I \neq 0$ un ideal de $R$. Luego, por ser $R$ un $DIP$, $I = \langle r \rangle = rR$ para algún $r \in R$. Ahora consideremos el anillo cociente $R/I$ y sea $I'$ un ideal de $R/I$. Entonces se tiene que $I' = \langle r_0 \rangle / \langle r \rangle$ para algún $r_0 \in R$. Nótese que para que el ideal $I'$ tenga sentido, debe ocurrir que $\langle r \rangle \leq \langle r_0 \rangle$; esto es, $r = r_0 a$, con $a \in R$, de donde $I' = \langle r_0 \rangle / \langle r \rangle = r_0 R/(r_0 a)R \cong R/aR$.

Sea $h : R/aR \longrightarrow R/I$ un $R-$homomorfismo y sea $I' \hookrightarrow R/I$ la inclusión canónica. Definimos $\bar{h} : R/I \longrightarrow R/I$ tal que para cada $x + (r_0 a)R \in R/I = R/(r_0 a)R$, $\bar{h}(x + (r_0 a)R) := h(x + aR)$. No es difícil verificar que $\bar{h}$ está bien definida y que $\bar{h} \,\big|_{I' \cong R/aR} = h$, como lo ilustra el siguiente diagrama:




Luego, por el Criterio de Baer, $R/I$ es autoinyectivo. □

### 1.3.4. Generar y Cogenerar, la Traza y el Rechazo

**Definición 1.98** *Sean* $\mathbf{A}$ *una clase de* $R-$*módulos y* $M$ *un* $R-$*módulo. Decimos que:*

1) *La clase* $\mathbf{A}$ *genera a* $M$*, si existe un epimorfismo* $\bigoplus_{A \in I} A \longrightarrow M \longrightarrow 0$*, con* $I \subseteq \mathbf{A}$*, un conjunto.*

2) *La clase* $\mathbf{A}$ *genera finitamente a* $M$*, si existe un epimorfismo* $\bigoplus_{i=1}^{n} A_i \longrightarrow M \longrightarrow 0$*, con* $A_i \in \mathbf{A}$ *para cada* $i = 1, 2, \ldots, n$*.*

**Definición 1.99** *Dados* $A, M$ *dos* $R-$*módulos, decimos que* $A$ *genera a* $M$ *si* $\{A\}$ *genera a* $M$*, es decir, si existe un epimorfismo* $A^{(X)} \longrightarrow M \longrightarrow 0$*, con* $X$ *un conjunto.*

Dualmente, se tiene:

**Definición 1.100** *Sean* $\mathbf{A}$ *una clase de* $R-$*módulos y* $M$ *un* $R-$*módulo. Decimos que:*

1) *La clase* $\mathbf{A}$ *cogenera a* $M$*, si existe un monomorfismo* $0 \longrightarrow M \longrightarrow \prod_{A \in I} A$*, con* $I \subseteq \mathbf{A}$*, un conjunto.*

2) *La clase* $\mathbf{A}$ *cogenera finitamente a* $M$*, si existe un monomorfismo* $0 \longrightarrow M \longrightarrow \prod_{i=1}^{n} A_i = \bigoplus_{i=1}^{n} A_i$*, con* $A_i \in \mathbf{A}$ *para cada* $i = 1, 2, \ldots, n$*.*

**Definición 1.101** *Dados* $A, M$ *dos* $R-$*módulos,* $A$ *cogenera a* $M$ *si* $\{A\}$ *cogenera a* $M$*, es decir, si existe un monomorfismo* $0 \longrightarrow M \longrightarrow A^X$*, con* $X$ *un conjunto.*

**Ejemplo 1.102** *Presentamos algunos ejemplos bien conocidos que ilustran los conceptos de generar y cogenerar.*

1) *Dado un* $\mathbb{Z}-$*módulo* $A$*,* $\{\mathbb{Z}_n \mid n > 1\}$ *genera a* $A$ *si y sólo si* $A$ *es de torsión.*

2) *Dado un* $\mathbb{Z}-$*módulo* $A$*,* $\mathbb{Q}$ *cogenera a* $A$ *si y sólo si* $A$ *es libre de torsión.*

3) *Dado un* $R-$*módulo* $M$*,* $R$ *genera a* $M$*.*

4) *Dado un* $R-$*módulo* $M$*,* $\prod_{R-simp} ES$ *cogenera a* $M$*.*

Sea $\mathbf{A}$ una clase de $R-$módulos. Se denota por:

$(F)Gen(\mathbf{A})$, a la clase de todos los $R-$módulos (finitamente) generados por $\mathbf{A}$.

$(F)Cog(\mathbf{A})$, a la clase de todos los $R-$módulos (finitamente) cogenerados por $\mathbf{A}$.

**Observación 1.103** *Sea* $\mathbf{A}$ *una clase de* $R-$*módulos y sea* $B \subseteq \mathbf{A}$ *un conjunto completo e irredundante de representantes de clases de isomorfismo de* $\mathbf{A}$*. Entonces* $Gen(\mathbf{A}) = Gen(B)$ *y* $Cog(\mathbf{A}) = Cog(B)$*.*

**Definición 1.104** *Sean* $\mathbf{A}$ *una clase de* $R-$*módulos y* $M$ *un* $R-$*módulo. Definimos:*

1) *La* Traza *de* $M$ *respecto a* $\mathbf{A}$ *(que denotaremos por* $\mathcal{T}_{R_{\mathbf{A}}}(M)$*), como:*

$$\mathcal{T}_{R_{\mathbf{A}}}(M) = \sum \{f(A) \mid f \in Hom_R(A, M),\ A \in \mathbf{A}\} \leq M.$$

2) *El* Rechazo *de* $M$ *respecto a* $\mathbf{A}$ *(que denotaremos por* $\mathcal{R}_{EJ_{\mathbf{A}}}(M)$*), como:*

$$\mathcal{R}_{EJ_{\mathbf{A}}}(M) := \bigcap \{ker\, g \mid g \in Hom_R(M, A),\ A \in \mathbf{A}\} \leq M.$$

En palabras, la Traza es el mayor submódulo $K$ de $M$ tal que $K \in Gen(\mathbf{A})$ y el Rechazo es el menor submódulo $K$ de $M$ tal que $M/K \in Cog(\mathbf{A})$. Como consecuencia inmediata se tiene la siguiente:

**Proposición 1.105** *Sean* $\mathbf{A}$ *una clase de* $R-$*módulos y* $M$ *un* $R-$*módulo. Entonces:*

1) $M \in Gen(\mathbf{A})$ *si y sólo si* $\mathcal{T}_{R_{\mathbf{A}}}(M) = M$.

2) $M \in Cog(\mathbf{A})$ *si y sólo si* $\mathcal{R}_{EJ_{\mathbf{A}}}(M) = 0$.

**Definición 1.106** *En particular, si* $\mathbf{S}$ *es la clase de todos los* $R-$*módulos simples y* $M$ *es un* $R-$*módulo, entonces se definen:*

1) *El* Zoclo *de* $M$ *(que denotaremos por* $Soc(M)$*), como:*

$$Soc(M) = \mathcal{T}_{R_{\mathbf{S}}}(M) = \sum \{f(A) \mid f \in Hom_R(A, M),\ A \text{ es simple}\} \leq M.$$

2) *El* Radical[9] *de* $M$ *(que denotaremos por* $Rad(M)$*), como:*

$$Rad(M) = \mathcal{R}_{EJ_{\mathbf{S}}}(M) := \bigcap \{ker\, g \mid g \in Hom_R(M, A),\ A \text{ es simple}\} \leq M.$$

**Observación 1.107** *Para todo* $R-$*módulo* $M$, $\mathcal{T}_{R_{\mathbf{S}}}(M) = \mathcal{T}_{R_{R-simp}}(M)$ *y* $\mathcal{R}_{EJ_{\mathbf{S}}}(M) = \mathcal{R}_{EJ_{R-simp}}(M)$.

[9] de Jacobson

Presentamos enseguida algunas propiedades de la Traza y el Rechazo.

**Proposición 1.108** *Si* $\mathbf{A}$ *es una clase de* $R-$*módulos,* $M, N$ *son dos* $R-$*módulos y* $h \in Hom_R(M,N)$*, entonces:*

*1)* $h(\mathcal{T}_{R_{\mathbf{A}}}(M)) \leq \mathcal{T}_{R_{\mathbf{A}}}(N)$.

*2)* $h(\mathcal{R}_{EJ_{\mathbf{A}}}(M)) \leq \mathcal{R}_{EJ_{\mathbf{A}}}(N)$.

*Demostración.*

*1)* : Dado cualquier $f \in Hom_R(A,M)$, con $A \in \mathbf{A}$, se tiene que $h \circ f \in Hom_R(A,N)$. Luego, $h(f(A)) = (h \circ f)(A) \leq \mathcal{T}_{R_{\mathbf{A}}}(N)$, de donde $h(\mathcal{T}_{R_{\mathbf{A}}}(M)) \leq \mathcal{T}_{R_{\mathbf{A}}}(N)$.

*2)* : Sea $g \in Hom_R(N,A)$, con $A \in \mathbf{A}$. Entonces $g \circ h \in Hom_R(M,A)$. Dado $x \in \mathcal{R}_{EJ_{\mathbf{A}}}(M)$, se tiene que $(g \circ h)(x) = g(h(x)) = 0$. Luego, $h(x) \in ker\, g$. Se sigue que $h(\mathcal{R}_{EJ_{\mathbf{A}}}(M)) \leq ker\, g$; es decir, $h(\mathcal{R}_{EJ_{\mathbf{A}}}(M)) \leq \mathcal{R}_{EJ_{\mathbf{A}}}(N)$. □

**Proposición 1.109** *Sean* $\mathbf{A}$ *una clase de* $R-$*módulos y* $M$ *un* $R-$*módulo. Se tiene que:*

*1)* $\mathcal{T}_{R_{\mathbf{A}}}(\mathcal{T}_{R_{\mathbf{A}}}(M)) = \mathcal{T}_{R_{\mathbf{A}}}(M)$.

*2)* $\mathcal{R}_{EJ_{\mathbf{A}}}(M/\mathcal{R}_{EJ_{\mathbf{A}}}(M)) = 0$.

*Demostración.*

*1)* : Como $\mathcal{T}_{R_{\mathbf{A}}}(M) \in Gen(\mathbf{A})$, se sigue del inciso *1)* de la Proposición 1.105 que $\mathcal{T}_{R_{\mathbf{A}}}(\mathcal{T}_{R_{\mathbf{A}}}(M)) = \mathcal{T}_{R_{\mathbf{A}}}(M)$.

La prueba de *2)* es similar. □

## 1.4. Categorías y Funtores

**Definición 1.110** *Una categoría* C *consiste de:*

1) *Una clase no vacía de objetos.*

2) *Para cada par de objetos* $A, B \in \mathtt{C}$*, un conjunto* $\mathtt{C}(A, B)$*, cuyos elementos se llaman morfismos y se denotan* $f : A \longrightarrow B$*, que cumple la siguiente condición:*

$$\mathtt{C}(A, B) = \mathtt{C}(D, E) \Leftrightarrow A = D \quad y \quad B = E.$$

3) *Para cada terna de objetos* $A, B, C \in \mathtt{C}$*, una ley de composición*

$$\circ : \mathtt{C}(A, B) \times \mathtt{C}(B, C) \longrightarrow \mathtt{C}(A, C),$$

*que satisface las siguientes propiedades:*

   (a) *Para todo objeto* $A$ *en* $\mathtt{C}$ *existe un morfismo* $\mathbf{1}_A : A \longrightarrow A$*, tal que para cualesquiera morfismos* $f : A \longrightarrow B$ *y* $g : C \longrightarrow A$ *en* $\mathtt{C}$ *se tiene que* $f \circ \mathbf{1}_A = f \quad y \quad \mathbf{1}_A \circ g = g$.[10]

   (b) *Si* $f : A \longrightarrow B$, $g : B \longrightarrow C$ *y* $h : C \longrightarrow D$*, entonces* $h \circ (g \circ f) = (h \circ g) \circ f$.

**Ejemplo 1.111** *Presentamos a continuación algunos ejemplos de categorías, así como la notación que en adelante usaremos al referirnos a ellas:*

1) *La categoría de los conjuntos (que denotaremos por* $Conj$*), donde los objetos son los conjuntos y los morfismos son las funciones de un conjunto a otro.*

2) *La categoría de* $R-$*módulos (que denotaremos por* $R - Mod$*), en la que los morfismos son los* $R-$*homomorfismos de módulos. En particular, si* $R = \mathbb{Z}$*, denotaremos por* $\mathbb{Z} - Mod$ *a la categoría de grupos abelianos.*

**Definición 1.112** *Sea* $\mathtt{C}$ *una categoría. Un objeto* $B \in \mathtt{C}$ *se llama inicial en* $\mathtt{C}$ *si, para cada objeto* $A \in \mathtt{C}$*, existe sólo un morfismo* $B \longrightarrow A$*. Un objeto*

[10] Al morfismo $\mathbf{1}_A$ se suele llamar *morfismo identidad* en $A$.

*$C \in \mathtt{C}$ se llama terminal en $\mathtt{C}$ si, para cada objeto $A \in \mathtt{C}$, existe sólo un morfismo $A \longrightarrow C$.*
*Un objeto cero en $\mathtt{C}$, denotado con $O$, es un objeto que es inicial y terminal a la vez en $\mathtt{C}$.*

**Definición 1.113** *Sea $\mathtt{C}$ una categoría. Un morfismo $f$ en $\mathtt{C}$ se llama:*

1) *Monomorfismo, si para todo par de morfismos $g_1, g_2$ en $\mathtt{C}$ que cumplen que $f \circ g_1 = f \circ g_2$, se tiene que $g_1 = g_2$; es decir, si $f$ es cancelable por la izquierda.*

2) *Epimorfismo, si para todo par de morfismos $g_1, g_2$ en $\mathtt{C}$ tales que $g_1 \circ f = g_2 \circ f$, se tiene que $g_1 = g_2$; es decir, si $f$ es cancelable por la derecha.*

3) *Isomorfismo, si $f$ es cancelable por la izquierda y por la derecha.*

**Definición 1.114** *Dadas $\mathtt{C}$ y $\mathtt{C}'$ dos categorías, definimos un funtor covariante $F : \mathtt{C} \longrightarrow \mathtt{C}'$ como una regla que asocia:*

1) *A cada objeto $A \in \mathtt{C}$, un objeto $A' \in \mathtt{C}'$.*

2) *A cada morfismo $f \in \mathtt{C}(A, B)$, un morfismo $F(f) \in \mathtt{C}'(F(A), F(B))$, que cumple las siguientes propiedades:*

   *(a) $F(f \circ g) = F(f) \circ F(g)$,*

   *(b) $F(\mathbf{1}_A) = \mathbf{1}_{F(A)}$.*

**Definición 1.115** *Dadas $\mathtt{C}$ y $\mathtt{C}'$ dos categorías, definimos un funtor contravariante $F : \mathtt{C} \longrightarrow \mathtt{C}'$ como una regla que asocia:*

1) *A cada objeto $A \in \mathtt{C}$, un objeto $A' \in \mathtt{C}'$.*

2) *A cada morfismo $f \in \mathtt{C}(A, B)$, un morfismo $F(f) \in \mathtt{C}'(F(B), F(A))$, que cumple las siguientes propiedades:*

(a) $F(f \circ g) = F(g) \circ F(f)$,

(b) $F(\mathbf{1}_A) = \mathbf{1}_{F(A)}$.

**Ejemplo 1.116** *Presentamos enseguida algunos ejemplos de funtores:*

1) *Dada una categoría* $\mathtt{C}$, *el funtor identidad*, $\bar{\mathbf{1}}_{\mathtt{C}} : \mathtt{C} \longrightarrow \mathtt{C}$, *que asigna a cada objeto y a cada morfismo de* $\mathtt{C}$ *los mismos objeto y morfismo, es claramente un funtor covariante.*

2) *Sea* $\mathtt{C}$ *una categoría y sea* $\mathtt{D}$ *una categoría con objeto cero,* $O$. *Se define el funtor cero como el funtor* $\bar{\mathbf{0}} : \mathtt{C} \longrightarrow \mathtt{D}$ *tal que:*

   (i) *A cada objeto* $A \in \mathtt{C}$ *le asocia el objeto* $O \in \mathtt{D}$.

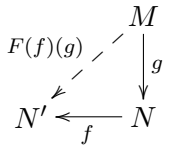
   (ii) *A cada morfismo* $f \in \mathtt{C}(A, B)$ *le asocia el morfismo* $O \longrightarrow O$ *en* $\mathtt{D}$.

   *Claramente, el funtor* $\bar{\mathbf{0}}$ *es covariante y contravariante.*

3.a) *Sea* $M \in R-Mod$. *Se define el funtor* $F : R-Mod \longrightarrow \mathbb{Z}-Mod$ *como sigue:*

   (i) *Para cada* $N \in R-Mod$, $F(N) = Hom_R(M, N)$.

   (ii) *Para cada homomorfismo de* $R-$*módulos* $f : N \longrightarrow N'$ *se cumple que* $F(f) : Hom_R(M, N) \longrightarrow Hom_R(M, N')$ *es tal que, para cada* $g \in Hom_R(M, N)$, $F(f)(g) = f \circ g$; *es decir, el siguiente diagrama conmuta:*

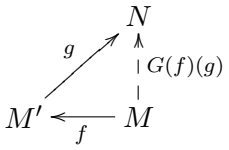



   *En tal caso, se llama a* $F$ *el funtor* $Hom$ *covariante.*

3.b) *Sea* $N \in R-Mod$. *Se define el funtor* $G : R-Mod \longrightarrow \mathbb{Z}-Mod$ *de la siguiente manera:*

(i) *Para cada* $M \in R-Mod$, $G(M) = Hom_R(M, N)$.

(ii) *Para cada homomorfismo de* $R-$*módulos* $f : M \longrightarrow M'$ *se cumple que* $G(f) : Hom_R(M', N) \longrightarrow Hom_R(M, N)$ *es tal que, para cada* $g \in Hom_R(M', N)$, $G(f)(g) = g \circ f$; *es decir, el siguiente diagrama conmuta:*




*En este último caso, se llama a* $G$ *el funtor* $Hom$ *contravariante.*

**Definición 1.117** *Sea* $F : R-Mod \longrightarrow R-Mod$ *un funtor. Si para toda sucesión exacta corta:*

$$0 \longrightarrow K \longrightarrow M \longrightarrow N \longrightarrow 0$$

*la sucesión:*

$$0 \longrightarrow F(K) \longrightarrow F(M) \longrightarrow F(N)$$

*también es exacta, se dice que* $F$ *es* exacto izquierdo. *Por su parte, si la sucesión:*

$$F(K) \longrightarrow F(M) \longrightarrow F(N) \longrightarrow 0$$

*es exacta, decimos que* $F$ *es* exacto derecho.
*Un funtor que es exacto izquierdo y derecho se llama* exacto.

**Definición 1.118** *Sean* $\mathtt{C}$ *y* $\mathtt{D}$ *dos categorías. Un funtor* $F : \mathtt{C} \longrightarrow \mathtt{D}$ *se llama* fiel *si para cada par de objetos* $A, B \in \mathtt{C}$ *y cada par de morfismos* $f, g \in \mathtt{C}(A, B)$, $F(f) = F(g) \in \mathtt{C}(F(A), F(B))$ *implica que* $f = g$.

**Definición 1.119** *Una categoría* concreta *es una pareja* $(\mathtt{C}, F)$ *tal que* $\mathtt{C}$ *es una categoría y* $F : \mathtt{C} \longrightarrow Conj$ *es un funtor fiel, de manera que es posible identificar a cada objeto* $A \in \mathtt{C}$ *con el conjunto* $F(A)$ *y a cada morfismo* $f \in \mathtt{C}$ *con la función* $F(f)$.

**Definición 1.120** *Sean* $\mathtt{C}$ *una categoría concreta,* $A, B \in \mathtt{C}$ *y* $f \in \mathtt{C}(A, B)$. *Si* $f$ *es monomorfismo, entonces* $A$ *se llama un* <u>subobjeto</u> *y* $f$ *se denomina la* <u>inclusión</u> *de* $A$ *en* $B$.

**Definición 1.121** *Sean* $\mathtt{C}$ *y* $\mathtt{D}$ *dos categorías y* $F, G : \mathtt{C} \longrightarrow \mathtt{D}$ *dos funtores. Una* <u>transformación natural</u> $t$ *de* $F$ *a* $G$, *que denotamos por* $t : F \longrightarrow G$, *es una clase de morfismos* $t_A : F(A) \longrightarrow G(A)$ *en* $\mathtt{D}$, *uno para cada objeto* $A \in \mathtt{C}$, *tal que, para cada morfismo* $f : A \longrightarrow B$ *en* $\mathtt{C}$, $G(f) \circ t_A = t_B \circ F(f)$; *es decir, el siguiente diagrama conmuta:*

$$\begin{array}{ccc} F(A) & \xrightarrow{t_A} & G(A) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(B) & \xrightarrow{t_B} & G(B) \end{array}$$

A continuación presentamos un ejemplo de transformación natural.

**Definición 1.122** *Sea* $\mathtt{C}$ *una categoría con subobjetos e inclusiones y sean* $F, G : \mathtt{C} \longrightarrow \mathtt{C}$ *dos funtores y* $t : F \longrightarrow G$ *una transformación natural. Diremos que* $F$ *es un* <u>subfuntor</u> *del funtor* $G$ *si, para cada objeto* $A \in \mathtt{C}$, *el morfismo* $t_A : F(A) \longrightarrow G(A)$ *es una inclusión.*

# Capítulo 2

# Prerradicales

Dedicamos este capítulo a las definiciones y propiedades básicas en la clase de todos los prerradicales sobre el anillo $R$, que, como veremos, es denotada por $R-pr$. Presentamos sus operaciones binarias y reticulares y definimos dos importantes tipos de prerradicales (*alfa* y *omega*), los cuales permiten probar que $R-pr$ es una gran retícula atómica y coatómica (describiendo completamente sus átomos y coátomos), además de caracterizar a cualquier prerradical, en particular a ciertas clases de ellos como los idempotentes, radicales y algunos prerradicales primos.

## 2.1. Definición y propiedades básicas

**Definición 2.1** *Un prerradical sobre el anillo $R$ es un subfuntor del funtor identidad en la categoría $R-Mod$; es decir, es un funtor*

$$\sigma : R-Mod \longrightarrow R-Mod$$

*tal que:*

*1) Para cada $M \in R-Mod$ se tiene que $\sigma(M) \leq M$.*

*2) Para cada $f \in Hom_R(M,N)$ se cumple que $f(\sigma(M)) \leq \sigma(N)$.*

**Ejemplo 2.2** *Dada* $\mathbf{A} \subseteq R-Mod$, *se tiene que* $\mathcal{T}_{R_{\mathbf{A}}}(\ )$ *y* $\mathcal{R}_{EJ_{\mathbf{A}}}(\ )$ *son prerradicales. En particular,* $Soc(\ ) = \mathcal{T}_{R_{\mathbf{S}}}(\ )$ *y* $Rad(\ ) = \mathcal{R}_{EJ_{\mathbf{S}}}(\ )$ *son prerradicales.*

Se denota por $R-pr$ a la clase de todos los prerradicales sobre $R$.

Presentamos a continuación propiedades relativas al comportamiento de los prerradicales respecto a la suma y el producto directos.

**Proposición 2.3** *Sean* $\sigma \in R-pr$ *y* $\{M_\alpha\}_{\alpha\in I} \subseteq R-Mod$, *entonces se tiene:*

*1)* $\sigma\left(\bigoplus_{\alpha\in I} M_\alpha\right) = \bigoplus_{\alpha\in I}\sigma(M_\alpha)$.

*2)* $\sigma\left(\prod_{\alpha\in I} M_\alpha\right) \leq \prod_{\alpha\in I}\sigma(M_\alpha)$.

*Demostración.*

*1)* : Para cada $\beta \in I$, sean $M_\beta \xrightarrow{i_\beta} \bigoplus_{\alpha\in I} M_\alpha$ y $\bigoplus_{\alpha\in I} M_\alpha \xrightarrow{p_\beta} M_\beta$ las inclusiones y proyecciones naturales, respectivamente. Entonces, para cada $\beta \in I$ se tiene que:

$$i_\beta(\sigma(M_\beta)) \leq \sigma\left(\bigoplus_{\alpha\in I} M_\alpha\right) \tag{2.1}$$

y

$$p_\beta\left(\sigma\left(\bigoplus_{\alpha\in I} M_\alpha\right)\right) \leq \sigma(M_\beta). \tag{2.2}$$

Sea $x = (x_\alpha)_{\alpha\in I} \in \sigma\left(\bigoplus_{\alpha\in I} M_\alpha\right)$. Entonces, por (2.2), para cada $\alpha \in I$ se tiene que $x_\alpha = p_\alpha(x) \in \sigma(M_\alpha)$, de donde $x \in \bigoplus_{\alpha\in I}\sigma(M_\alpha)$. Por tanto, $\sigma\left(\bigoplus_{\alpha\in I} M_\alpha\right) \leq \bigoplus_{\alpha\in I}\sigma(M_\alpha)$.

Por otro lado, si $x \in \bigoplus_{\alpha\in I}\sigma(M_\alpha)$, entonces $x = (x_\alpha)_{\alpha\in I}$, con $x_\alpha \in \sigma(M_\alpha)$ para cada $\alpha \in I$, por lo que existen $\beta_j \in I$, con $j \in \{1, 2, \ldots, n\}$, tales que para cada $\beta_j$ se tiene que $x = \sum_{j=1}^{n} i_{\beta_j} p_{\beta_j}(x)$. Ahora, nuevamente por (2.2), $p_{\beta_j}(x) \in$

$\sigma(M_{\beta_j})$, de donde, en virtud de (2.1), $i_{\beta_j}p_{\beta_j}(x) \in \sigma\left(\bigoplus_{\alpha\in I} M_\alpha\right)$ para cada $\beta_j \in I$ y $j \in \{1, 2, \ldots, n\}$. Luego, $x \in \sigma\left(\bigoplus_{\alpha\in I} M_\alpha\right)$. Por tanto, $\bigoplus_{\alpha\in I}\sigma(M_\alpha) \leq \sigma\left(\bigoplus_{\alpha\in I} M_\alpha\right)$, con lo que se tiene la igualdad.

*2)* : Para cada $\beta \in I$ consideremos las proyecciones naturales $\prod_{\alpha\in I} M_\alpha \xrightarrow{\pi_\beta} M_\beta$ y sea $x = (x_\alpha)_{\alpha\in I} \in \sigma\left(\prod_{\alpha\in I} M_\alpha\right)$. Entonces se tiene que $\pi_\beta\left(\sigma\left(\prod_{\alpha\in I} M_\alpha\right)\right) \leq \sigma(M_\beta)$, de donde $x_\beta = \pi_\beta(x) \in \sigma(M_\beta)$ para cada $\beta \in I$. Luego, $x \in \prod_{\alpha\in I}\sigma(M_\alpha)$. Por tanto, $\sigma\left(\prod_{\alpha\in I} M_\alpha\right) \leq \prod_{\alpha\in I}\sigma(M_\alpha)$, con lo que concluimos. □

## 2.2. Operaciones y propiedades

**Definición 2.4** *Para cada $\sigma, \tau \in R-pr$ se definen las siguientes operaciones binarias:*

1) *El producto $\sigma\tau$, tal que para cada $M \in R-Mod$ se tiene que $(\sigma\tau)(M) = \sigma(\tau(M))$.*

2) *El coproducto $(\sigma : \tau)$, tal que para cada $M \in R - Mod$ se cumple que $(\sigma : \tau)(M)/\sigma(M) = \tau(M/\sigma(M))$.*

La siguiente definición hace de $R - pr$ una clase parcialmente ordenada (ver sección 1.1.4 en el Capítulo 1).

**Definición 2.5** *Dados $\sigma, \tau \in R-pr$, diremos que $\sigma \preceq \tau$ si y sólo si para cada $M \in R - Mod$ se tiene que $\sigma(M) \leq \tau(M)$.*

Enseguida definimos más operaciones binarias en $R - pr$.

**Definición 2.6** *Para cada $\sigma, \tau \in R - pr$ se definen:*

1) *La conjunción $\sigma \wedge \tau$, tal que para cada $M \in R - Mod$ se tiene que $(\sigma \wedge \tau)(M) = \sigma(M) \cap \tau(M)$.*

*2) La disyunción $\sigma \vee \tau$, tal que para cada $M \in R - Mod$ se tiene que $(\sigma \vee \tau)(M) = \sigma(M) + \tau(M)$.*

**Observación 2.7** *En la definición anterior nos permitimos usar los símbolos "$\wedge$" y "$\vee$" para denotar a la conjunción y la disyunción, pues estas operaciones satisfacen las propiedades del ínfimo y el supremo, respectivamente, en $R - pr$.*

**Observación 2.8** *En $R - pr$ el producto, el coproducto, la conjunción y la disyunción están bien definidas.*[1] *Más aún, estas cuatro operaciones preservan el orden y son asociativas, mientras que sólo la conjunción y la disyunción son conmutativas.*

Las operaciones dadas en las Definiciones 2.4 y 2.6 se pueden comparar tal como se muestra en la siguiente proposición.

**Proposición 2.9** *Sean $\sigma, \tau \in R - pr$. Entonces, se tiene que*

$$\sigma\tau \preceq \sigma \wedge \tau \preceq \sigma \vee \tau \preceq (\sigma : \tau)$$

*Demostración.* Sea $M \in R - Mod$, entonces $\sigma\tau(M) = \sigma(\tau(M)) \leq \tau(M)$. Además, como $\tau(M) \leq M$, se tiene que $\sigma(\tau(M)) \leq \sigma(M)$. Luego, $\sigma(\tau(M)) \leq \sigma(M) \cap \tau(M)$, de donde $\sigma\tau \preceq (\sigma \wedge \tau)$. Por su parte, claramente, $(\sigma \wedge \tau)(M) = \sigma(M) \cap \tau(M) \leq \sigma(M) + \tau(M) = (\sigma \vee \tau)(M)$, de donde $\sigma \wedge \tau \preceq \sigma \vee \tau$. Consideremos ahora la proyección $\pi : M \longrightarrow M/\sigma(M)$. Se sigue que:

$$(\tau(M) + \sigma(M))/\sigma(M) = \pi(\tau(M)) \leq \tau(M/\sigma(M)) = (\sigma : \tau)(M)/\sigma(M).$$

Luego, por el Teorema de la Correspondencia,

$$(\sigma \vee \tau)(M) = (\tau(M) + \sigma(M)) \leq (\sigma : \tau)(M),$$

[1] Como consecuencia del Teorema de la Correspondencia, el coproducto en $R-pr$ está bien definido.

lo cual implica que $\sigma \vee \tau \preceq (\sigma : \tau)$, con lo que se prueba la desigualdad. $\square$

La conjunción y la disyunción de prerradicales pueden generalizarse para una clase arbitraria de ellos como sigue:

**Definición 2.10** *Sean* $\mathbf{I}$ *una clase de índices,* $\{\sigma_\alpha\}_{\alpha\in\mathbf{I}} \subseteq R-pr$ *y* $M \in R-Mod$. *Definimos:*[2]

*1) La conjunción arbitraria* $\bigwedge\limits_{\alpha\in\mathbf{I}} \sigma_\alpha$, *tal que* $\left(\bigwedge\limits_{\alpha\in\mathbf{I}} \sigma_\alpha\right)(M) = \bigcap\limits_{\alpha\in\mathbf{I}} \sigma_\alpha(M)$.

*2) La disyunción arbitraria* $\bigvee\limits_{\alpha\in\mathbf{I}} \sigma_\alpha$, *tal que* $\left(\bigvee\limits_{\alpha\in\mathbf{I}} \sigma_\alpha\right)(M) = \sum\limits_{\alpha\in\mathbf{I}} \sigma_\alpha(M)$.

Notemos que, aunque $\mathbf{I}$ es una clase, no necesariamente un conjunto, para cada $M \in R-Mod$, $\bigcap\limits_{\alpha\in\mathbf{I}} \sigma_\alpha(M)$ y $\sum\limits_{\alpha\in\mathbf{I}} \sigma_\alpha(M)$ son subconjuntos de $M$, pues $\{\sigma_\alpha(M) \mid \alpha \in \mathbf{I}\}$ es un conjunto.

**Observación 2.11** *Como consecuencia de la definición 2.10,* $\langle R{-}pr, \preceq, \vee, \wedge\rangle$ *resulta ser una gran*[3] *retícula completa, con elemento mayor el funtor identidad en* $R-Mod$, *que en adelante denotaremos simplemente por* $\bar{\mathbf{1}}$, *y elemento menor el funtor cero,* $\bar{\mathbf{0}} : R-Mod \longrightarrow R-Mod$.

Si bien la retícula $R-pr$ en general no es distributiva, en cambio sí es modular, como se afirma en la siguiente proposición fácil de verificar. Presentamos enseguida una serie de propiedades de distributividad del producto y el coproducto respecto de la conjunción y disyunción arbitrarias.

**Proposición 2.12** *(Ley Modular)*
*Dados* $\sigma, \tau, \eta \in R-pr$, *se cumple que:*

$$\sigma \preceq \tau \;\Rightarrow\; \sigma \vee (\tau \wedge \eta) = \tau \wedge (\sigma \vee \eta).$$

[2] Véase la Observación 2.7.

[3] Ver la sección 1.1.4 del Capítulo 1.

**Proposición 2.13** *Dados* $\mathbf{I}$ *una clase de índices,* $\{\sigma_\alpha\}_{\alpha\in\mathbf{I}} \subseteq R-pr$ *y* $\tau \in R-pr$*, se tiene que:*

*1.a)* $\left(\bigwedge\limits_{\alpha\in\mathbf{I}}\sigma_\alpha\right)\tau = \bigwedge\limits_{\alpha\in\mathbf{I}}(\sigma_\alpha\tau)$.

*1.b)* $\left(\bigvee\limits_{\alpha\in\mathbf{I}}\sigma_\alpha\right)\tau = \bigvee\limits_{\alpha\in\mathbf{I}}(\sigma_\alpha\tau)$.

*2.a)* $\left(\tau : \bigwedge\limits_{\alpha\in\mathbf{I}}\sigma_\alpha\right) = \bigwedge\limits_{\alpha\in\mathbf{I}}(\tau:\sigma_\alpha)$.

*2.b)* $\left(\tau : \bigvee\limits_{\alpha\in\mathbf{I}}\sigma_\alpha\right) = \bigvee\limits_{\alpha\in\mathbf{I}}(\tau:\sigma_\alpha)$.

*Demostración.*

*1.a)* : Dado $M \in R-Mod$, se tiene que:

$$\left(\left(\bigwedge_{\alpha\in\mathbf{I}}\sigma_\alpha\right)\tau\right)(M) = \bigcap_{\alpha\in\mathbf{I}}\sigma_\alpha(\tau(M)) = \bigcap_{\alpha\in\mathbf{I}}(\sigma_\alpha\tau)(M) = \bigwedge_{\alpha\in\mathbf{I}}(\sigma_\alpha\tau)(M).$$

*1.b)* : Dado $M \in R-Mod$, se tiene que:

$$\left(\left(\bigvee_{\alpha\in\mathbf{I}}\sigma_\alpha\right)\tau\right)(M) = \sum_{\alpha\in\mathbf{I}}\sigma_\alpha(\tau(M)) = \sum_{\alpha\in\mathbf{I}}(\sigma_\alpha\tau)(M) = \bigvee_{\alpha\in\mathbf{I}}(\sigma_\alpha\tau)(M).$$

*2.a)* : Dado $M \in R-Mod$, se tiene que:

$$\left(\tau : \bigwedge_{\alpha\in\mathbf{I}}\sigma_\alpha\right)(M)\Big/\tau(M) = \left(\bigwedge_{\alpha\in\mathbf{I}}\sigma_\alpha\right)(M/\tau(M)) =$$

$$\bigcap_{\alpha\in\mathbf{I}}\sigma_\alpha(M/\tau(M)) = \bigcap_{\alpha\in\mathbf{I}}((\tau:\sigma_\alpha)(M)/\tau(M)) =$$

$$\left(\bigcap_{\alpha\in\mathbf{I}}(\tau:\sigma_\alpha)(M)\right)\Big/\tau(M) = \left(\bigwedge_{\alpha\in\mathbf{I}}(\tau:\sigma_\alpha)\right)(M)\Big/\tau(M).$$

*2.b)* : Dado $M \in R-Mod$, se tiene que:

$$\left(\tau : \bigvee_{\alpha\in\mathbf{I}}\sigma_\alpha\right)(M)\Big/\tau(M) = \left(\bigvee_{\alpha\in\mathbf{I}}\sigma_\alpha\right)(M/\tau(M)) =$$

$$\sum_{\alpha\in\mathbf{I}}\sigma_\alpha(M/\tau(M)) = \sum_{\alpha\in\mathbf{I}}((\tau:\sigma_\alpha)(M)/\tau(M)) =$$

$$\left(\sum_{\alpha\in\mathbf{I}}(\tau:\sigma_\alpha)(M)\right)\Big/\tau(M)=\left(\bigvee_{\alpha\in\mathbf{I}}(\tau:\sigma_\alpha)\right)(M)\Big/\tau(M).$$

□

A continuación presentamos algunas clases especiales de prerradicales.

**Definición 2.14** *Sea $\sigma \in R-pr$. Se dice que:*

*1) $\sigma$ es idempotente, si $\sigma^2=\sigma$.*

*2) $\sigma$ es radical, si $(\sigma:\sigma)=\sigma$.*

*3) $\sigma$ es exacto izquierdo, si $\sigma$ es un funtor exacto izquierdo.*

*4) $\sigma$ es t-radical, si $\sigma(M)=\sigma(R)M$ para cada $M\in R-Mod$.*

*5) $\sigma$ es primo, si $\sigma\neq\bar{\mathbf{1}}$ y para cada $\tau,\eta\in R-pr$ se tiene que:*

$$\tau\eta\preceq\sigma \;\Rightarrow\; \tau\preceq\sigma \;\;\acute{o}\;\; \eta\preceq\sigma.$$

*5') $\sigma$ es coprimo, si $\sigma\neq\bar{\mathbf{0}}$ y para cada $\tau,\eta\in R-pr$ se tiene que:*

$$\sigma\preceq(\tau:\eta) \;\Rightarrow\; \sigma\preceq\tau \;\;\acute{o}\;\; \sigma\preceq\eta.$$

*6) $\sigma$ es irreducible, si para cada $\tau,\eta\in R-pr$ se tiene que:*

$$\tau\wedge\eta=\sigma \;\Rightarrow\; \tau=\sigma \;\;\acute{o}\;\; \eta=\sigma.$$

*6') $\sigma$ es coirreducible, si para cada $\tau,\eta\in R-pr$ se tiene que:*

$$\tau\vee\eta=\sigma \;\Rightarrow\; \tau=\sigma \;\;\acute{o}\;\; \eta=\sigma.$$

**Observación 2.15** *$\sigma\in R-pr$ es radical si y sólo si $\sigma(M/\sigma(M))=0$ para cada $M\in R-Mod$. En efecto, si $\sigma$ es radical y $M\in R-Mod$, entonces, por definición, $\sigma(M/\sigma(M))=(\sigma:\sigma)(M)/\sigma(M)=\sigma(M)/\sigma(M)=0$.*

**Proposición 2.16** *$\sigma \in R-pr$ es exacto izquierdo si y sólo si para cada $M \in R-Mod$ y para cada $N \leq M$ se tiene que $\sigma(N) = N \cap \sigma(M)$.*

*Demostración.* Sea $\sigma$ un prerradical exacto izquierdo y sean $M \in R-Mod$ y $N \leq M$. Consideremos la sucesión exacta $0 \longrightarrow N \hookrightarrow M \xrightarrow{\pi} M/N \longrightarrow 0$, entonces la sucesión $0 \longrightarrow \sigma(N) \hookrightarrow \sigma(M) \xrightarrow{\sigma(\pi)} \sigma(M/N)$ también es exacta, de donde $\sigma(N) = ker\,\sigma(\pi) = \sigma(M) \cap N$.

Para la suficiencia, sea $0 \longrightarrow K \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ una sucesión exacta corta. Notemos primero que, puesto que $f$ es monomorfismo, también $\sigma(f) : \sigma(K) \longrightarrow \sigma(M)$ lo es. Además, como $g \circ f = 0$, también se cumple que $\sigma(g) \circ \sigma(f) = 0$; es decir, $\sigma(f)(\sigma(K)) \leq \ker \sigma(g)$. Ahora, sea $K' := f(K) = ker\, g$, entonces existe un isomorfismo $h : K' \longrightarrow K$ tal que, si $y \in \sigma(K')$, entonces $y = f(h(y))$, con $h(y) \in \sigma(K)$. Luego, $y \in \sigma(f)(\sigma(K))$. Se sigue que $ker\,\sigma(g) = K' \cap \sigma(M) = \sigma(K') \leq \sigma(f)(\sigma(K))$. Por tanto, $\sigma(f)(\sigma(K)) = ker\,\sigma(g)$; esto es, la sucesión $0 \longrightarrow \sigma(K) \xrightarrow{\sigma(f)} \sigma(M) \xrightarrow{\sigma(g)} \sigma(N) \longrightarrow 0$ es exacta. □

**Observación 2.17** *Todo prerradical exacto izquierdo es idempotente y todo $t-$radical es radical.*

**Ejemplo 2.18** *Dada $\mathbf{A} \subseteq R-Mod$, por la Proposición 1.109 se tiene que $\mathcal{T}_{R_{\mathbf{A}}}(\ )$ es idempotente y $\mathcal{R}_{EJ_{\mathbf{A}}}(\ )$ es radical.*

En adelante, denotaremos por $R-id$ a la clase de todos los prerradicales idempotentes, por $R-rad$ a la clase de todos los radicales, por $R-ex$ a la clase de todos los prerradicales exactos izquierdos y por $R-trad$ a la clase de todos los $t-$radicales.

La siguiente proposición exhibe propiedades de cerradura de las clases de prerradicales idempotentes, $t-$radicales, radicales y prerradicales exactos izquierdos : las dos primeras, bajo disyunciones arbitrarias; las últimas, bajo conjunciones arbitrarias.

**Proposición 2.19** *Sean* $\mathbf{I}$ *una clase de índices y* $\{\sigma_\alpha\}_{\alpha\in\mathbf{I}} \subseteq R{-}pr$. *Se tienen las siguientes propiedades:*

*1) Si* $\{\sigma_\alpha\}_{\alpha\in\mathbf{I}} \subseteq R-id$, *entonces* $\bigvee\limits_{\alpha\in\mathbf{I}} \sigma_\alpha \in R-id$.

*2) Si* $\{\sigma_\alpha\}_{\alpha\in\mathbf{I}} \subseteq R-rad$, *entonces* $\bigwedge\limits_{\alpha\in\mathbf{I}} \sigma_\alpha \in R-rad$.

*3) Si* $\{\sigma_\alpha\}_{\alpha\in\mathbf{I}} \subseteq R-ex$, *entonces* $\bigwedge\limits_{\alpha\in\mathbf{I}} \sigma_\alpha \in R-ex$.

*4) Si* $\{\sigma_\alpha\}_{\alpha\in\mathbf{I}} \subseteq R-trad$, *entonces* $\bigvee\limits_{\alpha\in\mathbf{I}} \sigma_\alpha \in R-trad$.

*Demostración.*

*1)* : Supongamos que $\{\sigma_\alpha\}_{\alpha\in\mathbf{I}} \subseteq R-id$ y sea $\sigma = \bigvee\limits_{\alpha\in\mathbf{I}} \sigma_\alpha$, entonces por el inciso *1.b)* de la Proposición 2.13 se tiene que:

$$\sigma = \bigvee_{\alpha\in\mathbf{I}} \sigma_\alpha = \bigvee_{\alpha\in\mathbf{I}} (\sigma_\alpha\sigma_\alpha) \preceq \bigvee_{\alpha\in\mathbf{I}} (\sigma_\alpha\sigma) = \left(\bigvee_{\alpha\in\mathbf{I}} \sigma_\alpha\right)\sigma = \sigma\sigma \preceq \sigma,$$

de donde $\sigma\sigma = \sigma$; es decir, $\sigma = \bigvee\limits_{\alpha\in\mathbf{I}} \sigma_\alpha$ es idempotente.

*2)* : Supongamos que $\{\sigma_\alpha\}_{\alpha\in\mathbf{I}} \subseteq R-rad$ y sea $\tau = \bigwedge\limits_{\alpha\in\mathbf{I}} \sigma_\alpha$, entonces por el inciso *2.a)* de la Proposición 2.13 se tiene que:

$$\tau \preceq (\tau:\tau) = \left(\tau : \bigwedge_{\alpha\in\mathbf{I}} \sigma_\alpha\right) = \bigwedge_{\alpha\in\mathbf{I}} (\tau:\sigma_\alpha) \preceq \bigwedge_{\alpha\in\mathbf{I}} (\sigma_\alpha:\sigma_\alpha) = \bigwedge_{\alpha\in\mathbf{I}} \sigma_\alpha = \tau.$$

Por tanto, $(\tau:\tau) = \tau$; esto es, $\tau = \bigwedge\limits_{\alpha\in\mathbf{I}} \sigma_\alpha$ es radical.

*3)* : Supongamos ahora que $\{\sigma_\alpha\}_{\alpha\in\mathbf{I}} \subseteq R-ex$ y sean $M, N \in R-Mod$ tales que $N \leq M$. Sea $\eta = \bigwedge\limits_{\alpha\in\mathbf{I}} \sigma_\alpha$, entonces:

$$\eta(N) = \bigcap_{\alpha\in\mathbf{I}} \sigma_\alpha(N) = \bigcap_{\alpha\in\mathbf{I}} (\sigma_\alpha(M)\cap N) = \left(\bigcap_{\alpha\in\mathbf{I}} \sigma_\alpha(M)\right)\cap N = \eta(M)\cap N.$$

Por tanto, $\eta = \bigwedge\limits_{\alpha\in\mathbf{I}} \sigma_\alpha \in R-ex$.

*4)* : Finalmente, supongamos que $\{\sigma_\alpha\}_{\alpha\in\mathbf{I}} \subseteq R-trad$ y sea $M \in R-Mod$. Sea $\varsigma = \bigvee\limits_{\alpha\in\mathbf{I}} \sigma_\alpha$, entonces:

$$\varsigma(M) = \sum_{\alpha\in\mathbf{I}} \sigma_\alpha(M) = \sum_{\alpha\in\mathbf{I}} (\sigma_\alpha(R)M) = \left(\sum_{\alpha\in\mathbf{I}} \sigma_\alpha(R)\right) M = \varsigma(R)M.$$

Por tanto, $\varsigma = \bigvee_{\alpha \in \mathbf{I}} \sigma_\alpha \in R - trad.$ □

Presentamos enseguida un lema que nos será de gran utilidad.

**Lema 2.20** *Sea $\sigma \in R{-}pr$. Si $\sigma(ES) = 0$ para cada $S \in R{-}simp$, entonces $\sigma = \bar{\mathbf{0}}$.*

*Demostración.* Se sigue del inciso *4)* del Ejemplo 1.102 que para cada $M \in R - Mod$ existe un monomorfismo:

$$f : M \longrightarrow \left( \prod_{R-simp} ES \right)^X .$$

Luego, por el inciso *2)* de la Proposición 2.3:

$$f(\sigma(M)) \leq \sigma \left( \left( \prod_{R-simp} ES \right)^X \right) \leq \left( \prod_{R-simp} \sigma(ES) \right)^X = 0.$$

Por lo tanto, $\sigma(M) = 0$. Concluimos que $\sigma = \bar{\mathbf{0}}$. □

## 2.3. Prerradicales alfa y omega

**Definición 2.21** *Sean $M \in R - Mod$ y $N \in \mathcal{S}(M)$. Se dice que $N$ es un submódulo totalmente invariante de $M$ si para cada $f \in Hom_R(M, M)$ se tiene que $f(N) \leq N$*[4]*.*

**Ejemplo 2.22** *Presentamos a continuación un par de ejemplos importantes de submódulos totalmente invariantes.*

1) *Sea $S \in R - simp$. Si $f \in Hom_R(ES, ES)$, entonces $f(S) = S$, o bien, $f(S) = 0$. Se sigue que $S$ es totalmente invariante en $ES$.*

2) *Un ideal izquierdo $I$ del anillo $R$ es un submódulo totalmente invariante de $R$ si y sólo si $I$ es un ideal (bilateral) de $R$.*

[4]En tal caso, también suele llamarse a $N$ un *submódulo característico* (en inglés, 'fully-invariant') de $M$.

**Definición 2.23** *Sea $M \in R-Mod$ y sea $N$ un submódulo totalmente invariante de $M$. Se definen, para cada $K \in R-Mod$, los siguientes funtores:*

$$\alpha_N^M(K) := \sum \{f(N) \mid f \in Hom_R(M,K)\},$$

$$\omega_N^M(K) := \bigcap \left\{g^{-1}(N) \mid g \in Hom_R(K,M)\right\}.$$

**Observación 2.24** *En la definición anterior $\alpha_N^M(K)$ y $\omega_N^M(K)$ son submódulos de $K$. Más aún, $\alpha_N^M$ y $\omega_N^M$ son prerradicales sobre $R$.*

**Observación 2.25** *En particular, dados $M, K \in R-Mod$,*

$$\alpha_M^M(K) = \sum \{f(M) \mid f \in Hom_R(M,K)\} = \mathcal{T}_{R_M}(K)$$

*y*

$$\omega_0^M(K) := \bigcap \{ker\, g \mid g \in Hom_R(K,M)\} = \mathcal{R}_{EJ_M}(K)$$

*(0 y $M$ son, claramente, submódulos totalmente invariantes de $M$).*

**Observación 2.26** *De hecho, en principio, $\alpha_N^M$ y $\omega_N^M$ pueden ser definidos para todo submódulo $N$ de $M$; sin embargo, en caso de ser $N$ totalmente invariante en $M$, se tiene que $\alpha_N^M(M) = N$ y $\omega_N^M(M) = N$.*

A los prerradicales de la forma $\alpha_N^M$ y $\omega_N^M$ (siendo $N$ totalmente invariante en $M$) se les llama prerradicales *alfa* y *omega*, respectivamente.

La propiedad que presentamos a continuación es inmediata de la definición de prerradical alfa y omega.

**Lema 2.27** *Dado $M \in R-Mod$, si $K$ y $N$ son submódulos totalmente invariantes de $M$ tales que $K \leq N$, entonces:*

$$\alpha_K^M \leq \alpha_N^M \text{ y } \omega_K^M \leq \omega_N^M.$$

**Proposición 2.28** *Sea $M \in R-Mod$. Entonces $N$ es un submódulo totalmente invariante de $M$ si y sólo si existe $\sigma \in R-pr$ tal que $\sigma(M) = N$.*

*Demostración.* La necesidad es consecuencia inmediata de la Observación 2.26. Para probar la suficiencia supongamos que $N = \sigma(M)$, con $\sigma \in R - pr$, y sea $f \in Hom_R(M, M)$. Entonces, como $f(N) = f(\sigma(M)) \leq \sigma(M) = N$, se tiene que $N$ es submódulo totalmente invariante de $M$. □

**Proposición 2.29** *Sean $M \in R - Mod$ y $N$ un submódulo totalmente invariante de $M$. Se tiene que $\sigma(M) = N$ si y sólo si $\alpha_N^M \preceq \sigma \preceq \omega_N^M$.*

*Demostración.* Dado $L \in R - Mod$, si $N = \sigma(M)$ y $f \in Hom_R(M, L)$, se tiene que $f(N) = f(\sigma(M)) \leq \sigma(L)$, de donde $\alpha_N^M(L) \leq \sigma(L)$. Por otra parte, si $g \in Hom_R(L, M)$, entonces $g(\sigma(L)) \leq \sigma(M) = N$, de donde $\sigma(L) \leq g^{-1}g(\sigma(L)) \leq g^{-1}(\sigma(M)) = g^{-1}(N) \leq \omega_N^M(L)$. Por tanto, se ha demostrado que $\alpha_N^M \preceq \sigma \preceq \omega_N^M$.

Ahora, si $\alpha_N^M \preceq \sigma \preceq \omega_N^M$, entonces, por la Observación 2.26 se tiene que $N = \alpha_N^M(M) \leq \sigma(M) \leq \omega_N^M(M) = N$, es decir, $N = \sigma(M)$, con lo que concluimos. □

De la proposición anterior se sigue que, si $M \in R - Mod$ y $N$ es un submódulo totalmente invariante de $M$, entonces $\alpha_N^M$ y $\omega_N^M$ son, respectivamente, el menor y el mayor prerradicales que mandan a $M$ en $N$.

**Definición 2.30** *Dados $\tau$, $\eta \in R - pr$, es posible definir el intervalo:*

$$[\tau, \eta] := \{\sigma \in R - pr \mid \tau \preceq \sigma \preceq \eta\}$$

**Observación 2.31** *Sean $\tau$, $\eta \in R - pr$. Entonces:*

$$\tau \preceq \eta \Leftrightarrow [\tau, \eta] \neq \emptyset.$$

**Observación 2.32** *Así como $\mathcal{T}_{R_M}(K) = \alpha_M^M(K)$ y $\mathcal{R}_{EJ_M}(K) = \omega_0^M(K)$, también, dada una clase $\mathbf{A} \subseteq R - Mod$, se tiene, para todo $K \in R - Mod$, que:*

$$\mathcal{T}_{R_{\mathbf{A}}}(K) = \sum_{\mathbf{A}} \alpha_M^M(K) = \left(\bigvee_{\mathbf{A}} \alpha_M^M\right)(K)$$

*y*

$$\mathcal{R}_{EJ_{\mathbf{A}}}(K) = \bigcap_{\mathbf{A}} \omega_0^M(K) = \left( \bigwedge_{\mathbf{A}} \omega_0^M \right)(K).$$

*En particular,*

$$\bar{\mathbf{1}} = \mathcal{T}_{R_{R-Mod}}(\ ) = \left( \bigvee_{R-Mod} \alpha_M^M \right)$$

*y*

$$\bar{\mathbf{0}} = \mathcal{R}_{EJ_{R-Mod}}(\ ) = \left( \bigwedge_{R-Mod} \omega_0^M \right).$$

De hecho, se tiene que:

**Proposición 2.33** *Dada* $\sigma \in R - pr$,

*1)* $\sigma = \bigvee \left\{ \alpha^M_{\sigma(M)} \ \middle| \ M \in R - Mod \right\}$;

*2)* $\sigma = \bigwedge \left\{ \omega^M_{\sigma(M)} \ \middle| \ M \in R - Mod \right\}$.

*Demostración.*

*1)* : Sea $M \in R-Mod$. Por la Proposición 2.29 se tiene que $\alpha^M_{\sigma(M)} \preceq \sigma \preceq \omega^M_{\sigma(M)}$, de donde $\bigvee\limits_{R-Mod} \alpha^M_{\sigma(M)} \preceq \sigma$. Por otro lado, si $L \in R - Mod$, en virtud de la Observación 2.26 se sigue que $\sigma(L) = \alpha^L_{\sigma(L)}(L) \leq \left( \bigvee\limits_{R-Mod} \alpha^M_{\sigma(M)} \right)(L)$, es decir $\sigma \preceq \bigvee\limits_{R-Mod} \alpha^M_{\sigma(M)}$. Se tiene la igualdad.

*2)* : La desigualdad $\sigma \preceq \bigvee\limits_{R-Mod} \omega^M_{\sigma(M)}$ se sigue nuevamente de la Proposición 2.29. Similarmente, si $L \in R - Mod$, de la Observación 2.26 se sigue que $\left( \bigwedge\limits_{R-Mod} \omega^M_{\sigma(M)} \right)(L) \leq \omega^L_{\sigma(L)}(L) = \sigma(L)$, esto es $\bigwedge\limits_{R-Mod} \omega^M_{\sigma(M)} \preceq \sigma$, con lo que se prueba la igualdad. □

**Lema 2.34** *Sea* $\sigma \in R - pr$. *Entonces* $\sigma = \bar{\mathbf{1}}$ *si y sólo si* $\sigma(R) = R$.

*Demostración.* La necesidad es inmediata. Para la suficiencia, supongamos que $\sigma(R) = R$. Por el Lema 1.53, para cada $M \in R - Mod$, $\alpha^R_{\sigma(R)}(M) =$

$\sum\{f(\sigma(R)) \mid f \in Hom_R(R,M)\} = \sum\{d_x(\sigma(R)) \mid x \in M\} = \sigma(R)M$. Se sigue de la Observación 1.65 y de la Proposición 2.29 que $M = RM = \sigma(R)M = \alpha^R_{\sigma(R)}(M) \leq \sigma(M)$. Por otro lado, por definición, $\sigma(M) \leq M$, de donde $\sigma(M) = M$; es decir, $\sigma = \bar{\mathbf{1}}$. □

**Proposición 2.35** *$R - pr$ es una gran retícula atómica. El conjunto de sus átomos es:*

$$\left\{\alpha^{ES}_S \mid S \in R - simp\right\}.$$

*Demostración.* Sea $S \in R - simp$ y sea $\tau \in R - pr$ tal que $\tau \prec \alpha^{ES}_S$. Luego, por la Proposición 2.29, $\tau(ES) = 0$. Sea $S' \in R - simp$, con $S' \neq S$, entonces $\tau(ES') \leq \alpha^{ES}_S(ES') = 0$. Se sigue del Lema 2.20 que $\tau = \bar{\mathbf{0}}$. Por tanto, $\alpha^{ES}_S$ es un átomo en $R - pr$. Ahora, sea $\sigma \in R - pr$ tal que $\sigma \neq \bar{\mathbf{0}}$. Entonces, nuevamente por el Lema 2.20, existe $S \in R - simp$ tal que $\sigma(ES) \neq 0$. Se sigue que $S \leq \sigma(ES)$. Luego, por el Lema 2.27 y por la Proposición 2.29, $\alpha^{ES}_S \preceq \alpha^{ES}_{\sigma(ES)} \preceq \sigma$. En particular, si $\sigma \in R - pr$ es un átomo, entonces existe $S \in R - simp$ tal que $\bar{\mathbf{0}} \prec \alpha^{ES}_S \preceq \sigma$, de donde $\sigma = \alpha^{ES}_S$, con lo que concluimos. □

**Proposición 2.36** *$R - pr$ es una gran retícula coatómica. El conjunto de sus coátomos es:*

$$\left\{\omega^R_I \mid I \text{ es un ideal máximo de } R\right\}.$$

*Demostración.* Sea $I$ un ideal máximo de $R$ y sea $\tau \in R - pr$ tal que $\omega^R_I \prec \tau$. Entonces, por la Proposición 2.29 se tiene que $I < \tau(R)$. Luego, como $\tau(R)$ es un ideal de $R$ e $I$ es un ideal máximo, debe ocurrir que $\tau = \bar{\mathbf{1}}$ en virtud del Lema 2.34. Se sigue que $\omega^R_I$ es un coátomo. Ahora, sea $\sigma \in R - pr$, con $\sigma \neq \bar{\mathbf{1}}$. De nuevo por el Lema 2.34, $\sigma(R) \neq R$, y, por tanto, debe existir un ideal máximo $I$ de $R$ tal que $\sigma(R) \leq I$. Por el Lema 2.27 y por la Proposición 2.29 se sigue que $\sigma \preceq \omega^R_{\sigma(R)} \preceq \omega^R_I$. En particular, si $\sigma \in R - pr$ es un coátomo, entonces existe un ideal máximo $I$ de $R$ tal que $\sigma \prec \omega^R_I \preceq \bar{\mathbf{1}}$, de donde $\sigma = \omega^R_I$, con lo que concluimos. □

**Teorema 2.37** *Dado $\sigma \in R-pr$, se tiene que:*

*1)* $\sigma \in R-id \Leftrightarrow \sigma = \bigvee \{ \alpha_M^M \mid \sigma(M) = M,\ M \in R-Mod \}$.

*2)* $\sigma \in R-rad \Leftrightarrow \sigma = \bigwedge \{ \omega_0^M \mid \sigma(M) = 0,\ M \in R-Mod \}$.

*3)* $\sigma \in R-ex \Leftrightarrow \sigma = \bigwedge \left\{ \omega_{\sigma(Q)}^Q \mid Q \in \mathcal{E} \right\}$.

*4)* $\sigma$ *es un radical exacto izquierdo* $\Leftrightarrow \sigma = \bigwedge \left\{ \omega_0^Q \mid \sigma(Q) = 0,\ Q \in \mathcal{E} \right\}$.

*5)* $\sigma \in R-trad \Leftrightarrow \sigma = \alpha_{\sigma(R)}^R$.

*Demostración.*

*1)* : Sea $\sigma \in R-id$. Luego, por la Proposición 2.29, si $M \in R-Mod$ es tal que $\sigma(M) = M$, entonces se tiene que $\alpha_M^M \preceq \sigma$. Por tanto, se sigue que $\bigvee \{ \alpha_M^M \mid \sigma(M) = M,\ M \in R-Mod \} \preceq \sigma$. Por otra parte, si $L \in R-Mod$, entonces, como $\sigma$ es idempotente, $\sigma(\sigma(L)) = \sigma(L)$. Ahora bien, consideremos la inclusión canónica $\sigma(L) \hookrightarrow L$. De la Observación 2.26 se sigue que $\sigma(L) = \alpha_{\sigma(L)}^{\sigma(L)}(\sigma(L)) \leq \alpha_{\sigma(L)}^{\sigma(L)}(L)$, de donde $\sigma \preceq \bigvee \{ \alpha_M^M \mid \sigma(M) = M,\ M \in R-Mod \}$, lo que prueba la igualdad.

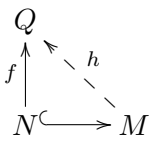
Recíprocamente, para cada $M \in R-Mod$ se sigue del Ejemplo 2.18 y de la Observación 2.25 que $\alpha_M^M = \mathcal{T}_{R_M}(\ )$ es idempotente. Luego, por el inciso *1)* de la Proposición 2.19, $\sigma = \bigvee \{ \alpha_M^M \mid \sigma(M) = M,\ M \in R-Mod \}$ es idempotente.

*2)* : Sea $\sigma \in R-rad$. De nuevo por la Proposición 2.29, para cada $M \in R-Mod$ tal que $\sigma(M) = 0$ se tiene que $\sigma \preceq \omega_0^M$. Por tanto, se sigue que $\sigma \preceq \bigwedge \{ \omega_0^M \mid \sigma(M) = 0,\ M \in R-Mod \}$. Por otro lado, dado $L \in R-Mod$, como $\sigma$ es radical, se sigue de la Observación 2.15 que $\sigma(L/\sigma(L)) = 0$. Consideremos ahora la proyección canónica $\pi : L \longrightarrow L/\sigma(L)$. Entonces $\omega_0^{L/\sigma(L)}(L) \leq ker\pi = \sigma(L)$, de donde $\bigwedge \{ \omega_0^M \mid \sigma(M) = 0,\ M \in R-Mod \} \preceq \sigma$, con lo que se tiene la igualdad.

Para la suficiencia, sea $M \in R-Mod$. Se sigue del Ejemplo 2.18 y de la Observación 2.25 que $\omega_0^M = \mathcal{R}_{EJ_M}(\ )$ es radical. Luego, por el inciso *2)* de la Proposición 2.19, $\sigma = \bigwedge \{\omega_0^M \mid \sigma(M) = 0,\ M \in R-Mod\}$ es radical.

*3)* : Sea $\sigma \in R-ex$ y sea $Q \in \mathcal{E}$. Luego, una vez más por la Proposición 2.29 se tiene que $\sigma \preceq \omega_{\sigma(Q)}^Q$. Por tanto, se sigue que $\sigma \preceq \bigwedge \left\{ \omega_{\sigma(Q)}^Q \mid Q \in \mathcal{E} \right\}$. Por otra parte, por la Proposición 2.16, para cada $L \in R-Mod$ se cumple que $\sigma(L) = L \cap \sigma(EL) = i^{-1}(\sigma(EL))$, donde $i : L \longrightarrow EL$ es la inclusión en la cápsula inyectiva. Luego, $\omega_{\sigma(EL)}^{EL}(L) \leq \sigma(L)$, de donde $\bigwedge \left\{ \omega_{\sigma(Q)}^Q \mid Q \in \mathcal{E} \right\} \preceq \sigma$, con lo que se verifica la igualdad.

Ahora supongamos que $\sigma = \bigwedge \left\{ \omega_{\sigma(Q)}^Q \mid Q \in \mathcal{E} \right\}$. Sean $M, N \in R-Mod$ tales que $N \leq M$, y $Q \in \mathcal{E}$. La contención $\omega_{\sigma(Q)}^Q(N) \subseteq N \cap \omega_{\sigma(Q)}^Q(M)$ es inmediata. Ahora, sea $x \in N \cap \omega_{\sigma(Q)}^Q(M)$. Entonces $x \in g^{-1}(\sigma(Q))$ para cualquier $g \in Hom_R(M, Q)$. Sea $f \in Hom_R(N, Q)$. Como $Q$ es inyectivo, existe $h \in Hom_R(M, Q)$ tal que el siguiente diagrama conmuta:




Se sigue que $x \in h^{-1}(\sigma(Q))$; esto es, $f(x) = h(x) \in \sigma(Q)$, pues $x \in N$. Luego, $x \in f^{-1}(\sigma(Q))$, de donde $x \in \omega_{\sigma(Q)}^Q(N)$. Por tanto, $N \cap \omega_{\sigma(Q)}^Q(M) \subseteq \omega_{\sigma(Q)}^Q(N)$. Por las Proposiciones 2.16 y 2.19,*3*) concluimos que $\sigma = \bigwedge \left\{ \omega_{\sigma(Q)}^Q \mid Q \in \mathcal{E} \right\}$ es exacto izquierdo.

*4)* : Sea $\sigma$ un radical exacto izquierdo y sea $Q \in \mathcal{E}$. Luego, si $\sigma(Q) = 0$, por la Proposición 2.29 se tiene que $\sigma \preceq \omega_0^Q$.

Por tanto, $\sigma \preceq \bigwedge \left\{ \omega_0^Q \mid \sigma(Q) = 0,\, Q \in \mathcal{E} \right\}$.

Por otra parte, dado $L \in R-Mod$, como $\sigma$ es radical, se sigue de la Observación 2.15 que $\sigma(L/\sigma(L)) = 0$. Sea $Q_0 := E\,L/\sigma(L)$, la cápsula inyectiva de $L/\sigma(L)$. Como $\sigma$ es exacto izquierdo se tiene que $L/\sigma(L) \cap \sigma(Q_0) = \sigma(L/\sigma(L)) = 0$, de donde, al ser $L/\sigma(L)$ esencial en $Q_0$, se sigue que $\sigma(Q_0) =$

0. Consideremos la proyección canónica $\pi : L \longrightarrow L/\sigma(L)$ y la inclusión $i : L/\sigma(L) \longrightarrow Q_0$. Entonces, $\omega_0^{Q_0}(L) \leq ker(i \circ \pi) = \sigma(L)$. Por lo tanto, $\bigwedge \left\{ \omega_0^Q \mid \sigma(Q) = 0, Q \in \mathcal{E} \right\} \preceq \sigma,$ lo que prueba la igualdad.

Para la suficiencia, dado $Q \in \mathcal{E}$, se tiene que $\omega_0^Q$ es un radical, por ser $\omega_0^Q = \mathcal{R}_{EJ_Q}(\ )$ y en virtud del Ejemplo 2.18 y de la Observación 2.25. Además, si $\sigma(Q) = 0$, entonces $\omega_0^Q = \omega_{\sigma(Q)}^Q$, que, por el inciso *3)*, es exacto izquierdo. Finalmente, por la Proposición 2.19, $\bigwedge \left\{ \omega_0^Q \mid \sigma(Q) = 0, Q \in \mathcal{E} \right\}$ es exacto izquierdo, siendo la clase de radicales exactos izquierdos cerrada bajo conjunciones arbitrarias.

*5)* : Sea $\sigma \in R - trad$. Recordemos que, por el Lema 1.53, para cada $M \in R - Mod$ tenemos que $\alpha_{\sigma(R)}^R(M) = \sum\{f(\sigma(R)) \mid f \in Hom_R(R, M)\} = \sum\{d_x(\sigma(R)) \mid x \in M\} = \sigma(R)M$. Luego, $\sigma(M) = \alpha_{\sigma(R)}^R(M)$.

Recíprocamente, si $\sigma = \alpha_{\sigma(R)}^R$, entonces, para cada $M \in R-Mod$, $\sigma(M) = \alpha_{\sigma(R)}^R(M) = \sigma(R)M = \alpha_{\sigma(R)}^R(R)M = \sigma(R)M$, con lo que concluimos. □

El siguiente lema no es difícil de verificar:

**Lema 2.38** *Sean $\{M_\beta\}_{\beta\in I}$, $\{N_\beta\}_{\beta\in I} \subseteq R - Mod$. Entonces:*

*1) Si $M = \bigoplus_{\beta\in I} M_\beta$, $N = \bigoplus_{\beta\in I} N_\beta$ y $N$ es submódulo totalmente invariante de $M$, entonces, para cada $\beta \in I$, $N_\beta$ es un submódulo totalmente invariante de $M_\beta$.*

*2) Si $M = \prod_{\beta\in I} M_\beta$, $N = \prod_{\beta\in I} N_\beta$ y $N$ es submódulo totalmente invariante de $M$, entonces, para cada $\beta \in I$, $N_\beta$ es un submódulo totalmente invariante de $M_\beta$.*

En virtud del lema anterior, la siguiente proposición, que generaliza el Lema 16 de [7], tiene sentido.

**Proposición 2.39** *Sean $\{M_\beta\}_{\beta\in I}$, $\{N_\beta\}_{\beta\in I} \subseteq R - Mod$. Entonces:*

*1) Si* $M = \bigoplus_{\beta\in I} M_\beta$, $N = \bigoplus_{\beta\in I} N_\beta$ *y* $N$ *es un submódulo totalmente invariante de* $M$*, se tiene que:*

$$\bigvee_{\beta\in I} \alpha_{N_\beta}^{M_\beta} = \alpha_N^M.$$

*2) Si* $M = \prod_{\beta\in I} M_\beta$, $N = \prod_{\beta\in I} N_\beta$ *y* $N$ *es un submódulo totalmente invariante de* $M$*, se cumple que:*

$$\bigwedge_{\beta\in I} \omega_{N_\beta}^{M_\beta} = \omega_N^M.$$

*Demostración.*

*1)* : Sean $M = \bigoplus_{\beta\in I} M_\beta$ y $N = \bigoplus_{\beta\in I} N_\beta$. Por definición tenemos, para cada $K \in R - Mod$, que:

$$\alpha_N^M(K) = \sum \left\{ f\left(\bigoplus_{\beta\in I} N_\beta\right) \;\middle|\; f \in Hom_R\left(\bigoplus_{\beta\in I} M_\beta, K\right) \right\}$$

y

$$\alpha_{N_\beta}^{M_\beta}(K) = \sum \{f(N_\beta) \mid f \in Hom_R(M_\beta, K)\}.$$

Para cada $\beta \in I$, sean $M_\beta \xrightarrow{i_\beta} \bigoplus_{\beta\in I} M_\beta$ y $\bigoplus_{\beta\in I} M_\beta \xrightarrow{p_\beta} M_\beta$ las inclusiones y proyecciones naturales, respectivamente. Por un lado tenemos, para cada $\beta \in I$, que:

$$f(N_\beta) = f\, p_\beta \left(\bigoplus_{\beta\in I} N_\beta\right) \leq \alpha_N^M(K).$$

Se sigue que $\bigvee_{\beta\in I} \alpha_{N_\beta}^{M_\beta} \preceq \alpha_N^M$.

Por otra parte,

$$f\left(\bigoplus_{\beta\in I} N_\beta\right) = \sum_{\beta\in I} f\, i_\beta(N_\beta) \leq \sum_{\beta\in I} \alpha_{N_\beta}^{M_\beta}(K).$$

Por tanto, $\bigvee_{\beta\in I} \alpha_{N_\beta}^{M_\beta} \succeq \alpha_N^M$, con lo que se prueba la igualdad.

*2)* : Sean $M = \prod_{\beta\in I} M_\beta$ y $N = \prod_{\beta\in I} N_\beta$. Por definición, para cada $K \in R - Mod$,

$$\omega_N^M(K) = \bigcap \left\{ f^{-1}\left(\prod_{\beta\in I} N_\beta\right) \;\middle|\; f \in Hom_R\left(K, \prod_{\beta\in I} M_\beta\right) \right\}$$

y

$$\omega_{N_\beta}^{M_\beta}(K) = \bigcap\{f^{-1}(N_\beta) \mid f \in Hom_R(K, M_\beta)\}.$$

Nuevamente, consideremos para cada $\beta \in I$ las inclusiones naturales $M_\beta \xrightarrow{i_\beta} \prod_{\beta\in I} M_\beta$ y las proyecciones naturales $\prod_{\beta\in I} M_\beta \xrightarrow{\pi_\beta} M_\beta$. Por un lado tenemos para cada $\beta \in I$ que:

$$\omega_N^M(K) \leq (i_\beta\, f^{-1}\left(\prod_{\beta\in I} N_\beta\right) = f^{-1}(N_\beta).$$

Luego, $\bigwedge_{\beta\in I} \omega_{N_\beta}^{M_\beta} \succeq \omega_N^M$.
Por otro lado,

$$\bigcap \omega_{N_\beta}^{M_\beta}(K) \leq \bigcap (\pi_\beta\, f)^{-1}(N_\beta) = f^{-1}(\prod_{\beta\in I} N_\beta),$$

de donde, $\bigwedge_{\beta\in I} \omega_{N_\beta}^{M_\beta} \preceq \omega_N^M$, con lo que concluimos. □

## 2.4. Prerradicales y submódulos primos

Presentamos a continuación una útil caracterización de prerradical primo.

**Proposición 2.40** *Sea $\sigma \in R-pr$, con $\sigma \neq \overline{\mathbf{1}}$. Entonces las siguientes condiciones son equivalentes:*

*(a) $\sigma$ es primo.*

*(b) Para cada $\tau, \eta \in R-pr$ tales que $\tau \succeq \sigma$, $\tau\,\eta \preceq \sigma$ implica que $\tau = \sigma$ ó $\eta \preceq \sigma$.*

*Demostración.*

$(a) \Rightarrow (b)$. Es inmediata de la definición de prerradical primo.

$(b) \Rightarrow (a)$. Sean $\tau, \eta \in R-pr$ tales que $\tau\,\eta \preceq \sigma$. Se sigue de la Proposición 2.13 que $(\tau\vee\sigma)\eta = \tau\,\eta \vee \sigma\,\eta \preceq \sigma$. Luego, por hipótesis, se tiene que $(\tau\vee\sigma) \preceq \sigma$ ó $\eta \preceq \sigma$; es decir, $\tau \preceq \sigma$ ó $\eta \preceq \sigma$. Concluimos que $\sigma$ es un prerradical primo.

□

**Observación 2.41** *Todos los coátomos de $R-pr$ son primos.*

Antes de dar la definición de submódulo primo se presenta el producto de submódulos totalmente invariantes.

**Definición 2.42** *Sea $M \in R-Mod$ y sean $K, L$ submódulos totalmente invariantes de $M$. Se define el producto de $K$ y $L$ como $KL := \alpha_K^M(L)$.*

**Definición 2.43** *Sean $M \in R-Mod$ y $N \neq M$, un submódulo totalmente invariante de $M$. Decimos que $N$ es primo en $M$ si para cualesquiera $K, L$ submódulos totalmente invariantes de $M$, se tiene que $KL \leq N$ implica que $K \leq N$ ó $L \leq N$.*

Como consecuencia de la definición anterior se tienen las siguientes propiedades:

**Proposición 2.44** *Sea $M \in R-Mod$. Entonces:*

1) *Si $N \neq M$ es un submódulo totalmente invariante máximo de $M$, entonces $N$ es primo en $M$.*

2) *Sean $\tau, \eta \in R-pr$. Entonces $\tau(M)\eta(M) \leq (\tau\,\eta)(M)$.*

A continuación se presenta una caracterización de submódulo primo en términos de prerradicales.

**Teorema 2.45** *Sean $M \in R-Mod$ y $N \neq M$, un submódulo totalmente invariante de $M$. Las siguientes condiciones son equivalentes:*

*(a) $N$ es primo en $M$.*

*(b) $\omega_N^M$ es un prerradical primo.*

*Demostración.*

$(a) \Rightarrow (b)$. Como $N \neq M$ se tiene que $\omega_N^M \neq \bar{\mathbf{1}}$. Sean $\tau, \eta \in R - pr$ tales que $\tau\,\eta \preceq \omega_N^M$. En virtud de la Proposición 2.44 se tiene que $\tau(M)\eta(M) \leq (\tau\,\eta)(M) \leq \omega_N^M(M) = N$, de donde, por hipótesis, $\tau(M) \leq N$ ó $\eta(M) \leq N$. Se sigue de la Proposición 2.29 que $\tau \preceq \omega_N^M$ ó $\eta \preceq \omega_N^M$. Por tanto, $\omega_N^M$ es primo.

$(b) \Rightarrow (a)$. Si $\omega_N^M$ es primo, entonces $N \neq M$. Sean $K, L$ submódulos totalmente invariantes de $M$ tales que $KL \leq N$. Por definición se tiene que $KL = \alpha_K^M(L) = \alpha_K^M \alpha_L^M(M)$, de donde, por la Proposición 2.29 y el Lema 2.27, $\alpha_K^M \alpha_L^M \preceq \omega_{KL}^M \preceq \omega_N^M$. Luego, como $\omega_N^M$ es primo, $\alpha_K^M \preceq \omega_N^M$ ó $\alpha_L^M \preceq \omega_N^M$, esto es, $K \leq N$ ó $L \leq N$. Se concluye que $N$ es primo en $M$. □

Existen dos clases disjuntas de prerradicales primos $\sigma$, dependiendo de cuántos $S \in R - simp$ son tales que $\alpha_S^S \not\preceq \sigma$. Dichas clases de prerradicales son presentadas en la siguiente:

**Definición 2.46** *Sea $\sigma$ un prerradical primo. Decimos que:*

*1) $\sigma$ es $\underline{1 - simple}$, si existe exactamente un $S \in R-simp$ tal que $\alpha_S^S \not\preceq \sigma$.*

*2) $\sigma$ es $\underline{0 - simple}$, si para todo $S \in R - simp$ se tiene que $\alpha_S^S \preceq \sigma$.*

**Teorema 2.47** *Sea $\sigma$ un prerradical primo. Entonces $\sigma$ es $1 - simple$ ó $\sigma$ es $0 - simple$.*

*Demostración.* Supongamos que existen $S, S' \in R - simp$ tales que $S \ncong S'$ y $\alpha_S^S \not\preceq \sigma$, $\alpha_{S'}^{S'} \not\preceq \sigma$. Entonces se tiene que $\alpha_S^S\,\alpha_{S'}^{S'} = \bar{\mathbf{0}} \preceq \sigma$, en contradicción con el hecho de que $\sigma$ es primo. Por tanto, $\sigma$ es $1-$simple, o bien, $\sigma$ es $0-$simple. □

**Teorema 2.48** *Sea $\sigma$ un prerradical primo. Si $\sigma$ es $1 - simple$, entonces existe $S \in R - simp$ tal que $\sigma = \omega_0^S$.*

*Demostración.* Sea $\sigma$ un prerradical primo $1-$simple. Entonces existe $S \in R - simp$ tal que $\alpha_S^S \not\preceq \sigma$. Por tanto, $\sigma(S) = 0$; es decir, $\sigma \preceq \omega_0^S$. Por otro lado, se tiene que $\omega_0^S \, \alpha_S^S = \bar{\mathbf{0}}$. Luego, como $\sigma$ es primo, debe ocurrir que $\omega_0^S \preceq \sigma$. Concluimos que $\sigma = \omega_0^S$. □

Notemos que los prerradicales primos $1-$simples son radicales y también son prerradicales primos mínimos, como se muestra en el siguiente resultado.

**Teorema 2.49** *Para cada $S \in R-simp$, $\omega_0^S$ es un prerradical primo mínimo.*

*Demostración.* Sean $S \in R - simp$ y $\sigma$ un prerradical primo tal que $\bar{\mathbf{0}} \neq \sigma \preceq \omega_0^S$. Si $\alpha_S^S \preceq \sigma$, entonces se tiene que $S = \alpha_S^S(S) \leq \omega_0^S(S) = 0$, una contradicción. Por tanto, $\alpha_S^S \not\preceq \sigma$ y, por el Teorema 2.48, $\sigma = \omega_0^S$. □

# Capítulo 3

# El Teorema de Kulikov

Tal como el título lo indica, el objetivo principal de este capítulo es presentar un importante teorema debido a Kulikov ([13]), el cual caracteriza a los $p-$grupos que son suma directa de grupos cíclicos. Posteriormente, como consecuencia de este teorema y de las propiedades intrínsecas de $\mathbb{Z}_{p^n}$, seremos capaces de describir a las retículas de prerradicales sobre estos anillos.

Comenzamos presentando algunos teoremas de descomposición de grupos de torsión y, en particular, de $p-$grupos elementales, que habrán de servirnos más adelante.

**Teorema 3.1** *Sea $A$ un grupo de torsión. Entonces $A$ es suma directa de sus $p-$componentes.*

*Demostración.* Notemos primero que las $p-$componentes $A_p$ son subgrupos de $A$. En efecto, como $0 \in A_p$, $A_p \neq \emptyset$. Además, si $a, b \in A_p$, entonces existen $m, n \in \mathbb{N}$ tales que $p^m a = 0 = p^n b$. Luego, si $l := \text{máx}\{m, n\}$, se tiene que $p^l(a - b) = 0$, de donde $a - b \in A_p$. Observemos también que la familia $\{A_{p_i}\}_{p_i \in \mathbb{P}}$ es independiente. Sea $a \in A_{p_i} \cap \sum_{j \neq i} A_{p_j}$, entonces:

$$a = a_1 + a_2 + \cdots + a_r,$$

con $a_k \in A_{p_{j_k}}$ y $j_k \neq i$ para cada $k \in \{1, 2, \ldots, r\}$. Por hipótesis existe $n_i \in \mathbb{N}$

tal que $p_i^{n_i}a = 0$. Asimismo, para cada $k \in \{1, 2, \ldots, r\}$ existe $n_{j_k} \in \mathbb{N}$ tal que $p_{j_k}^{n_{j_k}}a_k = 0$. Sea $q := p_{j_1}^{n_{j_1}}p_{j_2}^{n_{j_2}}\cdots p_{j_r}^{n_{j_r}}$. Entonces, por ser $p_i^{n_i}$ y $q$ primos relativos, existen $s, t \in \mathbb{Z}$ tales que $1 = sp_i^{n_i}+tq$, de donde $a = sp_i^{n_i}a+tqa = 0$. Luego, $A_{p_i} \cap \sum_{j\neq i} A_{p_j} = 0$. Ahora, sea $a \in A$ y supongamos que $o(a) = m = p_1^{r_1}\ldots p_n^{r_n}$, con $p_1, \ldots, p_n$ primos distintos y $r_i > 0$ para cada $i \in \{1, \ldots, n\}$. Puesto que los números $m_i := mp_i^{-r_i}$ cumplen que $mcd(m_1, \ldots, m_n) = 1$, se tiene que existen $s_1, \ldots, s_n \in \mathbb{Z}$ tales que $1 = s_1m_1 + \cdots + s_nm_n$. Luego, $a = s_1m_1a + \cdots + s_nm_na$, donde $s_im_ia \in A_{p_i}$ (pues $p_i^{r_i}s_im_ia = s_ima = 0$). Por tanto, $a \in A_{p_1} + \cdots + A_{p_n} \leq \bigoplus_{p\in\mathbb{P}} A_p$. Concluimos que $A = \bigoplus_{p\in\mathbb{P}} A_p$. □

**Lema 3.2** *Sea $A$ un grupo. Un conjunto $L = \{\, a_\alpha \,\}_{\alpha\in I}$ de elementos distintos de cero de $A$ es independiente si y sólo si $\langle\, L \,\rangle = \bigoplus_{\alpha\in I} \langle\, a_\alpha \,\rangle$.*

*Demostración.* Si $L$ es independiente, entonces para cada $\alpha \in I$ se tiene que $\langle\, a_\alpha \,\rangle \cap \langle\, a_\beta \mid \beta \neq \alpha \,\rangle = 0$. En efecto, si $a \in \langle\, a_\alpha \,\rangle \cap \langle\, a_\beta \mid \beta \neq \alpha \,\rangle$, entonces $a = n_\alpha a_\alpha$ para alguna $n_\alpha \in \mathbb{Z}$. Por otra parte, $a = n_1a_{\beta_1} + \cdots + n_ra_{\beta_r}$, con $\beta_i \neq \alpha$ y $n_i \in \mathbb{Z}$, para cada $i = 1, 2, \ldots, r$. Luego,

$$0 = a - a = n_\alpha a_\alpha - (n_1a_{\beta_1} + \cdots + n_ra_{\beta_r}).$$

Se sigue de la independencia de $L$ que $a = n_\alpha a_\alpha = -n_1a_{\beta_1} = \cdots = -n_rg_{\beta_r} = 0$. Además, es claro que $\langle\, L \,\rangle = \sum_{\alpha\in I} \langle\, a_\alpha \,\rangle$. Por tanto, $\langle\, L \,\rangle = \bigoplus_{\alpha\in I} \langle\, a_\alpha \,\rangle$.

Recíprocamente, si el grupo generado por $L$ es la suma directa de los subgrupos cíclicos generados por los elementos $a_\alpha$, con $\alpha \in I$, entonces, en particular, $0 = n_1a_{\alpha_1} + \cdots + n_ka_{\alpha_k}$, donde, para cada $i = 1, 2, \ldots, k$, $n_i \in \mathbb{Z}$ y los $\alpha_i \in I$ son distintos. Luego, para cada $i = 1, 2, \ldots, k$ se tiene que $-n_ia_{\alpha_i} = \sum_{j\neq i} n_ja_{\alpha_j} \in \langle\, a_{\alpha_i} \,\rangle \cap \langle\, a_{\alpha_j} \mid j \neq i \,\rangle = 0$. Por tanto, $n_1a_{\alpha_1} = \cdots = n_ka_{\alpha_k} = 0$, lo que prueba la independencia de $L$. □

**Observación 3.3** *No es difícil verificar que todo $p-$grupo elemental $A$ es un espacio vectorial sobre $\mathbb{Z}_p$. Más aún, el concepto de independencia de un*

*conjunto dada en la Definición 1.46 coincide con el de independencia lineal en este caso. En efecto, si* $\{ a_1, a_2, \ldots, a_k \}$ *es un conjunto independiente en* $A$ *y existen* $m_1, m_2, \ldots, m_k \in \mathbb{Z}$ *tales que* $m_1 a_1 + m_2 a_2 + \cdots + m_k a_k = 0$, *entonces* $m_1 a_1 = m_2 a_2 = \cdots = m_k a_k = 0$, *lo cual implica que* $p = o(a_i) \big| m_i$ *para toda* $i \in \{1, 2, \ldots, k\}$. *Luego,* $m_i \equiv 0 \, (mod\, p)$; *es decir,* $\overline{m}_i = \bar{0} \in \mathbb{Z}_p$ *para toda* $i \in \{1, 2, \ldots, k\}$, *lo que prueba nuestra afirmación.*

Como consecuencia de la observación anterior tenemos los siguientes corolarios:

**Corolario 3.4** *Todo* $p-$*grupo elemental es suma directa de grupos cíclicos de orden* $p$.

*Demostración.* Sea $A$ un $p-$grupo elemental. Entonces, por la Observación 3.3, $A$ es un $\mathbb{Z}_p-$espacio vectorial y, por tanto, tiene una base $\{ a_\alpha \}_{\alpha \in I}$. Luego, $A = \langle a_\alpha \mid \alpha \in I \rangle$, por ser $\{ a_\alpha \}_{\alpha \in I}$ un conjunto de generadores, y, por el Lema 3.2, $A = \bigoplus_{\alpha \in I} \langle a_\alpha \rangle$, pues toda base es un conjunto independiente. □

**Corolario 3.5** *En un* $p-$*grupo elemental, todo conjunto independiente máximo es una base.*

*Demostración.* Sean $A$ un $p-$grupo elemental y $L = \{ a_\alpha \}_{\alpha \in I}$ un conjunto independiente máximo en $A$. Entonces, nuevamente por la Observación 3.3, $L$ es un conjunto linealmente independiente en el $\mathbb{Z}_p-$espacio vectorial $A$, que es máximo, lo cual significa que $L$ es una base para $A$. Más aún, por la demostración del Corolario 3.4, $A = \langle L \rangle = \bigoplus_{\alpha \in I} \langle a_\alpha \rangle$. □

El corolario anterior, junto con el lema que presentamos a continuación, nos serán de gran utilidad para probar el Teorema de Kulikov.

**Lema 3.6** *Sea* $\{ N_\alpha \}_{\alpha \in I}$ *una familia de subgrupos de un* $p-$*grupo* $A$ *que cumple las siguientes condiciones:*

*1) Para toda* $a \in A \setminus \{0\}$ *y para toda* $\alpha \in I$ *existe* $n_\alpha \in \mathbb{N}$ *tal que si* $a \in N_\alpha$, *entonces* $h_p(a) = n_\alpha$.

*2) Para cada* $\alpha, \beta \in I$, *si* $\alpha \neq \beta$, *entonces* $n_\alpha \neq n_\beta$.

*Entonces, si* $N := \bigcup_{\alpha \in I} N_\alpha$, *se tiene que* $\langle N \rangle = \bigoplus_{\alpha \in I} N_\alpha$.

*Demostración.* Notemos primero que $\{ N_\alpha \}_{\alpha \in I}$ es una familia independiente. Sea $\alpha \in I$ y sea $a \in N_\alpha \cap \sum_{\beta \neq \alpha} N_\beta$, entonces:

$$a = a_1 + a_2 + \cdots + a_r, \tag{3.1}$$

con $a_i \in N_{\beta_i}$, $\beta_i \neq \alpha$ y $a_i \neq 0$ para cada $i \in \{1, 2, \ldots, r\}$. Supongamos que $a \neq 0$. Por hipótesis $h_p(a) = n_\alpha$ para alguna $n_\alpha \in \mathbb{N}$; por tanto, $a = p^{n_\alpha} b$, con $b \in A$. Del mismo modo, $h_p(a_i) = n_{\beta_i}$ para alguna $n_{\beta_i} \in \mathbb{N}$, de donde $a_i = p^{n_{\beta_i}} b_i$, con $b_i \in A$ para toda $i \in \{1, 2, \ldots, r\}$. Luego, sustituyendo en (3.1),

$$p^{n_\alpha} b = p^{n_{\beta_1}} b_1 + \cdots + p^{n_{\beta_r}} b_r. \tag{3.2}$$

Sea $n_0 := \min \{n_{\beta_1}, \ldots, n_{\beta_r}, n_\alpha\}$. Observemos que todos los elementos de $\{ n_{\beta_1}, \ldots, n_{\beta_r}, n_\alpha \}$ son distintos entre sí por la condición *2)* del lema. Tenemos los siguientes casos:

*Caso 1.* Si $n_0 = n_\alpha$, entonces $a = p^{n_0} b = \sum_{i=1}^{r} p^{n_{\beta_i}} b_i = p^m c$, con $c \in A$ y $m > n_0$, donde $m := \min \{ n_{\beta_1}, \ldots, n_{\beta_r} \}$. Por tanto, $h_p(a) > n_\alpha$, una contradicción.

*Caso 2.* Si $n_0 = n_{\beta_{i_0}}$ para algún $i_0 \in \{1, 2, \ldots, r\}$, entonces, de (3.2), $a_{i_0} = p^{n_0} b_{i_0} = \sum_{i \neq i_0} p^{n_{\beta_i}} b_i - p^{n_\alpha} b = p^{m'} c'$, con $c' \in A$ y $m' > n_0$, donde $m' := \min \{ n_{\beta_1}, \ldots, n_{\beta_r}, n_\alpha \} \setminus \{n_0\}$, lo cual implica que $h_p(a_{i_0}) > n_0$; nuevamente una contradicción.

Por lo tanto, $a = 0$; es decir, $N_\alpha \cap \sum_{\beta \neq \alpha} N_\beta = 0$. Por otra parte, claramente, $\langle N \rangle = \sum_{\alpha \in I} N_\alpha$. Se concluye que $\langle N \rangle = \bigoplus_{\alpha \in I} N_\alpha$. □

Ahora estamos en condiciones de probar el teorema central del capítulo.

**Teorema 3.7** *(Kulikov, 1941)*
*Sea $A$ un $p-$ grupo. Son equivalentes:*

*(a) $A$ es suma directa de grupos cíclicos.*

*(b) Existe una cadena ascendente*

$$A_1 \leq A_2 \leq \cdots \leq A_n \leq \ldots$$

*de subgrupos de $A$ que cumple las siguientes condiciones:*

*(i)* $\bigcup_{n=1}^{\infty} A_n = A$.

*(ii) Para todo $n \geq 1$ existe $k_n \geq 1$ tal que para todo $0 \neq a \in A_n$ se tiene que $h_p(a) < k_n$.*

*Demostración.*

$(a) \Rightarrow (b)$. Si $A$ es suma directa de subgrupos cíclicos, es decir, $A = \bigoplus_{\alpha \in I} \langle\, a_\alpha \,\rangle$, con $a_\alpha \in A$ para cada $\alpha \in I$, tomemos por separado a los sumandos directos del mismo orden $p^n$ para cada $n \in \mathbb{N}$, y denotemos por $B_n$ a la correspondiente suma directa. Así, $\forall\, n \geq 1,\ B_n := \bigoplus_{\alpha \in I} \{\, \langle\, a_\alpha \,\rangle \mid o(a_\alpha) = p^n \,\}$.

Para cada $n \geq 1$ definimos: $k_n := n$ y $A_n := B_1 \oplus B_2 \oplus \cdots \oplus B_n$.

Se afirma que $\bigcup_{n=1}^{\infty} A_n = A$. En efecto, si $a \in A = \bigoplus_{\alpha \in I} \langle\, a_\alpha \,\rangle$, entonces $a = a_1 + a_2 + \cdots + a_r$ para alguna $r \geq 1$, con $a_i \in \langle\, a_{\alpha_i} \,\rangle$ para cada $i \in \{1, \ldots, r\}$. Digamos que $o(a_{\alpha_i}) = p^{n_i}$. Así, $a_i \in B_{n_i} \leq A_{n_i}$. Sea $m := \max\{n_i \mid i = 1, 2, \ldots, r\}$, entonces $a_i \in A_m$ para cada $i = 1, 2, \ldots, r$. Luego, $a \in \bigcup_{n=1}^{\infty} A_n$, con lo que se verifica la afirmación.

Además, afirmamos que la $p-$altura de los elementos de $A_n$ distintos de cero es menor que la $k_n$ propuesta. Si $0 \neq a \in A_n$ y $h_p(a) \geq k_n = n$, digamos $h_p(a) = n + l$, con $l \geq 0$, entonces existe $b_0 \in A$ tal que $a = p^{h_p(a)} b_0 =$

$p^n(p^l b_0)$; o bien, haciendo $b := p^l b_0 \in A,\ a = p^n b$. Luego, puesto que $a \neq 0$, $o(b) > p^n$. Ahora, por la condición $(i)$, $b \in A_k$ para algún $k > n$. Como $A_k := B_1 \oplus B_2 \oplus \cdots \oplus B_k$, entonces $b = b_1 + b_2 + \cdots + b_k$, con $b_i \in B_i$, es decir $o(b_i) \leq p^i$ para $i = 1, 2, \ldots, k$. Luego, $p^n b_i = 0\ \forall\, i \leq n$, de donde:

$$a = p^n b = p^n b_1 + p^n b_2 + \cdots + p^n b_k = p^n b_{n+1} + \cdots + p^n b_k.$$

Por otro lado, por hipótesis, $a \in A_n := B_1 \oplus B_2 \oplus \cdots \oplus B_n$, lo cual implica que $a = a_1 + a_2 + \cdots + a_n$, con $a_i \in B_i$ para cada $i = 1, 2, \ldots, n$. Por tanto, $a \in A_n \leq A_k := B_1 \oplus B_2 \oplus \cdots \oplus B_n \oplus \cdots \oplus B_k$ tiene simultáneamente en $A_k$ expresiones de la forma:

$$a = 0 + 0 + \cdots + 0 + p^n b_{n+1} + \cdots + p^n b_k$$

y

$$a = a_1 + a_2 + \cdots + a_n + 0 + \cdots + 0,$$

de donde: $a_1 = a_2 = \cdots = a_n = p^n b_{n+1} = \cdots = p^n b_k = 0$. Se concluye que $a = 0$, en contradicción con nuestra suposición inicial. Por lo tanto, $\forall\, a \in A_n$ $(a \neq 0 \Rightarrow h_p(a) < k_n)$, lo que prueba la implicación.

$(b) \Rightarrow (a)$. Supongamos ahora que los subgrupos $A_n \leq A$ satisfacen las hipótesis $(i)$ y $(ii)$. Como podemos agregar ceros al inicio de la cadena

$$A_1 \leq A_2 \leq \cdots \leq A_n \leq \ldots$$

y también repetir (un número finito de veces) algunos términos $A_n$, no hay pérdida de generalidad al asumir $k_n = n$. El procedimiento anterior se puede justificar de la siguiente manera. Se construye una nueva cadena:

$$A'_1 \leq A'_2 \leq \cdots \leq A'_n \leq \ldots$$

a partir de la cadena original, pero con la peculiaridad de que $k'_n$, la cota superior de las $p-$alturas de los elementos de $A'_n$, sea precisamente $n$. Para ello, definimos primero la sucesión $\{ N_j \}_{j \geq 0}$ de números naturales de manera

recursiva como sigue: $N_0 := 0$ y $N_{j+1} := \text{máx}\{ N_j + 1, k_{j+1} \}$. Observemos que:

$$N_0 < N_1 < \cdots < N_j < N_{j+1} < \ldots$$

Sea $A_0 := 0$. Para $j \geq 0$ y $n \geq 1$ definimos los elementos $A'_n$ de la nueva cadena como:

$$A'_n := \begin{cases} A_j, & \text{si } N_j + 1 \leq n < N_{j+1}; \\ A_{j+1}, & \text{si } n = N_{j+1}. \end{cases}$$

Nótese que la nueva cadena ascendente $A'_1 \leq A'_2 \leq \cdots \leq A'_n \leq \ldots$ sigue satisfaciendo $(i)$, pues, si $a \in A = \bigcup_{j=1}^{\infty} A_j$, entonces $a \in A_j$ para algún $j \geq 1$. Luego, $a \in A'_n = A_j$, con $n = N_j$; es decir, $a \in \bigcup_{n \geq 1} A'_n$. Por tanto, $A = \bigcup_{n=1}^{\infty} A'_n$. Además, la cadena obtenida cumple la propiedad:

$$\forall\, n \geq 1\ \forall\, a \in A'_n\ (\, a \neq 0\ \Rightarrow\ h_p(a) < n.\,) \tag{3.3}$$

En efecto, sean $n \geq 1$ y $a \in A'_n$. Supongamos que $N_j + 1 \leq n \leq N_{j+1}$. Tenemos dos casos:

$$a \in A'_n = A_j, \text{ si } N_j + 1 \leq n < N_{j+1},$$

o bien,

$$a \in A'_n = A_{j+1}, \text{ si } n = N_{j+1}.$$

En el primer caso, $h_p(a) < k_j \leq \text{máx}\{ N_{j-1} + 1, k_j \} = N_j < N_j + 1 \leq n$.
En el segundo caso, $h_p(a) < k_{j+1} \leq \text{máx}\{ N_j + 1, k_{j+1} \} = N_{j+1} = n$.

En resumen, de ambos casos se concluye que $h_p(a) < n$, con lo que se verifica la propiedad (3.3).

Una vez construida la cadena $A'_1 \leq A'_2 \leq \cdots \leq A'_n \leq \ldots$, notemos que $A'_n \cap p^n A = 0$, pues, si $0 \neq a \in A'_n \cap p^n A$, entonces, por un lado, $a = p^n a$ para algún $a \in A$, de donde, $h_p(a) \geq n$. Por otra parte, $h_p(a) < n$, ya que $a \in A'_n$; una contradicción.

Consideremos el conjunto $\mathcal{K}$ de las cadenas ascendentes $C_1 \leq C_2 \leq \cdots \leq C_n \leq \ldots$ de subgrupos $C_n \leq A$ tales que para cada $n \geq 1$ satisfacen las siguientes condiciones:

$$A'_n \leq C_n \tag{3.4}$$

y

$$C_n \cap p^n A = 0 \tag{3.5}$$

Para dicho conjunto de cadenas, las cuales serán denotadas en adelante por $(C_1, C_2, \ldots, C_n, \ldots)$, se define el siguiente orden:
Sean $\mathcal{C}_1 = (C_1, C_2, \ldots, C_n, \ldots)$ y $\mathcal{C}_2 = (B_1, B_2, \ldots, B_n, \ldots)$ cadenas que satisfacen las condiciones (3.4) y (3.5), es decir, $\mathcal{C}_1, \mathcal{C}_2 \in \mathcal{K}$. Decimos que $\mathcal{C}_1 \preceq \mathcal{C}_2 \Leftrightarrow \forall\, n\, (C_n \leq B_n)$.
Se probará que con el orden antes definido $\mathcal{K}$ es un *copo* inductivo.

- " $\preceq$ " *define un orden parcial en* $\mathcal{K}$.

*Reflexividad.* Sea $\mathcal{C}_1 = (C_1^1, C_2^1, \ldots, C_n^1, \ldots) \in \mathcal{K}$. Claramente, $\forall\, n\, (C_n^1 \leq C_n^1)$; es decir, $\mathcal{C}_1 \preceq \mathcal{C}_1$.

*Antisimetría.* Sean $\mathcal{C}_1 = (C_1^1, C_2^1, \ldots, C_n^1, \ldots)$, $\mathcal{C}_2 = (C_1^2, C_2^2, \ldots, C_n^2, \ldots) \in \mathcal{K}$ tales que $\mathcal{C}_1 \preceq \mathcal{C}_2$ y $\mathcal{C}_2 \preceq \mathcal{C}_1$, esto es, $\forall\, n\, (C_n^1 \leq C_n^2)$ y $\forall\, n\, (C_n^2 \leq C_n^1)$. Entonces $\forall\, n\, (C_n^1 = C_n^2)$; es decir, $\mathcal{C}_1 = \mathcal{C}_2$.

*Transitividad.* Sean $\mathcal{C}_1 = (C_1^1, C_2^1, \ldots, C_n^1, \ldots)$, $\mathcal{C}_2 = (C_1^2, C_2^2, \ldots, C_n^2, \ldots)$, $\mathcal{C}_3 = (C_1^3, C_2^3, \ldots, C_n^3, \ldots) \in \mathcal{K}$ tales que $\mathcal{C}_1 \preceq \mathcal{C}_2$ y $\mathcal{C}_2 \preceq \mathcal{C}_3$, es decir, $\forall\, n\, (C_n^1 \leq C_n^2)$ y $\forall\, n\, (C_n^2 \leq C_n^3)$. Luego, $\forall\, n\, (C_n^1 \leq C_n^3)$, de donde $\mathcal{C}_1 \preceq \mathcal{C}_3$.

Además, se tiene que:

- $\mathcal{K}$ *es no vacío.* En efecto, pues $(A'_1, A'_2, \ldots, A'_n, \ldots) \in \mathcal{K}$.

- $\mathcal{K}$ *es inductivo.* Sea $\mathsf{C} := \{\, \mathcal{C}^\alpha \,\}_{\alpha \in I} \subseteq \mathcal{K}$, una cadena (de cadenas) en $\mathcal{K}$, donde, para cada $\alpha \in I$, $\mathcal{C}^\alpha = (C_1^\alpha, C_2^\alpha, \ldots, C_n^\alpha, \ldots)$, y sea $\mathcal{C}'$ la cadena

$(C'_1, C'_2, \ldots, C'_n, \ldots)$ tal que:

$$C'_1 := \bigcup_{\alpha\in I} C_1^\alpha,$$
$$C'_2 := \bigcup_{\alpha\in I} C_2^\alpha,$$
$$\ldots$$
$$C'_n := \bigcup_{\alpha\in I} C_n^\alpha,$$
$$\ldots$$

Entonces $\mathcal{C}'$ es una cota superior de $\mathsf{C}$ y $\mathcal{C}' \in \mathcal{K}$. En efecto, como $C_i^\alpha \leq C_{i+1}^\alpha \leq A$ para cada $\alpha \in I$ y para cada $i \geq 1$, se tiene que:

$$\bigcup_{\alpha\in I} C_i^\alpha \leq \bigcup_{\alpha\in I} C_{i+1}^\alpha,\ \forall\, \alpha \in I,\ i \geq 1.$$

Luego, $C'_1 \leq C'_2 \leq \cdots \leq C'_n \leq \cdots \leq A$. Por otro lado, $A'_n \leq C_n^\alpha \leq \bigcup\limits_{\alpha\in I} C_n^\alpha = C'_n$ y $C'_n \cap p^n A = \left(\bigcup\limits_{\alpha\in I} C_n^\alpha\right) \cap p^n A = \bigcup\limits_{\alpha\in I} (C_n^\alpha \cap p^n A) = 0$; es decir, $\mathcal{C}'$ satisface las condiciones (3.4) y (3.5).

Por el Lema de Zorn existe (al menos) una cadena $(G_1, G_2, \ldots, G_n, \ldots)$ que es máxima en $\mathcal{K}$, esto es, una cadena máxima que satisface (3.4) y (3.5). Dicha cadena satisface además que $\bigcup\limits_{n\geq 1} G_n = A$ ya que, por la condición (3.4), $\forall\, n \geq 1$, $A'_n \leq G_n$. Luego:

$$A \leq \bigcup_{n=1}^{\infty} A'_n \leq \bigcup_{n=1}^{\infty} G_n \leq A.$$

Ahora, para cada $n \geq 1$ tomemos un conjunto independiente máximo, $L_n$, de elementos en el subgrupo $G_n[p] \cap p^{n-1}A$, lo cual siempre es posible por la Observación 1.49. Sea $L := \bigcup\limits_{n\geq 1} L_n$. Enseguida, para cada $c_i \in L$ con $m_i := h_p(c_i)$, elegimos un $a_i \in A$ tal que $p^{m_i} a_i = c_i$.

Se afirma que $A = \bigoplus \langle\, a_i \,\rangle$.

La prueba de la última afirmación se divide en dos etapas:

*Se demostrará que* $\langle L \rangle = A[p]$.

Por el Corolario 3.5 se tiene que, $\forall\, n \geq 1$, $\langle L_n \rangle = G_n[p] \cap p^{n-1}A$.

Afirmamos que los elementos distintos de cero de $\langle L_n \rangle$ son todos de $p-$altura $n-1$. Así es, si $0 \neq x \in \langle L_n \rangle$, entonces $x \in G_n[p] \cap p^{n-1}A$; es decir, $x = p^{n-1}a$ para algún $a \in A$, ya que $x \in p^{n-1}A$. Además, si $x = p^n b$, con $b \in A$, entonces, por la condición (3.5), $x \in p^n A \cap G_n = 0$, lo cual es una contradicción. Luego, $k := n-1$ es el mayor entero no negativo para el cual se satisface la ecuación $x = p^k a$ para algún $a \in A$, es decir, $h_p(x) = n-1$.

Por tanto, del Lema 3.6 se sigue que $\bigoplus \langle L_n \rangle = \langle L \rangle$.

Observemos además que, como $A = \bigcup_{r\geq 1} G_r$, $A[p] = \bigcup_{r=1}^{\infty} G_r[p]$.

Luego, se tiene que $\langle L \rangle \leq A[p]$. Lo anterior se sigue del hecho de que, para cada $n \geq 1$, $\langle L_n \rangle \leq G_n[p] \leq A[p]$. Por tanto, $\langle L \rangle = \bigoplus \langle L_n \rangle \leq A[p]$.

A continuación probaremos por inducción sobre $r$ que $G_r[p] \leq \langle L \rangle$.

Si $a \in G_1[p]$, entonces $pa = 0$. Además, claramente $a \in p^0 A = A$. Por tanto, $a \in G_1[p] \cap p^0 A = \langle L_1 \rangle \leq \bigoplus \langle L_n \rangle = \langle L \rangle$. Supongamos que $G_r[p] \leq \langle L \rangle$. Sea $b \in G_{r+1}[p] \setminus G_r$. Entonces, como $b \notin G_r$, se tiene $\langle G_r, b \rangle \cap p^r A \neq 0$. De no ser así, contradecimos la maximalidad de la cadena $(G_1, G_2, \ldots, G_n, \ldots)$ que cumple las condiciones (3.4) y (3.5).

Sea:

$$0 \neq g' + kb =: c' \in p^r A,$$

donde $g' \in G_r$ y $k \in \mathbb{Z}$. Si tuviéramos que $p \mid k$, entonces, como $b \in G_{r+1}[p]$, $kb = 0$. Luego,

$$0 \neq c' = g' \in p^r A \cap G_r = 0,$$

una contradicción. Por tanto, $p \nmid k$ y existe $k' \in \mathbb{Z}$ tal que $kk' \equiv 1 (mod\, p)$. Se sigue que, para algún $l \in \mathbb{Z}$,

$$k'c' = k'g' + kk'b = k'g' + (b + plb) = k'g' + b,$$

es decir, $c = g + b$, donde $c := k'c' \in p^r A$, $g := k'g' \in G_r$.

Además, $c \neq 0$ (de otro modo, $b \in G_r$, una contradicción).

Notemos que $c \in G_{r+1}$ (pues $b \in G_{r+1}$ y $g \in G_r \leq G_{r+1}$). Por otro lado, $c \in p^r A$, de donde $h_p(c) \geq r$. Luego, por (3.5), $pc \in G_{r+1} \cap p^{r+1}A = 0$. Por lo tanto, $o(c) = p$ y $h_p(c) = r$ ($c \in p^{r+1}A$ implica $c = 0$, pues $G_{r+1} \cap p^{r+1}A = 0$). Se sigue que $c \in G_{r+1}[p] \cap p^r A = \langle L_{r+1} \rangle \leq \langle L \rangle$. Más aún, $pg = pc - pb = 0$, de donde $g \in G_r[p]$. Lo anterior, junto con la hipótesis de inducción, implica que $g \in \langle L \rangle$. Por tanto, $b = c - g \in \langle L \rangle$.

Se ha demostrado que, para $r \geq 1$, $G_r[p] \leq \langle L \rangle$. Luego, de la observación previa a la demostración anterior se sigue que $A[p] \leq \langle L \rangle$. Concluimos que $\langle L \rangle = A[p]$, que es lo que queríamos probar.

*Se demostrará que* $A = \bigoplus \langle a_i \rangle$.

Dado $a \in A$, se tiene que $o(a) = p^r$ para algún $r \geq 0$, ya que $A$ es un $p-$grupo. Para probar la última afirmación usaremos el segundo principio de inducción sobre $r$. Supongamos que todo $a \in A$ de orden $p^r$, con $r \leq n$, pertenece a $\bigoplus \langle a_i \rangle$. Ahora, sea $b \in A$ de orden $p^{n+1}$, con $n \geq 1$. Entonces $p^n b \in A[p] = \langle L \rangle$. Luego:

$$p^n b = m_1 c_1 + m_2 c_2 + \cdots + m_k c_k$$

para algunas $m_i \in \mathbb{Z}$, $c_i \in L = \bigcup_{m \geq 1} L_m$, y, por tanto, para cada $i \in \{1, 2, \ldots, k\}$ existe $n_i \geq 1$ tal que $c_i \in L_{n_i}$, de donde $h_p(c_i) = n_i - 1$.

Podemos suponer que:

$$\begin{cases} n_i - 1 \geq n, & \text{para } 1 \leq i \leq j; \\ n_i - 1 < n, & \text{para } j+1 \leq i \leq k. \end{cases}$$

Si escribimos $m_i c_i = p^n m_i' a_i$, con $m_i' \in A$, para cada $i = 1, 2, \ldots, j$, entonces $p^n(b - m_1' a_1 - m_2' a_2 - \cdots - m' a_j) = m_{j+1} c_{j+1} + m_{j+2} c_{j+2} + \cdots + m_{j+k} c_{j+k} \in G_n$, pues para $j+1 \leq i \leq k$ se tiene que $m_i c_i \in \langle L_{n_i} \rangle \leq G_{n_i} \leq G_n$.

Por tanto, la condición (3.5) implica que $b - m_1' a_1 - m_2' a_2 - \cdots - m_j' a_j$ es de orden a lo más $p^n$. Lo anterior es cierto, pues $p^n(b - m_1' a_1 - m_2' a_2 - \cdots -$

$m'_j a_j) \in p^n A$ y $G_n \cap p^n A = 0$. Luego, de la hipótesis de inducción se sigue que $b - m'_1 a_1 - m'_2 a_2 - \cdots - m'_j a_j \in \bigoplus \langle\, a_i \,\rangle$; es decir, $b \in \bigoplus \langle\, a_i \,\rangle$.

Se concluye que $A = \bigoplus \langle\, a_i \,\rangle$. □

**Corolario 3.8** *Sea $A$ un $p-$grupo acotado. Entonces $A$ es una suma directa de grupos cícilicos.*

*Demostración.* Si consideramos la cadena:

$$A \leq A \leq \cdots \leq A \leq \ldots,$$

ésta claramente satisface la propiedad $(b.i)$ del Teorema de Kulikov. Además, por ser $A$ acotado, existe $n \geq 1$ tal que $nA = 0$. Luego, $\forall\, a \in A\,(a \neq 0 \Rightarrow h_p(a) < n)$, es decir, la última cadena también satisface la condición $(b.ii)$ del mismo teorema. Por tanto, se sigue que $A$ es suma directa de subgrupos cíclicos. □

De hecho, por el Teorema 3.1, el corolario anterior puede ser enunciado de manera más general:

**Corolario 3.9** *(Prüfer, Baer)*
*Un grupo acotado es suma directa de grupos cíclicos.*

*Demostración.* Si $A$ es un grupo acotado, entonces sus $p-$componentes, $A_p$, también lo son. Consideremos la cadena:

$$A_p \leq A_p \leq \cdots \leq A_p \leq \ldots$$

Se sigue del Teorema de Kulikov que las $p-$componentes de $A$ son suma directa de subgrupos cíclicos, de donde, en virtud de la Observación 1.42 y del Teorema 3.1, $A$ es suma directa de sus $p-$componentes y, por tanto, $A$ es suma directa de subgrupos cíclicos. □

# Capítulo 4

# Tres retículas isomorfas

En este capítulo se presentan, para cada $n \geq 1$, tres retículas que resultan ser isomorfas: la retícula $L_n$, que se construye de manera recursiva, la retícula de caminos $1-$ascendentes, que llamaremos $C_n$, y, finalmente, el conjunto $B_n := \{0,1\}^n$ o de sucesiones binarias de longitud $n$, el cual, al ser dotado de un cierto orden, resulta ser una retícula distributiva, finita, de cardinalidad $2^n$, autodual y graduada. Dichas retículas, en especial la de sucesiones binarias, nos ofrecen una útil forma de representar y describir a $\mathbb{Z}_{p^n} - pr$, así como de conocer sus propiedades reticulares, ya que, como se verá en el siguiente capítulo, $\mathbb{Z}_{p^n} - pr$ y $B_n$ son isomorfas como retículas. Una advertencia respecto a la notación: denotaremos con frecuencia en lo subsecuente a una retícula $\langle L, \leq, \vee, \wedge \rangle$ simplemente por su conjunto subyacente, $L$ (siempre que no se preste a confusión).

## 4.1. Las retículas $L_n$

**Definición 4.1** *Para $n \in \mathbb{N}$ definimos recursivamente a los conjuntos $L_n$ como sigue: sea $L_0$ un conjunto con un sólo elemento, digamos, $L_0 = \{*\}$. Para cada $n \geq 1$ y suponiendo definido el conjunto $L_{n-1}$, sea $L_n := L_{n-1} \times \{0,1\}$.*

Por simplicidad, a lo largo de este capítulo y para cada $n \geq 1$, se usará el subíndice 1 en ambos elementos de una pareja ordenada en $L_n$ y para cada $n \geq 2$, se empleará el subíndice 2 en ambos elementos de una pareja ordenada en $L_{n-1}$. Así, por ejemplo, denotaremos por $(x_1, \delta_1)$ a un elemento de $L_n$ y por $(x_2, \delta_2)$ a un elemento típico de $L_{n-1}$.

**Observación 4.2** *Para cada $n \in \mathbb{N}$, $L_n$ es un conjunto finito de cardinalidad $2^n$.*

**Definición 4.3** *Sea $n \geq 1$. Definimos al hemisferio sur de $L_n$ como el conjunto:*

$$H_n^0 := \{\, x \in L_n \mid x = (x_1, 0),\, x_1 \in L_{n-1} \,\},$$

*y al hemisferio norte de $L_n$ como el conjunto:*

$$H_n^1 := \{\, x \in L_n \mid x = (x_1, 1),\, x_1 \in L_{n-1} \,\}.$$

**Definición 4.4** *Sea $n \geq 2$. Un puente de $z$ a $w$ en $L_n$ es una pareja $(z, w) \in L_n \times L_n$, tal que:*

$$z = (z_1, 0), \quad w = (w_1, 1), \quad z_1 = (z_2, 1), \quad w_1 = (w_2, 0)$$

*con $z_2 = w_2 \in L_{n-2}$.*

Nótese que para $n \geq 2$ existe una correspondencia biunívoca entre los puentes en $L_n$ y los elementos de $L_{n-2}$, de manera que se tiene la siguiente propiedad.

**Observación 4.5** *Para cada $n \geq 2$ existen $2^{n-2}$ puentes en $L_n$.*

**Definición 4.6** *Para cada $n \in \mathbb{N}$ definimos un orden para los conjuntos $L_n$ de la siguiente forma:*

$$\underset{0}{\leq} = \{\, (*, *) \,\},$$

$$\underset{1}{\leq} = \{\, ((*, 0), (*, 0)), ((*, 0), (*, 1)), ((*, 1), (*, 1)) \,\}.$$

*Ahora, sea* $n \geq 2$ *y sean* $x = (x_1, \delta_1)$, $y = (y_1, \varepsilon_1) \in L_n$ *tales que* $x_1 = (x_2, \delta_2)$, $y_1 = (y_2, \varepsilon_2) \in L_{n-1}$. *Decimos que* $x \underset{n}{\leq} y$ *si se cumple alguno de los siguientes casos:*

*1)* $\delta_1 = \varepsilon_1$ *(es decir,* $x, y$ *están en el mismo hemisferio) y* $x_1 \underset{n-1}{\leq} y_1$, *o bien,*

*2)* $\delta_1 = 0$, $\varepsilon_1 = 1$ *y existe un puente* $(z, w)$ *en* $L_n$, *tal que* $z = (z_1, 0)$, $w = (w_1, 1) \in L_n$, $x_1 \underset{n-1}{\leq} z_1$ *y* $w_1 \underset{n-1}{\leq} y_1$.

**Observación 4.7** *Sea* $n \geq 2$. *Si* $(z, w)$ *es un puente en* $L_n$, *entonces* $z \underset{n}{<} w$.

**Lema 4.8** *Sea* $n \geq 1$. *Si* $x, y, z \in L_n$ *y* $x \underset{n}{\leq} y \underset{n}{\leq} z$ *con* $x, z$ *en el mismo hemisferio* $H$, *entonces* $y \in H$.

*Demostración.* Sean $x = (x_1, \delta_1), y = (y_1, \varepsilon_1), z = (z_1, \varphi_1) \in L_n$. Como $x, z$ están en el mismo hemisferio, se tiene que $\delta_1 = \varphi_1$. Supongamos que $\varepsilon_1 \neq \delta_1, \varphi_1$, entonces, puesto que $x \underset{n}{\leq} y$ y $\delta_1 \neq \varepsilon_1$, debe ocurrir que $\delta_1 = 0$ y $\varepsilon_1 = 1$. Asimismo, ya que $y \underset{n}{\leq} z$ y $\varepsilon_1 \neq \varphi_1$, se sigue que $\varepsilon_1 = 0$, $\varphi_1 = 1$. Luego, $0 = \varepsilon_1 = 1$, una contradicción. Por lo tanto $\varepsilon_1 = \delta_1 = \varphi_1$, es decir, $y \in H$, que es lo que queríamos probar. □

**Observación 4.9** *Sea* $n \geq 1$. *Si* $x = (x_1, \delta_1)$, $y = (y_1, \varepsilon_1)$ *son elementos en el mismo hemisferio de* $L_n$, *entonces* $y$ *cubre a* $x$ *en* $L_n$ *si y sólo si* $y_1$ *cubre a* $x_1$ *en* $L_{n-1}$.

**Teorema 4.10** *Para* $n \in \mathbb{N}$, $\left\langle L_n, \underset{n}{\leq} \right\rangle$ *es un copo con elementos menor y mayor.*

*Demostración (por inducción sobre n).* Resulta inmediato que para $n = 0$ se cumple la afirmación. Supongamos que $\left\langle L_{n-1}, \underset{n-1}{\leq} \right\rangle$ es un *copo* con elementos menor y mayor $\widehat{0}_{n-1}$ y $\widehat{1}_{n-1}$, respectivamente.

• *Reflexividad.* Sea $x = (x_1, \delta_1) \in L_n$. Por hipótesis de inducción tenemos que $x_1 \underset{n-1}{\leq} x_1$, luego, por definición, $x \underset{n}{\leq} x$.

• *Antisimetría.* Sean $x = (x_1, \delta_1),\ y = (y_1, \varepsilon_1) \in L_n$ tales que $x \underset{n}{\leq} y$ y $y \underset{n}{\leq} x$. Por el Lema 4.8 $x, y$ están en el mismo hemisferio, esto es, $\delta_1 = \varepsilon_1$. Luego, por definición se tiene que $x_1 \underset{n-1}{\leq} y_1$ y $y_1 \underset{n-1}{\leq} x_1$. Por la hipótesis de inducción se concluye que $x_1 = y_1$, de donde $x = y$.

• *Transitividad.* Sean $x = (x_1, \delta_1),\ y = (y_1, \varepsilon_1),\ z = (z_1, \varphi_1) \in L_n$, tales que $x \underset{n}{\leq} y$ y $y \underset{n}{\leq} z$. Se tienen los siguientes casos:

*Caso 1:* $\delta_1 = \varphi_1$ ($x, z$ están en el mismo hemisferio). Luego, por el Lema 4.8, $y$ está en el mismo hemisferio que $x, z$, es decir, $\delta_1 = \varepsilon_1 = \varphi_1$. Luego, por definición, $x_1 \underset{n-1}{\leq} y_1$ y $y_1 \underset{n-1}{\leq} z_1$. Finalmente, por hipótesis de inducción tenemos que $x_1 \underset{n-1}{\leq} z_1$, de donde $x \underset{n}{\leq} z$.

*Caso 2:* $\delta_1 \neq \varphi_1$. Tenemos a su vez los siguientes subcasos:

*Subcaso 2.1:* $\delta_1 = \varepsilon_1 = 0$ y $\varphi_1 = 1$. Entonces, por la Definición 4.6, por un lado $x_1 \underset{n-1}{\leq} y_1$. Por otro lado, como $\varepsilon_1 \neq \varphi_1$ y $y \underset{n}{\leq} z$, existe un puente $(u, w)$ en $L_n$, tal que $u = (u_1, 0),\ w = (w_1, 1),\ y_1 \underset{n-1}{\leq} u_1$ y $w_1 \underset{n-1}{\leq} z_1$. Por tanto, $x_1 \underset{n-1}{\leq} y_1 \underset{n-1}{\leq} u_1$, de donde, por la hipótesis de inducción, $x_1 \underset{n-1}{\leq} u_1$. Luego, como consecuencia del caso *2*) de la Definición 4.6, se tiene que $x \underset{n}{\leq} z$.

*Subcaso 2.2:* $\delta_1 \neq \varepsilon_1$, por tanto, $\varepsilon_1 = \varphi_1$ ($y, z$ están en el mismo hemisferio). Luego, como $x \underset{n}{\leq} y$ y $y \underset{n}{\leq} z$, se tiene que $\delta_1 = 0$ y $\varepsilon_1 = \varphi_1 = 1$, de donde $y_1 \underset{n-1}{\leq} z_1$. Por otro lado, puesto que $\delta_1 \neq \varepsilon_1$ y $x \underset{n}{\leq} y$, existe un puente $(u, w)$ en $L_n$, con: $u = (u_1, 0), w = (w_1, 1),\ x_1 \underset{n-1}{\leq} u_1$ y $w_1 \underset{n-1}{\leq} y_1$. Por tanto, $w_1 \underset{n-1}{\leq} y_1 \underset{n-1}{\leq} z_1$ y, por la hipótesis de inducción, $w_1 \underset{n-1}{\leq} z_1$. Entonces, nuevamente por el caso *2*) de la Definición 4.6, se tiene que $x \underset{n}{\leq} z$.

Hemos probado que, para $n \geq 0$, $\left\langle L_n, \underset{n}{\leq} \right\rangle$ es un *copo*.

• *Elementos menor y mayor.* Supongamos que $\widehat{0}_{n-1}$ y $\widehat{1}_{n-1}$ son los elementos menor y mayor, respectivamente, de $L_{n-1}$. Definimos $\widehat{0}_n := (\widehat{0}_{n-1}, 0)$ y $\widehat{1}_n := (\widehat{1}_{n-1}, 1)$. Sea $x = (x_1, \delta_1) \in L_n$. Analizamos los siguientes casos:

*Caso 1:* $\delta_1 = 0$. Entonces, por hipótesis de inducción se tiene que $\widehat{0}_{n-1} \underset{n-1}{\leq} x_1$. Luego, $\widehat{0}_n \underset{n}{\leq} x$. Por otro lado, $((\widehat{1}_{n-2}, 1), 0)$, $((\widehat{1}_{n-2}, 0), 1)$ es un puente en $L_n$ tal que:

$$x_1 \underset{n-1}{\leq} \widehat{1}_{n-1} = (\widehat{1}_{n-2}, 1) \text{ y } (\widehat{1}_{n-2}, 0) \underset{n-1}{\leq} \widehat{1}_{n-1}.$$

Por tanto, por el caso *2)* de la Definición 4.6 se sigue que $x \underset{n}{\leq} \widehat{1}_n$.

*Caso 2:* $\delta_1 = 1$. En este caso, por hipótesis de inducción, $x_1 \underset{n-1}{\leq} \widehat{1}_{n-1}$. Por tanto, $x \underset{n}{\leq} \widehat{1}_n$. Por su parte, $((\widehat{0}_{n-2}, 1), 0)$, $((\widehat{0}_{n-2}, 0), 1)$ es un puente en $L_n$ tal que:

$$(\widehat{0}_{n-2}, 0) = \widehat{0}_{n-1} \underset{n-1}{\leq} x_1 \text{ y } \widehat{0}_{n-1} \underset{n-1}{\leq} (\widehat{0}_{n-2}, 1).$$

Nuevamente, del caso *2)* de la Definición 4.6, se tiene que $\widehat{0}_n \underset{n}{\leq} x$.

De lo anterior, se concluye que $\left\langle L_n, \underset{n}{\leq} \right\rangle$ es un copo con elemento menor $\widehat{0}_n$ y elemento mayor $\widehat{1}_n$, con lo que finaliza la prueba. □

Presentamos a continuación algunas propiedades útiles de los puentes.

**Lema 4.11** *Sean $(x, y)$ y $(z, w)$ puentes en $L_n$. Entonces $x \underset{n}{\leq} z$ si y sólo si $y \underset{n}{\leq} w$.*

*Demostración.* Sean $(x, y)$ y $(z, w)$ puentes en $L_n$ tales que:

$$x = (x_1, 0), \quad y = (y_1, 1), \quad z = (z_1, 0), \quad w = (w_1, 1),$$
$$x_1 = (x_2, 1), \quad y_1 = (y_2, 0), \quad z_1 = (z_2, 1), \quad w_1 = (w_2, 0).$$

Si $x \underset{n}{\leq} z$, entonces por la Definición 4.6 se tiene que $x_1 \underset{n-1}{\leq} z_1$ y que $x_2 \underset{n-2}{\leq} z_2$. Tenemos también que $x_2 = y_2$ y $z_2 = w_2$, de manera que $y_2 \underset{n-2}{\leq} w_2$ y, por tanto, $y_1 \underset{n-1}{\leq} w_1$. Se concluye que $y \underset{n}{\leq} w$. La recíproca es similar. □

**Corolario 4.12** *Sean $x, y, x', y' \in L_n$ tales que $(x, y)$ es un puente. Entonces se cumplen las siguientes propiedades:*

*1) Si $(x, y')$ es un puente, entonces $y = y'$.*

*2) Si* $(x', y)$ *es un puente, entonces* $x = x'$. □

**Corolario 4.13** *Sean* $(x, y)$ *y* $(z, w)$ *puentes en* $L_n$. *Entonces* $z$ *cubre a* $x$ *si y sólo si* $w$ *cubre a* $y$.

*Demostración (por inducción sobre n).* Para $n = 2$ la afirmación es clara. Sean $(x, y)$ y $(z, w)$ puentes tales como en la demostración del Lema 4.11. Si $z$ cubre a $x$, entonces $x \underset{n}{<} z$. Luego, por el Lema 4.11 se sigue que $y \underset{n}{\leq} w$ y, por el Corolario 4.12, debe ocurrir que $y \neq w$. Supongamos ahora que existe $u \in L_n$ tal que $y \underset{n}{\leq} u \underset{n}{\leq} w$. Como $y, w \in H_n^1$, por la Observación 4.8 se tiene que $u \in H_n^1$, de tal forma que $y_1 \underset{n-1}{\leq} u_1 \underset{n-1}{\leq} w_1$. Entonces, por la hipótesis de inducción se sigue que $u_1 = y_1$ ó $u_1 = w_1$, lo cual a su vez implica que $u = y$ ó $u = w$. Se concluye que $w$ cubre a $y$. La recíproca es similar. □

**Lema 4.14** *Sea* $n \geq 1$ *y sean* $u, v \in L_n$. *Las siguientes condiciones son equivalentes:*

*(a)* $u$ *y* $v$ *están en diferentes hemisferios y* $v$ *cubre a* $u$.

*(b)* $(u, v)$ *es un puente en* $L_n$.

*Demostración.* Supongamos que $u = (u_1, \delta_1)$, $v = (v_1, \varepsilon_1) \in L_n$ y $u_1 = (u_2, \delta_2)$, $v_1 = (v_2, \varepsilon_2) \in L_{n-1}$.

$(a) \Rightarrow (b)$. Como $v$ cubre a $u$, $u \underset{n}{<} v$, por tanto tenemos que $\delta_1 = 0$, $\varepsilon_1 = 1$ y existe un puente $(z, w)$ en $L_n$, tal que:

$$z = (z_1, 0), \quad w = (w_1, 1), \quad z_1 = (z_2, 1) \quad w_1 = (w_2, 0)$$

con $u_1 \underset{n-1}{\leq} z_1$ y $w_1 \underset{n-1}{\leq} v_1$. Luego, $u \underset{n}{\leq} z \underset{n}{<} w \underset{n}{\leq} v$. Más aún, como $v$ cubre a $u$, debe suceder que $u = z$ y $w = v$, es decir, $(u, v)$ es un puente en $L_n$.

$(b) \Rightarrow (a)$. Si $(u, v)$ es un puente en $L_n$, entonces, por la Observación 4.7, $u \underset{n}{<} v$, estando ambos en diferentes hemisferios. Supongamos que existe $z \in L_n$

tal que $u \underset{n}{\leq} z \underset{n}{\leq} v$, con $z = (z_1, \varphi_1) \in L_n$ y $z_1 = (z_2, \varphi_2) \in L_{n-1}$. Si $z \in H_n^0$, entonces debe existir un puente $(z', v')$ en $L_n$ tal que $z \underset{n}{\leq} z'$ y $v' \underset{n}{\leq} v$. Luego, por el Lema 4.11, $z' \underset{n}{\leq} u$, de donde, por transitividad se sigue que $u = z' = z$. Si $z \in H_n^1$ se concluye de manera similar que $z = v$. Por tanto, $v$ cubre a $u$, lo que concluye la demostración. □

Necesitamos el siguiente lema para describir al supremo e ínfimo en $L_n$.

**Lema 4.15** *Sean $n \geq 2$ y $x, y \in L_n$ tales que $x \in H_n^0$, $y \in H_n^1$. Entonces los conjuntos:*

$$P_n^x := \left\{ z \in H_n^0 \;\middle|\; \textit{para algún } w \in H_n^1,\ \textit{(z,w) es un puente en } L_n \textit{ y } x \underset{n}{\leq} z \right\}$$

*y*

$$Q_n^y := \left\{ w \in H_n^1 \;\middle|\; \textit{para algún } z \in H_n^0,\ \textit{(z,w) es un puente en } L_n \textit{ y } w \underset{n}{\leq} y \right\}$$

*tienen elemento menor y mayor, respectivamente.*

*Demostración (por inducción sobre n).* Primero notemos que, para toda $x \in H_n^0$, $y \in H_n^1$, $P_n^x$ and $Q_n^y$ son conjuntos no vacíos, pues, por una parte, $(((\widehat{1}_{n-2}, 1), 0), ((\widehat{1}_{n-2}, 0), 1))$ es un puente en $L_n$ tal que $x \underset{n}{\leq} (\widehat{1}_{n-2}, 1), 0)$, de manera que $((\widehat{1}_{n-2}, 1), 0) \in P_n^x$. Similarmente, $(((\widehat{0}_{n-2}, 1), 0), ((\widehat{0}_{n-2}, 0), 1))$ es un puente en $L_n$ tal que $((\widehat{0}_{n-2}, 0), 1)) \underset{n}{\leq} y$, de tal forma que $((\widehat{0}_{n-2}, 0), 1) \in Q_n^y$.

Se verifica de manera inmediata que, para toda $x \in H_2^0$ y $y \in H_2^1$, $P_2^x$ y $Q_2^y$ tienen elemento menor y mayor, respectivamente. Ahora supongamos cierta la afirmación para $n-1$. Sea $x = (x_1, 0) \in H_n^0$. Si $x_1 = (x_2, 1) \in H_{n-1}^1$, entonces $(((x_2, 1), 0), (x_2, 0), 1)$ es un puente en $L_n$ tal que $x \in P_n^x$ es elemento menor. De lo contrario, si $x_1 = (x_2, 0) \in H_{n-1}^0$, entonces por la hipótesis de inducción $P_{n-1}^{x_1}$ tiene un elemento menor $z_1' \in L_{n-1}$ tal que $(z_1', w_1')$ es un

puente para algún $w_1' \in L_{n-1}$. Afirmamos que $(w_1', 0)$ es el elemento menor de $P_n^x$. En efecto, sea $z = (z_1, 0) \in P_n^x$, entonces existe un puente $(z, w)$ en $L_n$ tal que $x \underset{n}{\leq} z$, de donde $x_1 \underset{n-1}{\leq} z_1$, lo cual, por la Definición 4.6 a su vez implica que existe un puente $(u_1, v_1) \in L_{n-1}$ tal que $x_1 \underset{n-1}{\leq} u_1$ y $v_1 \underset{n-1}{\leq} z_1$. Se sigue que $u_1 \in P_{n-1}^{x_1}$, luego $z_1' \underset{n-1}{\leq} u_1$. Entonces, por el Lema 4.11 se tiene que $w_1' \underset{n-1}{\leq} v_1 \underset{n-1}{\leq} z_1$. Por tanto, $(w_1', 0) \underset{n}{\leq} (z_1, 0) = z$, con lo que terminamos.

Dualmente se prueba que $Q_n^y$ tiene elemento mayor. □

**Teorema 4.16** *Para cada $n \in \mathbb{N}$, $\left\langle L_n, \underset{n}{\leq} \right\rangle$ es una retícula.*

*Demostración (por inducción sobre n).* Para $n = 0$ la afirmación es clara. Supongamos ahora que $n \geq 1$ y $\left\langle L_{n-1}, \underset{n-1}{\leq}, \underset{n-1}{\vee}, \underset{n-1}{\wedge} \right\rangle$ es una retícula. Sean $x = (x_1, \delta_1),\ y = (y_1, \varepsilon_1) \in L_n$. Tenemos los siguientes casos:

*Caso 1: $x, y$ están en el mismo hemisferio.* Entonces $\delta_1 = \varepsilon_1$ y se definen $x \overset{1}{\underset{n}{\vee}} y := (x_1 \underset{n-1}{\vee} y_1, \delta_1)$ y $x \overset{1}{\underset{n}{\wedge}} y := (x_1 \underset{n-1}{\wedge} y_1, \delta_1)$. Se verifica de inmediato que estos elementos satisfacen las propiedades de supremo e ínfimo, respectivamente, en $L_n$, de manera que en este caso, $x \underset{n}{\vee} y = x \overset{1}{\underset{n}{\vee}} y$ y $x \underset{n}{\wedge} y = x \overset{1}{\underset{n}{\wedge}} y$.

*Caso 2: $x, y$ no están en el mismo hemisferio.* Sin pérdida de generalidad, podemos suponer que $x \in H_n^0$ y $y \in H_n^1$. Luego, por el Lema 4.15, $P_n^x$ tiene un elemento menor, $z_x$, tal que para algún $w_x \in H_n^1$ se tiene que $(z_x, w_x)$ es un puente en $L_n$ y $x \underset{n}{\leq} z_x$. Afirmamos que $x \underset{n}{\vee} y = w_x \overset{1}{\underset{n}{\vee}} y$. En efecto, por el *Caso 1* tenemos que $y \underset{n}{\leq} w_x \overset{1}{\underset{n}{\vee}} y$ y $w_x \leq w_x \overset{1}{\underset{n}{\vee}} y$. Por lo tanto, por la Definición 4.6 y usando el puente $(z_x, w_x)$, se tiene que $x \underset{n}{\leq} w_x \overset{1}{\underset{n}{\vee}} y$. Ahora, sea $c \in L_n$ tal que $x, y \underset{n}{\leq} c$. Entonces $c \in H_n^1$ y, como $x \underset{n}{\leq} c$, existe un puente $(u, v)$ en $L_n$ tal que $x \underset{n}{\leq} u$ y $v \underset{n}{\leq} c$. Luego, puesto que $z_x$ es el menor elemento de $P_n^x$, $z_x \underset{n}{\leq} u$, y por el Lema 4.11, se tiene que $w_x \underset{n}{\leq} v \underset{n}{\leq} c$. Se sigue del *Caso 1* que $w_x \overset{1}{\underset{n}{\vee}} y \underset{n}{\leq} c$, estando $c$ y $w_x \overset{1}{\underset{n}{\vee}} y$ en el mismo hemisferio. Así, hemos probado que $x \underset{n}{\vee} y$ es supremo en $L_n$ para $x$ y $y$. Por otro lado, nuevamente por el Lema 4.15, $Q_y^n$ tiene un elemento mayor, $w_y$, tal que para algún $z_y \in H_n^0$ se tiene

que $(z_y, w_y)$ es un puente en $L_n$ y $w_y \underset{n}{\leq} y$. De manera similar se prueba que $x \underset{n}{\wedge} y = x \overset{1}{\underset{n}{\wedge}} z_y$. □

En las Figuras 4.1 y 4.2 presentadas a continuación se muestran los diagramas de Hasse de las retículas $L_n$ para $n = 0, 1, 2, 3, 4$. Se ilustra también la construcción recursiva de dichas retículas, indicando los puentes mediante líneas segmentadas.

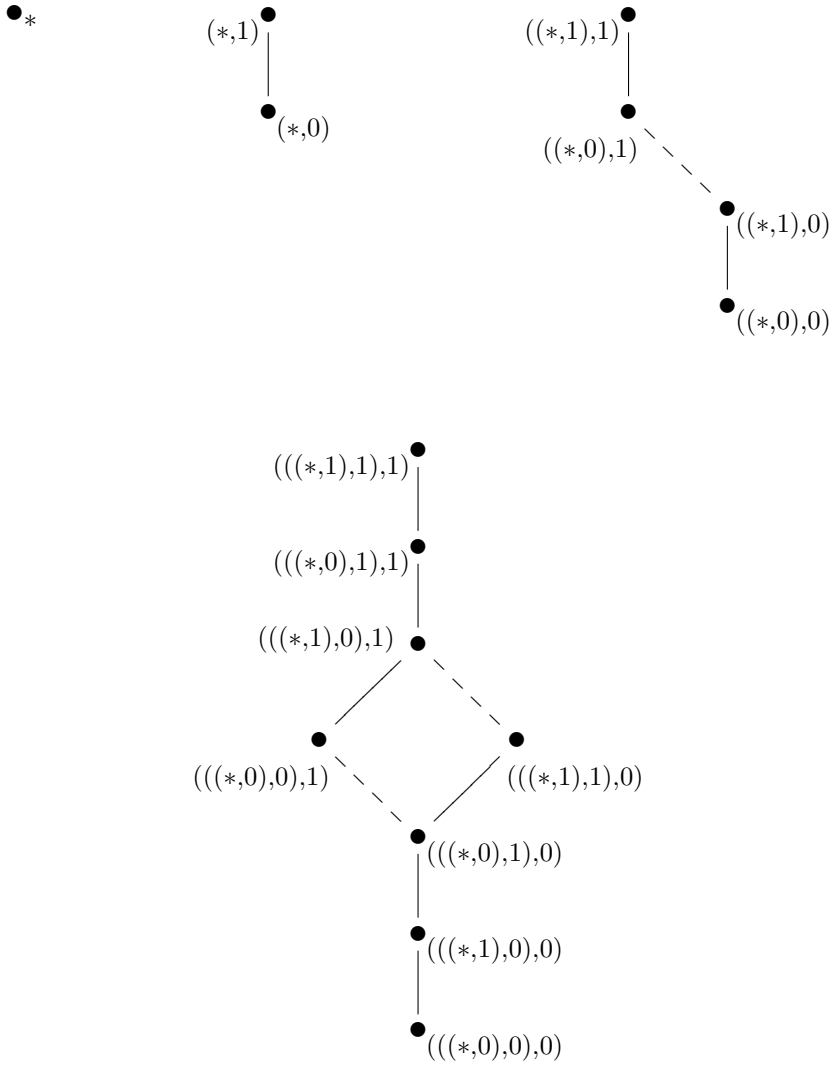



Figura 4.1: Diagramas de Hasse de $L_n$ para $n = 0, 1, 2, 3$.

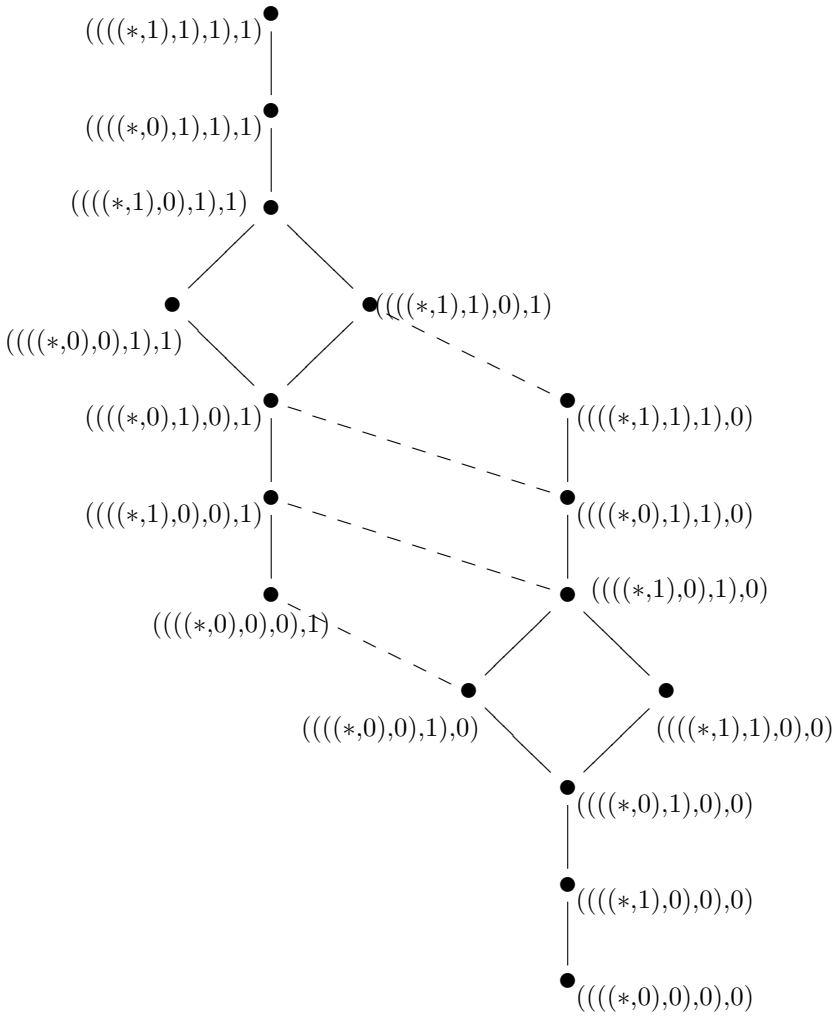



Figura 4.2: Diagrama de Hasse de $L_4$.

## 4.2. Las retículas $C_n$

Para cada $n \in \mathbb{N}$ presentamos las siguientes definiciones:

**Definición 4.17** *Un* $\underline{n-camino}$[1] *es una sucesión finita* $(v_0, v_1, \ldots, v_r)$ *tal que* $v_i \in (\mathbf{n+1})^2$ *para cada* $i = 0, 1, \ldots, r$.

**Definición 4.18** *Un* $\underline{n-camino\ funcional}$ *es un* $n-camino$

$$\mathbf{c} = ((0, c_0), (1, c_1), \ldots, (n, c_n)),$$

*tal que* $c_i \in \mathbf{n+1}$ *para cada* $i \in \mathbf{n+1}$.

Con el fin de simplificar la notación, identificaremos cada $n-$camino funcional $\mathbf{c} = ((0, c_0), (1, c_1), \ldots, (n, c_n))$ con una sucesión $\mathbf{c} = (c_0, c_1, \ldots, c_n) \in F_n$, donde $F_n := \{\mathbf{c} : \mathbf{n+1} \longrightarrow \mathbf{n+1} \mid \mathbf{c} \text{ es función}\}$.

**Definición 4.19** *Dados dos* $n-caminos\ funcionales$ $\mathbf{c} = (c_0, c_1, \ldots, c_n)$ *y* $\mathbf{c}' = (c'_0, c'_1, \ldots, c'_n)$, *definimos:*[2]

*1)* $\mathbf{c} \underset{n}{\preceq} \mathbf{c}'$ *si* $c_i \leq c'_i$ *para cada* $i \in \mathbf{n+1}$.

*2)* $\mathbf{c} \vee \mathbf{c}' = (t_0, t_1, \ldots, t_n)$, *con* $t_i = \max\{c_i, c'_i\}$ *para cada* $i \in \mathbf{n+1}$.

*3)* $\mathbf{c} \wedge \mathbf{c}' = (s_0, s_1, \ldots, s_n)$, *con* $s_i = \min\{c_i, c'_i\}$ *para cada* $i \in \mathbf{n+1}$.

**Observación 4.20** $\langle F_n, \underset{n}{\preceq}, \vee, \wedge \rangle$ *es una retícula finita y de cardinalidad* $(n+1)^{n+1}$.

**Definición 4.21** *Un* $n-camino\ funcional$ $\mathbf{c} = (c_0, c_1, \ldots, c_n)$ *es* $\underline{1\text{-}ascendente}$ *si* $c_0 = 0$ *y* $0 \leq c_{i+1} - c_i \leq 1$ *para cada* $i \in \{0, 1, \ldots, n-1\}$.

[1] En inglés, "$n$-lattice path".

[2] Nos permitimos emplear de antemano los símbolos " $\vee$ " y " $\wedge$ " para los elementos definidos en *2)* y *3)*, toda vez que éstos claramente satisfacen las propiedades de supremo e ínfimo, respectivamente, en $F_n$.

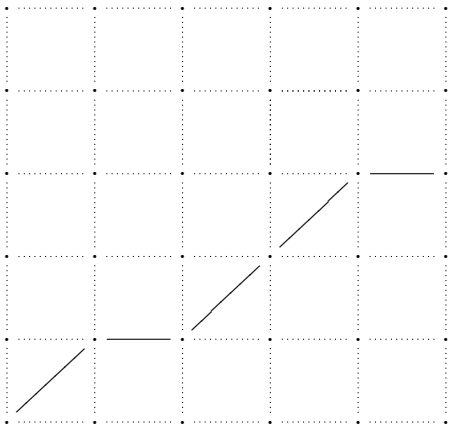


Figura 4.3: Un elemento particular de $C_5$.

En adelante denotaremos por $C_n$ al conjunto de todos los $n-$caminos funcionales 1-ascendentes. Otra forma de visualizar a los elementos de $C_n$ es como caminos en la cuadrícula $(\mathbf{n+1}) \times (\mathbf{n+1})$ desde $(0,0)$ hasta algún punto de la recta vertical $x = n$, con saltos horizontales o saltos diagonales (véase la Figura 4.3).

La siguiente propiedad es fácil de verificar.

**Lema 4.22** *Para cada $a, b \in \mathbb{N}$,*

*1)* $\text{máx}\{a,b\} \leq \text{máx}\{a,b+1\} \leq \text{máx}\{a,b\}+1 = \text{máx}\{a+1,b+1\}$*;*

*2)* $\text{mín}\{a,b\} \leq \text{mín}\{a,b+1\} \leq \text{mín}\{a,b\}+1 = \text{mín}\{a+1,b+1\}$. □

**Teorema 4.23** *Para cada $n \in \mathbb{N}$, $C_n$ es una subretícula de $F_n$.*

*Demostración.* Se probará que, para cada $n \in \mathbb{N}$, $C_n$ es cerrado bajo supremos e ínfimos. Sea $\mathbf{c} = (c_0, c_1, \ldots, c_n)$, $\mathbf{c'} = (c'_0, c'_1, \ldots, c'_n) \in C_n$. Por definición tenemos que $\mathbf{c} \vee \mathbf{c'} = (t_0, t_1, \ldots, t_n)$, con $t_i = \text{máx}\{\, c_i, c'_i \,\}$ y $\mathbf{c} \wedge \mathbf{c'} = (s_0, s_1, \ldots, s_n)$, con $s_i = \text{mín}\{\, c_i, c'_i \,\}$, para cada $i \in \mathbf{n+1}$. Notemos primero que $t_0 = s_0 = 0$ porque $c_0 = c'_0 = 0$. Ahora, sea $k \in \{0, 1, \ldots, n-1\}$. Como

$\mathbf{c}, \mathbf{c}' \in C_n$ se sigue que $0 \leq c_{k+1} - c_k \leq 1$ y $0 \leq c'_{k+1} - c'_k \leq 1$. Se tienen los siguientes casos:

*Caso 1:* $c_{k+1} - c_k = c'_{k+1} - c'_k = 0$. Luego, $c_{k+1} = c_k$ y $c'_{k+1} = c'_k$. Entonces $t_{k+1} = \text{máx}\{ c_{k+1}, c'_{k+1} \} = \text{máx}\{ c_k, c'_k \} = t_k$ y $s_{k+1} = \text{mín}\{ c_{k+1}, c'_{k+1} \} = \text{mín}\{ c_k, c'_k \} = s_k$. Por lo tanto, $t_{k+1} - t_k = s_{k+1} - s_k = 0$.

*Caso 2:* $c_{k+1} - c_k = c'_{k+1} - c'_k = 1$. Luego, $c_{k+1} = c_k + 1$ y $c'_{k+1} = c'_k + 1$. Entonces, del Lema 4.22 se sigue que $t_{k+1} = \text{máx}\{ c_{k+1}, c'_{k+1} \} = \text{máx}\{ c_k + 1, c'_k + 1 \} = t_k + 1$ y también que $s_{k+1} = \text{mín}\{ c_{k+1}, c'_{k+1} \} = \text{mín}\{ c_k + 1, c'_k + 1 \} = s_k + 1$. Por tanto, en este caso, $t_{k+1} - t_k = s_{k+1} - s_k = 1$.

*Caso 3:* $c_{k+1} - c_k = 0$ y $c'_{k+1} - c'_k = 1$. Luego, $c_{k+1} = c_k$ y $c'_{k+1} = c'_k + 1$. Entonces, por la parte *1*) del Lema 4.22 tenemos que $t_{k+1} = \text{máx}\{ c_{k+1}, c'_{k+1} \} = \text{máx}\{ c_k, c'_k + 1 \} \leq \text{máx}\{ c_k, c'_k \} + 1 = t_k + 1$ y también $t_k = \text{máx}\{ c_k, c'_k \} \leq \text{máx}\{ c_k, c'_k + 1 \} = \text{máx}\{ c_{k+1}, c'_{k+1} \} = t_{k+1}$, de donde $0 \leq t_{k+1} - t_k \leq 1$. Por otro lado, por el inciso *2*) del Lema 4.22, $s_k = \text{mín}\{ c_k, c'_k \} \leq \text{mín}\{ c_k, c'_k + 1 \} = \text{mín}\{ c_{k+1}, c'_{k+1} \} = s_{k+1}$ y $s_{k+1} = \text{mín}\{ c_{k+1}, c'_{k+1} \} = \text{mín}\{ c_k, c'_k + 1 \} \leq \text{mín}\left\{ c_k, c'_k \right\} + 1 = s_k + 1$, lo cual implica que $0 \leq s_{k+1} - s_k \leq 1$.

*Caso 4:* $c_{k+1} - c_k = 1$ y $c'_{k+1} - c'_k = 0$. La prueba es similar a la del *Caso 3.* □

Nótese que $C_n$ tiene elemento menor $\tilde{\mathbf{0}} = (0, 0, \ldots, 0)$ y elemento mayor $\tilde{\mathbf{1}} = (0, 1, \ldots, n)$.[3]

## 4.3. Las retículas $B_n$

**Definición 4.24** *Para cada $n \geq 1$ se define el conjunto de sucesiones binarias de longitud $n$, que en adelante denotaremos por $B_n$, como el conjunto $\{0, 1\}^n$.*

[3]Si bien para cada $n \in \mathbb{N}$ $C_n$ es una subretícula de $F_n$ en el sentido de que es un subconjunto cerrado bajo supremos e ínfimos, el elemento mayor de $C_n$ no es el elemento mayor de $F_n$, que es $(n, n, \ldots, n)$.

**Definición 4.25** *Dados* $n \geq 1$ *y* $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in B_n$, *tenemos las siguientes definiciones:*[4]

*1)* $a \leq b$ *si para toda* $k \in \{1, \ldots, n\}$ *se tiene que* $\sum_{i=1}^{k} a_i \leq \sum_{i=1}^{k} b_i$.

*2)* $a \vee b := (c_1, \ldots, c_n)$, *donde* $c_1 := \text{máx}\{a_1, b_1\}$ *y para cada* $k \in \{2, \ldots, n\}$,

$$c_k := \begin{cases} 0, & si \ \ \text{máx}\left\{\sum_{i=1}^{k-1} a_i, \sum_{i=1}^{k-1} b_i\right\} = \text{máx}\left\{\sum_{i=1}^{k} a_i, \sum_{i=1}^{k} b_i\right\}; \\ 1, & si \ \ \text{máx}\left\{\sum_{i=1}^{k-1} a_i, \sum_{i=1}^{k-1} b_i\right\} \neq \text{máx}\left\{\sum_{i=1}^{k} a_i, \sum_{i=1}^{k} b_i\right\}. \end{cases}$$

*3)* $a \wedge b := (d_1, \ldots, d_n)$, *donde* $d_1 := \text{mín}\{a_1, b_1\}$ *y, para cada* $k \in \{2, \ldots, n\}$,

$$d_k := \begin{cases} 0, & si \ \ \text{mín}\left\{\sum_{i=1}^{k-1} a_i, \sum_{i=1}^{k-1} b_i\right\} = \text{mín}\left\{\sum_{i=1}^{k} a_i, \sum_{i=1}^{k} b_i\right\}; \\ 1, & si \ \ \text{mín}\left\{\sum_{i=1}^{k-1} a_i, \sum_{i=1}^{k-1} b_i\right\} \neq \text{mín}\left\{\sum_{i=1}^{k} a_i, \sum_{i=1}^{k} b_i\right\}. \end{cases}$$

Observemos que, como consecuencia de la definición anterior, si $a \vee b := c = (c_1, \ldots, c_n)$, entonces para cada $k \in \{1, \ldots, n\}$ se tiene que $\sum_{i=1}^{k} c_i = \text{máx}\left\{\sum_{i=1}^{k} a_i, \sum_{i=1}^{k} b_i\right\}$. Para verificarlo procederemos por inducción sobre $k$. La afirmación es clara para $k = 1$. Ahora supongámosla cierta para $k - 1$, con $k > 2$. Tenemos dos casos:

Si $\text{máx}\left\{\sum_{i=1}^{k-1} a_i, \sum_{i=1}^{k-1} b_i\right\} = \text{máx}\left\{\sum_{i=1}^{k} a_i, \sum_{i=1}^{k} b_i\right\}$, entonces, por la hipótesis de inducción:

$$\sum_{i=1}^{k} c_i = \sum_{i=1}^{k-1} c_i + c_k = \sum_{i=1}^{k-1} c_i + 0 = \text{máx}\left\{\sum_{i=1}^{k-1} a_i, \sum_{i=1}^{k-1} b_i\right\} = \text{máx}\left\{\sum_{i=1}^{k} a_i, \sum_{i=1}^{k} b_i\right\}.$$

[4]De nuevo usamos los símbolos " $\vee$ " y " $\wedge$ " para los elementos definidos en *2)* y *3)*, pues, como se verifica enseguida, estas sucesiones binarias tienen las propiedades de supremo e ínfimo, respectivamente, en $B_n$.

Si, por el contrario, $\text{máx}\left\{\sum_{i=1}^{k-1} a_i, \sum_{i=1}^{k-1} b_i\right\} \neq \text{máx}\left\{\sum_{i=1}^{k} a_i, \sum_{i=1}^{k} b_i\right\}$, entonces debe ocurrir que $\text{máx}\left\{\sum_{i=1}^{k} a_i, \sum_{i=1}^{k} b_i\right\} = \text{máx}\left\{\sum_{i=1}^{k-1} a_i, \sum_{i=1}^{k-1} b_i\right\} + 1$. Luego, nuevamente por la hipótesis de inducción:

$$\sum_{i=1}^{k} c_i = \sum_{i=1}^{k-1} c_i + c_k = \sum_{i=1}^{k-1} c_i + 1 = \text{máx}\left\{\sum_{i=1}^{k-1} a_i, \sum_{i=1}^{k-1} b_i\right\} + 1 = \text{máx}\left\{\sum_{i=1}^{k} a_i, \sum_{i=1}^{k} b_i\right\}.$$

De manera similar se verifica que si $a \wedge b := d = (d_1, \ldots, d_n)$, entonces $\sum_{i=1}^{k} d_i = \text{mín}\left\{\sum_{i=1}^{k} a_i, \sum_{i=1}^{k} b_i\right\}$ para cada $k \in \{1, \ldots, n\}$.

En vista de la observación anterior es inmediato que $a \vee b$ y $a \wedge b$ satisfacen las propiedades de supremo e ínfimo, respectivamente, de $a$ y $b$ en $B_n$.

Se sigue que $\langle B_n, \leq, \vee, \wedge \rangle$ es una retícula con elemento menor $\bar{0} = (0, \ldots, 0)$ y elemento mayor $\bar{1} = (1, \ldots, 1)$.

El resultado que presentamos a continuación nos será de utilidad más adelante.

**Lema 4.26** *Sean $n \geq 1$ y $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in B_n$. Entonces $a$ cubre $a$ $b$ si y sólo si existe $k \in \{1, \ldots, n\}$ tal que:*

*1) $a_i = b_i$ para $i \neq k, k+1$.*

*2) $b_k = 0$, $a_k = 1$.*

*3) Si $k < n$, entonces $b_{k+1} = 1$ y $a_{k+1} = 0$.*

*Demostración.* Para la necesidad, supongamos que $a$ cubre a $b$ y sea $k := \text{mín}\{i \in \{1, \ldots, n\} \mid b_i < a_i\}$. Entonces $a_i = b_i$ para $i < k$ y $b_k = 0$, $a_k = 1$, de donde, si $k = n$, las condiciones se satisfacen. Ahora, si $k < n$ y $b_{k+1} = 0$ ó $a_{k+1} = 1$, entonces existiría $c \in B_n$ tal que $b < c < a$. En efecto, si $b_{k+1} = 0$,

tómese $c = (c_1, \ldots, c_n)$ como sigue:

$$c_i := \begin{cases} b_i, & \text{para } i \in \{1, \ldots, k\}; \\ 1, & \text{para } i = k+1; \\ a_i, & \text{para } i \in \{k+2, \ldots, n\}. \end{cases}$$

Por otro lado, si $a_{k+1} = 1$, escójase $c = (c_1, \ldots, c_n)$ tal que:

$$c_i := \begin{cases} b_i, & \text{para } i \in \{1, \ldots, k-1\}; \\ a_i, & \text{para } i = k; \\ 0, & \text{para } i = k+1; \\ a_i, & \text{para } i \in \{k+2, \ldots, n\}. \end{cases}$$

Luego, en ambos casos contradecimos el hecho de que $a$ cubre a $b$. Finalmente, si $a_j \neq b_j$ para algún $j > k+1$, entonces debe ocurrir que $b_j < a_j$ para algún $j > k+1$. En tal caso, $b_j = 0$ y $a_j = 1$. Luego, si tomamos $c = (c_1, \ldots, c_n)$ tal que

$$c_i := \begin{cases} b_i, & \text{para } i \in \{1, \ldots, j-1\} \\ a_i, & \text{para } i \in \{j, \ldots, n\}, \end{cases}$$

resulta que $a < c < b$; nuevamente una contradicción. Por lo tanto, las condiciones *1*) $-$ *3*) se cumplen.

Recíprocamente, si se satisfacen las condiciones *1*) $-$ *3*), entonces, claramente, $b < a$. Supongamos que existe $c \in B_n$ tal que $b \leq c \leq a$. En virtud de la condición *1*) se tiene que $c_i = a_i = b_i$ para $i \neq k, k+1$. Por otra parte, no es posible que suceda que $c_k = c_{k+1} = 0$, o bien, que $c_k = c_{k+1} = 1$. Por tanto, $c = b$ ó $c = a$. Concluimos que $a$ cubre a $b$. □

### 4.3.1. Propiedades de $B_n$

Presentamos a continuación varias propiedades de las retículas $B_n$.

**Teorema 4.27** *Para cada $n \geq 1$, $B_n$ es una retícula distributiva y finita, de cardinalidad $2^n$.*

*Demostración.* Sea $n \geq 1$. Es claro de la definición de $B_n$ que $|B_n| = 2^n$. Definimos la función $\nu : B_n \longrightarrow (\mathbf{n+1})^n$ como:

$$\nu(a_1, \ldots, a_n) := (a_1, \ldots, \sum_{i=1}^{k} a_i, \ldots, \sum_{i=1}^{n} a_i).$$

Claramente $\nu$ está bien definida. Más aún, no es difícil verificar que $\nu$ es una función inyectiva que además satisface que para cada $a, b \in B_n$, $a \leq b \Leftrightarrow \nu(a) \leq \nu(b)$. En efecto, sean $a = (a_1, \ldots, a_n), (b_1, \ldots, b_n) \in B_n$, entonces $a \leq b$ si y sólo si $\sum_{i=1}^{k} a_i \leq \sum_{i=1}^{k} b_i$ para cada $k \in \{1, \ldots, n\}$ si y sólo si $\nu(a) = (a_1, \ldots, \sum_{i=1}^{k} a_i, \ldots, \sum_{i=1}^{n} a_i) \leq (b_1, \ldots, \sum_{i=1}^{k} b_i, \ldots, \sum_{i=1}^{n} b_i) = \nu(b)$. Se tiene que $\nu$ es un homomorfismo de *copos* inyectivo sobre su imagen $\nu(B_n)$. Luego, del Teorema 1.25 se sigue que la retícula $B_n$ es isomorfa a una subretícula de $(\mathbf{n+1})^n$. Por tanto, como $(\mathbf{n+1})^n$ es una retícula distributiva, también $B_n$ lo es. □

En la Figura 4.4 se ilustra la inmersión de $B_n$ en la retícula $(\mathbf{n+1})^n$ bajo el monomorfismo $\nu$ definido en el Teorema 4.27.

**Teorema 4.28** *Para $n \geq 5$, $B_n$ no es una retícula plana.*

*Demostración.* Sean $x = (0,1,0,1,0)$, $u = (1,0,0,1,0)$, $v = (0,1,1,0,0)$ y $w = (0,1,0,1,1) \in B_5$. Se sigue del Lema 4.26 que $u, v$ y $w$ cubren a $x$, de donde, en virtud del Teorema 1.31, $B_5$ no es plana. Por tanto, como para cada $n \geq 5$ existe una subretícula de $B_n$ que es isomorfa a $B_5$ (defínase la función $\iota : B_5 \longrightarrow B_n$ tal que para cada $a = (a_1, a_2, a_3, a_4, a_5) \in B_5$, $\iota(a) = (b_1, \ldots, b_n) \in B_n$, donde:

$$b_i := \begin{cases} 0, & \text{si } i \in \{1, \ldots, n-5\}; \\ a_i & \text{si } i \in \{n-4, \ldots, n\}. \end{cases}$$

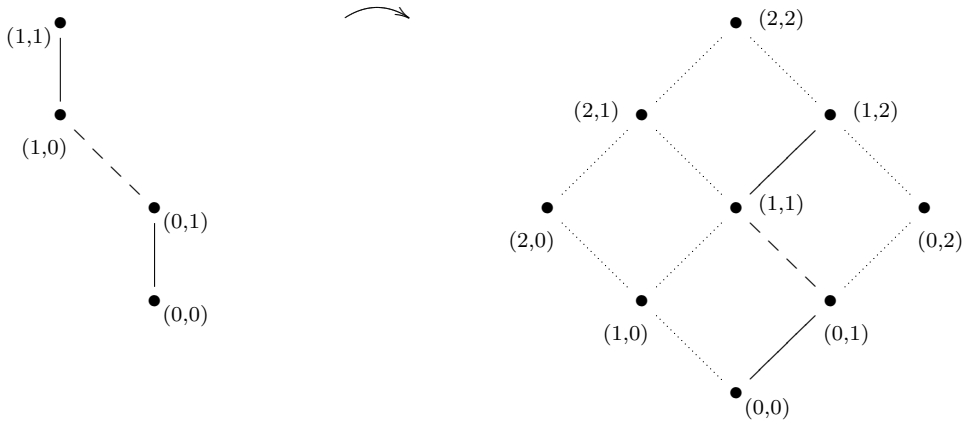



Figura 4.4: $B_n$ como subretícula de $(\mathbf{n}+\mathbf{1})^n$, con $n = 2$.

Luego, por un argumento análogo al usado en el Teorema 4.27 se tiene que $\iota$ es un isomorfismo de retículas sobre su imagen). Concluimos que para $n \geq 5$ $B_n$ no es una retícula plana. □

Para simplificar la notación, definimos para cada $x \in \{0, 1\}$:

$$x^* := \begin{cases} 0, & \text{si } x = 1; \\ 1, & \text{si } x = 0. \end{cases}$$

**Teorema 4.29** *Para cada $n \geq 1$, $B_n$ es una retícula autodual.*

*Demostración.* Definimos a la función $\mu : B_n \longrightarrow B_n$ como $\mu(a_1, \ldots, a_n) := (a_1^*, \ldots, a_n^*)$ para cada $(a_1, \ldots, a_n) \in B_n$. Se sigue que $\mu$ es un anti-isomorfismo de retículas. En efecto, claramente $\mu$ es una función biyectiva. Además, si $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n) \in B_n$, entonces $a \leq b$ si y sólo si $\sum_{i=1}^{k} a_i \leq \sum_{i=1}^{k} b_i$ para cada $k \in \{1, \ldots, n\}$ si y sólo si $\mu(a) = \sum_{i=1}^{k} a_i^* \geq \sum_{i=1}^{k} b_i^* = \mu(b)$ para cada $k \in \{1, \ldots, n\}$. Se sigue que $\mu$ es un anti-isomorfismo de *copos* y, por el Teorema 1.25, $\mu$ es también un anti-isomorfismo de retículas. □

Más adelante haremos referencia a la función $\mu$ antes definida.

**Teorema 4.30** *Para cada $n \geq 1$, $B_n$ es una retícula graduada, con rango $\frac{n(n+1)}{2}$.*

*Demostración.* Sea $n \geq 1$. Definimos la función $\rho : B_n \longrightarrow \mathbb{N}$ tal que para cada $(a_1, \ldots, a_n) \in B_n$, $\rho((a_1, \ldots, a_n)) := \sum_{i=1}^{n} a_i(n - i + 1)$. Claramente $\rho(\bar{0}) = 0$. Ahora, sean $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n) \in B_n$ tales que $a$ cubre a $b$. Luego, para alguna $k \in \{1, \ldots, n\}$, las condiciones del Lema 4.26 se cumplen. Si $k < n$, entonces $\rho(a) = \sum_{i \neq k, k+1} a_i(n-i+1) + a_k(n-k+1) + a_{k+1}(n-k) = \sum_{i \neq k, k+1} a_i(n-i+1) + n - k + 1 = \sum_{i \neq k, k+1} b_i(n-i+1) + b_k(n-k+1) + b_{k+1}(n-k) + 1 = \rho(b) + 1$. Si, por el contrario, $k = n$, entonces $\rho(a) = \sum_{i=1}^{n-1} a_i(n - i + 1) + a_n = \sum_{i=1}^{n-1} b_i(n - i + 1) + 1 = \rho(b) + 1$. Por lo tanto, $B_n$ es graduada, con rango $\rho(\bar{1}) = \frac{n(n+1)}{2}$. □

## 4.4. $L_n$, $C_n$ y $B_n$ son isomorfas

En los siguientes teoremas se prueba que, dada $n \geq 1$, las retículas $L_n$, $C_n$ y $B_n$ son isomorfas. Los isomomorfismos correspondientes serán de gran utilidad, por lo que nos referiremos a ellos más adelante.

**Teorema 4.31** *Para cada $n \in \mathbb{N}$, las retículas $L_n$ y $C_n$ son isomorfas.*

*Demostración (por inducción sobre n).* Por el Teorema 1.25 basta mostrar que $L_n$ y $C_n$ son isomorfos como *copos*. Se definen los isomorfismos inversos $\epsilon_0 : C_0 \longrightarrow L_0$ y $\varphi_0 : L_0 \longrightarrow C_0$ trivialmente: $\epsilon_0(0) = *$ y $\varphi_0(*) = 0$.

Ahora supongamos definidos los isomorfismos inversos de *copos*:

$$\epsilon_{n-1} : C_{n-1} \longrightarrow L_{n-1}, \quad \varphi_{n-1} : L_{n-1} \longrightarrow C_{n-1}.$$

Definimos los homomorfismos $\epsilon_n : C_n \longrightarrow L_n$ y $\varphi_n : L_n \longrightarrow C_n$ de la siguiente manera:

$$\epsilon_n(c_0, c_1, \ldots, c_n) := (\epsilon_{n-1}(c_1 - c_1, c_2 - c_1, \ldots, c_n - c_1), c_1)$$

y

$$\varphi_n(x) = \varphi_n(x_1, \delta_1) := (0, \delta_1, c_1 + \delta_1, \ldots, c_{n-1} + \delta_1),$$

donde $\varphi_{n-1}(x_1) = (c_0, c_1, \ldots, c_{n-1}) \in C_{n-1}$.

Entonces, se tiene lo siguiente:

*$\varphi_n$ y $\epsilon_n$ son inversas una de la otra.*

Sea $\mathbf{c} = (c_0, c_1, c_2, ..., c_n) \in C_n$. Definimos:

$$\underline{\mathbf{c}} := (c_1 - c_1, c_2 - c_1, \ldots, c_n - c_1) \in C_{n-1}.$$

Se sigue que $(\varphi_n \circ \epsilon_n)(\mathbf{c}) = \varphi_n(\epsilon_n(\mathbf{c})) = \varphi_n(\epsilon_{n-1}(\underline{\mathbf{c}}), c_1) = (0, c_1, (c_2 - c_1) + c_1, (c_3 - c_1) + c_1, \ldots, (c_n - c_1) + c_1) = (c_0, c_1, c_2, \ldots, c_n) = \mathbf{c}$, pues $(\varphi_{n-1} \circ \epsilon_{n-1})(\underline{\mathbf{c}}) = \underline{\mathbf{c}}$ por la hipótesis de inducción. Ahora bien, sea $x = (x_1, \delta_1) \in L_n$ y supongamos que $\varphi_{n-1}(x_1) = (d_0, d_1, \ldots, d_{n-1}) \in C_{n-1}$.

Entonces $(\epsilon_n \circ \varphi_n)(x) = \epsilon_n(\varphi_n(x_1, \delta_1)) = \epsilon_n(0, \delta_1, d_1 + \delta_1, \ldots, d_{n-1} + \delta_1) = (\epsilon_{n-1}(0, (d_1 + \delta_1) - \delta_1, \ldots, (d_{n-1} + \delta_1) - \delta_1), \delta_1) = (\epsilon_{n-1}(0, d_1, \ldots, d_{n-1}), \delta_1) = (\epsilon_{n-1}(\varphi_{n-1}(x_1)), \delta_1) = (x_1, \delta_1) = x$, pues $(\epsilon_{n-1} \circ \varphi_{n-1})(x_1) = x_1$, de nuevo por la hipótesis de inducción. Por tanto, $\varphi_n \circ \epsilon_n = Id_{C_n}$ y $\epsilon_n \circ \varphi_n = Id_{L_n}$, con lo que se verifica la afirmación.

*$\epsilon_n : (C_n, \underset{n}{\preceq}) \longrightarrow (L_n, \underset{n}{\leq})$ es un homomorfismo de copos que preserva el orden.*

Sean $\mathbf{c} = (c_0, c_1, \ldots, c_n)$, $\mathbf{c}' = (c'_0, c'_1, \ldots, c'_n) \in C_n$ y consideremos a los elementos $\underline{\mathbf{c}} := (c_1 - c_1, \ldots, c_n - c_1)$, $\underline{\mathbf{c}'} := (c'_1 - c'_1, \ldots, c'_n - c'_1) \in C_{n-1}$. Supongamos que $\mathbf{c} \underset{n}{\preceq} \mathbf{c}'$. Entonces $c_i \leq c'_i$ para cada $i \in \mathbf{n+1}$. Tenemos los siguientes casos:

*Caso 1:* $c_1 = c'_1$. Entonces $c_i - c_1 \leq c'_i - c'_1$ para cada $i \in \{1, \ldots, n\}$, es decir, $\underline{\mathbf{c}} \underset{n-1}{\preceq} \underline{\mathbf{c}}'$. Luego, como $\epsilon_{n-1} : C_{n-1} \longrightarrow L_{n-1}$ preserva el orden, se tiene que $\epsilon_{n-1}(\underline{\mathbf{c}}) \underset{n-1}{\leq} \epsilon_{n-1}(\underline{\mathbf{c}}')$. Por tanto, se concluye que $\epsilon_n(\mathbf{c}) = (\epsilon_{n-1}(\underline{\mathbf{c}}), c_1) \underset{n}{\leq} (\epsilon_{n-1}(\underline{\mathbf{c}}'), c'_1) = \epsilon_n(\mathbf{c}')$.

*Caso 2:* $c_1 \neq c'_1$. Se sigue que $c_1 < c'_1$ y, como $\mathbf{c}$, $\mathbf{c}'$ son $1-$ascendentes, se tiene que $c_1 = 0$ y $c'_1 = 1$. Consideremos a continuación los $n-$caminos $\mathbf{d} = (0, 0, 1, d_3, \ldots, d_n)$ y $\mathbf{d}' = (0, 1, 1, d_3, \ldots, d_n)$, donde $d_i := \text{máx}\{1, c_i\}$ para $i = 3, \ldots, n$. Nótese que $\mathbf{d}, \mathbf{d}' \in C_n$. Ahora, sean:

$$z := \epsilon_n(\mathbf{d}) = (\epsilon_{n-1}(0, 1, d_3, \ldots, d_n), 0)$$

y

$$w := \epsilon_n(\mathbf{d}') = \epsilon_{n-1}(0, 0, d_3 - 1, \ldots, d_n - 1), 1).$$

De acuerdo a la notación presentada después de la Definición 4.1 se tiene que:

$$z_1 = \epsilon_{n-1}(0, 1, d_3, \ldots, d_n) = (\epsilon_{n-2}(0, d_3 - 1, \ldots, d_n - 1), 1)$$

y

$$w_1 = \epsilon_{n-1}(0, 0, d_3 - 1, \ldots, d_n - 1) = (\epsilon_{n-2}(0, d_3 - 1, \ldots, d_n - 1), 0),$$

de manera que $z_2 = \epsilon_{n-2}(0, d_3 - 1, \ldots, d_n - 1) = w_2$. Se sigue que $(z, w)$ es un puente en $L_n$.

Ahora consideremos:

$$x = \epsilon_n(\mathbf{c}) = \epsilon_{n-1}(c_1 - c_1, c_2 - c_1, \ldots, c_n - c_1), c_1) = (\epsilon_{n-1}(0, c_2, \ldots, c_n), 0)$$

y

$$y = \epsilon_n(\mathbf{c}') = (\epsilon_{n-1}(c'_1 - c'_1, c'_2 - c'_1, \ldots, c'_n - c'_1), c'_1) = (\epsilon_{n-1}(0, c'_2 - 1, \ldots, c'_n - 1), 1).$$

Notemos que $c_2 \leq 1$, por la $1-$ascendencia de $\mathbf{c}$. Luego, por la hipótesis de inducción y puesto que $(0, c_2, c_3, \ldots, c_n) \underset{n-1}{\preceq} (0, 1, d_3, \ldots, d_n)$, tenemos que $x_1 = \epsilon_{n-1}(0, c_2, c_3, \ldots, c_n) \underset{n-1}{\leq} \epsilon_{n-1}(0, 1, d_3, \ldots, d_n) = z_1$.

Por otro lado, nótese que $0 \leq c'_2 - 1$, por la 1−ascendencia de $\mathbf{c}'$ y que $c_i - 1 \leq c'_i - 1$ para cada $i \in \{3, \ldots, n\}$, ya que $\mathbf{c} \underset{n}{\preceq} \mathbf{c}'$. Además, de la definición de $\mathbf{d}$ se sigue que $d_i - 1 = 0$ ó $d_i - 1 = c_i - 1$ para $i = 3, \ldots, n$. En cualquier caso, $(0, 0, d_3 - 1, \ldots, d_n - 1) \underset{n}{\preceq} (0, c'_2 - 1, c'_3 - 1, \ldots, c'_n - 1)$, de donde, por la hipótesis de inducción,

$$w_1 = \epsilon_{n-1}(0, 0, d_3 - 1, \ldots, d_n - 1) \underset{n-1}{\leq} \epsilon_{n-1}(0, c'_2 - 1, c'_3 - 1, \ldots, c'_n - 1) = y_1.$$

Luego, por la Definición 4.6 se tiene que $\epsilon_n(\mathbf{c}) \underset{n}{\leq} \epsilon_n(\mathbf{c}')$. Se concluye así que $\epsilon_n$ preserva el orden.

$\varphi_n : (L_n, \underset{n}{\leq}) \longrightarrow (C_n, \underset{n}{\preceq})$ *es un homomorfismo de copos que preserva el orden.*

Sean $x = (x_1, \delta_1)$, $y = (y_1, \varepsilon_1) \in L_{n-1} \times \{0, 1\}$ tales que $x \underset{n}{\leq} y$. Entonces

$$\varphi_n(x) = \varphi_n(x_1, \delta_1) = (0, \delta_1, c_1 + \delta_1, \ldots, c_{n-1} + \delta_1)$$

y

$$\varphi_n(y) = \varphi_n(y_1, \varepsilon_1) = (0, \varepsilon_1, c'_1 + \varepsilon_1, \ldots, c'_{n-1} + \varepsilon_1),$$

donde $\varphi_{n-1}(x_1) = (c_0, c_1, \ldots, c_{n-1})$, $\varphi_{n-1}(y_1) = (c'_0, c'_1, ..., c'_{n-1}) \in C_{n-1}$.

Tenemos los siguientes casos:

*Caso 1:* $\delta_1 = \varepsilon_1$. Entonces debe ocurrir que $x_1 \underset{n-1}{\leq} y_1$. Por la hipótesis de inducción tenemos que $\varphi_{n-1}(x_1) \underset{n-1}{\preceq} \varphi_{n-1}(y_1)$, de manera que $c_i \leq c'_i$ para cada $i \in \{0, 1, \ldots, n-1\}$. Más aún, como $\delta_1 = \varepsilon_1$, se tiene que $c_i + \delta_1 \leq c'_i + \varepsilon_1$ para cada $i \in \{0, 1, \ldots, n-1\}$, lo cual implica que $\varphi_n(x) \underset{n}{\preceq} \varphi_n(y)$.

*Caso 2:* $\delta_1 = 0$, $\varepsilon_1 = 1$. En este caso, por la Definición 4.6, debe existir un puente $(z, w)$ en $L_n$, tal que $z = (z_1, 0)$, $w = (w_1, 1)$, con $z_1 = (z_2, 1)$, $w_1 = (w_2, 0) \in L_{n-1}$, donde $z_2 = w_2$, $x_1 \underset{n-1}{\leq} z_1$ y $w_1 \underset{n-1}{\leq} y_1$. Consideremos:

$$\varphi_n(z) = \varphi_n(z_1, 0) = (0, 0, d_1, \ldots, d_{n-1})$$

y

$$\varphi_n(w) = \varphi_n(w_1, 1) = (0, 1, d'_1 + 1, \ldots, d'_{n-1} + 1),$$

donde $\varphi_{n-1}(z_1) = (d_0, d_1, \ldots, d_{n-1})$, $\varphi_{n-1}(w_1) = (d'_0, d'_1, \ldots, d'_{n-1}) \in C_{n-1}$. Como $x_1 \underset{n-1}{\leq} z_1$, tenemos por la hipótesis de inducción que $\varphi_{n-1}(x_1) \underset{n-1}{\preceq} \varphi_{n-1}(z_1)$, esto es, $(c_0, c_1, \ldots, c_{n-1}) \underset{n-1}{\preceq} (d_0, d_1, \ldots, d_{n-1})$. Análogamente, como $w_1 \underset{n-1}{\leq} y_1$, se sigue que $\varphi_{n-1}(w_1) \underset{n-1}{\preceq} \varphi_{n-1}(y_1)$, lo cual significa que $(d'_0, d'_1, \ldots, d'_{n-1}) \underset{n-1}{\preceq} (c'_0, c'_1, \ldots, c'_{n-1})$. Además, tenemos que:

$$(d_0, d_1, \ldots, d_{n-1}) = \varphi_{n-1}(z_1) = \lambda_{n-1}(z_2, 1) = (0, 1, e_1 + 1, \ldots, e_{n-2} + 1),$$

donde $\varphi_{n-2}(z_2) = (e_0, e_1, \ldots, e_{n-2}) \in C_{n-2}$. También:

$$(d'_0, d'_1, \ldots, d'_{n-1}) = \varphi_{n-1}(w_1) = \varphi_{n-1}(w_2, 0) = (0, 0, e'_1, \ldots, e'_{n-2}),$$

con $\varphi_{n-2}(w_2) = (e'_0, e'_1, \ldots, e'_{n-2}) \in C_{n-2}$.

Más aún, puesto que $\varphi_{n-2}(z_2) = \varphi_{n-2}(w_2)$, se sigue que $e_i = e'_i$ para cada $i \in \{0, 1, \ldots, n-2\}$. Asimismo, tenemos que $d_0 = 0 = d'_0$, $d_1 = 1$, $d'_1 = 0$ y $d_i = e_{i-1} + 1 = e'_{i-1} + 1 = d'_i + 1$ para $i \in \{2, \ldots, n-1\}$. Finalmente, como $\delta_1 = 0$, se sigue que:

$$\varphi_n(x) = \varphi_n(x_1, 0) = (0, 0, c_1, \ldots, c_{n-1}).$$

Por su parte, como $\varepsilon_1 = 1$, se tiene que:

$$\varphi_n(y) = \varphi_n(y_1, 1) = (0, 1, c'_1 + 1, \ldots, c'_{n-1} + 1)$$

Por tanto, ya que para cada $i \in \{1, \ldots, n-1\}$, $c_i \leq d_i = d'_i + 1 \leq c'_i + 1$, se sigue que $\varphi_n(x) \underset{n}{\preceq} \varphi_n(y)$. Concluimos que $\varphi_n$ preserva el orden.

Luego, como consecuencia de la Observación 1.4, tanto $\epsilon_n$ como $\varphi_n$ son isomorfismos de *copos*, con lo que concluye la demostración del Teorema. □

**Teorema 4.32** *Para cada $n \geq 1$, las retículas $C_n$ y $B_n$ son isomorfas.*

*Demostración.* Nuevamente, por el Teorema 1.25, basta mostrar que $C_n$ y $B_n$ son isomorfos como *copos*. Para cada $n \geq 1$ definimos a las funciones $\kappa_n : C_n \longrightarrow B_n$ y $\theta_n : B_n \longrightarrow C_n$ de la siguiente manera:

Para cada $\mathbf{c} = (c_0, c_1, \ldots, c_n) \in C_n$, $\kappa_n(\mathbf{c}) := (a_1, \ldots, a_n)$, donde, para cada $k \in \{1, \ldots, n\}$,

$$a_k := \begin{cases} 0, & \text{si } c_k = c_{k-1}; \\ 1, & \text{si } c_k \neq c_{k-1}, \end{cases}$$

Para cada $a = (a_1, \ldots, a_n) \in B_n$, $\theta_n(a) := (c_0, \ldots, c_n)$, donde:

$$c_k := \begin{cases} 0, & \text{para } k = 0; \\ \sum_{i=1}^{k} a_i, & \text{para } k \in \{1, \ldots, n\}. \end{cases}$$

Sea $\mathbf{c} = (c_0, \ldots, c_n) \in C_n$ y supongamos que $\kappa_n(\mathbf{c}) := (a_1, \ldots, a_n)$. Probaremos por inducción sobre $k$ que $c_k = \sum_{i=1}^{k} a_i$ para $k \in \{1, \ldots, n\}$. Es claro que $a_1 = c_0 + c_1 = 0 + c_1 = c_1$. Supongamos cierta la afirmación para $k-1$, con $k > 2$. Entonces $c_k = c_{k-1}$ ó $c_k = c_{k-1} + 1$, pues $\mathbf{c}$ es $1-$ascendente. Luego, si $c_k = c_{k-1}$, entonces $a_k = 0$ y, por la hipótesis de inducción, $c_k = c_{k-1} = \sum_{i=1}^{k-1} a_i + 0 = \sum_{i=1}^{k-1} a_i + a_k = \sum_{i=1}^{k} a_i$. De manera análoga, si $c_k = c_{k-1} + 1$, entonces $a_k = 1$ y, por la hipótesis de inducción, $c_k = c_{k-1} + 1 = \sum_{i=1}^{k-1} a_i + 1 = \sum_{i=1}^{k-1} a_i + a_k = \sum_{i=1}^{k} a_i$.

Ahora, tenemos que:

*$\kappa_n$ y $\theta_n$ son inversas una de la otra.*

Dado $\mathbf{c} = (c_0, \ldots, c_n) \in C_n$, se tiene que $\kappa_n(\mathbf{c}) = (a_1, \ldots, a_n)$, donde, para cada $k \in \{1, \ldots, n\}$,

$$a_k = \begin{cases} 0, & \text{si } c_k = c_{k-1}; \\ 1, & \text{si } c_k \neq c_{k-1}. \end{cases}$$

Luego, por la última afirmación se tiene que $(\theta_n \circ \kappa_n)(\mathbf{c}) = \theta_n(a_1, \ldots, a_n) = (0, a_1, \ldots, \sum_{i=1}^{k} a_i, \ldots, \sum_{i=1}^{n} a_i) = (c_0, c_1, \ldots, c_k, \ldots, c_n) = \mathbf{c}$. Por otro lado, si $a = (a_1, \ldots, a_n) \in B_n$, entonces $(\kappa_n \circ \theta_n)(a) = \kappa_n(0, a_1, \ldots, \sum_{i=1}^{k} a_i, \ldots, \sum_{i=1}^{n} a_i) =: (b_1, \ldots, b_n)$. Luego, si $\sum_{i=1}^{k-1} a_i = \sum_{i=1}^{k} a_i$, entonces $b_k = 0 = a_k$. De manera análoga, si $\sum_{i=1}^{k-1} a_i \neq \sum_{i=1}^{k} a_i$, entonces $b_k = 1 = a_k$. Por tanto, $(\kappa_n \circ \theta_n)(a) = a$.

Concluimos que $\theta_n \circ \kappa_n = Id_{C_n}$ y $\kappa_n \circ \theta_n = Id_{B_n}$.

$\kappa_n : (C_n, \underset{n}{\preceq}) \longrightarrow (B_n, \leq)$ *es un homomorfismo de copos que preserva el orden.*

Sean $\mathbf{c} = (c_0, \ldots, c_n)$, $\mathbf{d} = (d_0, \ldots, d_n) \in C_n$ tales que $\mathbf{c} \underset{n}{\preceq} \mathbf{d}$. Entonces $c_i \leq d_i$ para cada $i \in \mathbf{n+1}$. Supongamos que $\kappa_n(\mathbf{c}) = (a_1, \ldots, a_n)$ y $\kappa_n(\mathbf{d}) = (b_1, \ldots, b_n)$. Entonces, por la observación previa, $\sum_{i=1}^{k} a_i = c_k \leq d_k = \sum_{i=1}^{k} b_i$ para cada $k \in \{1, \ldots, n\}$. Por tanto, $\kappa_n(\mathbf{c}) \leq \kappa_n(\mathbf{c})$.

$\theta_n : (B_n, \leq) \longrightarrow (C_n, \underset{n}{\preceq})$ *es un homomorfismo de copos que preserva el orden.*

Sean $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$ tales que $a \leq b$; es decir, $\sum_{i=1}^{k} a_i \leq \sum_{i=1}^{k} b_i$ para cada $k \in \{1, \ldots, n\}$. Luego, $\theta_n(a) = (0, a_1, \ldots, \sum_{i=1}^{k} a_i, \ldots, \sum_{i=1}^{n} a_i) \underset{n}{\preceq} (0, b_1, \ldots, \sum_{i=1}^{k} b_i, \ldots, \sum_{i=1}^{n} b_i) = \theta_n(b)$.

De nuevo, de la Observación 1.4 se sigue que $\kappa_n$ y $\theta_n$ son isomorfismos de *copos*, con lo que concluimos. □

Como consecuencia de los teoremas anteriores, las retículas $L_n$ y $C_n$ comparten las propiedades de $B_n$, tal como se afirma en el siguiente:

**Corolario 4.33** *Para cada $n \geq 1$, $\left\langle L_n, \underset{n}{\leq} \right\rangle$ y $\left\langle C_n, \underset{n}{\preceq} \right\rangle$ son retículas finitas, distributivas, autoduales, de cardinalidad $2^n$ y graduadas, con rango $\frac{n(n+1)}{2}$. Para $n \geq 5$, $L_n$ y $C_n$ no son planas.* □

Una consecuencia adicional es que los diagramas de Hasse de las retículas $C_n$ y $B_n$ son los mismos que los de $L_n$.

# Capítulo 5

# Las retículas $\mathbb{Z}_{p^n} - pr$

Consideremos el grupo cíclico finito de orden $p^n$, $\mathbb{Z}_{p^n}$, con $n \geq 1$. Como anillo, $\mathbb{Z}_{p^n}$ es conmutativo y su retícula de ideales es una cadena finita:

$$0 < p^{n-1}\mathbb{Z}_{p^n} < \cdots < p^2\mathbb{Z}_{p^n} < p\mathbb{Z}_{p^n} < \mathbb{Z}_{p^n}$$

que consta precisamente de los $\mathbb{Z}_{p^n}-$submódulos totalmente invariantes de $\mathbb{Z}_{p^n}$. También, se sigue de inmediato que $\mathbb{Z}_{p^n}$ tiene un único ideal máximo:

$$p\mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^{n-1}},$$

y un único (salvo isomorfismo) $\mathbb{Z}_{p^n}-$submódulo simple:

$$p^{n-1}\mathbb{Z}_{p^n} \cong \mathbb{Z}_{p.}$$

En este capítulo veremos que, en virtud de las propiedades inherentes a $\mathbb{Z}_{p^n}$ antes mencionadas, del Corolario 3.8 y de la Proposición 5.2 presentada enseguida, el comportamiento de los prerradicales sobre $\mathbb{Z}_{p^n}$ se reduce al comportamiento de los prerradicales sobre los ideales del mismo. Esta conducta singular nos permitirá, en primer lugar, describir completamente a $\mathbb{Z}_{p^n} - pr$; enseguida, caracterizar a sus elementos idempotentes y radicales, (co)irreducibles y (co)primos y, finalmente, dar una descripción de los *copos* correspondientes a estas clases especiales de prerradicales sobre $\mathbb{Z}_{p^n}$.

Las siguientes observación y proposición se siguen de los Corolarios 1.72 y 1.73.

**Observación 5.1** *Todo $\mathbb{Z}_{p^n}-$módulo es un $p-$grupo acotado.*

**Proposición 5.2** *Todo $\mathbb{Z}_{p^n}-$módulo cíclico es isomorfo a un ideal de $\mathbb{Z}_{p^n}$.*

*Demostración.* En efecto, dado un $\mathbb{Z}_{p^n}-$módulo cíclico $M$, éste es también un $\mathbb{Z}-$módulo cíclico que, además, es $p-$grupo. Luego, su generador es de orden $p^k$ con $k \in \mathbf{n+1}$. Por tanto, $M \cong p^{n-k}\mathbb{Z}_{p^n}$ como $\mathbb{Z}-$módulos, pero dicho isomorfismo también es un isomorfismo de $\mathbb{Z}_{p^n}-$módulos. □

Como consecuencia de la Observación 5.1, de la Proposición 5.2 y del Corolario 3.8, se tiene el siguiente:

**Corolario 5.3** *Todo $\mathbb{Z}_{p^n}-$módulo es isomorfo a una suma directa de ideales de $\mathbb{Z}_{p^n}$.*

Se sigue del corolario anterior y del comportamiento de los prerradicales respecto de la suma directa presentado en la Proposición 2.3 que, dados $n \geq 1$ y $p$, todo prerradical sobre $\mathbb{Z}_{p^n}$ está determinado por su valor sobre la cadena de ideales de este anillo. Más aún, el comportamiento de todo prerradical sobre los ideales de $\mathbb{Z}_{p^n}$ está sujeto a ciertas restricciones, mismas que presentamos en los siguientes proposición y corolario.

**Proposición 5.4** *Sean $\sigma \in \mathbb{Z}_{p^n} - pr$ y $m \in \{1, \ldots, n\}$. Si $\sigma(p^m\mathbb{Z}_{p^n}) = p^k\mathbb{Z}_{p^n}$ para alguna $k \in \{1, \ldots, n\}$, entonces:*

$$\sigma(p^{m-1}\mathbb{Z}_{p^n}) = p^k\mathbb{Z}_{p^n} \quad \acute{o} \quad \sigma(p^{m-1}\mathbb{Z}_{p^n}) = p^{k-1}\mathbb{Z}_{p^n}.$$

*Demostración.* Notemos primero que, como $\sigma \in R - pr$, $\sigma(p^{m-1}\mathbb{Z}_{p^n}) \geq \sigma(p^m\mathbb{Z}_{p^n}) = p^k\mathbb{Z}_{p^n}$. Luego, debe suceder que $\sigma(p^{m-1}\mathbb{Z}_{p^n}) = p^r\mathbb{Z}_{p^n}$, con $r \in \{0, 1, \ldots, k\}$.

Consideremos el homomorfismo de $\mathbb{Z}_{p^n}-$módulos $f : p^{m-1}\mathbb{Z}_{p^n} \longrightarrow p^m\mathbb{Z}_{p^n}$ dado por $f(\overline{x}) = p \cdot \overline{x}$. Se sigue que $p^{r+1}\mathbb{Z}_{p^n} = f(p^r\mathbb{Z}_{p^n}) = f(\sigma(p^{m-1}\mathbb{Z}_{p^n})) \leq \sigma(p^m\mathbb{Z}_{p^n}) = p^k\mathbb{Z}_{p^n}$.

Luego, $r + 1 \geq k$ y, por tanto, $k - 1 \leq r \leq k$. Concluimos que $r = k$ ó $r = k - 1$, que es lo que se quería probar. □

**Corolario 5.5** *Sean $\sigma \in \mathbb{Z}_{p^n} - pr$ y $m \in \{0, 1, \ldots, n-1\}$. Si $\sigma(p^m\mathbb{Z}_{p^n}) = p^k\mathbb{Z}_{p^n}$ para alguna $k \in \{0, 1, \ldots, n-1\}$, entonces:*

$$\sigma(p^{m+1}\mathbb{Z}_{p^n}) = p^k\mathbb{Z}_{p^n} \quad \acute{o} \quad \sigma(p^{m+1}\mathbb{Z}_{p^n}) = p^{k+1}\mathbb{Z}_{p^n}.$$

*Demostración.* Supongamos que $\sigma(p^m\mathbb{Z}_{p^n}) = p^k\mathbb{Z}_{p^n}$ y que $\sigma(p^{m+1}\mathbb{Z}_{p^n}) = p^r\mathbb{Z}_{p^n}$. Aplicando la Proposición 5.4 se tiene que $k = r$ ó $k = r - 1$; es decir, $r = k$ ó $r = k + 1$. □

Por simplicidad, en adelante denotaremos por $I_0 = 0 < I_1 < \cdots < I_n = \mathbb{Z}_{p^n}$ a la cadena de ideales de $\mathbb{Z}_{p^n}$. Con esta notación podemos reenunciar a la Proposición 5.4 como sigue:

**Proposición 5.6** *Sean $\sigma \in \mathbb{Z}_{p^n} - pr$ y $m \in \{0, 1 \ldots, n-1\}$. Si $\sigma(I_m) = I_k$ para alguna $k \in \{0, 1, \ldots, n-1\}$, entonces:*

$$\sigma(I_{m+1}) = I_k \quad \acute{o} \quad \sigma(I_{m+1}) = I_{k+1}.$$

El teorema que presentamos a continuación nos permitirá tener una útil representación de las retículas $\mathbb{Z}_{p^n} - pr$ como retículas de sucesiones binarias de longitud $n$ definidas en el capítulo anterior.

**Teorema 5.7** *Para cada $n \geq 1$, $\mathbb{Z}_{p^n} - pr$ y $B_n$ son retículas isomorfas.*

*Demostración.* Sea $n \geq 1$. Definimos la función $\phi_n : \mathbb{Z}_{p^n} - pr \longrightarrow B_n$, tal que, para toda $\sigma \in \mathbb{Z}_{p^n} - pr$, $\phi_n(\sigma) = (a_1, \ldots, a_n)$, donde:

$$a_k := \begin{cases} 0, & \text{si } \sigma(I_k) = \sigma(I_{k-1}); \\ 1, & \text{si } \sigma(I_k) \neq \sigma(I_{k-1}) \end{cases}$$

para cada $k \in \{1, \ldots, n\}$.

Definimos también la función $\psi_n : B_n \longrightarrow \mathbb{Z}_{p^n} - pr$, tal que, para cada $(a_1, \ldots, a_n) \in B_n$,

$$\psi_n(a_1, \ldots, a_n) := \bigvee_{k=1}^{n} \alpha_{I_{\sum_{i=1}^{k} a_i}}^{I_k} .$$

Notemos en primer lugar que ambas funciones están bien definidas. Presentamos enseguida una observación importante.

Sea $\sigma \in \mathbb{Z}_{p^n} - pr$ tal que $\sigma(I_1) = I_{j_1}, \sigma(I_2) = I_{j_2}, \ldots, \sigma(I_n) = I_{j_n}$, con $j_k \in \mathbf{n+1}$ para cada $k \in \{1, \ldots, n\}$. De la Proposición 5.6 se sigue que $j_k = j_{k-1}$ ó $j_k = j_{k-1} + 1$ para cada $j_k \in \mathbf{n+1}$, $k \in \{1, \ldots, n\}$. Supongamos que $\phi_n(\sigma) = (a_1, a_2, \ldots, a_n) \in B_n$. Entonces, se tiene que $\sum_{i=1}^{k} a_i = j_k$ para cada $k \in \{1, \ldots, n\}$. Probaremos por inducción sobre $k$ esta aseveración. Claramente $a_1 = j_1$. Supongamos que $\sum_{i=1}^{k-1} a_i = j_{k-1}$ para $k > 2$. Si $j_k = j_{k-1}$, entonces $a_k = 0$ y se tiene que $\sum_{i=1}^{k} a_i = \sum_{i=1}^{k-1} a_i + a_k = j_{k-1} + 0 = j_{k-1} = j_k$. Si, por el contrario, $j_k = j_{k-1} + 1$, entonces $a_k = 1$ y tenemos que $\sum_{i=1}^{k} a_i = \sum_{i=1}^{k-1} a_i + a_k = j_{k-1} + 1 = j_k$.

Se tienen las siguientes afirmaciones:

*$\phi_n$ es una función biyectiva con inversa $\psi_n$.*

Sea $\sigma \in \mathbb{Z}_{p^n} - pr$. Entonces, se sigue de la Proposición 2.33 que $\sigma = \bigvee\{\alpha_{\sigma(M)}^{M} \mid M \in \mathbb{Z}_{p^n} - Mod\}$. Ahora, por el Corolario 5.3, cada $M \in \mathbb{Z}_{p^n} - Mod$ se escribe como $M = I_1^{(x_1)} \oplus \cdots \oplus I_n^{(x_n)}$, donde, para cada $k \in \{1, \ldots, n\}$, $I_k^{(x_k)}$ designa a la suma directa de cardinal $x_k$ copias de $I_k$. Por tanto,

$$\sigma = \bigvee \left\{ \alpha_{\sigma(M)}^{M} \;\middle|\; M \in \mathbb{Z}_{p^n} - Mod,\ M = I_1^{(x_1)} \oplus \cdots \oplus I_n^{(x_n)} \right\},$$

donde $\sigma(M) = (\sigma(I_1))^{(x_1)} \oplus \cdots \oplus (\sigma(I_n))^{(x_n)}$.

Luego, por el inciso *1*) de la Proposición 2.39,

$$\sigma = \bigvee \left\{ \bigvee_{k=1}^{n} \alpha_{(\sigma(I_k))^{(x_k)}}^{I_k^{(x_k)}} \;\middle|\; M \in \mathbb{Z}_{p^n} - Mod,\ M = I_1^{(x_1)} \oplus \cdots \oplus I_n^{(x_n)} \right\} = \bigvee_{k=1}^{n} \alpha_{\sigma(I_k)}^{I_k}.$$

Supongamos que $\sigma(I_1) = I_{j_1}, \sigma(I_2) = I_{j_2}, \ldots, \sigma(I_n) = I_{j_n}$, con $j_k \in \mathbf{n+1}$ para cada $k \in \{1, \ldots, n\}$, y que $\phi_n(\sigma) = (a_1, a_2, \ldots, a_n) \in B_n$. De la última observación se sigue que $\psi_n(\phi_n(\sigma)) = \psi_n(a_1, \ldots, a_n) = \bigvee_{i=1}^{n} \alpha_{I_{j_k}}^{I_k} = \bigvee_{k=1}^{n} \alpha_{\sigma(I_k)}^{I_k} = \sigma$. Concluimos que $\psi_n \circ \phi_n = Id_{\mathbb{Z}_{p^n} - pr}$.

Por otro lado, si $a = (a_1, \ldots, a_n) \in B_n$, entonces se tiene que $\psi_n(a)(I_k) = I_{\sum_{i=1}^{k} a_i} := I_{j_k}$, con $j_k = j_{k-1}$ ó $j_k = j_{k-1} + 1$ para cada $j_k \in \{1, \ldots, n\}$, $k \in \{1, \ldots, n\}$. Supongamos que $\phi_n(\psi_n(a)) = (b_1, \ldots, b_n)$. Entonces, si $j_k = j_{k-1}$ se sigue que $b_k = 0 = a_k$. De manera similar, si $j_k = j_{k-1} + 1$, $b_k = 1 = a_k$. Por tanto, $\phi_n(\psi_n(a)) = (a_1, \ldots, a_n) = a$. Se concluye que $\phi_n \circ \psi_n = Id_{B_n}$, con lo que se prueba la afirmación.

*$\phi_n$ es un homomorfismo de copos que preserva el orden.*

Sean $\sigma, \tau \in \mathbb{Z}_{p^n} - pr$ tales que $\sigma(I_k) = I_{j_k}$ y $\tau(I_k) = I_{j'_k}$, con $j_k, j'_k \in \mathbf{n+1}$ para cada $k \in \{1, \ldots, n\}$. Supongamos que $\phi_n(\sigma) = a = (a_1, \ldots, a_n)$ y $\phi_n(\tau) = b = (b_1, \ldots, b_n)$. Si $\sigma \preceq \tau$, entonces, por la observación previa, $I_{\sum_{i=1}^{k} a_i} = I_{j_k} = \sigma(I_k) \leq \tau(I_k) = I_{j'_k} = I_{\sum_{i=1}^{k} b_i}$ para cada $k \in \{1, \ldots, n\}$. Se sigue que $\sum_{i=1}^{k} a_i \leq \sum_{i=1}^{k} b_i$ para cada $k \in \{1, \ldots, n\}$; es decir, $\phi_n(\sigma) = a \leq b = \phi_n(\tau)$.

*$\psi_n$ es un homomorfismo de copos que preserva el orden.*

Sean $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n) \in B_n$ tales que $a \leq b$. Entonces $\sum_{i=1}^{k} a_i \leq \sum_{i=1}^{k} b_i$ para cada $k \in \{1, \ldots, n\}$, de donde, por el Lema 2.27, $\alpha_{I_{\sum_{i=1}^{k} a_i}}^{I_k} \preceq \alpha_{I_{\sum_{i=1}^{k} b_i}}^{I_k}$ para cada $k \in \{1, \ldots, n\}$. Se sigue que $\psi_n(a) \preceq \psi_n(b)$.

Luego, en virtud de la Observación 1.4, tanto $\phi_n$ como $\psi_n$ son isomorfismos de *copos* y, por el Teorema 1.25, $\phi_n$ y $\psi_n$ son isomorfismos de retículas, con lo que concluimos. □

En adelante haremos referencia a los isomorfismos $\phi_n$ y $\psi_n$ definidos en la prueba del teorema anterior.

Del Teorema 5.7 se sigue de inmediato el corolario que presentamos a continuación.

**Corolario 5.8** *Para $n \geq 1$, la retícula $\mathbb{Z}_{p^n} - pr$ es distributiva, finita, de cardinalidad $2^n$ y graduada, con rango $\frac{n(n+1)}{2}$. Además, para $n \geq 5$, $\mathbb{Z}_{p^n} - pr$ no es plana.*

Una consecuencia adicional del Teorema 5.7 es que los diagramas de Hasse de $\mathbb{Z}_{p^n} - pr$ son los mismos que los de $L_n$.

Los siguientes teoremas describen el algoritmo para calcular en $B_n$ las operaciones correspondientes al producto y al coproducto en $\mathbb{Z}_{p^n} - pr$.

**Teorema 5.9** *Sean $\sigma, \tau \in \mathbb{Z}_{p^n} - pr$ tales que $\phi_n(\sigma) = (a_1, \ldots, a_n)$, $\phi_n(\tau) = (b_1, \ldots, b_n)$ y $\phi_n(\sigma\tau) = (p_1, \ldots, p_n)$. Supongamos que $\tau(I_k) = I_{j_k}$, con $j_k \in \mathbf{n+1}$ para cada $k \in \{1, \ldots, n\}$; es decir, $j_k = \sum_{i=1}^{k} b_i$. Entonces se cumplen las siguientes condiciones:*

*1) Si $b_k = 0$, entonces $p_k = 0$;*

*2) Si $b_k = 1$ y $a_{j_k} = 0$, entonces $p_k = 0$;*

*3) Si $b_k = 1$ y $a_{j_k} = 1$, entonces $p_k = 1$.*

*Demostración.* Sea $k \in \{1, \ldots, n\}$ y sean $\sigma, \tau \in \mathbb{Z}_{p^n} - pr$ tales que satisfacen las hipótesis del teorema. Si $b_k = 0$, entonces $\tau(I_k) = \tau(I_{k-1})$. Luego, $(\sigma\tau)(I_k) = (\sigma\tau)(I_{k-1})$, de donde $p_k = 0$. Supongamos ahora que $b_k = 1$, esto es, $\tau(I_k) \neq \tau(I_{k-1})$. Entonces, por la Proposición 5.6 se tiene que $\tau(I_{k-1}) = I_{j_k - 1}$. Se tienen dos casos. Si $a_{j_k} = 0$, es decir, $\sigma(I_k) = \sigma(I_{k-1})$, entonces $(\sigma\tau)(I_k) = (\sigma\tau)(I_{k-1})$, de donde $p_k = 0$. Si, por el contrario, $a_{j_k} = 1$, es decir, $\sigma(I_k) \neq \sigma(I_{k-1})$, entonces $(\sigma\tau)(I_k) \neq (\sigma\tau)(I_{k-1})$ y, por tanto, $p_k = 1$. □

Dualmente, se tiene el siguiente:

**Teorema 5.10** *Sean* $\sigma, \tau \in \mathbb{Z}_{p^n} - pr$ *tales que* $\phi_n(\sigma) = (a_1, \ldots, a_n)$, $\phi_n(\tau) = (b_1, \ldots, b_n)$ *y* $\phi_n((\tau : \sigma)) = (q_1, \ldots, q_n)$. *Supongamos que* $\tau(I_k) = I_{j_k}$, *con* $j_k \in \mathbf{n+1}$ *para cada* $k \in \{1, \ldots, n\}$; *es decir,* $j_k = \sum_{i=1}^{k} b_i$. *Entonces se cumplen las siguientes condiciones:*

*1) Si* $b_k = 1$, *entonces* $q_k = 1$;

*2) Si* $b_k = 0$ *y* $a_{k-j_k} = 1$, *entonces* $q_k = 1$;

*3) Si* $b_k = 0$ *y* $a_{k-j_k} = 0$, *entonces* $q_k = 0$.

*Demostración.* Sea $k \in \{1, \ldots, n\}$ y sean $\sigma, \tau \in \mathbb{Z}_{p^n} - pr$ tales que cumplen las hipótesis del teorema. Si $b_k = 1$, entonces $\tau(I_k) \neq \tau(I_{k-1})$. Nuevamente por la Proposición 5.6 se tiene que $\tau(I_{k-1}) = I_{j_k - 1}$. Por tanto, $(\tau : \sigma)(I_k)/\tau(I_k) = \sigma(I_k/\tau(I_k)) = \sigma(I_k/I_{j_k}) \cong \sigma(I_{k-j_k}) \cong \sigma(I_{k-1}/I_{j_k - 1}) = \sigma(I_{k-1}/\tau(I_{k-1})) = (\tau : \sigma)(I_{k-1})/\tau(I_{k-1})$. Luego, se sigue que $(\tau : \sigma)(I_k) \neq (\tau : \sigma)(I_{k-1})$, de donde $q_k = 1$. Supongamos ahora que $b_k = 0$, es decir, $\tau(I_k) = \tau(I_{k-1}) = I_{j_k}$. Entonces se tiene que $(\tau : \sigma)(I_k)/\tau(I_k) = \sigma(I_k/\tau(I_k)) = \sigma(I_k/I_{j_k}) \cong \sigma(I_{k-j_k})$ y $(\tau : \sigma)(I_{k-1})/\tau(I_{k-1}) = \sigma(I_{k-1}/\tau(I_{k-1})) = \sigma(I_{k-1}/I_{j_k}) \cong \sigma(I_{k-j_k-1})$. Tenemos dos casos. Si $a_{k-j_k} = 1$, esto es, $\sigma(I_{k-j_k}) \neq \sigma(I_{k-j_k-1})$, entonces $(\tau : \sigma)(I_k) \neq (\tau : \sigma)(I_{k-1})$, de donde $q_k = 1$. Por otro lado, si $a_{k-j_k} = 0$, es decir, $\sigma(I_{k-j_k}) = \sigma(I_{k-j_k-1})$, entonces $(\tau : \sigma)(I_k) = (\tau : \sigma)(I_{k-1})$, esto es, $q_k = 0$. □

Si bien del Teorema 5.7 se deduce de inmediato la autodualidad de las retículas $\mathbb{Z}_{p^n} - pr$, la importancia del teorema que se presenta a continuación radica en que se define un anti-isomorfismo de $\mathbb{Z}_{p^n} - pr$ en $\mathbb{Z}_{p^n} - pr$ que manda productos en coproductos.

**Teorema 5.11** *Para cada* $n \geq 1$, $\mathbb{Z}_{p^n} - pr$ *es una retícula autodual. Más aún, existe un anti-isomorfismo de retículas* $\lambda : \mathbb{Z}_{p^n} - pr \longrightarrow \mathbb{Z}_{p^n} - pr$ *tal que para cada* $\sigma, \tau \in \mathbb{Z}_{p^n} - pr$, $\lambda(\sigma\tau) = (\lambda(\tau) : \lambda(\sigma))$.

*Demostración.* Sea $n \geq 1$. Se define $\lambda := \psi_n \circ \mu \circ \phi_n$, donde $\phi_n$ y $\psi_n$ son los isomorfismos de *copos* definidos en el Teorema 5.7 y $\mu$ es el anti-isomorfismo del Teorema 4.29. Se sigue que $\lambda$ es un anti-isomorfismo de retículas. Ahora bien, sean $\sigma, \tau \in \mathbb{Z}_{p^n} - pr$ tales que $\phi_n(\sigma) = (a_1, \ldots, a_n)$ y $\phi_n(\tau) = (b_1, \ldots, b_n)$. Supongamos que $\phi_n(\sigma\tau) = (p_1, \ldots, p_n)$. Entonces, por el Teorema 5.9, si $\tau(I_k) = I_{j_k}$, con $j_k \in \mathbf{n+1}$ para cada $k \in \{1, \ldots, n\}$, esto es, $j_k = \sum_{i=1}^{k} b_i$, se tiene que:

1) Si $b_k = 0$, entonces $p_k = 0$;

2) Si $b_k = 1$ y $a_{j_k} = 0$, entonces $p_k = 0$;

3) Si $b_k = 1$ y $a_{j_k} = 1$, entonces $p_k = 1$.

Observemos que $\sum_{i=1}^{k} b_i^* = k - j_k$ para cada $k \in \{1, \ldots, n\}$. Sea $k = 1$, entonces, si $b_1^* = 0$ se tiene que $b_1 = 1$, de donde $j_1 = 1$. Luego, $b_1^* = 0 = 1 - 1 = 1 - j_1$. Similarmente, si $b_1^* = 1$ se sigue que $j_1 = 0$, de donde $b_1^* = 1 - 0 = 1 - j_1$. Supongamos cierta la observación para $k-1$, con $k \geq 2$. Tenemos que $\sum_{i=1}^{k} b_i^* = \sum_{i=1}^{k-1} b_i^* + b_k^* = [(k-1) - j_{k-1}] + b_k^*$ por la hipótesis de inducción. Se siguen dos casos: si $b_k^* = 0$, entonces se tiene que $b_k = 1$, de donde $j_k = \sum_{i=1}^{k} b_i = \sum_{i=1}^{k-1} b_i + b_k = j_{k-1} + 1$. Luego, $\sum_{i=1}^{k} b_i^* = [(k-1) - j_{k-1}] + b_k^* = [k - (1 + j_{k-1})] + 0 = k - j_k$. De manera similar, si $b_k^* = 1$, entonces $b_k = 0$ y $j_k = j_{k-1}$, de donde $\sum_{i=1}^{k} b_i^* = [(k-1) - j_{k-1}] + b_k^* = [k - 1 - j_k] + 1 = k - j_k$, con lo que se verifica la observación.

Afirmamos que $\lambda(\tau)(I_k) = I_{k-j_k}$. En efecto, $\lambda(\tau)(I_k) = [(\psi_n \circ \mu \circ \phi_n)(\tau)](I_k) = [(\psi_n \circ \mu)(b_1, \ldots, b_n)](I_k) = [(\psi_n(b_1^*, \ldots, b_n^*)](I_k) = I_{\sum_{i=1}^{k} b_i^*}$. Luego, nuestra afirmación es consecuencia inmediata de la última observación.

Se afirma que $\phi_n(\lambda(\sigma)) = (a_1^*, \ldots, a_n^*)$ y que $\phi_n(\tau(\sigma)) = (b_1^*, \ldots, b_n^*)$. Para verificarlo, supongamos primero que $\phi_n(\lambda(\sigma)) = (c_1, \ldots, c_n)$. Sea $k \in \{1, \ldots, n\}$. Si $c_k = 0$, entonces $I_{\sum_{i=1}^{k} a_i^*} = (\lambda(\sigma))(I_k) = (\lambda(\sigma))(I_{k-1}) = I_{\sum_{i=1}^{k-1} a_i^*}$.

Se sigue que $\sum_{i=1}^{k} a_i^* = \sum_{i=1}^{k-1} a_i^*$, de donde $a_k^* = 0 = c_k$. Si, por el contrario, $c_k = 1$, entonces $(\lambda(\sigma))(I_k) \neq (\lambda(\sigma))(I_{k-1})$ y $\sum_{i=1}^{k} a_i^* = \sum_{i=1}^{k-1} a_i^* + a_k^* \neq \sum_{i=1}^{k-1} a_i^*$, de donde $a_k^* = 0 = c_k$. De manera totalmente análoga se verifica que $\phi_n(\tau(\sigma)) = (b_1^*, \ldots, b_n^*)$.

Por tanto, $\phi_n((\lambda(\tau) : \lambda(\sigma))) = (q_1, \ldots, q_n)$, donde, por el Teorema 5.10 y por una afirmación anterior:

1) Si $b_k^* = 1$, entonces $q_k = 1$;

2) Si $b_k^* = 0$ y $a_{k-(k-j_k)}^* = a_{j_k}^* = 1$, entonces $q_k = 1$;

3) Si $b_k^* = 0$ y $a_{k-(k-j_k)}^* = a_{j_k}^* = 0$, entonces $q_k = 0$.

Esto es, para cada $k \in \{1, \ldots, n\}$, $q_k = 1 \Leftrightarrow p_k = 0$, de donde $\mu(\phi_n(\sigma\tau)) = \phi_n((\lambda(\tau) : \lambda(\sigma)))$. Aplicando $\psi_n$ a ambos miembros de la última igualdad se tiene que $\lambda(\sigma\tau) = (\lambda(\tau) : \lambda(\sigma))$. □

Notemos que el anti-isomorfismo $\lambda$ definido en el Teorema 5.11 es su propio inverso, pues $\mu$ lo es. Más adelante haremos referencia a dicho anti-isomorfismo.

## 5.1. Idempotentes y radicales en $\mathbb{Z}_{p^n} - pr$

Por simplicidad, si $0 \leq r \leq m \leq n$, denotaremos a los prerradicales $\alpha_{I_r}^{I_m}$ y $\omega_{I_r}^{I_m}$ en $\mathbb{Z}_{p^n} - pr$ por $\alpha_r^m$ y $\omega_r^m$, respectivamente. Comenzamos esta sección dando la descripción de los elementos en $B_n$ que corresponden a $\alpha_r^m$ y $\omega_r^m$ en $\mathbb{Z}_{p^n} - pr$.

**Teorema 5.12** *Sean $n \geq 1$ y $0 \leq r \leq m \leq n$. Entonces:*

*1) $\phi_n(\alpha_r^m) = (a_1, \ldots, a_n)$, donde:*

$$a_k := \begin{cases} 0, & si\ 1 \leq k \leq m - r; \\ 1, & si\ m - r < k \leq m; \\ 0, & si\ m < k \leq n. \end{cases}$$

*2)* $\phi_n(\omega_r^m) = (b_1, \ldots, b_n)$*, donde:*

$$b_k := \begin{cases} 1, & si\ \ 1 \leq k \leq r; \\ 0, & si\ \ r < k \leq m; \\ 1, & si\ \ m < k \leq n. \end{cases}$$

*Demostración.* Sea $n \geq 1$. Supongamos que $\alpha_r^m(I_k) = I_{j_k}$, con $j_k \in \mathbf{n} + \mathbf{1}$ para cada $k \in \{1, \ldots, n\}$. Ya hemos visto que $j_k = \sum_{i=1}^{k} a_i$ para cada $k \in \{1, \ldots, n\}$. Ahora, sean $m, r$ tales que $0 \leq r \leq m \leq n$. Notemos que $a := (a_1, \ldots, a_n)$, tal como ha sido definida en *1)*, es el menor elemento de $B_n$ tal que $j_m = r$. En efecto, si existe $c := (c_1, \ldots, c_n) \in B_n$ tal que $c < a$ y $\sum_{i=1}^{m} c_i = r$, entonces necesariamente $c_k = 0$ para $1 \leq k \leq m - r$ y $\sum_{i=1}^{l} c_i < \sum_{i=1}^{l} a_i$ para alguna $l \in \{m - r + 1, \ldots, m - 1\}$. Entonces $c_l = 0$ y, como $a_k = 1$ para $k \in \{m - r + 1, \ldots, m - 1\}$, se sigue que:

$$\sum_{i=1}^{l+1} c_i < \sum_{i=1}^{l+1} a_i$$

$$\ldots$$

$$\sum_{i=1}^{l+(m-l-1)} c_i < \sum_{i=1}^{l+(m-l-1)} a_i$$

$$r = \sum_{i=1}^{m} c_i < \sum_{i=1}^{m} a_i = r,$$

una contradicción. Por tanto, $\psi_n(a)$ es el menor $\sigma \in \mathbb{Z}_{p^n} - pr$ tal que $\sigma(I_m) = I_{j_m} = I_r$. En virtud de la Proposición 2.29 se concluye que $\psi_n(a) = \alpha_r^m$, de donde $\phi_n(\alpha_r^m) = a$.

Por otra parte, $b := (b_1, \ldots, b_n)$ es el mayor elemento de $B_n$ tal que $j_m = r$. De lo contrario, existiría $d := (d_1, \ldots, d_n) \in B_n$ tal que $b < d$ y $\sum_{i=1}^{m} d_i = r$, de donde $d_k = 1$ para $1 \leq k \leq r$ y $\sum_{i=1}^{l} b_i < \sum_{i=1}^{l} d_i$ para alguna $l \in \{r + 1, \ldots, m - 1\}$. Entonces $d_l = 1$ y, dado que $b_k = 0$ para

$k \in \{m-r+1, \ldots, m-1\}$, por un argumento similar al empleado en el caso anterior se llega a la contradicción:

$$r = \sum_{i=1}^{m} b_i < \sum_{i=1}^{m} d_i = r.$$

Luego, $\psi_n(b)$ es el mayor $\sigma \in \mathbb{Z}_{p^n} - pr$ tal que $\sigma(I_m) = I_{j_m} = I_r$. Nuevamente por la Proposición 2.29 se concluye que $\psi_n(b) = \omega_r^m$; es decir $\phi_n(\omega_r^m) = b$, con lo que se verifican las expresiones *1)* y *2)*. □

**Corolario 5.13** *Sean $n \geq 1$ y $0 \leq r \leq m \leq n$. Entonces $\lambda(\alpha_r^m) = \omega_{m-r}^m$, donde $\lambda$ es el anti-isomorfismo del Teorema 5.11.*

*Demostración.* Sean $a = (a_1, \ldots, a_n) = \phi_n(\alpha_r^m)$ y $b = (b_1, \ldots, b_n) = \phi_n(\omega_{m-r}^m)$. Luego, por el Teorema 5.12:

$$a_k := \begin{cases} 0, & \text{si } 1 \leq k \leq m-r; \\ 1, & \text{si } m-r < k \leq m; \\ 0, & \text{si } m < k \leq n \end{cases}$$

y

$$b_k := \begin{cases} 1, & \text{si } 1 \leq k \leq m-r; \\ 0, & \text{si } m-r < k \leq m; \\ 1, & \text{si } m < k \leq n. \end{cases}$$

Luego, $\mu(a) = b$, donde $\mu$ es el anti-isomorfismo definido en el Teorema 4.29. Se tiene entonces que $\mu(\phi_n(\alpha_r^m)) = \mu(a) = b = \phi_n(\omega_{m-r}^m)$. Aplicando $\psi_n$ a ambos miembros de la última igualdad se obtiene que $\lambda(\alpha_r^m) = \omega_{m-r}^m$, que es lo que se quería verificar. □

Los teoremas que presentamos a continuación nos ofrecen caracterizaciones de los prerradicales idempotentes y de los radicales sobre $\mathbb{Z}_{p^n}$, para $n \geq 1$. En el caso particular de estos anillos se tiene que todo prerradical idempotente es exacto izquierdo y todo radical es t-radical.

**Teorema 5.14** *Sea $\sigma \in \mathbb{Z}_{p^n} - pr$. Las siguientes condiciones son equivalentes:*

*(a) $\sigma = \alpha_m^m$ para alguna $0 \leq m \leq n$.*

*(b) $\sigma$ es exacto izquierdo.*

*(c) $\sigma$ es idempotente.*

*Demostración.*

$(a) \Rightarrow (b)$. Notemos que $\alpha_m^m = \omega_m^n$. En efecto, por el Teorema 5.12 se tiene que $\phi_n(\alpha_m^m) = \phi_n(\omega_m^n)$, de donde, como $\phi_n$ es inyectiva, se sigue que $\alpha_m^m = \omega_m^n$. Luego, puesto que $I_n = \mathbb{Z}_{p^n}$ es un $\mathbb{Z}_{p^n}-$módulo inyectivo (en virtud de la Proposición 1.97), y $\alpha_m^m(I_n) = I_m$, se sigue del inciso *3)* del Teorema 2.37 que $\alpha_m^m = \omega_m^n = \omega^{\mathbb{Z}_{p^n}}_{\alpha_m^m(\mathbb{Z}_{p^n})}$ es exacto izquierdo.

$(b) \Rightarrow (c)$. Se cumple para todo anillo (ver Observación 2.17).

$(c) \Rightarrow (a)$. Supongamos que $\sigma \neq \alpha_m^m$ para toda $0 \leq m \leq n$. Entonces $\phi_n(\sigma) \neq \phi_n(\alpha_m^m)$ para toda $0 \leq m \leq n$. Sea $\phi_n(\sigma) = a = (a_1, \ldots, a_n)$. Luego, existen $0 \leq i < j \leq n$ tales que $a_i = 0$ y $a_j = 1$.

Sean $s := \text{mín}\{i \mid a_i = 0\}$ y $t := \text{mín}\{j \mid j > s,\ a_j = 1\}$. Entonces $j_t := \sum_{i=1}^{t} a_i = s$, de donde $a_{j_t} = 0$. Supongamos ahora que $\sigma^2 = (p_1, \ldots, p_n)$. Se sigue de la condición *2)* del Teorema 5.9 que, como $a_t = 1$ y $a_{j_t} = 0$, necesariamente debe ocurrir que $p_t = 0$. Por tanto, $\sigma^2 \neq \sigma$; es decir, $\sigma$ no es idempotente. Se concluye que $\sigma = \alpha_m^m$ para alguna $0 \leq m \leq n$. □

**Teorema 5.15** *Sea $\sigma \in \mathbb{Z}_{p^n} - pr$. Las siguientes condiciones son equivalentes:*

*(a) $\sigma = \omega_0^m$ para alguna $0 \leq m \leq n$.*

*(b) $\sigma$ es t-radical.*

*(c) $\sigma$ es radical.*

*Demostración.*

$(a) \Rightarrow (b)$. Por el Teorema 5.12 se tiene que $\omega_0^m = \alpha_{n-m}^n$, el cual es un t-radical en virtud del Teorema 2.37 y del hecho de que $\omega_0^m(I_n) = I_{n-m}$.

$(b) \Rightarrow (c)$. Se cumple para todo anillo (ver Observación 2.17).

$(c) \Rightarrow (a)$. Si $\sigma$ es un radical, entonces $\lambda(\sigma)$ es idempotente, donde $\lambda$ es el anti-isomorfismo del Teorema 5.11. En efecto, por un lado, $(\sigma : \sigma) = \sigma$. Por otra parte, del Teorema 5.11 se sigue que:

$$\lambda(\lambda(\sigma)\,\lambda(\sigma)) = ((\lambda\,\lambda)(\sigma) : (\lambda\,\lambda)(\sigma)) = (\sigma : \sigma) = \sigma.$$

Luego, aplicando $\lambda$ a ambos miembros de la última igualdad se obtiene que $\lambda(\sigma)\,\lambda(\sigma) = \lambda(\sigma)$, que es lo que se quería verificar.

Por tanto, por el Teorema 5.14, $\lambda(\sigma) = \alpha_m^m$ para alguna $0 \leq m \leq n$, de donde, por el Corolario 5.13, $\sigma = \lambda(\alpha_m^m) = \omega_0^m$. □

Como consecuencia de los teoremas anteriores se tiene el siguiente resultado:

**Corolario 5.16** *El subcopo de prerradicales idempotentes y el subcopo de radicales en $\mathbb{Z}_{p^n} - pr$ son cadenas.*

En las Figuras 5.1 y 5.2 presentadas a continuación se muestran los diagramas de Hasse de $\mathbb{Z}_{p^n} - pr$, con $n = 2, 3$ y $4$, indicando mediante círculos blancos a los radicales (o t-radicales), junto con sus imágenes bajo $\phi_n$. Nótese que, en vista del Corolario 5.13, los prerradicales idempotentes (o exactos izquierdos) de $\mathbb{Z}_{p^n} - pr$ para $n = 2, 3$ y $4$ coinciden con los elementos indicados en las Figuras 5.1 y 5.2 si los diagramas de dichas figuras son volteados al revés.

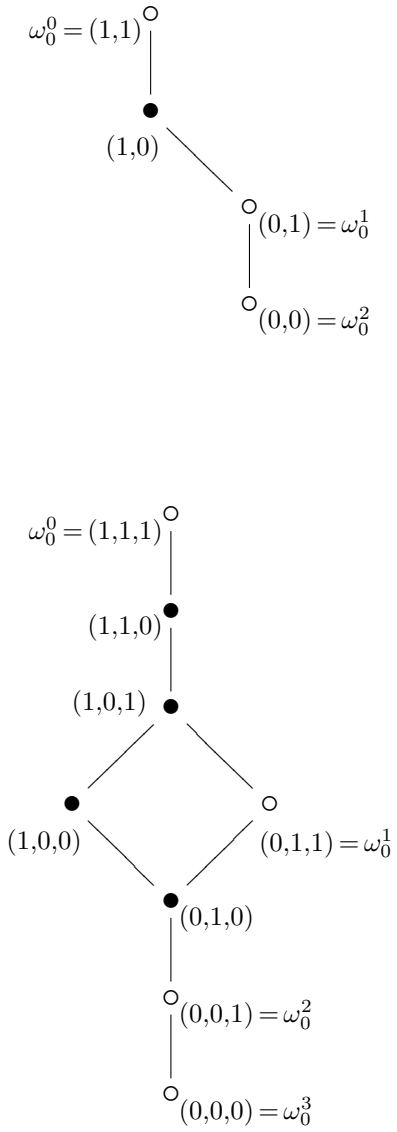



Figura 5.1: Radicales (t-radicales) en $\mathbb{Z}_{p^n} - pr,\ n = 2, 3$.

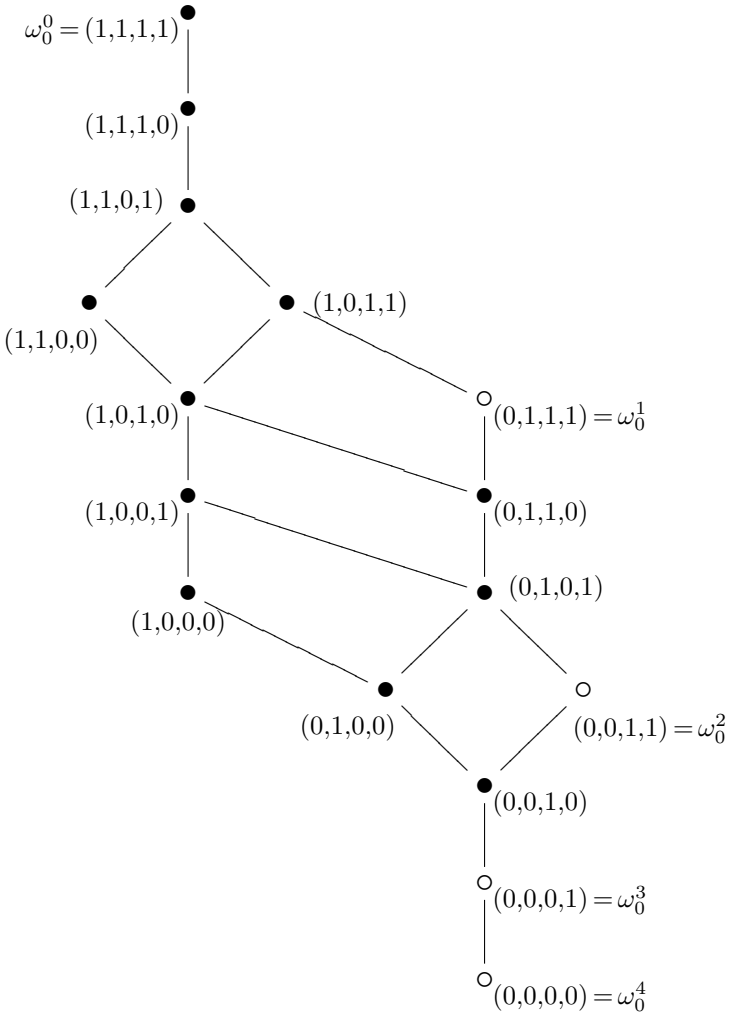



Figura 5.2: Radicales (t-radicales) en $\mathbb{Z}_{p^4} - pr$.

## 5.2. Irreducibles y coirreducibles en $\mathbb{Z}_{p^n} - pr$

A continuación se caracterizan los elementos irreducibles y coirreducibles en $\mathbb{Z}_{p^n} - pr$.

**Teorema 5.17** *Sea $\sigma \in \mathbb{Z}_{p^n} - pr$, con $\sigma \neq \bar{\mathbf{1}}$. Entonces $\sigma$ es irreducible si y sólo si $\sigma = \omega_r^m$ para algunas $0 \leq r < m \leq n$.*

*Demostración.* Sea $\sigma \neq \bar{\mathbf{1}}$ irreducible y supongamos que $\phi_n(\sigma) = (a_1, \ldots, a_n)$. Definimos:

$$r := \begin{cases} 0, & \text{si } a_1 = 0; \\ \text{máx}\{i \mid a_1 = \cdots = a_i = 1\}, & \text{si } a_1 \neq 0. \end{cases}$$

Luego, como $\sigma \neq \bar{\mathbf{1}}$, se tiene que $r < n$, de donde $a_{r+1} = 0$. Sea $m := \text{máx}\{i \mid a_{r+1} = \cdots = a_i = 0\}$. Se sigue que $r < m$. Luego, si $m = n$, entonces $\phi_n(\sigma) = \phi_n(\omega_r^m)$ y ya acabamos. Si, por el contrario, $m < n$, entonces $a_{m+1} = 1$. Sea $j := \text{máx}\{i \mid a_{m+1} = \cdots = a_i = 1\}$ y supongamos que $j < n$. Entonces $a_{j+1} = 0$. Ahora, sea $d = (d_1, \ldots, d_n)$ tal que:

$$d_k := \begin{cases} 1, & \text{si } 1 \leq k \leq r + j - m; \\ 0, & \text{si } r + j - m < k \leq j; \\ a_k, & \text{si } j < k \leq n. \end{cases}$$

Luego, no es difícil verificar que $\phi_n(\sigma) = \phi_n(\omega_r^m) \wedge d$, con $\phi_n(\omega_r^m), d > \phi_n(\sigma)$, contradiciendo el hecho de que $\sigma$ y, por tanto, $\phi_n(\sigma)$, es irreducible. Por lo tanto, $j = n$ y $\phi_n(\sigma) = \phi_n(\omega_r^m)$; es decir, $\sigma = \omega_r^m$.

Recíprocamente, supongamos ahora que $\sigma = \omega_r^m$ para algunas $0 \leq r < m \leq n$. Nótese que $\omega_r^m \neq \bar{\mathbf{1}}$, pues $\omega_r^m(I_m) = I_r$. Supongamos que $\omega_r^m = \tau \wedge \eta$ en $\mathbb{Z}_{p^n} - pr$, de donde, por ser $\phi_n$ un isomorfismo de retículas, $\phi_n(\omega_r^m) = \phi_n(\tau) \wedge \phi_n(\eta)$ en $B_n$. Digamos que $\phi_n(\tau) = (c_1, \ldots, c_n)$ y $\phi_n(\eta) = (d_1, \ldots, d_n)$. Como $(\tau \wedge \eta)(I_m) = I_r$, se tiene que $r = \text{mín}\{\sum_{i=1}^{m} c_i, \sum_{i=1}^{m} d_i\}$, es decir $r = \sum_{i=1}^{m} c_i$ ó $r = \sum_{i=1}^{m} d_i$, esto es, $\tau(I_m) = I_r$ ó $\eta(I_m) = I_r$. Luego, por la Proposición 2.29,

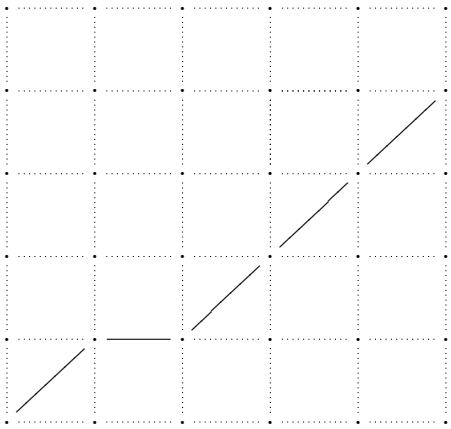


Figura 5.3: Un elemento irreducible en $C_5$.

$\tau \preceq \omega_r^m$ ó $\eta \preceq \omega_r^m$. Por lo tanto, $\tau = \omega_r^m$ ó $\eta = \omega_r^m$. Concluimos que $\omega_r^m$ es irreducible. □

En la Figura 5.3 presentamos la imagen bajo $\theta_n \circ \phi_n$ del elemento irreducible $\omega_1^2 \in \mathbb{Z}_{p^5} - pr$.

**Corolario 5.18** *Sea $\sigma \in \mathbb{Z}_{p^n} - pr$, con $\sigma \neq \bar{\mathbf{0}}$. Entonces $\sigma$ es coirreducible si y sólo si $\sigma = \alpha_r^m$ para algunas $0 < r \leq m \leq n$.*

*Demostración.* Supongamos que $\sigma \neq \bar{\mathbf{0}}$ es coirreducible. Entonces, claramente, $\lambda(\sigma)$ es irreducible. Luego, por el Teorema 5.17, $\lambda(\sigma) = \omega_r^m$ para algunas $0 \leq r < m \leq n$. Se sigue del Corolario 5.13 que $\sigma = \lambda^{-1}(\omega_r^m) = \lambda(\omega_r^m) = \alpha_{m-r}^m$, donde $0 < m - r \leq m \leq n$.

Para la suficiencia, supongamos ahora que $\sigma = \alpha_r^m$ para algunas $0 < r \leq m \leq n$. Entonces, como $\lambda(\sigma) = \omega_{m-r}^m$, con $m - r < m$ (pues $r > 0$), se sigue del Teorema 5.17 que $\lambda(\sigma)$ es irreducible. Por tanto, $\sigma$ es coirreducible. □

En la Figura 5.4 presentamos la imagen bajo $\theta_n \circ \phi_n$ del elemento coirreducible $\alpha_2^3 \in \mathbb{Z}_{p^5} - pr$.

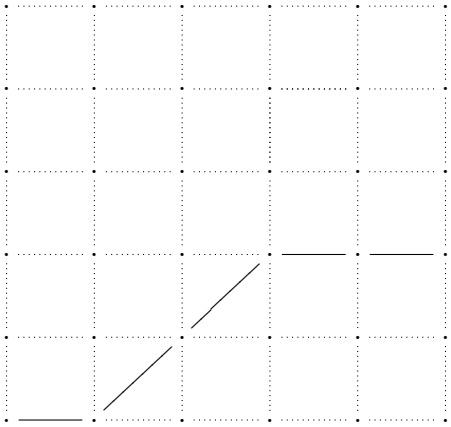


Figura 5.4: Un elemento coirreducible en $C_5$.

En las Figuras 5.5 y 5.6 presentamos los diagramas de Hasse de $\mathbb{Z}_{p^n} - pr$, para $n = 2, 3$ y 4, indicando a sus elementos irreducibles distintos de $\bar{\mathbf{1}}$ mediante círculos blancos.

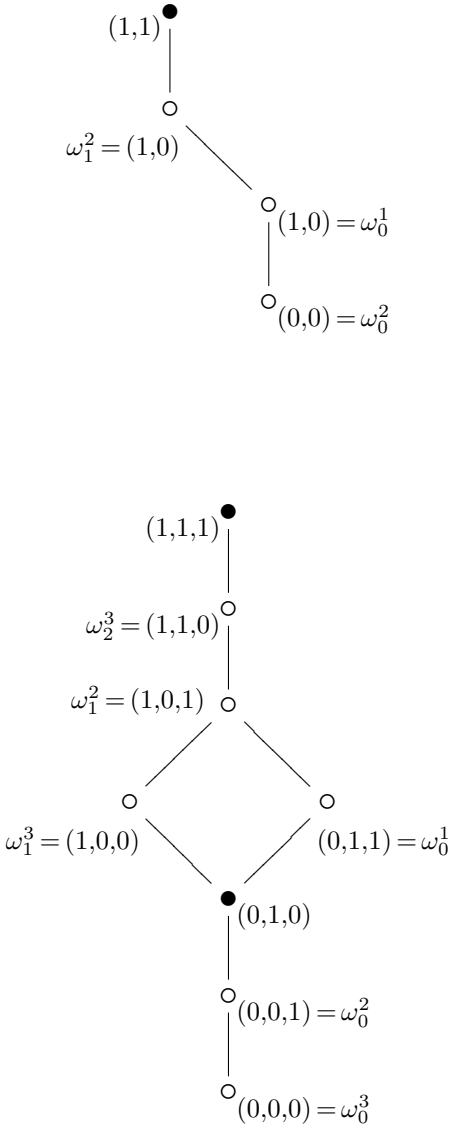



Figura 5.5: Elementos de $[\mathbb{Z}_{p^n} - pr]_\wedge,\ n = 2, 3.$

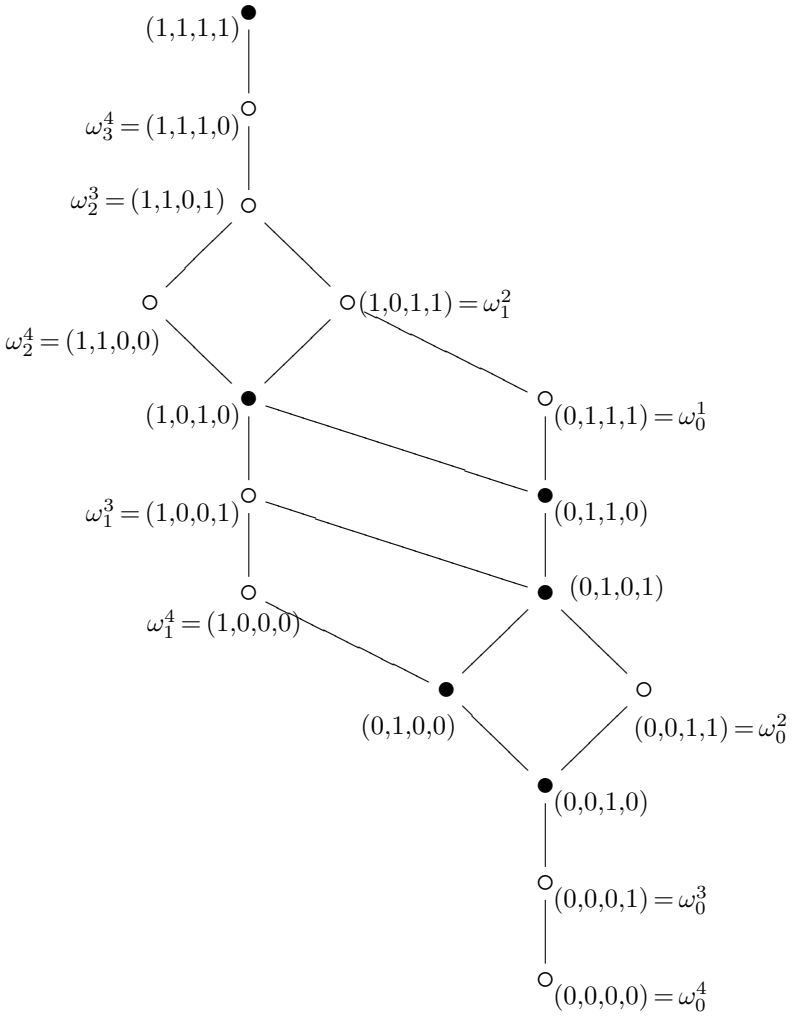



Figura 5.6: Elementos de $[\mathbb{Z}_{p^4} - pr]_\wedge$.

### 5.2.1. *Subcopos* de irreducibles y coirreducibles en $\mathbb{Z}_{p^n} - pr$

Gracias a los resultados previos es posible describir fácilmente a los *subcopos* de elementos irreducibles y coirreducibles en $\mathbb{Z}_{p^n} - pr$.

Comenzamos con un lema que nos da una manera de comparar dos prerradicales de la forma $\alpha_r^m$ ($\omega_r^m$) en términos de $m$ y $r$.

**Lema 5.19** *Dada $n \geq 1$, sean $m, r, l, s \in \{1, \ldots, n\}$.*

*1) Si $0 < r \leq m$ y $0 < s \leq l$, entonces $\alpha_r^m \preceq \alpha_s^l$ si y sólo si $r \leq s$ y $l - s \leq m - r$.*

*2) Si $r < m$ y $s < l$, entonces $\omega_r^m \preceq \omega_s^l$ si y sólo si $r \leq s$ y $l - s \leq m - r$.*

*Demostración.*

*1)* : Sean $0 < r \leq m$ y $0 < s \leq l$. Supongamos que $\phi_n(\alpha_r^m) = (a_1, \ldots, a_n)$ y $\phi_n(\alpha_s^l) = (a'_1, \ldots, a'_n)$, donde, para cada $i \in \{1, \ldots, n\}$, las coordenadas $a_i$ y $a'_i$ son definidas de acuerdo al Teorema 5.12. Si $\alpha_r^m \preceq \alpha_s^l$, entonces, en particular, $r = \sum_{i=1}^{n} a_i \leq \sum_{i=1}^{n} a'_i = s$. Ahora, supongamos que $m - r < l - s$. Entonces $l - s = m - r + t$, con $t > 0$. Luego, $t = \sum_{i=1}^{m-r+t} a_i \leq \sum_{i=1}^{m-r+t} a'_i = \sum_{i=1}^{l-s} a'_i = 0$, que es una contradicción. Por tanto, debe ocurrir que $l - s \leq m - r$.

Recíprocamente, supongamos ahora que $r \leq s$ y que $l - s \leq m - r$. No es difícil verificar que para toda $k \in \{1, \ldots, n\}$ se tiene que $\sum_{i=1}^{k} a_i \leq \sum_{i=1}^{k} a'_i$. Por tanto, $\phi_n(\alpha_r^m) \leq \phi_n(\alpha_s^l)$, de donde $\alpha_r^m \preceq \alpha_s^l$.

La prueba de *2)* es similar. □

Sea $n \geq 1$. Consideremos en $\{1, \ldots, n\}^2$ el siguiente orden: $(i, j) \preceq (k, l)$ siempre que $i \leq k$ y $j \leq l$. Entonces $\langle \{1, \ldots, n\}^2, \preceq \rangle$ es un *copo*. Más aún, es una retícula con supremo e ínfimo dados como sigue:

$$(i, j) \vee (k, l) = (\text{máx}\{i, k\}, \text{máx}\{j, l\}),$$

$$(i, j) \wedge (k, l) = (\text{mín}\{i, k\}, \text{mín}\{j, l\}).$$

Sea $T_n := \{(i,j) \in \mathbb{N} \mid 0 < i \leq j \leq n\}$. Obsérvese que $T_n$ es una subretícula de $\{1,\ldots,n\}^2$.

**Teorema 5.20** *Para cada $n \geq 1$ existen isomorfismos de copos:*

*1)* $f_n : [\mathbb{Z}_{p^n} - pr]_\wedge \longrightarrow T_n$,

*2)* $g_n : [\mathbb{Z}_{p^n} - pr]_\vee \longrightarrow T_n$.

*Demostración.*

*1)* : Para cada $n \geq 1$ se define $f_n$ como sigue. Sea $\sigma \in [\mathbb{Z}_{p^n} - pr]_\wedge$. Por el Teorema 5.17 se tiene que $\sigma = \omega_r^m$ para algunas $m, r$ tales que $0 \leq r < m \leq n$. Sea $f_n(\sigma) = f_n(\omega_r^m) := (r+1, n-m+r+1)$. Entonces $f_n$ es una función bien definida de $[\mathbb{Z}_{p^n} - pr]_\wedge$ a $T_n$. Si $(i,j) \in T_n$, entonces $f_n(\omega_{i-1}^{n-j+i}) = (i,j)$, con $0 \leq i-1 < n-j+i \leq n$, pues $0 < i \leq j \leq n$. Por tanto, $f_n$ es suprayectiva. Ahora, si $\omega_r^m,\ \omega_s^l \in [\mathbb{Z}_{p^n} - pr]_\wedge$ entonces, por el Lema 5.19 tenemos que $\omega_r^m \preceq \omega_s^l$ si y sólo si $r \leq s$ y $l - s \leq m - r$, lo cual, por la definición de orden en $T_n$, significa que $f_n(\omega_r^m) \preceq f_n(\omega_s^l)$. Por lo tanto, $f_n$ es inyectiva y es un isomorfismo de copos.

La prueba de *2)* es similar. □

Como consecuencia del Teorema 5.20, y considerando el Teorema 1.25, $[\mathbb{Z}_{p^n} - pr]_\wedge$ y $[\mathbb{Z}_{p^n} - pr]_\vee$ son retículas que son ambas isomorfas a $T_n$.

En la Figura 5.7 presentamos los *subcopos* de los elementos irreducibles distintos de $\bar{\mathbf{1}}$ en $\mathbb{Z}_{p^n} - pr$, para $n = 2, 3$ y $4$. Para el caso de $n = 2$ ilustramos la demostración del Teorema 5.20.

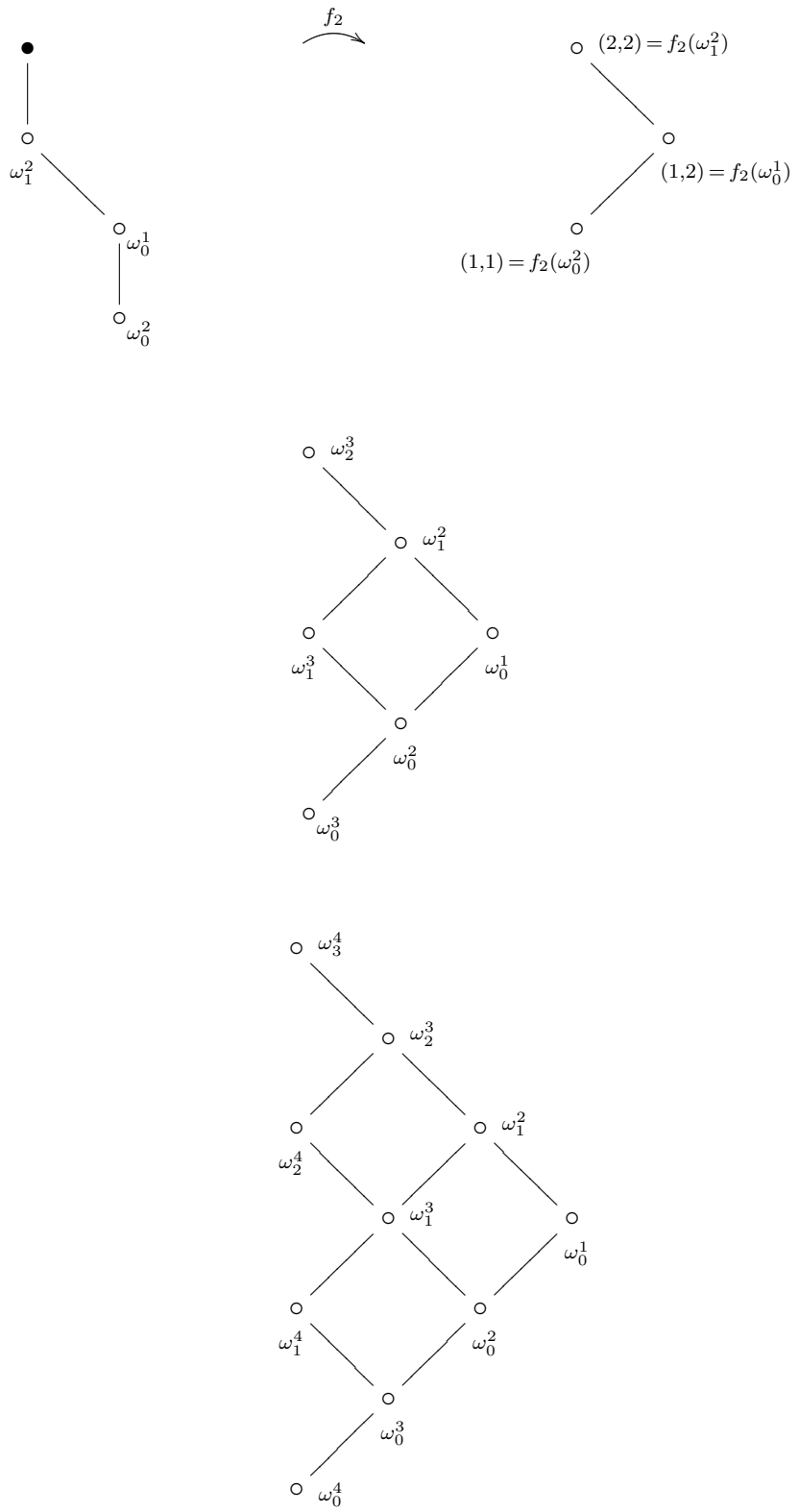



Figura 5.7: *Subcopos* de $[\mathbb{Z}_{p^n} - pr]_\wedge$, $n = 2, 3, 4$.

## 5.3. Primos y coprimos en $\mathbb{Z}_{p^n} - pr$

Sea $n \geq 1$ y consideremos los isomorfismos de *copos* $\varphi_n$ y $\kappa_n$, definidos en los Teoremas 4.31 y 4.32, respectivamente. A lo largo de esta sección llamaremos *hemisferio sur* de $B_n$ a la imagen bajo $\kappa_n \circ \varphi_n$ del conjunto $H_n^0$ en $L_n$, y lo denotaremos por $H_0^n$. Así:

$$H_0^n := (\kappa_n \circ \varphi_n)(H_n^0) = \{(a_1, \ldots, a_n) \in B_n \mid a_1 = 0\}$$

Análogamente, llamaremos *hemisferio norte* de $B_n$ a $(\kappa_n \circ \varphi_n)(H_n^1)$, y lo denotaremos por $H_1^n$. Esto es,

$$H_1^n := (\kappa_n \circ \varphi_n)(H_n^1) = \{(a_1, \ldots, a_n) \in B_n \mid a_1 = 1\}$$

Usaremos también los términos *hemisferio sur* y *hemisferio norte* para nombrar a las correspondientes imágenes en $\mathbb{Z}_{p^n} - pr$ bajo el isomorfismo $\psi_n$ del Teorema 5.7.

El lema técnico que presentamos a continuación nos será de gran utilidad para caracterizar a los prerradicales primos sobre $\mathbb{Z}_{p^n}$.

**Lema 5.21** *Sea $n \geq 2$ y supongamos que $\sigma \in \mathbb{Z}_{p^n} - pr$ se encuentra en el hemisferio norte. Supongamos también que $\phi_n(\sigma) = (1, a_2, \ldots, a_n)$. Si $\sigma$ es primo en $\mathbb{Z}_{p^n} - pr$, entonces $\psi_{n-1}((a_2, \ldots, a_n))$ es primo en $\mathbb{Z}_{p^{n-1}} - pr$.*

*Demostración.* Sea $n \geq 2$ y supongamos que $\sigma \in \mathbb{Z}_{p^n} - pr$ satisface las hipótesis del lema. Definimos $\sigma_1 := \psi_{n-1}(a_2, \ldots, a_n)$. Sean $\tau_1, \eta_1 \in \mathbb{Z}_{p^{n-1}} - pr$ tales que $\tau_1 \eta_1 \preceq \sigma_1$ y supongamos que $\phi_{n-1}(\tau_1) = (b_2, \ldots, b_n)$ y que $\phi_{n-1}(\eta_1) = (c_2, \ldots, c_n)$. Entonces, puesto que $\phi_{n-1}(\tau_1 \eta_1) \leq \phi_{n-1}(\sigma_1)$ y $\phi_{n-1}(\tau_1 \eta_1) = (p_2, \ldots, p_n)$, donde las $p_k's$ satisfacen las condiciones $1) - 3)$ del Teorema 5.9 para cada $k \in \{2, \ldots, n\}$, se sigue que $\sum_{i=2}^{k} p_i \leq \sum_{i=2}^{k} a_i$ para cada $k \in \{2, \ldots, n\}$. Se define $\tau := \psi_n((1, b_2, \ldots, b_n))$ y $\eta := \psi_n((1, c_2, \ldots, c_n))$. Luego, como $\phi_n(\tau \eta) = (1, p_2, \ldots, p_n)$ y $\phi_n(\sigma) = (1, a_2, \ldots, a_n)$, claramente se

sigue que $\tau\,\eta \preceq \sigma$, lo cual implica que $\tau \preceq \sigma$ ó $\eta \preceq \sigma$, por ser $\sigma$ primo. Por tanto, $\tau_1 \preceq \sigma_1$ ó $\eta_1 \preceq \sigma_1$. Concluimos que $\sigma_1$ es primo en $\mathbb{Z}_{p^{n-1}} - pr$. □

Ahora estamos en condiciones de dar una caracterización de los primos en $\mathbb{Z}_{p^n} - pr$.

**Teorema 5.22** *Sea $\sigma \in \mathbb{Z}_{p^n} - pr$, con $\sigma \neq \bar{\mathbf{1}}$. Entonces $\sigma$ es primo si y sólo si $\sigma = \omega_{m-1}^m$, para alguna $m$ tal que $0 < m \leq n$.*

*Demostración.* Para la necesidad procedemos por inducción sobre n. La implicación es clara para $n = 1$. Supongamos que el conjunto de prerradicales primos en $\mathbb{Z}_{p^{n-1}} - pr$ es $\{\omega_{m-1}^m \mid 0 < m \leq n-1\}$. Del Teorema 2.49 se sigue que $\omega_0^1$, que es el elemento mayor de $H_0^n$, es un prerradical primo mínimo en $\mathbb{Z}_{p^n} - pr$; es decir, $\omega_0^1$ es el único prerradical primo en el hemisferio sur de $\mathbb{Z}_{p^n} - pr$. Ahora, supongamos que $\sigma \in \mathbb{Z}_{p^n} - pr$ se encuentra en el hemisferio norte. Entonces $\phi_n(\sigma) = (1, a_2, \ldots, a_n) \in B_n$. Luego, por el Lema 5.21, $\psi_{n-1}((a_2, \ldots, a_n))$ debe ser primo en $\mathbb{Z}_{p^{n-1}} - pr$, de donde, por la hipótesis de inducción, $\psi_{n-1}((a_2, \ldots, a_n)) = \omega_{m-1}^m$ para alguna $m$ tal que $0 < m \leq n-1$. Por tanto, $\sigma = \omega_m^{m+1}$.

Recíprocamente, si $0 < m \leq n$, entonces se sigue del primer inciso de la Proposición 2.44 que $I_{m-1}$ es primo en $I_m$, por ser $I_{m-1}$ isomorfo a un $\mathbb{Z}_{p^n}-$submódulo totalmente invariante máximo de un $\mathbb{Z}_{p^n}-$módulo isomorfo a $I_m$. Luego, en virtud del Teorema 2.45, $\omega_{m-1}^m$ es primo en $\mathbb{Z}_{p^n} - pr$. □

Como consecuencia inmediata del Teorema 5.22, del Corolario 5.13 y de la definición del anti-isomorfismo $\lambda$ del Teorema 5.11, se tiene el siguiente resultado dual:

**Corolario 5.23** *Sea $\sigma \in \mathbb{Z}_{p^n} - pr$, con $\sigma \neq \bar{\mathbf{0}}$. Entonces $\sigma$ es coprimo si y sólo si $\sigma = \alpha_1^m$, para alguna $m$ tal que $0 < m \leq n$.* □

Tenemos como consecuencia de los resultados anteriores el siguiente:

**Corolario 5.24** *El subcopo de prerradicales (co)primos sobre* $\mathbb{Z}_{p^n}$ *es una cadena.*

En la Figuras 5.8 y 5.9 presentamos los diagramas de Hasse de $\mathbb{Z}_{p^n} - pr$, para $n = 2, 3$ y $4$, indicando a los elementos primos con círculos blancos.

Ahora bien, puesto que $\mathbb{Z}_{p^n} - pr$ es autodual mediante un anti-isomorfismo que manda productos en coproductos, podemos obtener los diagramas de Hasse que muestran a los prerradicales coirreducibles y coprimos sobre $\mathbb{Z}_{p^n}$ a partir de los correspondientes diagramas en donde se localizan los elementos irreducibles y primos, simplemente volteándolos al revés.

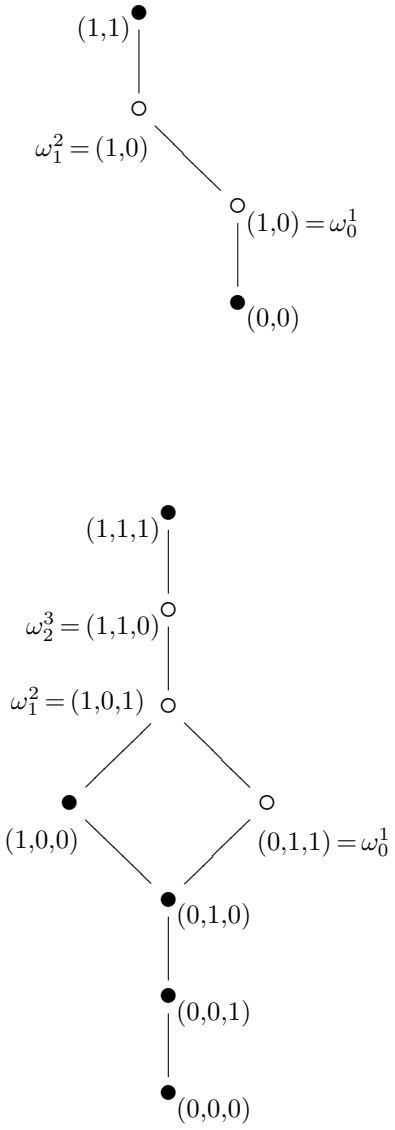



Figura 5.8: Elementos primos en $\mathbb{Z}_{p^n} - pr,\ n = 2, 3.$

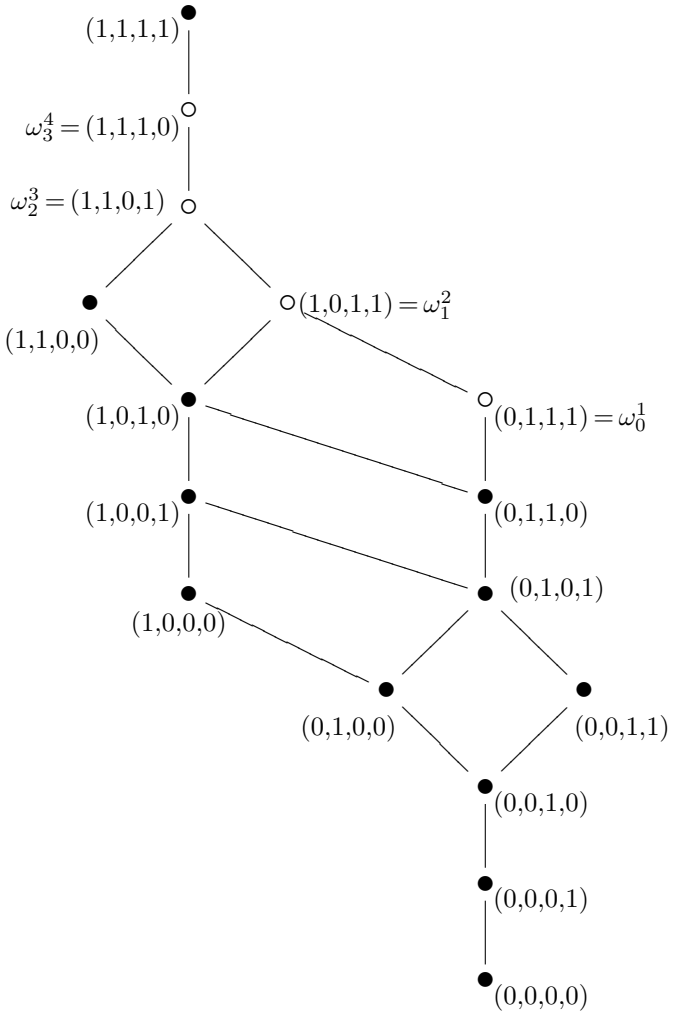



Figura 5.9: Elementos primos en $\mathbb{Z}_{p^4} - pr$.

# Bibliografía


[1] Anderson, F.; Fuller, K. *Rings and Categories of Modules*. Graduate Texts in Mathematics (Vol. 13), Spinger-Verlag, Nueva York, 1992.

[2] Bican, L.; Jambor, P.; Kepka, T.; Němec, P. *Preradicals*. Commentationes Mathematicae Universitatis Carolinae, **15** (1) (1974), 75–83.

[3] Bican, L.; Kepka, T.; Němec, P. *Rings, Modules and Preradicals*. Marcel Dekker, Nueva York, 1982.

[4] Birkhoff, G. *Lattice theory*. American Mathematical Society Colloquium Publications (Vol. XXV), Nueva York, 1948.

[5] Faith, C. *On Köthe Rings*. Math. Annalen, **164** (1966), 207–212.

[6] Faith, C. *Algebra: Rings, Modules and Categories*, (Vol. I). Springer-Verlag, Berlín, 1981.

[7] Fernández-Alonso, R.; Raggi, F.; Ríos, J.; Rincón, H.; Signoret, C. *The lattice structure of preradicals*. Communications in Algebra, **30** (3) (2002), 1533–1544.

[8] Fernández-Alonso, R.; Raggi, F.; Ríos, J.; Rincón, H.; Signoret, C. *The lattice structure of preradicals II: Partitions*. Journal of Algebra and Its Applications, **1** (2) (2002), 201–214.

[9] Fernández-Alonso, R.; Raggi, F.; Ríos, J.; Rincón, H.; Signoret, C. *Prime and irreducible preradicals.* Por aparecer en Journal of Algebra and Its Applications.

[10] Fernández-Alonso, R.; Gavito, S. *The lattice of preradicals over local uniserial rings.* Enviado a Journal of Algebra and Its Applications.

[11] Fuchs, L. *Infinite Abelian Groups*, (Vol. I). Academic Press, Londres, 1970.

[12] Grätzer, G. *General Lattice Theory.* Birkhäuser, Winnipeg, MB, Canadá, 2003.

[13] Kulikov, L. *On the theory of abelian groups of arbitrary cardinality* [Russian]. Mat. Sb., **9** (1941), 165–182.

[14] Mac Lane, S. *Categories for the Working Mathematician.* Springer-Verlag, Nueva York, 1971.

[15] Rotman, J. J. *An Introduction to Homological Algebra.* Academic Press, Nueva York, 1979.

[16] Stanley, R. P. *Enumerative Combinatorics.* Wadsworth and Brooks/Cole Advanced Books and Software (Vol. I), Monterrey, CA, 1986.

[17] Stenström, B. *Rings of Quotients. An Introduction to Methods of Ring Theory.* Springer-Verlag, Berlín, 1975.

# Notaciones y abreviaturas

Como es usual en la mayor parte de la bibliografía matemática, denotamos por:

$\in$, al símbolo de pertenencia;

$\forall$ ($\exists$), al cuantificador universal (existencial);

$\Rightarrow$ ($\Leftrightarrow$), a la implicación (equivalencia) lógica;

$\infty$, al infinito;

$\emptyset$, al conjunto vacío;

$P \subseteq Q$, al subconjunto $P$ de $Q$;

$P \setminus Q$, a la diferencia de los conjuntos $P$ y $Q$;

$\mathbb{N}$, al conjunto de los números naturales: $\{0, 1, \dots\}$;

$\mathbb{Z}$, al conjunto de los números enteros;

$a \big| b$, con $a, b \in \mathbb{Z}$, para decir que "$a$ divide a $b$";

$mcd(a_1, \dots, a_n)$, al máximo común divisor de $a_1, \dots, a_n \in \mathbb{Z}$;

$a \equiv b \,(mod\, m)$, con $a, b, m \in \mathbb{Z}$, para afirmar que "$a$ es congruente con $b$ módulo $m$";

$\mathbb{Z}_m$, al conjunto de los enteros módulo $m$: $\{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$;

$\mathbb{Q}$, al conjunto de los números racionales;

$f \circ g$, para designar la composición de las funciones $f$ y $g$;

$f\big|_K$, para significar la restricción de la función $f : P \longrightarrow Q$ al conjunto $K \subseteq P$.

Asimismo, adoptamos la convención de superponer una diagonal a un

símbolo para indicar la negación de su condición; v.gr. : $\neq$, $\notin$, $\subsetneq$, $\nmid$, etc.

Finalmente, en el transcurso del trabajo aparecen las notaciones, símbolos y abreviaturas siguientes (por orden de aparición):

# Índice de figuras

# Índice alfabético

Casa abierta al tiempo

UAM – Iztapalapa

# Las retículas de prerradicales sobre los anillos $\mathbb{Z}_{p^n}$

Silvia Claudia Gavito Ticozzi

Director de Tesis: Dr. Rogelio Fernández-Alonso González



Marzo, 2005.